UG S3-01(SEC)

চাৰি বছৰীয়া স্নাতক পাঠ্যক্ৰম

(চি বি চি এচ আৰু এন ই পি ২০২০ অনুসৰি)

তৃতীয় ষাণ্মাসিক

চাইবাৰ নিৰাপত্তা

কৌশল বিকাশ পাঠ্যবিষয়

হিৰণ্য চন্দ্ৰ ভূঞা বিজ্ঞান আৰু প্ৰযুক্তিবিদ্যা অধ্যয়ন সত্ৰ

কৃষ্ণকান্ত সন্দিকৈ ৰাজ্যিক মুক্ত বিশ্ববিদ্যালয়

বিষয় বিশেষজ্ঞ মণ্ডলী

অধ্যাপক শিখৰ শর্মা, তথ্য প্রযুক্তিবিজ্ঞান বিভাগ, গুৱাহাটী বিশ্ববিদ্যালয়

অধ্যাপক হীৰেন কুমাৰ দেৰ শর্মা, তথ্য প্রযুক্তিবিজ্ঞান বিভাগ, গুৱাহাটী বিশ্ববিদ্যালয়

ড° সঞ্জীৱ কুমাৰ কলিতা, কম্পিউটাৰ বিজ্ঞান বিভাগ, গুৱাহাটী বিশ্ববিদ্যালয়

পাঠ্যবিষয়ৰ সমন্বয়ৰক্ষীঃ

ড° ৰিদিপ দেৰ চৌধুৰী, ড° তাপসী কাশ্যপ দাস, ড° শ্রুতি শ্রুৱা ভৰালী, কৃ.স.ৰা.মু.বি

প্রস্তুতি গোটৰ সদস্য

অধ্যায়	**লেখক**
১,২	ড° তাপসী কাশ্যপ দাস, কৃ.স.ৰা.মু.বি
৩, ৪, ৫	ড° শ্রুতি শ্রুৱা ভৰালী, কৃ.স.ৰা.মু.বি
৬, ৭	ড° নৰজ্যোতি শর্মা, মহাপুৰুষ শংকৰদেৰ বিশ্ববিদ্যালয়
৮, ৯	ড° নবাঙ্কুৰ পাঠক, কৃ.স.ৰা.মু.বি
১০, ১১, ১৪	ড° ৰিদিপ দেৰ চৌধুৰী, কৃ.স.ৰা.মু.বি
১২, ১৩	ড° শান্তনু কলিতা, মহাপুৰুষ শংকৰদেৰ বিশ্ববিদ্যালয়

অসমীয়া অনুবাদঃ ড° সঞ্জীৱ ৰৰা, কৃ.স.ৰা.মু.বি, (**অধ্যায় ১, ২, ৩, ৪, ৫, ৬, ৭)**

ড° মৃণাল জ্যোতি গোস্বামী, কৃ.স.ৰা.মু.বি, (**অধ্যায় ৮, ৯, ১০, ১১, ১২, ১৩, ১৪)**

সম্পাদনাঃ ড° ৰিদিপ দেৰ চৌধুৰী (১-৮), ড° শ্রুতি শ্রুৱা ভৰালী (৯-১৪), কৃ.স.ৰা.মু.বি

ভাষা সম্পাদনাঃ (ইংৰাজী) **অধ্যাপক প্রসেনজিৎ দাস,** কৃ.স.ৰা.মু.বি

গাঁথনিক সম্পাদনাঃ **ড° নবাঙ্কুৰ পাঠক,** (১-৮), কৃ.স.ৰা.মু.বি

ড° তাপসী কাশ্যপ দাস, (৯-১৪), কৃ.স.ৰা.মু.বি

জুলাই, ২০২৩

This Self Learning Material (SLM) of the Krishna Kanta Handiqui State Open University is made available under a Creative Commons Attribution-Non Commercial-Share Alike 4.0 License (international) http://creativecommons.org/licenses/by-nc-sa/4.0/

কৃষ্ণকান্ত সন্দিকৈ ৰাজ্যিক মুক্ত বিশ্ববিদ্যালয়ৰ হৈ পঞ্জীয়কৰ দ্বাৰা মুদ্রিত আৰু প্রকাশিত

মুখ্য কার্যালয়ঃ পাটগাঁও, ৰাণী গেট, গুৱাহাটী- ৭৮১ ০১৭

নগৰ চৌহদঃ ৰেচম নগৰ, খানাপাৰা, গুৱাহাটী ৭৮১ ০২২

বিষয়সূচী

অধ্যায় **পৃষ্ঠা**

অধ্যায় ১ : চাইবাৰস্পেচৰ পৰিচয় **৭ - ২২**

চাইবাৰস্পেচৰ সংজ্ঞা আৰু কম্পিউটাৰ আৰু ৰেব টেকন'লজিৰ সাধাৰণ ধাৰণা, চাইবাৰস্পেচ আৰ্কিটেকচাৰ, যোগাযোগ আৰু ৰেব টেকন'লজি।

অধ্যায় ২ : ইণ্টাৰনেট আৰু চাইবাৰ নিৰাপত্তাৰ পৰিচয় **২৩ - ৪৩**

ইণ্টাৰনেট, ৱৰ্ল্ড ৱাইড ৰেব, ইণ্টাৰনেটৰ আগমন, ডেটা স্থানান্তৰ আৰু পৰিচালনাৰ বাবে ইণ্টাৰনেটৰ আন্তঃগাঁথনি, ইণ্টাৰনেট ছ'চাইটি, চাইবাৰস্পেচৰ নিয়ন্ত্রণ, চাইবাৰ নিৰাপত্তাৰ ধাৰণা, চাইবাৰ নিৰাপত্তাৰ সমস্যা আৰু প্রত্যাহ্বান।

অধ্যায় ৩ : চাইবাৰ অপৰাধ ১ **৪৪ - ৫৮**

চাইবাৰ অপৰাধৰ শ্রেণীবিভাজন, সাধাৰণ চাইবাৰ অপৰাধ- কম্পিউটাৰ আৰু ম'বাইল সম্পর্কিত চাইবাৰ অপৰাধ, মহিলা আৰু শিশুৰসৈতে জড়িত চাইবাৰ অপৰাধ।

অধ্যায় ৪ : চাইবাৰ অপৰাধ ২ **৫৯ - ৭৭**

অর্থনৈতিক প্রতাৰণা, ছ'চিয়েল ইঞ্জিনিয়াৰিং আক্রমণ, মেলৰেৰ আৰু ৰেনছমৰেৰ আক্রমণ, জিৰ' ডে আৰু জিৰ' ক্লিক আক্রমণ।

অধ্যায় ৫ : চাইবাৰ আইন **৭৮ - ৯২**

চাইবাৰ অপৰাধীৰ ক্রিয়া-কলাপ, চাইবাৰ অপৰাধৰ গোচৰ দাখিল, প্রতিকাৰ আৰু হ্রাসকৰণৰ ব্যৱস্থা, চাইবাৰ অপৰাধৰ আইনী দৃষ্টিভংগী, আই টি আইন ২০০০ আৰু ইয়াৰ সংশোধনী, ভাৰতত চাইবাৰ অপৰাধ আৰু চাইবাৰ ছিকিউৰিটিৰ সৈতে জড়িত সংস্থা, ক্ষেত্র অধ্যয়ন ।

অধ্যায় ৬ : সামাজিক মাধ্যমৰ পৰিচয় **৯৩ - ১০৫**

সামাজিক মাধ্যমৰ পৰিচয়, সামাজিক মাধ্যমৰ প্রকাৰ, সামাজিক মাধ্যমৰ প্লেটফর্ম।

অধ্যায় ৭ : সামাজিক মাধ্যমৰ ব্যৱহাৰ **১০৬ - ১১৭**

সামাজিক মাধ্যমৰ নিৰীক্ষণ, হেচটেগ, ভাইৰেল কণ্টেণ্ট, সামাজিক মাধ্যমত মার্কেটিং, সামাজিক মাধ্যমত গোপনীয়তা, অনলাইন সামাজিক মাধ্যমৰ প্রত্যাহ্বান, সুযোগ আৰু ফান্দ।

অধ্যায় ৮ : ছ'চিয়েল মিডিয়াত নিৰাপত্তাৰ বিষয় **১১৮ - ১৩১**

ছ'চিয়েল মিডিয়া সুৰক্ষাৰ সমস্যাসমূহ; আপত্তিজনক বিষয়বস্তু সম্পৰ্কে জাননী দিয়া আৰু তথ্য চিহ্নিত কৰা; আপত্তিজনক বিষয়বস্তু প্ৰকাশ নিয়ন্ত্ৰণ কৰা আইন; ছ' চিয়েল মিডিয়াৰ ব্যৱহাৰৰ বাবে উত্তম পদ্ধতি; কেছ ষ্টাডিজ

অধ্যায় ৯ : ই-কমার্চৰ পৰিচয় **১৩২ - ১৪১**

ই-কমার্চৰ সংজ্ঞা; ই-কমার্চৰ মুখ্য উপাদানসমূহ; ই-কমার্চ সুৰক্ষাৰ উপাদানসমূহ; ই-কমার্চৰ ভয়-ভীতি বা সংকটসমূহ; ই-কমার্চৰ সুৰক্ষাৰ উৎকৃষ্ট অনুশীলনসমূহ।

অধ্যায় ১০ : ডিজিটেল পেমেণ্টৰ পৰিচয় **১৪২ - ১৬১**

ডিজিটেল পেমেণ্ট : ডিজিটেল পেমেণ্টৰ গুৰুত্ব, ডিজিটেল পেমেণ্টৰ ইতিবৃত্ত, ডিজিটেল পেমেণ্টৰ উপাদানসমূহ, ডিজিটেল পেমেণ্টত জড়িত অংশীদাৰসকল; ডিজিটেল পেমেণ্টৰ বিভিন্ন পদ্ধতি : ডেবিট কার্ড, ক্রেডিট কার্ড, Unified Payment Interface (UPI), ই-ৱালেট (e-Wallets), Unstructured Supplementary Service Data (USSD), আধাৰ-ভিত্তিক পেমেণ্ট (Aadhaar-enabled Payments)।

অধ্যায় ১১ : ডিজিটেল পেমেণ্টত সুৰক্ষা সম্পৰ্কীয় দিশ **১৬২ - ১৮৫**

ডিজিটেল পেমেণ্টত সাধাৰণ ঠগবাজি : পৰিচয় চুৰি আৰু ফিছিং স্কেম,অনাধিকাৰ লেনদেন আৰু পেমেণ্ট গেটৱে ঠগবাজি, নকল পেমেণ্ট এপ আৰু মেলৱেৰ আক্ৰমণ, QR ক' ড ঠগবাজি আৰু SIM ছৱাপ ঠগবাজি; ডিজিটেল পেমেণ্টৰ ঠগবাজিৰ ৰোধ ব্যৱস্থা, নিৰাপদ ব্ৰাউজিং আৰু পাছৱর্ড ব্যৱস্থাপনা, দুই-স্তৰীয় প্ৰমাণীকৰণ আৰু বায়োমেট্ৰিক প্ৰমাণীকৰণ,পাব্লিক Wi-Fi এৰাই চলা আৰু বিশ্বাসযোগ্য পেমেণ্ট গেটৱে ব্যৱহাৰ, লেনদেন ইতিহাস নিয়মিত পৰীক্ষা আৰু লেনদেন সতর্কতা নির্ধাৰণ; ডিজিটেল পেমেণ্ট সম্পৰ্কে RBI নির্দেশনা : ডিজিটেল পেমেণ্টত RBIৰ ভূমিকা, ডিজিটেল লেনদেনত গ্ৰাহক সুৰক্ষাৰ ক্ষেত্ৰত RBI নির্দেশনা, অভিযোগ নিষ্পত্তি আৰু বিবাদ নিষ্পত্তি প্ৰক্ৰিয়া; পেমেণ্ট চেটলমেণ্ট আইন, ২০০৭ : পেমেণ্ট চেটলমেণ্ট আইন, ২০০৭ ৰ পৰিচয়, পেমেণ্ট ছিষ্টেম, গেটৱে আৰু চেটলমেণ্ট সম্পৰ্কীয় বিধান, অনাধিকাৰ লেনদেন আৰু ঠগবাজিৰ আইনী প্ৰভাৱ।

অধ্যায় ১২ : ডিজিটেল ডিভাইচৰ সুৰক্ষা–১ **১৮৬ - ২১০**

এণ্ড পইণ্ট ডিভাইচ আৰু মোবাইল ফোনৰ সুৰক্ষা; পাছৱর্ড নীতি; সুৰক্ষা পেটচ ব্যৱস্থাপনা; ডাটা বেকআপ; তৃতীয় পক্ষৰ চফটৱেৰ ডাউনলোড আৰু পৰিচালনা

অধ্যায় ১৩ : ডিজিটেল ডিভাইচৰ সুৰক্ষা–২ **২১১ - ২৩৩**

ডিভাইচ সুৰক্ষা নীতি; চাইবাৰ সুৰক্ষাৰ উত্তম পদ্ধতি; হ'ষ্ট ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছৰ তাৎপর্য; হ'ষ্ট ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছৰ ব্যৱস্থাপনা

অধ্যায় ১৪ : ৱাই-ফাই সুৰক্ষা **২৩৪ - ২৪৪**

ৱাই-ফাই ব্যৱহাৰৰ সুবিধা; ৱাই-ফাই ব্যৱহাৰৰ ভাবুকি; ৱাই-ফাই নেটৱর্কৰ প্রকাৰ; ৱাই-ফাইৰ ধৰণ; ৱাই-ফাই-এ কেনেকৈ কাম কৰে ?; ৱাই-ফাই সুৰক্ষাৰ বাবে গ্রহণ কৰিব পৰা পদক্ষেপ; এণ্ড্রইড মোবাইলত ৱাই-ফাই সুৰক্ষাৰ বাবে গ্রহণ কৰিব লগা পদক্ষেপ; IOS মোবাইলত ৱাই-ফাই সুৰক্ষাৰ বাবে গ্রহণ কৰিব লগা পদক্ষেপ।

পাঠ্যবিষয়ৰ পৰিচয়ঃ চাইবাৰ নিৰাপত্তা

এইখন চাৰিবছৰীয়া স্নাতক পাঠ্যক্ৰমৰ কৌশল বিকাশ পাঠ্যবিষয় "চাইবাৰ নিৰাপত্তা"। এই পাঠ্যক্ৰম চৈধ্যটা অধ্যায়ত ভাগ কৰা হৈছে। চাইবাৰস্পেচ আৰু চাইবাৰ নিৰাপত্তাৰ বিভিন্ন দিশৰ ওপৰত গভীৰ দৃষ্টিকোণ প্ৰদান কৰিবলৈ প্ৰস্তুত কৰা হৈছে। তথ্য প্ৰযুক্তি (ICT) যি গতিত আগবাঢ়ি গৈ আছে, ইয়াৰ সৈতে জড়িত সুৰক্ষা চিন্তাবোৰো অধিক জটিল আৰু বহুমুখী হৈ পৰিছে। ফলত, এই প্ৰত্যাহ্বানসমূহ সফলতাৰে মোকাবিলা কৰিবলৈ চাইবাৰ নিৰাপত্তাৰ আলোচনা আৰু প্ৰয়োজনীয়তা আহি পৰিছে। ICT-ৰ দ্ৰুত উন্নতিয়ে ডিজিটেল প্লেটফৰ্ম আৰু ডিভাইচৰ প্ৰসাৰ আৰু জনপ্ৰিয়তা বঢ়াইছে, য'ত সামাজিক মাধ্যম, ই-কমাৰ্ছ, ডিজিটেল পেমেণ্ট, আৰু অন্যান্য ডিজিটেল সেৱা আদি অন্তৰ্ভুক্ত হৈ পৰিছে। এই উন্নতিসমূহে বহু সুবিধা প্ৰদান কৰাৰ লগতে একাধিক সুৰক্ষা দুৰ্বলতা আৰু ভাবুকিৰ সৃষ্টিও কৰিছে। তথ্যৰ আইন উলংঘা, পৰিচয় চুৰি, চাইবাৰ জালিয়াতি, আৰু বেয়া অভিপ্ৰায়ৰ ছফ্টৱেৰ আক্ৰমণ আদি সমস্যাসমূহ স্বাভাৱিক হৈ পৰিছে। ব্যক্তি, ব্যৱসায়, আৰু চৰকাৰৰ বাবে প্ৰত্যাহ্বানৰ সৃষ্টি কৰিছে। এই পাঠ্যবিষয়ে ডিজিটেল চাইবাৰ পৰিৱেশক বুজি উঠিবলৈ আৰু সুৰক্ষিত কৰিবলৈ প্ৰয়োজনীয় জ্ঞান আৰু দক্ষতাৰে শিক্ষাৰ্থীক সজ্জিত কৰি এই গুৰুত্বপূৰ্ণ সমস্যাসমূহ সমাধান কৰিবলৈ সহায় কৰিব বুলি আশা কৰা হৈছে।

এই পাঠ্যবিষয়টিৰ প্ৰাথমিক উদ্দেশ্য হৈছে ডিজিটেল নাগৰিকসকলৰ মাজত চাইবাৰ নিৰাপত্তাৰ গুৰুত্ব সম্পৰ্কে সজাগতা বৃদ্ধি কৰা। ব্যৱহাৰকাৰীক বিভিন্ন ভাবুকি আৰু ব্যক্তিগত আৰু সংগঠনগত তথ্য সুৰক্ষিত ৰখাৰ সৰ্বোত্তম অনুশীলনৰ বিষয়ে শিক্ষা দি, এই পাঠ্যবিষয়তত সজাগতা আৰু সক্ৰিয় সুৰক্ষা ব্যৱস্থাৰ এক পৰিৱেশ গঢ়ি তুলিবলৈ চেষ্টা কৰা হৈছে। পাঠ্যক্ৰমৰ চৈধ্যটা অধ্যায়ত চাইবাৰ নিৰাপত্তাৰ এক সামগ্ৰিক আলোচনা দাঙি প্ৰয়াস কৰা হৈছে। এই অধ্যায়সমূহে চাইবাৰ নিৰাপত্তাৰ মৌলিক নীতিসমূহ, চাইবাৰ ভাবুকি আৰু আক্ৰমণৰ প্ৰকাৰ, আৰু এনে ঘটনা প্ৰতিৰোধ আৰু প্ৰতিক্ৰিয়া কৰাৰ পদ্ধতিসমূহৰ বিষয়ে গভীৰভাৱে আলোচনা কৰিছে। চাইবাৰ অপৰাধ, চাইবাৰ আইন, সামাজিক মাধ্যম আৰু ডিজিটেল পেমেণ্টত সুৰক্ষাৰ সমস্যা, আৰু ডিজিটেল ডিভাইচ আৰু ৱাই-ফাই সুৰক্ষাৰ সৈতে জড়িত সমস্যাসমূহৰ দৰে বিষয়বোৰ বিশদভাৱে আলোচনা কৰা হৈছে আৰু ই শিক্ষাৰ্থীক এই ক্ষেত্ৰত এক কৌশলী শিক্ষা প্ৰদান কৰিব।

পাঠ্যক্ৰমৰ অধ্যায়ৰ মূল পাঠৰ কাষত কিছুমান বাকচ অন্তৰ্ভুক্ত কৰা হৈছে। আপোনাৰ অধ্যয়নত সহায় হোৱাকৈ কিছুমান 'ক্ৰিয়া-কলাপ' অন্তৰ্ভুক্ত কৰা হৈছে। আপুনি কিছুমান বাকচত 'জানি থও আহক' বুলি পাব পাৰে। এই বাকচবোৰে আপোনাক কিছু অতিৰিক্ত প্ৰাসংগিক তথ্য প্ৰদান কৰিব। আকৌ, আপুনি 'আপোনাৰ অগ্ৰগতি পৰীক্ষা কৰক' বাকচত কিছু প্ৰশ্ন পাব। এইবোৰ আপোনাৰ অধ্যয়নৰ অগ্ৰগতি নিজে পৰীক্ষা কৰিবলৈ প্ৰস্তুত কৰা হৈছে। আপুনি অধ্যায়বোৰ পঢ়াৰ পিছত ততালিকে এই বাকচবোৰত দিয়া সমস্যাসমূহ সমাধান কৰিলে আৰু প্ৰতিটো অধ্যায়ৰ শেষত দিয়া 'অগ্ৰগতিৰ খতিয়ান'ৰ সৈতে আপোনাৰ উত্তৰ মিলাই চালে আপোনাৰ বাবে সহায়ক হ'ব। লতে অধিক জানিবলৈ অধ্যয়নৰ সামগ্ৰীৰ বিতং তথ্যও অধ্যয়বোৰৰ শেষত আছে।

অধ্যায় ১: চাইবাৰস্পেচৰ পৰিচয়

অধ্যায় গাঁথনি

১.১ উদ্দেশ্য
১.২ পৰিচয়
১.৩ চাইবাৰস্পেচ (Cyberspace)ৰ পৰিচয়
১.৪ চাইবাৰস্পেচৰ আৰ্কিটেকচাৰ (Architecture)
১.৫ কম্পিউটাৰৰ আভাস
১.৫.১ কম্পিউটাৰৰ বৈশিষ্ট্য
১.৫.২ কম্পিউটাৰৰ মূল উপাদানসমূহ
১.৬ ৱেব প্ৰযুক্তিৰ আভাস
১.৬.১ ৱৰ্ল্ড ৱাইড ৱেব
১.৭ অধ্যায়টিৰ পৰা আমি কি কি শিকিলোঁ
১.৮ অগ্ৰগতিৰ খতিয়ান
১.৯ অধিক জানিবলৈ
১.১০ আৰ্হি প্ৰশ্ন

১.১ উদ্দেশ্য

এই অধ্যায়টি অধ্যয়ন কৰি আপুনি-

- চাইবাৰস্পেচৰ ধাৰণা লাভ কৰিব, ইয়াৰ পৰিসৰ, তাৎপর্য্য আৰু আধুনিক সমাজত প্ৰভাৱ বুজিব পাৰিব।
- ডিজিটেল যোগাযোগ আৰু অনলাইন কার্য্যকলাপৰ অবিৰত কার্য্যকলাপ সম্পন্ন কৰা চাইবাৰস্পেচৰ আৰ্কিটেকচাৰ (Architecture) ৰ বিষয়ে জানিব পাৰিব।
- কম্পিউটাৰৰ প্ৰয়োজনীয় দিশসমূহৰ সৈতে পৰিচয় হোৱাৰ লগতে, ইয়াৰ বৈশিষ্ট্যসমূহ, মৌলিক উপাদানসমূহ, আৰু কার্য্যকাৰীতাৰ বিষয়ে অৱগত হ'ব।
- ৱেব প্ৰযুক্তি আৰু ইয়াৰ বিভিন্ন আনুষংগিক প্ৰযুক্তিৰ আভাস লাভ কৰিব।

১.২ পৰিচয়

এইটো চাইবাৰ নিৰাপত্তা (Cyber Security) পাঠ্যবিষয়ৰ প্ৰথম অধ্যায়। প্ৰথমে আমি প্ৰাথমিক কথা- চাইবাৰস্পেচৰ সংজ্ঞাৰ পৰা আৰম্ভ কৰিম। ইয়াৰ গঠন, যোগাযোগ আৰু ৰেব প্ৰযুক্তিৰ ভূমিকা, যোগাযোগ, বাণিজ্য, শিক্ষা আৰু সমাজত ইয়াৰ প্ৰভাৱ সম্পৰ্কে আলোচনা কৰিম।

তাৰ পাছত, আমি কম্পিউটাৰ চিষ্টেমৰ প্ৰাথমিক কথাবোৰ আলোচনা কৰিম। ইয়াৰ বৈশিষ্ট্য, কাৰ্য্য আৰু মূল উপাদানসমূহ আলোকপাত কৰিম। ক্ৰমে আমি ৰেব প্ৰযুক্তিলৈ আগবাঢ়িম, ৱৰ্ল্ড ৱাইড ৰেবৰ ওপৰত গুৰুত্ব দিম। আমি ৰেব কেনেকৈ সংগঠিত আৰু ই কেনেকৈ অনলাইন পাৰস্পৰিক ক্ৰিয়া-কলাপ আৰু কাৰ্য্যকলাপ চলাই নিয়ে সেই বিষয়ে ব্যাখ্যা কৰিম।

১.৩ চাইবাৰস্পেচৰ পৰিচয়

'চাইবাৰস্পেচ' শব্দটো প্ৰথমে ১৯৮৪ চনত কল্পবিজ্ঞান লেখক উইলিয়াম গিবছনে তেওঁৰ উপন্যাস *নিউৰ'মেন্সাৰ*-ত ব্যৱহাৰ কৰিছিল। যদিও গিবছনৰ বৰ্ণনা কাল্পনিক আছিল, তথাপিও ইয়াত চাইবাৰস্পেচক কম্পিউটাৰ সংযোগী নেটৱৰ্কৰ দ্বাৰা সৃষ্টি হোৱা ভাৰ্চুৱেল এখন জগত হিচাপে দেখুওৱা হৈছিল। চাইবাৰস্পেচৰ বহুতো ব্যাখ্যা আমি পাওঁ। সাধাৰণতে ই আন্তঃসংযোগী কম্পিউটাৰ, চাৰ্ভাৰ আৰু নেটৱৰ্কৰ দ্বাৰা গঠিত ভাৰ্চুৱেল পৰিৱেশক বুজায়। ই এনে এখন ঠাই বা পৰিৱেশ য'ত ডিজিটেল যোগাযোগ, তথ্য বিনিময়, আৰু অনলাইন ক্ৰিয়া-কলাপসমূহ অন্তৰ্ভূক্ত হৈ থাকে।

চাইবাৰস্পেচ কেৱল ইণ্টাৰনেটতে সীমাবদ্ধ নহয়। ই ইয়াৰ অন্তৰ্ভুক্ত সকলো ধৰণৰ ডিজিটেল যোগাযোগ, তথ্য সংৰক্ষণ আৰু প্ৰক্ৰিয়াকৰণভৰ সেই ভাৰ্চুৱেল পৰিৱেশক সামৰি লয়। এই স্পেচ কোনো ভৌতিক অৱস্থানৰ দ্বাৰা সীমাবদ্ধ নহয়, আৰু ইয়াৰ ফলশ্ৰুতিতে বিশ্বব্যাপী তাৎক্ষণিক যোগাযোগ আৰু তথ্য বিনিময় সম্ভৱ হৈ উঠিছে। ভৌতিক উপস্থিতিৰ নথকা সত্ত্বেও, চাইবাৰস্পেচে আধুনিক জগতত গভীৰ প্ৰভাৱ পেলাইছে আৰু ৰাষ্ট্ৰীয় সীমা অতিক্ৰম কৰিছে। ই তথ্য প্ৰেৰণ, গ্ৰহণ, সংৰক্ষণ আৰু প্ৰক্ৰিয়াকৰণ (প্ৰচেচিঙৰ)ৰ বাবে এটা মঞ্চ হিচাপে কাম কৰে।তথ্য বিনিময়, আন্তঃকৰ্ম, গেম খেলা আৰু সামাজিক মাধ্যমত সক্ৰিয় হৈ থাকি বহুলোকে চাইবাস্পেচত বিশেষ সময় অতিবাহিত কৰে। শিক্ষাৰ ক্ষেত্ৰ, অৰ্থনীতি, বিপণন আৰু বিনোদনৰ দৰে বিভিন্ন উদ্যোগ ব্যাপকভাৱে চাইবাৰস্পেচৰ ওপৰত নিৰ্ভৰশীল। অনুষ্ঠান প্ৰতিষ্ঠানসমূহেও তথ্য সংৰক্ষণ আৰু ব্যৱস্থাপনাৰ বাবে চাইবাৰস্পেচ ব্যৱহাৰ কৰে।

ফোন আৰু কম্পিউটাৰত ডেটা লাভ কৰা, ইণ্টাৰনেট বেংকিং, অনলাইন শ্বপিং, এপইণ্টমেণ্ট বুকিং কৰা, টিকট ক্ৰয় কৰা আদি কামবোৰ এতিয়া একেবাৰে সহজ হৈ পৰিছে। উদাহৰণস্বৰূপে, ক'ভিড-১৯ সংকটৰ সময়ত অনলাইন শিক্ষাই শিক্ষক আৰু ছাত্ৰ-ছাত্ৰীক দূৰৈৰ পৰা সংযোগ স্থাপনৰ সুবিধা প্ৰদান কৰিছিল, সামাজিক দূৰত্ব বজাই ৰাখিও শ্ৰেণীসমূহ নিয়াৰিকৈ অবিৰতভাৱে চালি থকাত সহায় কৰিছিল। ইণ্টাৰনেট আৰু ডিভাইচ থকাসকলৰ

বাবে এইটো একেবাৰে সাধাৰণ কথা হৈ পৰিছিল। অনলাইন গেমিং আন এক উদাহৰণ, য'ত বিভিন্ন স্থানৰ লোকে সংযোগ স্থাপন কৰে আৰু ভাৰ্চুৱেল ভাৱে একেলগে খেলে। যোগাযোগ আৰু তথ্যৰ সুবিধাৰ বাবে ইণ্টাৰনেট ব্যৱহাৰ কৰি আজিকালি বহু কৰ্মচাৰীয়ে ঘৰৰ পৰাই অফিচৰ কাম-কাজ কৰে। ছাত্ৰ-ছাত্ৰী আৰু শিশুসকলেও শিক্ষা আৰু মনো�ৰঞ্জনৰ বাবে ইণ্টাৰনেট ব্যৱহাৰ কৰে।

১.৪ চাইবাৰস্পেচৰ আৰ্কিটেকচাৰ

চাইবাৰস্পেচৰ আৰ্কিটেকচাৰ কেইবাটাও স্তৰেৰে গঠিত আৰু প্ৰত্যেকেই যোগাযোগ আৰু তথ্য বিনিময় কাৰ্য সম্পাদন কৰাৰ ক্ষেত্ৰত বিশেষ বিশেষ কাম কৰে। ইয়াত বিভিন্ন উপাদান থাকে যিবোৰে একেলগে ডিজিটেল যোগাযোগ আৰু তথ্য বিনিময় প্ৰক্ৰিয়া চলাই নিয়ে। আৰ্কিটেকচাৰত ভৌতিক আন্তঃগাঁথনি, চষ্টৰেৰ ব্যৱস্থা প্ৰণালী, প্ৰটোকল, আৰু নিয়ন্ত্ৰণ ব্যৱস্থাসমূহ অন্তৰ্ভুক্ত কৰা হৈছে ধাৰু এইবোৰেই চাইবাৰস্পেচত পাৰস্পৰিক ক্ৰিয়া-কলাপসমূহ সক্ষম আৰু নিয়ন্ত্ৰণ কৰে। এই উপাদানসমূহক বহল ভাৱে চাৰিটা ধাৰণাগত স্তৰত ভাগ কৰিব পাৰি: *ভৌতিক স্তৰ, নেটৱৰ্ক স্তৰ, এপ্লিকেচন স্তৰ,* আৰু *সামাজিক স্তৰ।*

- প্ৰাথমিক পৰ্যায়ত আমি পাওঁ ***ভৌতিক স্তৰ*** । ইয়াত হাৰ্ডৱেৰসমূহ সামৰি লোৱা হয়। ইয়াত ডিজিটেল যোগাযোগৰ আন্তঃগাঁথনি গঠন কৰা সকলো ভৌতিক, মূৰ্ত উপাদান সোমাই থাকে। এই স্তৰে অন্তৰ্ভুক্ত কৰে:
  হাৰ্ডৱেৰ : ইয়াত ইণ্টাৰনেটৰ মেৰুদণ্ড স্বৰূপ কম্পিউটাৰ, চাৰ্ভাৰ, ৰাউটাৰ, চুইচ, আৰু কেবলসমূহ অন্তৰ্ভুক্ত কৰা হয়, যাৰ ফলত সমগ্ৰ বিশ্বতে তথ্যৰ সংবাহন হয়।
  ডেটা কেন্দ্ৰসমূহ : ডেটা কেন্দ্ৰসমূহে ৱেবছাইট, এপ্লিকেচনসমূহ, আৰু ডেটা হ'ষ্ট কৰাৰ বাবে প্ৰয়োজনীয় চাৰ্ভাৰ, সংৰক্ষণ চিষ্টেম, আৰু নেটৱৰ্কিং সঁজুলিসমূহৰ সুবিধা কৰি দিয়ে।

- ***নে'টৱৰ্ক স্তৰ***-টো ভৌতিক স্তৰৰ ওপৰৰ এটা স্তৰ। ইয়াত আন্তঃগাঁথনিৰ মাজেৰে তথ্য প্ৰেৰণ কৰিবলৈ সহায় কৰা প্ৰটোকল আৰু প্ৰযুক্তিসমূহ অন্তৰ্ভুক্ত কৰা হৈছে। নে'টৱৰ্ক স্তৰৰ মূল উপাদানসমূহ হ'ল:
  ইণ্টাৰনেট প্ৰটোকল (IP): ই ইণ্টাৰনেটৰ ডেটা পেকেটসমূহ ৰাউটিং কৰাৰ বাবে প্ৰাথমিক প্ৰটোকল।
  সৰবৰাহ (ট্ৰেন্সমিশ্যন) নিয়ন্ত্ৰণ প্ৰটোকল (TCP): TCP এ ডিভাইচসমূহৰ মাজত নিৰ্ভৰযোগ্য তথ্য ট্ৰেন্সমিশ্যন সুনিশ্চিত কৰে।

- ***এপ্লিকেচন স্তৰ*** সেইটো স্তৰ- য'ত চাইবাৰস্পেচৰ সৈতে ব্যৱহাৰকাৰীৰ প্ৰত্যক্ষ সংযোগ যেনে- ৰেব *ব্ৰাউজাৰ, ইমেইল ক্লায়েণ্ট, ছ'চিয়েল মিডিয়া প্লেটফৰ্ম, অনলাইন সেৱাৰ* যোগেদি চলি থাকে।

  ৰেব ব্ৰাউজাৰসমূহ হ'ল চফ্টৱেৰ এপ্লিকেচনসমূহ যিয়ে ব্যৱহাৰকাৰীসকলক ৰেবছাইটসমূহত প্ৰৱেশ আৰু মত-বিনিময় কৰাত সহায় কৰে।

  ইমেইল ক্লায়েণ্ট হৈছে ইমেইল প্ৰেৰণ আৰু গ্ৰহণ কৰিবলৈ ব্যৱহাৰ কৰা প্ৰগ্ৰেম।

  ছ'চিয়েল মিডিয়া প্লেটফৰ্ম হৈছে এনে ৰেবছাইট আৰু এপ্লিকেচন যিয়ে ব্যৱহাৰকাৰীক কণ্টেণ্ট সৃষ্টি আৰু শ্বেয়াৰ কৰিবলৈ আৰু ছ'চিয়েল নেটৱৰ্কিঙত অংশগ্ৰহণ কৰিবলৈ সক্ষম কৰে।

  অনলাইন সেৱাসমূহৰ ভিতৰত ইণ্টাৰনেটৰ জৰিয়তে বিভিন্ন কাৰ্য্যকৰীতা প্ৰদান কৰা-কমাৰ্চ প্লেটফৰ্ম, ক্লাউড সেৱা, ষ্ট্ৰীমিং সেৱা, আৰু অন্যান্য এপ্লিকেচনসমূহ অন্তৰ্ভুক্ত হৈ আছে ।

- সামাজিক ***স্তৰটোৰে*** চাইবাৰস্পেচৰ ব্যক্তি দিশটো সামৰি লৈছে। ইয়াত ব্যৱহাৰকাৰী আৰু ডিজিটেল পাৰস্পৰিক ক্ৰিয়াৰ পৰা উদ্ভৱ হোৱা সমাজৰ গাঁথনি অন্তৰ্ভুক্ত হৈ আছে। এই স্তৰত আছে:

  ব্যৱহাৰকাৰী সম্প্ৰদায় (কমিউনিটি) অৰ্থাৎ চাইবাৰস্পেচৰ ভিতৰত মত বিনিময় কৰা আৰু যোগাযোগ কৰা ব্যক্তিৰ গোট।

  সাংস্কৃতিক নীতি : ডিজিটেল সম্প্ৰদায় (কমিউনিটি) ৰ ভিতৰত বিকশিত হোৱা আচৰণ, পদ্ধতি আৰু মূল্যবোধ।

  আইনী আৰু নিয়ন্ত্ৰণ পৰিকাঠামো (ফ্ৰেমৱৰ্ক) : অনলাইন কাৰ্য্যকলাপ নিয়ন্ত্ৰণ কৰা আৰু ব্যৱহাৰকাৰীৰ অধিকাৰ আৰু গোপনীয়তা সুৰক্ষিত কৰা আইন আৰু নিয়মসমূহ ইয়াৰ অধীনত আহে।

চাইবাৰস্পেচৰ আভ্যন্তৰীণ বিষয়বোৰ বুজিবলৈ, কম্পিউটাৰ আৰু ৰেব প্ৰযুক্তিয়ে কেনেকৈ কাম কৰে তাক বুজি লোৱাতো প্ৰয়োজন। তলৰ খণ্ডসমূহত কম্পিউটাৰ আৰু ৰেব প্ৰযুক্তিৰ আভাস দিয়া হ'ব।

১.৫ কম্পিউটাৰৰ আভাস

কম্পিউটাৰ আধুনিক সমাজ-জীৱনৰ এক অবিচ্ছেদ্য অংগ হৈ পৰিছে আৰু আমাৰ জীৱনৰ প্ৰায় প্ৰতিটো দিশতেই প্ৰভাৱান্বিত কৰিছে। ঘৰত ব্যক্তিগত ব্যৱহাৰৰ পৰা আৰম্ভ কৰি শিক্ষা, ব্যৱসায়, স্বাস্থ্যসেৱা আৰু ইয়াৰ বাহিৰেও কম্পিউটাৰে আমাক অধিক কাৰ্যক্ষম কৰাত, ফলপ্ৰসূভাৱে যোগাযোগ কৰাত আৰু জটিল সমস্যা সমাধান কৰাত সহায় কৰে। এই খণ্ডত

কম্পিউটাৰ কি, ইয়াৰ বৈশিষ্ট্য, মূল উপাদান, আৰু কম্পিউটাৰৰ কার্য্যকৰীতাৰ এক আভাস প্রদান কৰিব।

কম্পিউটাৰৰ সংজ্ঞা:

কম্পিউটাৰ হৈছে এটা *ইলেক্ট্রনিক যন্ত্র* যিয়ে তথ্য বিন্যাস-বিশ্লেষণ কৰে আৰু প্রগ্রেম বা চষ্টৰেৰত নির্দেশনা অনুসৰি কাম কৰে। ইয়াক জটিল গণনা কৰিবলৈ, তথ্য পৰিচালনা কৰিবলৈ আৰু বহুতো কাম দ্রুত আৰু সঠিকভাৱে সম্পন্ন কৰিবলৈ যুগুত কৰা হৈছে।

আগতে কম্পিউটাৰ অত্যন্ত ডাঙৰ আছিল আৰু পৰিচালনা কৰিবলৈ প্রায়ে এটা সম্পূর্ণ কোঠাৰ প্রয়োজন হৈছিল। এই মেচিনবোৰে বহু পৰিমাণৰ শক্তি খৰচ কৰিছিল আৰু বাণিজ্যিক ব্যৱহাৰৰ বাবে অতি ব্যয়বহুল আছিল। ফলস্বৰূপে সেইবোৰ বিশেষ কামত সীমাবদ্ধ হৈ পৰিছিল, যেনে সৌৰবিজ্ঞান বা সামৰিক বিশেষ কামৰ সহায়ক হিচাপে। কিন্তু প্রযুক্তিগত উন্নতিৰ লগে লগে কম্পিউটাৰবোৰ সৰু হৈ আহিল আৰু শক্তিৰ প্রয়োজনীয়তা যথেষ্ট হ্রাস পালে। এই পৰিৱর্তনে ইয়াক বাণিজ্যিক প্রয়োগৰ পথ সুগম কৰিলে। আজি কম্পিউটাৰ ইমানেই ব্যাপক ভাৱে ব্যৱহৃত যে ই বিভিন্ন ইণ্টাৰেক্টিভ ডিভাইচ যেনে চেল ফোন, গ্লবেল পজিচনিং চিষ্টেম (জিপিএছ), অটোমেটিক টেলাৰ মেচিন (এটিএম) আদিৰ নিত্য ব্যৱহার্য প্রযুক্তিৰ অবিচ্ছেদ্য অংগ হৈ পৰিছে।

১.৫.১ কম্পিউটাৰৰ বৈশিষ্ট্য

কম্পিউটাৰ হৈছে প্রগ্রেম নামৰ নির্দেশনাৰ এটা গোটৰ ওপৰত ভিত্তি কৰি কাম কৰা ইলেক্ট্রনিক যন্ত্র। ই ডেটা (Data) গ্রহণ কৰে, ইয়াক প্রচেচ কৰে আৰু তথ্য (Infromation) সৃষ্টি কৰে। ইয়াত ডেটাই কেঁচা (Raw) সমল, তথ্য বা পৰিসংখ্যাক বুজায়, আনহাতে তথ্য (Infromation)এ প্রক্রিয়াকৃত (processed) তথ্যক বুজায়।

কম্পিউটাৰৰ মূল উদ্দেশ্য হৈছে সমস্যা দ্রুত আৰু সঠিকভাৱে সমাধান কৰা। কম্পিউটাৰৰ মূল বৈশিষ্ট্যসমূহ হ'ল: ***গতি, সংৰক্ষণ, সঠিকতা, স্বয়ংক্রিয়তা বা অটমেচন, কষ্টসাধ্যতা, বহুমুখীতা,*** আৰু ***খৰচৰ কার্যকাৰিতা*** । চাইবাৰ সুৰক্ষাৰ ক্ষেত্রত এই বৈশিষ্ট্যসমূহ বুজাটো অতি গুৰুত্বপূর্ণ।

- **বেগ:** কম্পিউটাৰৰ অন্যতম উল্লেখযোগ্য বৈশিষ্ট্য হ'ল ইয়াৰ গতি। কম্পিউটাৰে তথ্য প্রচেচ কৰিব পাৰে আৰু নির্দেশনাসমূহ অসাধাৰণ গতিৰে সম্পন্ন কৰিব পাৰে। কম্পিউটাৰৰ গতি সাধাৰণতে নেন'ছেকেণ্ড আৰু পিকোছেকেণ্ডত দিয়া হয়, য'ত ১ নেন'ছেকেণ্ড = ১×১০ $^{-৯}$ ছেকেণ্ড আৰু ১ পিকোছেকেণ্ড =১×১০ $^{-১২}$ ছেকেণ্ড। এই গতিবেগে কম্পিউটাৰৰ জটিল গণনা আৰু কামসমূহ দ্রুতভাৱে সম্পন্ন কৰে, যাৰ

ফলত বৈজ্ঞানিক গৱেষণা, বিত্তীয় মডেলিং, আৰু ৰিয়েল-টাইম ব্যৱস্থাৰ দৰে ক্ষেত্ৰতই অপৰিহাৰ্য হৈ পৰিছে।

- **ষ্ট'ৰেজ (Storage):** মানুহৰ দৰে কম্পিউটাৰতো স্মৃতিশক্তি থাকে। আমি যেনেকৈ সকলো কথা মনত ৰাখিব নোৱাৰো আৰু গুৰুত্বপূৰ্ণ তথ্য লিপিবদ্ধ কৰিবলৈ বহীৰ দৰে গৌণ মাধ্যমৰ ওপৰত নিৰ্ভৰশীল হওঁ, তেনেকৈ কম্পিউটাৰেও আভ্যন্তৰীণ (প্ৰাথমিক) আৰু বাহ্যিক (গৌণ) দুয়োটা মেমৰি ব্যৱহাৰ কৰে। আভ্যন্তৰীণ মেমৰি ব্যয়বহুল আৰু ক্ষমতা সীমিত, আনহাতে গৌণ ষ্ট'ৰেজ অধিক সুলভ আৰু অধিক ক্ষমতা প্ৰদান কৰে। তথ্য সংৰক্ষণৰ বাবে গৌণ মেমৰি অতি গুৰুত্বপূৰ্ণ। গৌণ ষ্ট'ৰেজৰ উদাহৰণ হাৰ্ড ডিস্ক ড্ৰাইভসমূহ (HDDs), চলিড ষ্টেট ড্ৰাইভসমূহ (SSDs), অপটিকেল ডিস্কসমূহ (CDs আৰু DVDs), আৰু পেন ড্ৰাইভসমূহ।

- **সঠিকতা:** কম্পিউটাৰ হৈছে এটা দ্ৰুত, নিৰ্ভৰযোগ্য আৰু শক্তিশালী ইলেক্ট্ৰনিক যন্ত্ৰ যিয়ে সঠিক তথ্য আৰু নিৰ্দেশনাত সদায় সঠিক ফলাফল দিযয়ে। গতিকে কোনো ভুল হ'লে ভুল তথ্য বা প্ৰগ্ৰেম দেখিলে জানিব লাগিব যে সেয়া ব্যৱহাৰকাৰীৰ নিৰ্দেশনা বা ভুল প্ৰয়োগৰ ফলত হোৱা। ইয়াৰ পৰা দেখা যায় যে কম্পিউটাৰৰ পৰা লাভ কৰা আউটপুট ইনপুট ডেটা আৰু নিৰ্দেশনা ওপৰত নিৰ্ভৰ কৰে। কম্পিউটাৰৰ পৰিভাষাত এই নীতিক "গাৰেজ-ইন, গাৰেজ-আউট" বুলি জনা যায়।

- **স্বয়ংক্ৰিয়কৰণ বা অটমেচন (Automation):** কম্পিউটাৰত অটমেচনে নিৰ্দেশনা বা প্ৰগ্ৰেম নিৰ্ধাৰণ কৰাৰ পিছত মানুহৰ হস্তক্ষেপ অবিহনে এটা ব্যৱস্থাৰ ক্ৰম বা কাম সম্পন্ন কৰাৰ ক্ষমতাক বুজায়। এই ক্ষমতাই কমপিউটাৰসমূহক পূৰ্বনিৰ্ধাৰিত আদেশসমূহ পদ্ধতিগতভাৱে আৰু সঠিকভাৱে কৰিবলৈ সহায় কৰে, দক্ষতা বৃদ্ধি কৰে, মানুহৰ দ্বাৰা হ'ব পৰা ভুল হ্ৰাস কৰে, আৰু অধিক জটিল কামসমূহৰ পৰা মানুহক মুক্ত কৰে। অটমেচনে চাইবাৰ সুৰক্ষাকে ধৰি বিভিন্ন ডমেইনত উৎপাদনশীলতা, সঠিকতা, আৰু দক্ষতা বৃদ্ধি কৰে।

- **কষ্টসাধ্যতা:** মানুহৰ দৰে কম্পিউটাৰ কেতিয়াও পুনৰাবৃত্তিমূলক কামত ভাগৰি নাযায়। ভুল নকৰাকৈ ঘণ্টাৰ পিছত ঘণ্টা ধৰি অবিৰতভাৱে কাম কৰিব পাৰে। যিমানেই জটিল নহওক কিয়, দীঘলীয়া নহওক কিয়, সময় নালাগক কিয়- ইয়াক সামঞ্জস্যপূৰ্ণ সঠিকতাৰে আয়াসতে সম্পন্ন কৰি দিয়ে।

- **বহুমুখীতা:** কম্পিউটাৰে বহুতো কাম কৰিবলৈ সক্ষম। এই বহুমুখীতা, *নমনীয়* হোৱাৰ এক গুণৰ বাবেই দৈনন্দিন জীৱনৰ বিভিন্ন ক্ষেত্ৰত কম্পিউটাৰ ব্যৱহাৰ প্ৰচুৰ।

উদাহৰণস্বৰূপে, ঘৰুৱা ব্যৱহাৰৰ বাবে ব্যক্তিগত কম্পিউটাৰ, শিক্ষামূলক সঁজুলি, ব্যৱসায়িক সহায়ক, শিক্ষণ সামগ্ৰী, বতৰ পূৰ্বাভাস ব্যৱস্থা, জটিল অনুকৰণ আৰু ৰেলৱে, বেংকিং, চিকিৎসাৰ লগতে মনোৰঞ্জনৰ সঁজুলি হিচাপে ই কাম কৰে। যিয়াত একে সময়তে বিভিন্ন কাম একেলগে কৰিব পৰা যায়। কম্পিউটাৰৰ বহুমুখী-প্ৰচেছিং ক্ষমতাই ইয়াক অধিক প্ৰয়োজনীয় প্ৰযুক্তি কৰি তুলিছে, যাৰ ফলত যিকোনো ক্ষেত্ৰতেই ইয়াৰ ব্যৱহাৰ এৰাব নোৱৰা অংগ হৈ পৰিছে।

- **খৰচৰ ফলপ্ৰসূতা** : কম্পিউটাৰ ব্যৱহাৰে জনশক্তিৰ প্ৰয়োজনীয়তা হ্ৰাস কৰে আৰু বিভিন্ন কাম সম্পন্ন কৰাৰ এক সুচল আৰু কাৰ্যক্ষম সহায়ক হিচাপে ই প্ৰস্তুত থাকে। উদাহৰণস্বৰূপে, সাধাৰণ ডাক ব্যৱস্থাৰ জৰিয়তে গুৰুত্বপূৰ্ণ নথিপত্ৰ প্ৰেৰণ কৰিবলৈ কমেও ২-৩ দিন সময় লাগে, আনহাতে ইমেইলৰ জৰিয়তে প্ৰেৰণ কৰা একে তথ্য তৎক্ষণাত হাতত পৰেগৈ। ইয়াৰ ফলত কাগজ-পত্ৰকে ধৰে আৰু মানুহৰ প্ৰচেষ্টা হ্ৰাস পায়, যাৰ ফলত খৰচো কম হয়।

যদিও আজিৰ দিনত কম্পিউটাৰক কৃত্ৰিম বুদ্ধিমত্তা (AI)ৰ জৰিয়তে বুদ্ধিমান কৰি তোলাৰ প্ৰচেষ্টা কৰা হৈছে, তথাপিও ইয়াত স্বতন্ত্ৰ সিদ্ধান্ত গ্ৰহণৰ ক্ষমতাৰ অভাৱ। ইয়াৰ বুদ্ধিমত্তাৰ স্তৰ মূলতঃ শূন্য, আৰু কামবোৰ কৰিবলৈ তেওঁলোকক মানুহৰ নিৰ্দেশনা আৰু সহায়ৰ প্ৰয়োজন।

১.৫.২ কম্পিউটাৰৰ মূল উপাদানসমূহ

কম্পিউটাৰ এটাই সুকলমে কাম কৰিবলৈ হাৰ্ডৱেৰ আৰু চফ্টৱেৰ একেলগে নিৰৱচ্ছিন্নভাৱে কাম কৰিব লাগে। চফ্টৱেৰক হাৰ্ডৱেৰ অংগসমূহৰ সৈতে ফলপ্ৰসূভাৱে কাম চলাই নিবলৈ ইয়াত অপাৰেটিং চিষ্টেম এটা মধ্যস্থতাকাৰী হিচাপে কাম কৰে। গতিকে এইখিনিতে আমি হাৰ্ডৱেৰ আৰু চফ্টৱেৰৰ বিষয়ে অলপ জানি লওঁ আহক।

কম্পিউটাৰ হাৰ্ডৱেৰ হৈছে কম্পিউটাৰৰ ভৌতিক উপাদানসমূহ, যিবোৰ স্পষ্ট, যাক দেখা পোৱা যায় আৰু স্পৰ্শ কৰিব পাৰি। ইয়াত CPU, RAM, ইনপুট/আউটপুট ডিভাইচসমূহ, আৰু সংৰক্ষণ উপাদানসমূহৰ দৰে প্ৰয়োজনীয় অংশসমূহ অন্তৰ্ভুক্ত। ইয়াৰ প্ৰত্যেকেই কম্পিউটাৰৰ সামগ্ৰিক কাৰ্য্যকলাপত এল নিৰ্দিষ্ট ভূমিকা পালন কৰে।

আনহাতে, **কম্পিউটাৰ চফ্টৱেৰ** বুলিলে নিৰ্দেশনা, তথ্য বা প্ৰগ্ৰেমসমূহক বুজায় যিয়ে কম্পিউটাৰক কাম সম্পন্ন কৰিবলৈ সহায় কৰে। ই হাৰ্ডৱেৰৰ দৰে ভৌতিক নহয়। চফ্টৱেৰৰ স্পৰ্শ কৰিব নোৱাৰি। ইয়াক বহলভাৱে দুটা ভাগত ভাগ কৰিব পাৰি:

- **চিষ্টেম চফ্টৱেৰ**
- **এপ্লিকেচন চফ্টৱেৰ**

চিষ্টেম চফ্টৱেৰে কম্পিউটাৰ হার্ডৱেৰক পৰিচালনা আৰু সহায় কৰে, অন্য চফ্টৱেৰবোৰ ফলপ্ৰসূভাৱে চলিবলৈ প্লেটফর্ম প্ৰদান কৰে। এই শ্ৰেণীত *অপাৰেটিং চিষ্টেমসমূহ* (যেনে Windows, Linux, আৰু macOS), *ডিভাইচ ড্ৰাইভাৰসমূহ* (যি হার্ডৱেৰ আৰু অপাৰেটিং ছিষ্টেমৰ মাজত যোগাযোগ স্থাপন কৰে), আৰু *ইউটিলিটিছ* (ভাইৰাছ স্কেনিং আৰু ডিস্ক মেনটেইননেন্সৰ দৰে কার্য্যসমূহৰ বাবে প্ৰয়োগ হোৱা প্ৰগ্ৰামসমূহ) অন্তর্ভুক্ত থাকে।

এপ্লিকেচন চফ্টৱেৰবোৰ ব্যৱহাৰকাৰীসকলক নির্দিষ্ট কামসমূহ সম্পন্ন কৰাত সহায় কৰিবলৈ ডিজাইন কৰা হৈছে। উদাহৰণস্বৰূপে প্ৰডাক্টিভিটি চফ্টৱেৰ (যেনে ৱার্ড প্ৰচেছৰ আৰু স্প্ৰেডশ্বীট), মিডিয়া প্লেয়াৰ আৰু সম্পাদনাৰ (অডিঅ', ভিডিঅ', আৰু ছবিৰ বাবে), ৱেব ব্ৰাউজাৰ (যেনে গুগল ক্ৰ'ম, ফায়াৰফক্স, ইত্যাদি), আৰু মনোৰঞ্জনৰ উদ্দেশ্যে বিভিন্ন গেমবিলাক ইয়াৰ ভিতৰত পৰে।

কম্পিউটাৰৰ বিভিন্ন উপাদানসমূহে কেনেকৈ কাম কৰে সেই কথা বুজাতো অতি গুৰুত্বপূর্ণ। এতিয়া প্ৰাথমিক উপাদানসমূহৰ বিষয়ে অতি চমুকৈ আলোচনা কৰোঁ আহক-

1. **চেণ্ট্ৰেল প্ৰচেছিং ইউনিত (CPU):** প্ৰায়ে কম্পিউটাৰৰ মগজু বুলি কোৱা চিপিইউয়ে নির্দেশনাসমূহ এক্সিকিউট কৰা আৰু গণনা কৰাৰ দায়িত্ব লয়। ই ডেটা প্ৰচেচ কৰে আৰু সমগ্ৰ কম্পিউটাৰত তথ্যৰ প্ৰবাহ পৰিচালনা কৰে। এটা দ্ৰুত CPU এ প্ৰগ্ৰাম নির্দেশসমূহৰ দ্ৰুততৰ ভাৱে সম্পন্ন কৰে।
2. **মেমৰি:** ৰেণ্ডম একচেচ মেমৰি (RAM) হৈছে কম্পিউটাৰে CPU দ্বাৰা সক্ৰিয়ভাৱে ব্যৱহাৰ কৰা বা প্ৰচেচ কৰা তথ্য সংৰক্ষণ কৰিবলে ব্যৱহাৰ কৰা এক ধৰণৰ ক্ষণস্থায়ী মেমৰি। কম্পিউটাৰ বন্ধ কৰিলেই এই অস্থায়ী ডেটা হেৰাই যায়। RAMএ দ্ৰুততৰ ভাৱে পঢ়া আৰু লিখাৰ সুবিধা কৰি দিয়ে, কম্পিউটাৰৰ সামগ্ৰিক প্ৰয়োগ (কাম কৰাৰ পৰিৱেশ) উন্নত কৰে। এটা দ্ৰুত CPUৰ বাবে পর্যাপ্ত RAM দৰকাৰ, কাৰণ ই চিষ্টেমৰ সামগ্ৰিক পার্ফমেন্সত ব্যাঘাত নোহোৱাকৈ একেলগে বহু এপ্লিকেচন চলোৱাৰ বাবে সুবিধা দিয়ে।
3. **ৰিড অনলি মেমৰি (ROM):** এই মেমৰি স্থায়ী ষ্টৰেজ। ই কম্পিউটাৰ বুট কৰা, মূল কার্য্যসমূহ সম্পাদন কৰাৰ বাবে প্ৰয়োজনীয় নির্দেশসমূহৰ দায়িত্ব লয়।
4. **ষ্টৰেজ:** ষ্টৰেজ ডিভাইচসমূহ, যেনে হার্ড ডিস্ক ড্ৰাইভসমূহ (HDDs) আৰু চলিড ষ্টেট ড্ৰাইভসমূহ (SSDs), ডেটা স্থায়ীভাৱে সংৰক্ষণ কৰিবলৈ ব্যৱহাৰ কৰা হয়। এই ডিভাইচসমূহত ডকুমেণ্ট আৰু প্ৰগ্ৰেমসমূহকে ধৰি সকলো ধৰণৰ ডেটা থাকে। ষ্টৰেজৰ ক্ষমতা যিমানেই ডাঙৰ হ'ব সিমানেই অধিক ডেটা সংৰক্ষণ কৰিব পাৰি।
5. **মাডাৰবর্ড:** মাডাৰবর্ড হৈছে কম্পিউটাৰৰ সকলো উপাদান সংযোগ কৰা মূল চার্কিট বর্ড। ইয়াৰ দ্বাৰাই সকলো উপাদানৰ মাজত পাৰস্পৰিক যোগাযোগ স্থাপন হয়। মাডাৰবর্ড হৈছে এটা প্ৰিণ্ট চার্কিট য'ত এক্সপান্সন কার্ড, মেমৰি মডিউল, প্ৰচেছৰ আদিৰ বাবে সংযোগকাৰী স্থান থাকে।

6. **ইনপুট ডিভাইচসমূহ:** ইনপুট ডিভাইচসমূহে ব্যৱহাৰকাৰীসকলক এটা কম্পিউটাৰৰ সৈতে যোগাযোগ আৰু নিয়ন্ত্রণ কৰাৰ অনুমতি দিয়ে। এই ডিভাইচসমূহে ব্যৱহাৰকাৰীক তথ্য, আদেশ, আৰু সঁহাৰিসমূহ ইনপুট কৰিবলে সামর্থবান কৰে, চিস্টেমৰ সৈতে যোগাযোগ সহজ কৰি। সাধাৰণ উদাহৰণসমূহৰ ভিতৰত কিবর্ড, মাউছ, আৰু টাচস্ক্রীণসমূহ অন্তর্ভুক্ত। অন্য ইনপুট ডিভাইচসমূহৰ ভিতৰত আছে স্ক্যানাৰ, যিয়ে ভৌতিক দস্তাবেজসমূহ ডিজিটেলাইজ কৰে, আৰু মাইক্র'ফোনসমূহ, যিয়ে ভয়েচ কমাণ্ড আৰু ৰেকর্ডিঙৰ বাবে অডিঅ' ইনপুট ধৰি ৰাখে।

7. **আউটপুট ডিভাইচসমূহ:** আউটপুট ডিভাইচসমূহ হৈছে হার্ডৱেৰ উপাদানসমূহ যিয়ে কম্পিউটাৰৰ প্রচেছিঙৰ ফলাফল ব্যৱহাৰকাৰীলৈ প্রেৰণ কৰে। তেওঁলোকে ডিজিটেল তথ্যক এনে এটা ৰূপলৈ অনুবাদ কৰে যিটো দৃশ্যগতভাৱে হওক, শ্রৱণীয়ভাৱে হওক বা শাৰীৰিকভাৱে হওক। সাধাৰণ আউটপুট ডিভাইচসমূহৰ ভিতৰত আছে:
    - **মনিটৰসমূহ** : কম্পিউটাৰৰ পৰা দৃশ্যমান আউটপুট প্রদর্শন কৰক, লিখনী, ছবি, আৰু ভিডিঅ'সমূহ অন্তর্ভুক্ত কৰি।
    - **প্রিন্টাৰ** : ডিজিটেল নথিপত্র আৰু ছবিৰ ভৌতিক কপি প্রস্তুত কৰা।
    - **স্পীকাৰ** : ডিজিটেল অডিঅ' সংকেতক শব্দলৈ ৰূপান্তৰ কৰা।
    - **প্রজেক্টৰ** : উপস্থাপন আৰু মাল্টিমিডিয়া প্রদর্শনৰ বাবে ডাঙৰ পর্দাত দৃশ্যমান বিষয়বস্তু প্রদর্শন কৰা।
    - **হেডফোন** : উন্নত শব্দৰ মানদণ্ডৰ সৈতে ব্যক্তিগত অডিঅ' আউটপুট প্রদান কৰে।

8. **পাৱাৰ চাপ্লাই অধ্যায় (PSU):** পিএছইউয়ে এটা আউটলেটৰ পৰা বৈদ্যুতিক শক্তিক কম্পিউটাৰ আৰু ইয়াৰ উপাদানসমূহৰ বাবে ব্যৱহাৰযোগ্য ৰূপলৈ ৰূপান্তৰিত কৰে।

কম্পিউটাৰৰ কার্য্যকৰীতা :

মূল কার্য্যক্ষমতাসমূহ হ'ল -

- **তথ্য প্রক্রিয়াকৰণ:** কম্পিউটাৰে চফ্টৱেৰ প্রগ্রেমত দিয়া নির্দেশনা অনুসৰি গণনা কৰি, তথ্য সজাই পৰাই আৰু তথ্যৰ পৰিৱর্তন কৰি তথ্য প্রক্রিয়াকৰণ কৰে।
- **তথ্য সংৰক্ষণ:** কম্পিউটাৰে সাময়িকভাৱে ৰেমত আৰু সংৰক্ষণ ডিভাইচত স্থায়ীভাৱে দুয়োটা তথ্য সংৰক্ষণ কৰে। ইয়াত চিস্টেম ফাইলসমূহৰ পৰা ব্যৱহাৰকাৰী দস্তাবেজসমূহলৈকে সকলো অন্তর্ভুক্ত কৰা হৈছে।
- **নেটৱর্কিং:** কম্পিউটাৰে তাঁৰযুক্ত বা বেতাঁৰ নেটৱর্কৰ জৰিয়তে অন্য কম্পিউটাৰ আৰু ডিভাইচসমূহৰ সৈতে সংযোগ কৰিব পাৰে, যাৰ ফলত তথ্য অংশীদাৰী, ইণ্টাৰনেট প্রৱেশ আৰু যোগাযোগ সক্ষম হয়।

- **ব্যৱহাৰকাৰী আন্তঃপৃষ্ঠ:** কমপিউটাৰসমূহে ব্যৱহাৰকাৰীসকলক তেওঁলোকৰ সৈতে পাৰস্পৰিক ক্ৰিয়া কৰিবলে আন্তঃপৃষ্ঠসমূহ প্ৰদান কৰে, যেনে গ্ৰাফিকেল ব্যৱহাৰকাৰী আন্তঃপৃষ্ঠসমূহ (GUIs) আৰু আদেশ-শাৰী আন্তঃপৃষ্ঠসমূহ (CLIs)।
- **স্বয়ংক্ৰিয়কৰণ:** কম্পিউটাৰে প্ৰগ্ৰেমিংৰ জৰিয়তে পুনৰাবৃত্তিমূলক কামসমূহ স্বয়ংক্ৰিয় কৰিব পাৰে, যাৰ ফলত দক্ষতা বৃদ্ধি পায় আৰু মানুহৰ ভুলৰ সম্ভাৱনা হ্ৰাস পায়।

১.৬ ৱেব প্ৰযুক্তিৰ আভাস

ৱেব প্ৰযুক্তিয়ে ইণ্টাৰনেটৰ জৰিয়তে বিভিন্ন যন্ত্ৰৰ মাজত যোগাযোগ কৰিবলৈ ব্যৱহাৰ কৰা সা-সঁজুলি আৰু কৌশলসমূহ সামৰি লয়। ই HTML, JavaScript, PHP, আৰু অন্যান্য ভাষা ব্যৱহাৰ কৰি ৱেব উপাদান সমূহ সৃষ্টি, পৰিচালনা, আৰু প্ৰদানত সহায় কৰে। ইণ্টাৰনেটত অসংখ্য ৰাজহুৱা ৱেবছাইট আছে, যিবোৰৰ প্ৰতিটোৱে টেক্স্ট, ভিডিঅ', অডিঅ', আৰু ছবিৰ ফৰ্মেটত তথ্য থকা ৱেব পৃষ্ঠাৰে গঠিত। এই উপাদানসমূহ ৱৰ্ল্ড ৱাইড ৱেবত হাইপাৰলিংকৰ দ্বাৰা আন্তঃসংযুক্ত হৈ থাকে, যিবোৰ ৱেব ব্ৰাউজাৰৰ দ্বাৰা প্ৰদান কৰা চফ্টৱেৰ ইণ্টাৰফেচৰ জৰিয়তে ব্যৱহাৰকাৰীৰ বাবে প্ৰৱেশযোগ্য হৈ পৰে।

চাইবাৰস্পেচ অধ্যয়নৰ বাবে ৱেব প্ৰযুক্তিৰ বিষয়ে জনাটো গুৰুত্বপূৰ্ণ কাৰণ ইয়ে অনলাইনত তথ্য কেনেকৈ আদান প্ৰদান কৰা হয় সেইটো বৰ্ণনা কৰে। ৱেব ব্ৰাউজাৰসমূহ, যেনে Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, আৰু Internet Explorer, ইণ্টাৰনেটৰ পৰা টেক্স, ডেটা, ছবি, এনিমেচন, আৰু ভিডিঅ' প্ৰদৰ্শন কৰাত এক গুৰুত্বপূৰ্ণ ভূমিকা পালন কৰে। এইবিলাকে এনে ইণ্টাৰফেচ প্ৰদান কৰে যাৰ জৰিয়তে ব্যৱহাৰকাৰীয়ে ৱেব সামগ্ৰীৰ সৈতে কাৰ্য সম্পাদন কৰে আৰু নেভিগেট কৰে, ইয়াৰ ফলতে চাইবাৰস্পেচৰ ডিজিটেল লেণ্ডস্কেপ বুজিব উঠিবলৈ সহজ হৈ পৰে।

এটা ৱেব ছাৰ্ভাৰে এটা কম্পিউটাৰ বা একাধিক কম্পিউটাৰৰ নেটৱৰ্কক বুজায় যিটো একাধিক ব্যৱহাৰকাৰীলৈ ৱেব পৃষ্ঠা আৰু সামগ্ৰী প্ৰদান কৰিবলৈ ডিজাইন কৰা হয়। ই নেটৱৰ্কৰ জৰিয়তে ব্যৱহাৰকাৰীৰ পৰা অনুৰোধ, নিৰ্দেশনা প্ৰচেছ কৰে আৰু সেই অনুসৰি ৱেব পেজত থকা ফাইল প্ৰদান কৰে। মূলতঃ, এটা ৱেব ছাৰ্ভাৰ হৈছে এটা চফ্টৱেৰ এপ্লিকেচন যিয়ে ৱেব পৃষ্ঠাৰ অনুৰোধ, নিৰ্দেশনা মানে আৰু ডেটা সঞ্চয়, প্ৰক্ৰিয়াকৰণ, আৰু তাৎক্ষণিকভাৱে প্ৰদান কৰা কাম সম্পন্ন কৰে। এই আন্তঃক্ৰিয়া হাইপাৰটেক্স ট্ৰান্সফাৰ প্ৰটকল (HTTP)ৰ জৰিয়তে হয়।

ৱেবত, সকলো নথিপত্ৰ এটা বিশেষ মাৰ্কআপ ভাষাত ফৰ্মেট কৰা হয় যাক হাইপাৰটেক্স মাৰ্কআপ ভাষা (HTML) বুলি কোৱা হয় । এইবোৰে অন্যান্য নথিপত্ৰ, গ্ৰাফিক্স, অডিঅ', আৰু ভিডিঅ' ফাইলৰ লিংক সামৰি লয়। ৱেব ছাৰ্ভাৰসমূহে প্ৰাথমিকভাৱে HTML নথিপত্ৰ, ছবি, ষ্টাইল চিট, আৰু টেক্সৰ দৰে উপাদানসমূহ পৰিচালনা কৰে। HTTPৰ উপৰিও,

ইহঁতে ইমেইলৰ বাবে SMTP (Simple Mail Transfer Protocol) আৰু ফাইল সংৰক্ষণ আৰু স্থানান্তৰৰ বাবে FTP (File Transfer Protocol)ৰ দৰে প্ৰটোকলসমূহক সহায় কৰে। যেতিয়া কোনোৱে ৱেব পৃষ্ঠাৰ অনুৰোধ কৰে, ছাৰ্ভাৰে হয় প্ৰত্যক্ষভাৱে অনুৰোধ কৰা ফাইল পঠিয়াই দিয়ে বা ডেটাবেচৰ সৈতে ইণ্টাৰেক্ট কৰিব পৰা স্ক্ৰিপ্টৰ জৰিয়তে এক গতিশীল প্ৰতিক্ৰিয়া সৃষ্টি কৰে। ৱেব ছাৰ্ভাৰৰ জনপ্ৰিয় উদাহৰণসমূহৰ ভিতৰত Apache Web Server, Microsoftৰ Internet Information Services (IIS), Apache Tomcat, আৰু NGINX আদি অন্তৰ্ভুক্ত।

১.৬.১ ৱৰ্ল্ড ৱাইড ৱেব

ইণ্টাৰনেট আৰু ৱেব শব্দবোৰ এতিয়া তেনেই সাধাৰণ হৈ পৰিছে। ৱৰ্ল্ড **ৱাইড ৱেব** (WWW), যাক সাধাৰণ ভাষাত কেৱল **ৱেব** বুলি কোৱা হয়, ই ইণ্টাৰনেটৰ দ্বাৰা প্ৰদান কৰা এক গুৰুত্বপূৰ্ণ সেৱা। ই বিশ্বজুৰি বিভিন্ন লিখিত, গ্ৰাফিকেল, আৰু অডিঅ'-ভিজুৱেল তথ্য সংগঠিত আৰু প্ৰদৰ্শন কৰাৰ এক গোলকীয় প্লেটফৰ্ম হিচাপে কাম কৰে। ৱেবৰ লগতে জনপ্ৰিয় ইণ্টাৰনেট সেৱাসমূহৰ ভিতৰত ইমেইল, টেলনেট, এফটিপি, আৰু ই-কমাৰ্চ অন্তৰ্ভুক্ত। ৱেবে বিভিন্ন কাৰ্য্যকলাপ সক্ষম কৰে:

- সংবাদ, ই-পেপাৰ, সময়সূচী, ই-বুক্স, চলিত ঘটনাবলী, বিজ্ঞান, প্ৰযুক্তি, আৰু ৰাজনীতি সম্পৰ্কীয় তথ্য সন্ধান।
- তথ্য বিশ্বব্যাপী বিতৰণ।
- অনলাইন বেংকিং লেনদেন আৰু বিনিয়োগ সম্পন্ন কৰা।
- চফট্ ৱেৰ আৰু এপ্লিকেচন ডাউনলোড কৰা।
- ইমেইল আৰু চৰকাৰী চিঠিপত্ৰ প্ৰেৰণ কৰা।
- ফাইল, চফ্টৱেৰ, সংগীত, আৰু ভিডিঅ' আপলোড আৰু ডাউনলোড কৰা।
- দূ�ৰৱৰ্তী কম্পিউটাৰ, তথ্য সেৱা লাভ কৰা, অনলাইন আলোচনা, ভিডিঅ' কনফাৰেন্স, আৰু ছাটিঙৰ অংশগ্ৰহণ কৰা।

১৯৮৯ চনত চুইজাৰলেণ্ডৰ CERN (European Organization for Nuclear Research) ত ব্ৰিটিছ বিজ্ঞানী **টিম বার্নার্ছ-লীয়ে** ৱৰ্ল্ড ৱাইড ৱেব আৱিষ্কাৰ কৰিছিল।১৯৯০ চনত তেওঁ তিনিটা মূল প্ৰযুক্তি বিকশিত কৰিছিল: হাইপাৰলিংকড সম্পদ উদ্ধাৰৰ বাবে হাইপাৰটেক্সট ট্ৰেন্সফাৰ প্ৰট'কল (HTTP) ইউনিফৰ্ম ৰিচ'ৰ্চ আইডেন্টিফায়াৰ (URL) ৱেবত সম্পদ চিনাক্তকৰণৰ বাবে, আৰু হাইপাৰটেক্সট মাৰ্কআপ ভাষা (HTML) টেগসমূহ ব্যৱহাৰ কৰি ৱেবপেজসমূহ ডিজাইন কৰাৰ বাবে যি গঠন, সংস্থাপন, আৰু বিষয়বস্তু সংজ্ঞায়িত কৰে।

জানো আহক

ৰেবৰ নিয়মীয়া কথা বতৰাৰ বাহিৰৰ চিন্তা কৰিব লাগিবলগীয়া কথা এটা কওঁ। তথ্যৰ স্বাৰ্থত আমি প্ৰতিদিনে যোৱা ৰেবছাইটবোৰে সমগ্ৰ ইণ্টাৰনেটৰ এটা সৰু অংশহে প্ৰতিনিধিত্ব কৰে। প্ৰকৃততৰ ইণ্টাৰনেটৰ স্তৰক- পৃষ্ঠৰ ৰেব, গভীৰ ৰেব আৰু ডাৰ্ক ৰেবভেই ভাগত ভাগ কৰা হৈছে।

ছাৰ্ফেচ ৰেব : ইণ্টাৰনেটৰ এইটোৱেই আটাইতকৈ দৃশ্যমান আৰু সুলভ অংশ যিটো আমি দৈনিক ব্যৱহাৰ কৰো। ইয়াত গুগল আৰু বিঙৰ দৰে চাৰ্চ ইঞ্জিনৰ দ্বাৰা সূচীভুক্ত ৰেবছাইট থাকে। এই ৰেবছাইটসমূহত বাতৰি আৰু মনোৰঞ্জনৰ পৰা আৰম্ভ কৰি শৈক্ষিক সম্পদ আৰু ই-কমাৰ্চ প্লেটফৰ্মলৈকে তথ্য থাকে।

ডিপ ৰেব : ডিপ ৰেবে ছাৰ্ফেচ ৰেবতকৈ ইণ্টাৰনেটৰ বৃহৎ অংশক বুজায়। ইয়াত এনে বিষয়বস্তু অন্তৰ্ভুক্ত কৰা হয় যিবোৰ চাৰ্চইঞ্জিনৰ দ্বাৰা সূচীভুক্ত নহয় আৰু প্ৰৱেশ কৰিবলৈ নিৰ্দিষ্ট URL বা প্ৰমাণপত্ৰৰ প্ৰয়োজন হয়। ইয়াত, আপুনি ব্যক্তিগত ডেটাবেছ, চিকিৎসা ৰেকৰ্ড, বিত্তীয় তথ্য, আৰু শৈক্ষিক সম্পদৰ দৰে তথ্য পাব যিবোৰ ৰাজহুৱাকৈ উপলব্ধ কৰোৱা নহয়।

ডাৰ্ক ৰেব : ডাৰ্ক ৰেব ইচ্ছাকৃতভাৱে লুকুৱাই ৰখা হয় আৰু ইয়াত প্ৰৱেশ কৰিবলৈ বিশেষ সঁজুলি বা চফ্টৱেৰৰ প্ৰয়োজন হয়, যেনে TOR (The Onion Router) বা I2P (Invisible Internet Project)। ই এটা অভাৱলে নেটৱৰ্কত কাম কৰে যি ব্যৱহাৰকাৰীসকলক তেওঁলোকৰ IP ঠিকনাসমূহ এনক্ৰিপচনৰ একাধিক স্তৰৰ যোগেদি মাস্ক কৰি বেনামী (নামহীন) কৰে। ডাৰ্ক ৰেবত অবৈধ ব্যৱসায়, হেকিং সেৱা, অবৈধ পৰ্ণগ্ৰাফী, ড্ৰাগছ সৰৱৰাহৰ, উগ্ৰবাদী মতাদৰ্শকে ধৰি অবৈধ কাৰ্যকলাপ আৰু বিষয়ৰ বাবে জনাজাত। ইয়াক ব্যৱহাৰকাৰীসকলৰ উপস্থিতিহীন আৰু গোপনীয়তা প্ৰদান কৰিবলৈ ডিজাইন কৰা হৈছে, যাৰ ফলত ইণ্টাৰনেটৰ এই ক্ষেত্ৰখনৰ ভিতৰত চলোৱা কাৰ্য্যকলাপসমূহৰ সন্ধান কৰাটো কৰ্তৃপক্ষৰ বাবে প্ৰত্যাহ্বানজনক হৈ পৰিছে।

এই অধ্যায়ত আমি চাইবাৰ স্পেচৰ জটিল জগতখনৰ পৰিচয় দিলোঁ। আধুনিক সমাজত ইয়াৰ বহল পৰিসৰ, গুৰুত্ব আৰু গভীৰ প্ৰভাৱৰ বিষয়ে আমি বৰ্ণনা কৰিছো।



অগ্ৰগতি নিৰীক্ষণ

Q1) চাইবাৰ স্পেচৰ ভৌতিক স্তৰত কি কি অন্তৰ্ভুক্ত হৈ আছে?

Q2) চাইবাৰস্পেচত নেটৰৰ্ক স্তৰৰ প্ৰধান কাম কি?

Q3) নে'টৰৰ্ক স্তৰৰ দুটা মূল উপাদানৰ নাম লিখক।

Q4) এপ্লিকেচন স্তৰত ৱেব ব্ৰাউজাৰৰ ভূমিকা কি?

Q5) কি ধৰণৰ প্লেটফৰ্ম চাইবাৰস্পেচৰ সামাজিক স্তৰত অন্তৰ্ভুক্ত কৰা হৈছে?

Q6) ডেটা চেণ্টাৰ কি, আৰু ই কি প্ৰদান কৰে?

Q7) নে'টৰৰ্ক স্তৰৰ প্ৰসংগত ইন্টাৰনেট প্ৰটোকল (IP) ৰ সংজ্ঞা নিৰোপণ কৰক।

Q8) দৈনন্দিন জীৱনৰ বিভিন্ন ক্ষেত্ৰত কম্পিউটাৰৰ বহুমুখীতাই ইয়াক কেনেকৈ ব্যৱহাৰ কৰিবলৈ অনুমতি দিয়ে বৰ্ণনা কৰক

Q9) বিভিন্ন ক্ষেত্ৰত অপৰিহাৰ্য হৈ পৰা কম্পিউটাৰৰ মূল বৈশিষ্ট্যসমূহ ব্যাখ্যা কৰক

Q10) খালী ঠাই পূৰণ কৰক:

i. _____ ত তথ্যৰে ভৰা ৱেবছাইটসমূহ অন্তৰ্ভুক্ত কৰা হয় যিবোৰ চাৰ্চ ইঞ্জিনৰ দ্বাৰা সূচীভুক্ত কৰা হয়।

ii. _____ই ইচ্ছাকৃতভাৱে লুকুৱাই ৰখা ইণ্টাৰনেটক বুজায়।

iii. "চাইবাৰস্পেচ" শব্দটো প্ৰথমে কল্পবিজ্ঞান লেখক _____ য়ে তেওঁৰ উপন্যাস _____ ত ব্যৱহাৰ কৰিছিল।

iv. _____ ত এনে বিষয়বস্তু অন্তৰ্ভুক্ত কৰা হয় যিবোৰ চাৰ্চ ইঞ্জিনৰ দ্বাৰা সূচীভুক্ত নহয় আৰু প্ৰৱেশ কৰিবলৈ নিৰ্দিষ্ট URL বা প্ৰমাণপত্ৰৰ প্ৰয়োজন হয়।



১.৭ অধ্যায়টিৰ পৰা আমি কি কি শিকিলোঁ

- চাইবাৰস্পেচ হৈছে আন্তঃসংযোগী কম্পিউটাৰ, চাৰ্ভাৰ, আৰু নেটৰৰ্কৰ দ্বাৰা গঠিত এটা ভাৰ্চুৱেল পৰিৱেশ, যিয়ে ডিজিটেল যোগাযোগ আৰু কাৰ্য্যকলাপসমূহ সম্পন্ন কৰে।
- ই স্মাৰ্টফোন আৰু IoT ডিভাইচৰ ব্যৱহাৰৰ সৈতে বিস্তাৰিত হয়, যিয়ে ভাৰ্চুৱেল মিটিং, অনলাইন পৰামৰ্শ, আৰু ব্যৱসায়িক চুক্তিসমূহক সহায় কৰে।
- চাইবাৰস্পেছে কম্পিউটাৰ, নেটৰৰ্ক, ডেটা সংৰক্ষণ, ৱেবছাইট, ইমেইল, আৰু এটিএমসমূহক সামৰি লৈছে আৰু শিক্ষা, বিত্ত, বিপণন আৰু মনোৰঞ্জনৰ বাবে ই অতি প্ৰয়োজনীয়।
- ইয়াৰ আৰ্কিটেকচাৰত কেইবাটাও স্তৰ অন্তৰ্ভুক্ত কৰা হৈছে: ভৌতিক (হাৰ্ডৱেৰ), নেটৰৰ্ক (আইপি আৰু টিচিপিৰ দৰে প্ৰট'কল), এপ্লিকেচন (ৱেব ব্ৰাউজাৰ, ইমেইল ক্লায়েণ্ট, অনলাইন সেৱা), আৰু সামাজিক (ব্যৱহাৰকাৰী সম্প্ৰদায়, সাংস্কৃতিক নীতি, আইনী কাঠামো)।
- কম্পিউটাৰে ডেটা প্ৰচেচ কৰে আৰু কামসমূহ দক্ষতাৰে সম্পন্ন কৰে, যাৰ বৈশিষ্ট্য হৈছে গতি, সংৰক্ষণ, সঠিকতা আৰু বহুমুখীতা।

- ৱেব প্ৰযুক্তিয়ে ইণ্টাৰনেটৰ সহায়ত যোগাযোগ সহজ কৰি তোলে, ১৯৮৯ চনত টিম বার্নার্ছ-লীয়ে সৃষ্টি কৰা ৱর্ল্ড ৱাইড ৱেব (WWW)ৰ সহায়ত তথ্য সন্ধান, অনলাইন বেংকিং, চফ্টৱেৰ ডাউনলোড, ইমেইল, ফাইল শ্বেয়াৰিং, ৰিমোট প্ৰৱেশ, আৰু অনলাইন আলোচনা আদি কার্য্যকলাপ সম্পন্ন কৰিবলৈ সহায় কৰে।

১.৮ অগ্ৰগতিৰ খতিয়ান

প্ৰশ্ন ১ ৰ উত্তৰঃ ভৌতিক স্তৰত হার্ডৱেৰ যেনে কম্পিউটাৰ, চার্ভাৰ, ৰাউটাৰ, চুইচ, আৰু কেবুল, লগতে চার্ভাৰ, সংৰক্ষণ চিস্টেম, আৰু নে'টৱর্কিং সঁজুলি হস্ট কৰা ডেটা কেন্দ্ৰসমূহ অন্তর্ভুক্ত কৰা হয়।

প্ৰশ্ন ২ ৰ উত্তৰ: নেটৱর্ক স্তৰত প্ৰটোকল আৰু প্ৰযুক্তিসমূহ অন্তর্ভুক্ত কৰা হৈছে যিয়ে আন্তঃগাঁথনিৰ মাজেৰে তথ্য প্ৰেৰণ কৰিবলৈ সক্ষম হয়।

Q3 ৰ উত্তৰ : ইণ্টাৰনেট প্ৰট'কল (IP) আৰু ট্ৰেন্সমিছন কন্ট্ৰ'ল প্ৰট'কল (TCP)।

Q4 ৰ উত্তৰ: ৱেব ব্ৰাউজাৰ হৈছে এনে চফট্ ৱেৰ এপ্লিকেচন যিয়ে ব্যৱহাৰকাৰীক ৱেবছাইটত প্ৰৱেশ আৰু ইণ্টাৰেক্ট কৰিবলৈ অনুমতি দিয়ে।

প্ৰশ্ন ৫ৰ উত্তৰ: সামাজিক স্তৰত ব্যৱহাৰকাৰী সমাজ, সাংস্কৃতিক নীতি, আৰু আইনী আৰু নিয়ন্ত্ৰণ কাঠামো অন্তর্ভুক্ত কৰা হৈছে।

Q6 ৰ উত্তৰ: ডেটা কেন্দ্ৰসমূহে ৱেবছাইট, এপ্লিকেচন, আৰু ডেটা হ'ষ্ট কৰাৰ বাবে প্ৰয়োজনীয় চার্ভাৰ, সংৰক্ষণ চিস্টেম, আৰু নেটৱর্কিং সঁজুলিসমূহৰ বাবে সুবিধাসমূহ প্ৰদান কৰে।

Q7 ৰ উত্তৰ : ইণ্টাৰনেট প্ৰটোকল (IP) হৈছে সমগ্ৰ ইণ্টাৰনেটত ডেটা পেকেটসমূহ ৰাউট কৰাৰ বাবে প্ৰাথমিক প্ৰটোকল।

Q8 ৰ উত্তৰ : বহুমুখীতা, নমনীয় হোৱাৰ মানদণ্ডই কম্পিউটাৰক বহু ক্ষেত্ৰত যেনে ঘৰুৱা ব্যৱহাৰ, শিক্ষা, ব্যৱসায়, বতৰৰ পূৰ্বাভাস, চিমুলেচন, বেংকিং, চিকিৎসা, আৰু মনোৰঞ্জন আদিত ব্যৱহাৰ কৰিবলৈ অনুমতি দিয়ে। ইহঁতৰ বহু-প্ৰচেছিং ক্ষমতাই একেলগে বিভিন্ন কাম চম্ভালিবলৈ সক্ষম কৰে, যিকোনো ক্ষেত্ৰত সহজে খাপ খাই পৰে আৰু বিভিন্ন ক্ষেত্ৰত ইয়াৰ প্ৰযোজ্যতা বৃদ্ধি কৰে।

প্রশ্ন ৯ ৰ উত্তৰ: মূল বৈশিষ্ট্যসমূহৰ ভিতৰত গতি, সংৰক্ষণ, সঠিকতা, স্বয়ংক্রিয়তা, অধ্যৱসায়, বহুমুখীতা, আৰু খৰচ-বহনক্ষমতা আদি অন্তর্ভুক্ত। এই বৈশিষ্ট্যসমূহে কম্পিউটাৰক তথ্য দ্রুতভাৱে প্রক্রিয়াকৰণ কৰিবলৈ, বৃহৎ পৰিমাণৰ তথ্য সংৰক্ষণ কৰিবলৈ, কামসমূহ সঠিকভাৱে সম্পন্ন কৰিবলৈ, পুনৰাবৃত্তিমূলক কামসমূহ স্বয়ংক্রিয় কৰিবলৈ, ভুল নোহোৱাকৈ অক্লান্তভাৱে কাম কৰিবলৈ, বিভিন্ন কামৰ সৈতে খাপ খুৱাবলৈ আৰু কার্য্যকৰী খৰচ কম কৰিবলৈ অনুমতি দিয়ে।

প্রশ্ন ১০ ৰ উত্তৰঃ i) চার্ফেচ ৱেব ii) ডার্ক ৱেব
iii) উইলিয়াম গিবছন, নিউৰ'মেন্সাৰ iv) ডিপ ৱেব



১.৯ অধিক জানিবলৈ

1) Sunit, B., & Nina, G. (2011). Cyber Security: Understanding Cybercrimes, computer forensics and Legal Perspectives. *Wiley India*.
2) Cole, E. (2011). *Network security bible*. John Wiley & Sons.
3) Maiwald, E. (2003). *Fundamentals of network security*. Dreamtech press.
4) https://wisdomplexus.com/blogs/secure-cyberspace/
5) https://www.kaspersky.com/resource-center/threats/deep-web
6) https://keerthicomputerstudymaterials.files.wordpress.com/2016/10/chapter-1-overview-of-computer.pdf



১.১০ আৰ্হি প্রশ্ন

প্রশ্ন ১. চাইবাৰস্পেচে সাধাৰণতে কি বুজায়?

প্রশ্ন ২। চাইবাৰ স্পেছে কেনেকৈ বিশ্বব্যাপী যোগাযোগ সাধন কৰে?

প্রশ্ন ৩। কম্পিউটাৰ ব্যৱস্থাৰ মূল উপাদানসমূহ কি আৰু ইহঁতে কেনেকৈ পাৰস্পৰিক ক্রিয়া কৰে?

প্রশ্ন ৪। কম্পিউটাৰৰ বৈশিষ্ট্যসমূহ কি কি?

প্রশ্ন ৫। কম্পিউটাৰৰ কার্য্যকৰী উপাদানসমূহ উল্লেখ কৰক।

প্রশ্ন ৬। ৱেব ব্রাউজাৰ আৰু ৱেব চার্ভাৰ কি? উদাহৰণ দিয়ক।

প্রশ্ন ৭। ৱর্ল্ড ৱাইড ৱেবৰ বিষয়ে টোকা লিখক।

প্রশ্ন ৮। WWW ৰ দ্বাৰা সম্পন্ন হোৱা কিছুমান সাধাৰণ কার্য্যকলাপ কি কি?

প্ৰশ্ন ৯। "চাইবাৰস্পেচ" শব্দটো কোনে উদ্ভাৱন কৰিছিল, আৰু কোনখন উপন্যাসত ইয়াৰ প্ৰয়োগ কৰিছিল?

প্ৰশ্ন ১০। ৰেব ব্ৰাউজাৰে ৰেব বিষয়বস্তুৰ ব্যাখ্যা আৰু প্ৰদৰ্শন কেনেকৈ কৰে?

প্ৰশ্ন ১১। চাইবাৰস্পেচৰ আৰ্কিটেকচাৰ স্তৰসমূহৰ বৰ্ণনা কৰক।

প্ৰশ্ন ১২। চাইবাৰস্পেচ আৰ্কিটেকচাৰৰ ভৌতিক স্তৰটো কি কি উপাদানে গঠন কৰে?

প্ৰশ্ন ১৩। চাইবাৰ স্পেচৰ সামাজিক স্তৰটোৱে কি সামৰি লয়?

প্ৰশ্ন ১৪। চাৰ্ফেচ, ডিপ আৰু ডাৰ্ক ৰেব কি?

প্ৰশ্ন ১৫। চাইবাৰস্পেচৰ আৰ্কিটেকচাৰত ভৌতিক স্তৰৰ ভূমিকা আৰু গুৰুত্বৰ বিষয়ে আলোচনা কৰক। মূল উপাদানসমূহৰ উদাহৰণ দাঙি ধৰক।

*****

অধ্যায় ২: ইণ্টাৰনেট আৰু চাইবাৰ নিৰাপত্তাৰ পৰিচয়

অধ্যায় গাঁথনি

২.১ উদ্দেশ্য
২.২ পৰিচয়
২.৩ ইণ্টাৰনেট
২.৩.১ ইণ্টাৰনেটৰ আগমন
২.৩.২ তথ্য স্থানান্তৰ আৰু শাসনৰ বাবে ইণ্টাৰনেট আন্তঃগাঁথনি
২.৩.৩ ইণ্টাৰনেট সমাজ
২.৪ সমাজত ইণ্টাৰনেটৰ গুৰুত্ব আৰু প্ৰভাৱ
২.৫ প্ৰত্যাহ্বান আৰু চিন্তা
২.৬ চাইবাৰস্পেচত নিয়মাৱলী
২.৭ চাইবাৰ নিৰাপত্তাৰ ধাৰণা
২.৭.১ চাইবাৰ নিৰাপত্তাৰ বিষয় আৰু প্ৰত্যাহ্বানসমূহ
২.৮ অধ্যায়টিৰ পৰা আমি কি কি শিকিলোঁ
২.৯ অগ্ৰগতিৰ খতিয়ান
২.১০ অধিক জানিবলৈ
২.১১ আৰ্হি প্ৰশ্ন

২.১ উদ্দেশ্য

এই অধ্যায়ৰ আলোচনাৰ পৰা আপুনি-

- ইণ্টাৰনেটৰ এক আভাস লাভ কৰিব
- ইণ্টাৰনেট আন্তঃগাঁথনিৰ বিষয়ে শিকিব
- ইণ্টাৰনেট ছ'চাইটি, ইয়াৰ মিছন আৰু কার্য্যকলাপৰ বিষয়ে জানিব পাৰিব
- চাইবাৰ নিৰাপত্তাৰ মৌলিক ধাৰণাসমূহ বিচাৰ কৰিব পাৰিব
- চাইবাৰ স্পেচত নিয়মৰ বিষয়ে আলোচনা কৰা

- চাইবাৰ নিৰাপত্তাই সন্মুখীন হোৱা প্ৰত্যাহ্বানসমূহ চিনাক্ত আৰু আলোচনা কৰিব পাৰিব।

২.২ পৰিচয়

পূৰ্বৰ অধ্যায়ত আমি কম্পিউটাৰ আৰু ৰেব প্ৰযুক্তিৰ এক আভাস দিছিলোঁ। আমি চাইবাৰ স্পেচ, অৰ্থাৎ ভাৰ্চুৱেল পৰিৱেশত আমি অতিবাহিত কৰা সময়, ৱৰ্ল্ড ৱাইড ৰেব আৰু বিভিন্ন আনুষংগিক প্ৰযুক্তিৰ সৈতে ক্ৰিয়া-কলাপৰ দিশবোৰ অধ্যয়ন কৰিলোঁ।

তথ্য প্ৰযুক্তিৰ ক্ষেত্ৰখনত তথ্য নিৰাপত্তা অতি গুৰুত্বপূৰ্ণ। এই অধ্যায়টোৱে ইণ্টাৰনেট আৰু চাইবাৰ নিৰাপত্তাৰ এক আভাস প্ৰদান কৰিব। আমি ইণ্টাৰনেটৰ উৎপত্তি আৰু তথ্য স্থানান্তৰ আৰু শাসনৰ বাবে ইয়াৰ আন্তঃগাঁথনিৰ পৰা আৰম্ভ কৰোঁ। তাৰ পিছত, আমি চাইবাৰ নিৰাপত্তাৰ সংজ্ঞা দিওঁ আৰু চাইবাৰ স্পেচত নিয়মৰ প্ৰয়োজনীয়তাৰ বিষয়ে আলোচনা কৰোঁ। এই অধ্যায়ত চাইবাৰ নিৰাপত্তাৰ ধাৰণাটোও বৰ্ণনা কৰা হ'ব, ইয়াৰ সমস্যা আৰু প্ৰত্যাহ্বানসমূহ পৰীক্ষা কৰা হ'ব।

২.৩ ইণ্টাৰনেট

বিংশ শতিকাত কম্পিউটাৰৰ আৱিষ্কাৰৰ পিছত ইণ্টাৰনেটৰ আবিৰ্ভাৱক তথ্য প্ৰযুক্তিৰ বাবে এক বৃহৎ সফলতা বুলি ধৰিব পাৰি। সহজ ভাষাত ক'বলৈ গ'লে ইণ্টাৰনেট হৈছে বিশ্বজুৰি মানুহ আৰু কম্পিউটাৰক সংযোগ কৰা নেটৱৰ্কসমূহৰ নেটৱৰ্ক। "ইণ্টাৰনেট" শব্দটো, যাক প্ৰায়ে "নেট" বুলি কোৱা হয়, এতিয়া ই অতি সাধাৰণ আৰু ই আমাৰ জীৱনৰ এক গুৰুত্বপূৰ্ণ অংশ হৈ পৰিছে। ইয়াৰ ফলতে বিশ্বব্যাপী সংযোগ সম্ভৱ হৈ উঠিছে। ইণ্টাৰনেটৰ জৰিয়তে আমি সমগ্ৰ বিশ্বতে তথ্য ভাগ-বতৰা কৰিব পাৰো, বন্ধুত্ব গঢ়িব পাৰো, সংগীত শুনিব পাৰো, চিনেমা চাব পাৰো, বিল পৰিশোধ কৰিব পাৰো, বস্তু অৰ্ডাৰ কৰিব পাৰো, আৰু বন্ধু-বান্ধৱৰ আৰু আত্মীয়ক সম্ভাষণ জনাব পাৰো, ইয়াৰ লগতে আন আন বহুতো কাম কৰিব পাৰোঁ।

এতিয়া ইণ্টাৰনেট কি সেই বিষয়ে আলোচনা কৰা যাওক। ইণ্টাৰনেট হৈছে আন্তঃসংযোগী কম্পিউটাৰ আৰু অন্যান্য ডিভাইচসমূহৰ এক বিশাল বিশ্বব্যাপী নেটৱৰ্ক যিয়ে বিশেষ প্ৰটোকল ব্যৱহাৰ কৰি তথ্য যোগাযোগ আৰু ভাগ-বতৰা কৰে। ইণ্টাৰনেটে বিশ্বজুৰি বহু লক্ষ ব্যক্তিগত, ৰাজহুৱা, শৈক্ষিক, ব্যৱসায়িক আৰু চৰকাৰী নেটৱৰ্ক সংযোগ কৰে। নেটৱৰ্কৰ এই আন্তঃসংযোগী ৰেবে সমগ্ৰ বিশ্বৰ ডিভাইচসমূহক পৰস্পৰে পৰস্পৰৰ সৈতে যোগাযোগ কৰাৰ

অনুমতি দিয়ে। ইণ্টাৰনেটৰ পৰিসৰ বহল আৰু সেয়েহে বিভিন্ন গোটৰ লোকে ইয়াক বেলেগ বেলেগ ধৰণে সংজ্ঞায়িত কৰে।

ইণ্টাৰনেটৰ কার্য্যকলাপ ভার্চুৱেল সম্পদৰ সংমিশ্রণৰ ওপৰত নির্ভৰশীল বিভিন্ন উপাদানৰ ওপৰত নির্ভৰশীল । ই তিনিটা স্তৰত বিভক্ত: **ভৌতিক (physical), পৰিবহণ (transport)** আৰু **প্রয়োগ (application)** । ভৌতিক স্তৰে বিভিন্ন সংযুক্ত ডিভাইচসমূহৰ মাজত তথ্য স্থানান্তৰৰ বাবে ব্যৱহাৰ কৰা তাঁৰযুক্ত আৰু বেতাঁৰ দূৰসংযোগ আন্তঃগাঁথনিক সামৰি লয়। পৰিবহণ স্তৰে প্রয়োজনীয় ইন্টাৰনেট প্রটোকলসমূহ অন্তর্ভুক্ত কৰে, যেনে TCP/IP, DNS, আৰু ৱর্ল্ড ৱাইড ৱেব, যি নেটৱর্কসমূহৰ মাজেৰে তথ্য বিনিময়ৰ সুবিধা কৰে। ইণ্টাৰনেটে TCP/IP (Transmission Control Protocol/Internet Protocol) নামেৰে জনাজাত প্রটোকলৰ এটা বিশেষ ব্যৱস্থাপনাৰ মাজেৰে কাম কৰে। এই প্রটোকলসমূহে তথ্য কেনেকৈ নেটৱার্কৰ যোগেদি প্রেৰণ আৰু গ্রহণ কৰা হয় সেয়া তদাৰক কৰে, ডিভাইচসমূহৰ মাজত নির্ভৰযোগ্য আৰু প্রামাণিককৃত যোগাযোগ সুনিশ্চিত কৰে। এপ্লিকেচন স্তৰত ব্যৱহাৰকাৰীসকলক বিভিন্ন সেৱা প্রদান কৰা ইণ্টাৰনেটত চলি থকা এপ্লিকেচনসমূহ সামৰি লোৱা হয়।

২.৩.১ ইণ্টাৰনেটৰ আগমন

ইণ্টাৰনেটৰ উৎপত্তি ১৯৬০ চনৰ আৰম্ভণিলৈকে বিচাৰি যাব পাৰি। এই সময়ছোৱাতে গুৰুত্বপূর্ণ প্রযুক্তিগত বিকাশ হৈছিল। এই সময়ছোৱাত আমেৰিকা যুক্তৰাষ্ট্রৰ প্রতিৰক্ষা বিভাগৰ এডভান্সড ৰিচার্ছ প্রজেক্টছ এজেন্সি (ARPA)-এ এটা শক্তিশালী, ত্রুটি সাপেক্ষেও কার্যক্ষম যোগাযোগ ব্যৱস্থা বিকাশ কৰাৰ প্রচেষ্টা কৰিছিল, যাতে সম্ভাব্য সামৰিক আক্রমণৰ পৰা বাচি থাকিব পাৰে। এই প্রচেষ্টাৰ ফলত ARPANET (এডভান্সড ৰিচার্ছ প্রজেক্টছ এজেন্সি নেটৱর্ক)ৰ সৃষ্টি হৈছিল। ই আধুনিক ইণ্টাৰনেটৰ ভেটি স্থাপন কৰা এক অগ্রগামী প্রকল্প আছিল। ARPANET-ৰ প্রাথমিক লক্ষ্য আছিল বিজ্ঞানী আৰু গৱেষকসকলৰ মাজত সহযোগিতা আৰু তথ্য বিনিময় বৃদ্ধি কৰিবৰ বাবে বিভিন্ন বিশ্ববিদ্যালয় আৰু গৱেষণা প্রতিষ্ঠানত অৱস্থিত কম্পিউটাৰসমূহৰ মাজত নির্ভৰযোগ্য যোগাযোগ সক্ষম কৰি তোলা।

TCP/IP লৈ পৰিৱর্তন

ইণ্টাৰনেটৰ বিকাশৰ ক্ষেত্রত কিছুমান গুৰুত্বপূর্ণ প্রটোকল, যেনে নেটৱর্ক কণ্ট্রে'ল প্রটোকল (NCP) আৰু পাছত ট্রান্সমিছন কণ্ট্রে'ল প্রটোকল/ইণ্টাৰনেট প্রটোকল (TCP/IP)-ৰ বিকাশে ARPANET-ৰ ক্ষমতা আৰু বঢ়াই তুলিছিল। এই প্রটোকলসমূহে ডেটা প্রেৰণক অধিক সুগম

আৰু নিৰ্ভৰযোগ্য কৰি তুলিছিল। ১৯৭০ চনত, ট্ৰান্সমিছন কণ্ট্ৰ'ল প্ৰটোকল (TCP) আৰু ইণ্টাৰনেট প্ৰটোকল (IP)-ৰ বিকাশ হৈছিল, যিয়ে পিছলৈ ইণ্টাৰনেট যোগাযোগৰ মূল ভেটি হৈ পৰিল। TCP/IP-ৰ জৰিয়তে বিভিন্ন নেটৱৰ্কসমূহে এটা আনটোৰ লগত সংযোগ স্থাপন কৰিবলৈ সক্ষম হৈছিল, আৰু ইয়াৰ ফলতেই আধুনিক ইণ্টাৰনেটৰ ভেটি স্থাপন হৈছিল।

১৯৮০ চনৰ আৰম্ভণিলৈকে, ARPANET এটা উন্নত নেটৱৰ্কলৈ ৰূপান্তৰিত হৈছিল। ই কেৱল শিক্ষানুষ্ঠান আৰু গৱেষণা প্ৰতিষ্ঠানসমূহকে নাসামৰি, নতুন নেটৱৰ্কিং প্ৰযুক্তিৰ পৰীক্ষা-নিৰীক্ষাৰ বাবে এক প্ৰধান মাধ্যম হৈ পৰিছিল। এই বিকাশে আজিৰ এই বৃহৎ, আন্তঃসংযুক্ত ইণ্টাৰনেটৰ বাট মুকলি কৰি দিলে, যিয়ে ডিজিটেল যোগাযোগ আৰু সহযোগিতাৰ সীমাহীন সম্ভাৱনাৰ পৰিচয় দিলে। ১৯৮৩ চনলৈকে, ARPANET সম্পূৰ্ণৰূপে TCP/IP-লৈ স্থানান্তৰিত হৈছিল, আৰু ইয়াৰ জৰিয়তে বিশ্বব্যাপী সংযোগৰ সূচনা হৈছিল।

১৯৮৯ চনত টিম বার্নার্ছ লী-এ ৱৰ্ল্ড ৱাইড ৱেব (WWW) আৱিষ্কাৰ কৰি ইণ্টাৰনেটক এক নতুন স্তৰলৈ লৈ গ'ল। ১৯৮০ চনৰ শেষৰ ফালে, আমেৰিকা যুক্তৰাষ্ট্ৰৰ নেচনেল চাইন্স ফাউণ্ডেশ্যন (NFS)-এ ছুপাৰ কম্পিউটাৰ কেন্দ্ৰসমূহ সংযোগ কৰিবলৈ NSFNET নামৰ এটা নেটৱৰ্ক গঠন কৰিছিল। বহুতো বিশ্ববিদ্যালয় আৰু গৱেষণা প্ৰতিষ্ঠানক এই নেটৱৰ্কৰ লগত সংযোগ কৰিবলৈ উৎসাহিত কৰা হৈছিল। NSFNET-ৰ সৃষ্টি আছিল ইণ্টাৰনেট প্ৰযুক্তিৰ প্ৰথম বৃহৎ পৰ্যায়ৰ প্ৰয়োগ, য'ত বহু স্বাধীনভাৱে পৰিচালিত নেটৱৰ্কসমূহ একেলগে কাম কৰিছিল। এই বৃহৎ বিশ্বব্যাপী নেটৱৰ্ক আৰু কম্পিউটাৰ ব্যৱস্থাসমূহে একে প্ৰটোকল অনুসৰি যোগাযোগ কৰাটোকেই আমি আজি ইণ্টাৰনেট বুলি কওঁ।

বাণিজ্যিক প্ৰতিষ্ঠানসমূহে ইণ্টাৰনেটৰ জনপ্ৰিয়তা আৰু কাৰ্যক্ষমতা লক্ষ্য কৰি নিজৰ নেটৱৰ্ক গঠন কৰিবলৈ আৰম্ভ কৰিলে। ১৯৯০ চনৰ আৰম্ভণিতে, বাণিজ্যিক নেটৱৰ্কসমূহক নিজৰ ইণ্টাৰনেট এক্সচেঞ্জ বা গেটৱেৰেৰে ইণ্টাৰনেটত ব্যৱসায় কৰিবলৈ অনুমতি দিয়া হৈছিল। ১৯৯৮ চনত, NFS-ৰ ইণ্টাৰনেটত প্ৰত্যক্ষ ভূমিকা শেষ হৈছিল, আৰু নেটৱৰ্কৰ কাৰ্য্যসমূহ বাণিজ্যিক খণ্ডলৈ স্থানান্তৰিত কৰা হৈছিল। এইদৰেই ইণ্টাৰনেটে এটা বিশ্বব্যাপী যোগাযোগ আৰু তথ্য বিনিময়ৰ মাধ্যম হিচাপে গঢ় লৈ উঠিল।

২.৩.২ ডেটা ট্ৰানচফাৰৰ বাবে ইণ্টাৰনেট আন্তঃগাঁথনি আৰু শাসন ব্যৱস্থা

ইণ্টাৰনেটৰ ডেটা ট্ৰানচফাৰ (স্থানান্তৰ) আৰু পৰিচালনাৰ ব্যৱস্থা এক জটিল আৰু নিতৌ বিকশিত ক্ষেত্ৰ। ইয়াত ব্যৱহাৰকাৰীসকলৰ চাহিদা পূৰণ কৰাৰ লগতে নিয়ম-কানুনৰ মানদণ্ড

ৰক্ষা কৰিবলৈ সদায়ে উন্নতি আৰু পৰিৱৰ্তনৰ প্ৰয়োজন হয়। ইয়াৰ ভিতৰত নানান স্তৰ আৰু উপাদান জড়িত হৈ থাকে, যেনে— ভৌতিক হাৰ্ডৱেৰ, ছফ্টৱেৰ, প্ৰটোকল, ডেটা কেন্দ্ৰ, সেৱা, আৰু পৰিচালনাৰ ব্যৱস্থা। এই সকলোবোৰ উপাদানে মিলি-জুলি কাম কৰি ইণ্টাৰনেটক এক সংগঠিত, নিৰ্ভৰযোগ্য আৰু কাৰ্যক্ষম মাধ্যম হিচাপে গঢ়ি তোলে।

১. ভৌতিক আন্তঃগাঁথনি

ভৌতিক আন্তঃগাঁথনিয়ে সকলো হাৰ্ডৱেৰ উপাদান অন্তৰ্ভুক্ত কৰে। নে'টৱৰ্কিং হাৰ্ডৱেৰে উপাদানসমূহ যেনে ৰাউটাৰসমূহ, চুইচসমূহ, ফাইবাৰ অপটিক কেবলসমূহ, সাগৰৰ তলৰ কেবলসমূহ, আৰু ৰাইৰলেছ একচেচ পইন্টসমূহ সামৰি লয়। সাগৰৰ তলৰ কেবল হৈছে সাগৰৰ তলত ৰখা বৃহৎ পৰিসৰৰ ফাইবাৰ অপটিক কেবল, যিয়ে মহাদেশসমূহক সংযোগ কৰে আৰু বিশ্বব্যাপী তথ্য স্থানান্তৰ সক্ষম কৰে। এই উপাদানসমূহ স্থানীয়, আঞ্চলিক আৰু বিশ্বব্যাপী নেটৱৰ্কসমূহৰ মাজেৰে তথ্যৰ ভৌতিক সংক্ৰমণৰ বাবে অতি গুৰুত্বপূৰ্ণ। নিৰৱচ্ছিন্ন তথ্য প্ৰবাহৰ সুবিধা কৰি, নেটৱৰ্কিং হাৰ্ডৱেৰে শক্তিশালী আৰু সংযোগ নিশ্চিত কৰে, ইণ্টাৰনেটক শক্তি প্ৰদান কৰা তথ্যৰ বিশাল বিনিময় সামৰ্থবান কৰে।

২. তথ্য স্থানান্তৰ প্ৰটোকলসমূহ

ডেটা স্থানান্তৰ প্ৰটোকলসমূহ ইণ্টাৰনেটৰ সুচল কাৰ্যকলাপৰ বাবে অতি গুৰুত্বপূৰ্ণ, যিয়ে নিৰ্ভৰযোগ্য আৰু সুৰক্ষিত যোগাযোগ সম্ভৱ কৰে। ট্ৰান্সমিছন কণ্ট্ৰ' ল প্ৰটোকল/ইণ্টাৰনেট প্ৰটোকল (TCP/IP) হৈছে ইয়াৰ ভেটি, য' ত TCP-য়ে সংযোগ স্থাপন আৰু ত্ৰুটি-পৰীক্ষাৰ জৰিয়তে নিৰ্ভৰযোগ্য ডেটা স্থানান্তৰ নিশ্চিত কৰে, আনহাতে IP-য়ে পেকেটৰ ঠিকনা আৰু ৰাউটিং নিয়ন্ত্ৰণ কৰি ডেটা সঠিক গন্তব্যস্থানলৈ পোৱাত সহায় কৰে। হাইপাৰটেক্সট ট্ৰান্সফাৰ প্ৰটোকল (HTTP) হৈছে ৱৰ্ল্ড ৱাইড ৱেবত ডেটা যোগাযোগৰ মূল প্ৰটোকল, আৰু ইয়াৰ সুৰক্ষিত সংস্কৰণ HTTPS-এ এনক্ৰিপশন যন্ত্ৰ যোগ কৰে। ফাইল ট্ৰান্সফাৰ প্ৰটোকল (FTP)-এ নেটৱৰ্কৰ জৰিয়তে ক্লায়েণ্ট আৰু ছাৰ্ভাৰৰ মাজত ফাইল স্থানান্তৰ কৰাত সহায় কৰে, যাৰ ফলত ডাঙৰ পৰিমাণৰ ডেটা স্থানান্তৰ কৰাটো সহজ হয়। আন গুৰুত্বপূৰ্ণ প্ৰটোকলসমূহৰ ভিতৰত আছে চিম্পল মেইল ট্ৰান্সফাৰ প্ৰটোকল (SMTP), যিটো ইমেইল প্ৰেৰণৰ বাবে ব্যৱহাৰ হয়, আৰু ড' মেইন নেম চিষ্টেম (DNS), যিয়ে ড' মেইন নামক IP ঠিকানালৈ ৰূপান্তৰিত কৰি ৱেব নেভিগেচন সহজ কৰে। এই প্ৰটোকলসমূহে একেলগে ইণ্টাৰনেটৰ জৰিয়তে দক্ষ, নিৰ্ভৰযোগ্য আৰু সুৰক্ষিত ডেটা স্থানান্তৰ নিশ্চিত কৰে।

৩. ডেটা চেণ্টাৰ আৰু ক্লাউড আন্তঃগাঁথনি

ডেটা কেন্দ্ৰসমূহ হৈছে এক গুৰুত্বপূৰ্ণ ব্যৱস্থা, যিয়ে চাৰ্ভাৰ, সংৰক্ষণ যন্ত্ৰ, আৰু নেটৱৰ্কিং সজুলিসমূহ অন্তৰ্ভুক্ত থাকে। এইবোৰে ইণ্টাৰনেট ব্যৱস্থাপনাৰ মূল ভেটি গঠন কৰে। ডেটা

কেন্দ্রসমূহে ডেটা প্রচেছিং আৰু সংৰক্ষণৰ বাবে প্রয়োজনীয় ভৌতিক স্থান আৰু শক্তিৰ যোগান ধৰে। ক্লাউড সেৱা প্রদানকাৰী যেনে এমাজন ৰেব ছার্ভিছেচ (AWS), গুগল ক্লাউড, আৰু মাইক্রচফ্ট এজুৰে ইণ্টাৰনেটৰ জৰিয়তে অনলাইন সম্পদ আৰু সংৰক্ষণ সেৱা আগবঢ়ায়। এই সেৱাবোৰে ব্যৱসায় আৰু ব্যক্তিগত প্রয়োজনীয়তাসমূহক সহজ আৰু কার্যক্ষমভাৱে পূৰণ কৰাত গুৰুত্বপূর্ণ ভূমিকা পালন কৰে।

৪. ডেটা গভার্নেন্স

ডেটা গভার্নেন্সএ নিয়ন্ত্রণ কাঠামো, তথ্য ব্যৱস্থাপনা নীতি, আৰু প্রামাণিক আৰু উত্তম পদ্ধতিসমূহ সামৰি লয়। তথ্য শাসনে, বিশেষকৈ নিয়ন্ত্রণ কাঠামোৰ ভিতৰত, সংস্থাসমূহে তথ্য কেনেকৈ পৰিচালনা আৰু নিৰাপত্তা কৰে তাক নিয়ন্ত্রণ কৰিবলৈ নিয়ম আৰু মানদণ্ড স্থাপন কৰাত মনোনিৰেশ কৰে। এই ক্ষেত্রত অন্যতম বিশিষ্ট নিয়ম হৈছে ইউৰোপীয় সংঘই (ইউৰোপীয় সংঘ) কার্যকৰী কৰা *সাধাৰণ তথ্য নিৰাপত্তা নিয়ম (GDPR)*। জিডিপিআৰ হৈছে ইউৰোপীয় ইউনিয়নৰ ভিতৰৰ ব্যক্তিসকলৰ ব্যক্তিগত তথ্য সুৰক্ষিত কৰা আৰু ইয়াৰ প্রক্রিয়াকৰণ নিয়ন্ত্রণ কৰা এক বিস্তৃত আইন। ই তথ্য সংগ্রহ, সংৰক্ষণ আৰু ব্যৱহাৰৰ বাবে কঠোৰ নির্দেশনা নির্ধাৰণ কৰে, স্বচ্ছতা, জবাবদিহিতা, আৰু ব্যক্তিসকলৰ ব্যক্তিগত তথ্যৰ ওপৰত অধিকাৰৰ ওপৰত গুৰুত্ব আৰোপ কৰে। জিডিপিআৰৰ উপৰিও আন এটা উল্লেখযোগ্য নিয়ন্ত্রণ কাঠামো হৈছে *কেলিফর্ণিয়া কনজিউমাৰ প্রাইভেচি এক্ট* (চিচিপিএ), যিটো আমেৰিকাত ৰাজ্যিক পর্যায়ত প্রণয়ন কৰা হৈছিল। চিচিপিএই কেলিফর্ণিয়াৰ বাসিন্দাসকলৰ বাবে গোপনীয়তা অধিকাৰ আৰু গ্রাহকৰ নিৰাপত্তা বৃদ্ধি কৰে, তেওঁলোকক ব্যৱসায়ৰ দ্বাৰা ৰখা তেওঁলোকৰ ব্যক্তিগত তথ্যৰ ওপৰত অধিক নিয়ন্ত্রণ প্রদান কৰে।

ডেটা ব্যৱস্থাপনা নীতিসমূহে ডেটা গোপনীয়তাৰ ওপৰত গুৰুত্ব আৰোপ কৰে, নিশ্চিত কৰে যে ব্যক্তিগত ডেটা গোপনীয়তা আইনসমূহ মানি চলি সংগ্রহ, সংৰক্ষণ আৰু প্রক্রিয়াকৰণ কৰা হয়। এই নীতিসমূহে অকর্তৃত্বশীল প্ররেশ, ভংগ, আৰু অন্যান্য চাইবাৰ ভাবুকিৰ পৰা তথ্যক সুৰক্ষিত কৰাৰ ব্যৱস্থা কৰি তথ্য নিৰাপত্তাৰ ওপৰতো গুৰুত্ব আৰোপ কৰে, আৰু ইয়াৰ সমগ্র জীৱনচক্রত তথ্যৰ সঠিকতা আৰু সামঞ্জস্যতা বজাই ৰাখে।

ফলপ্রসূ তথ্য শাসনৰ বাবে মানদণ্ড আৰু উত্তম পদ্ধতিসমূহ অতি প্রয়োজনীয়। নেচনেল *ইনষ্টিটিউট অৱ ষ্টেণ্ডার্ডছ এণ্ড টেকন'লজি* (এনআইএছটি) চাইবাৰ নিৰাপত্তা কাঠামোৱে চাইবাৰ নিৰাপত্তাৰ বিপদসমূহ পৰিচালনাৰ বাবে নির্দেশনা প্রদান কৰে, যিয়ে সংস্থাসমূহক তেওঁলোকৰ তথ্য নিৰাপত্তা ব্যৱস্থাসমূহ শক্তিশালী কৰাত সহায় কৰে। এই উপাদানসমূহে একেলগে আজিৰ ডিজিটেল পৰিৱেশত তথ্য পৰিচালনা আৰু নিৰাপত্তাৰ এক ব্যাপক পদ্ধতিৰ সৃষ্টি কৰে।

অগ্রগত প্রযুক্তিৰ ব্যৱহাৰ আৰু শ্রেষ্ঠ অনুশীলনসমূহ মানি চলি সংস্থাই দক্ষ, সুৰক্ষিত আৰু নিয়মমতে ডেটা পৰিচালনা আৰু স্থানান্তৰ নিশ্চিত কৰিব পাৰে।

২.৩.৩ ইণ্টাৰনেট সংস্থা

১৯৯০ চনৰ শেষৰ ফালে ৱর্ল্ড ৱাইড ৱেবৰ আৱির্ভাৱৰ বাবে বিশ্বজুৰি দিনক দিনে ইণ্টাৰনেট বৃদ্ধি পাইছে। কেৱল ইণ্টাৰনেটৰ প্রসাৰেই নহয়, ইণ্টাৰনেটৰ প্রসাৰণৰ বাবে মোবাইল আৰু বেতাঁৰ নেটৱর্কৰ গুৰুত্বও আছে। মাল্টিমিডিয়া এপ্লিকেচন যেনে ভইচ অভাৰ আই পি, ভিডিঅ' অভাৰ আই পি, টেলিভিছন অভাৰ আই পি আদিৰ শেহতীয়া উন্নয়নে ব্যৱহাৰকাৰীৰ সংখ্যা আৰু প্রতিজন ব্যৱহাৰকাৰীয়ে নেটৱর্কত কটোৱা সময়ৰ পৰিমাণ বহু পৰিমাণে বৃদ্ধি কৰিছে। ইমান বিশাল নেটৱর্ক নিৰীক্ষণৰ বাবে এনে এটা আন্তঃৰাষ্ট্রীয় সংস্থাৰ প্রয়োজনীয়তা আছে যিয়ে নেটৱর্কত যোগদান আৰু ব্যৱহাৰ কৰিবলৈ নিয়ম আৰু বিধি, প্রট'কল ফ্রেমৱর্ক কৰিব পাৰে। ১৯৯২ চনত এনেবোৰ বিষয়ৰ যত্ন ল'বলৈ "The Internet Society" নামেৰে জনাজাত এটা আন্তঃৰাষ্ট্রীয় সংস্থা গঠন কৰা হয়।

ইণ্টাৰনেট ছ'চাইটি হৈছে এক বিশ্বব্যাপী অনাব্যৱসায়ীক সংস্থা যিয়ে মানুহক তথ্য বিনিময় কৰাৰ সময়ত ইণ্টাৰনেট সুৰক্ষিত কৰি ৰাখিবলৈ সুবিধা কৰি দিয়ে। সংস্থাটোৰ লক্ষ্য হৈছে ইণ্টাৰনেটক মুকলি, বিশ্বব্যাপী সংযুক্ত, সুৰক্ষিত আৰু বিশ্বাসযোগ্য কৰি ৰখা যাতে বিশ্বৰ সকলো কোণৰ পৰা অহা জনসাধাৰণে সহযোগিতা কৰিব পাৰে। মিছন আৰু সংস্থাটোৰ বিভিন্ন কার্য্যকলাপ অফিচিয়েল ৱেবছাইট https://www.internetsociety.org/ ত চব পাৰি।

সংস্থাটোৰ অফিচিয়েল ৱেবছাইট অনুসৰি ইণ্টাৰনেট ছ'চাইটিৰ মিছন আৰু ছ'চাইটিৰ কাম-কাজ তলত দিয়া ধৰণৰ।

দৃষ্টি	ইণ্টাৰনেট সকলোৰে বাবে
উদ্দেশ্য	ইণ্টাৰনেট ছ'চাইটিয়ে ইণ্টাৰনেটক বিশ্বব্যাপী কাৰিকৰী আন্তঃগাঁথনি, মানুহৰ জীৱন সমৃদ্ধ কৰাৰ সম্পদ, সমাজত ভালৰ শক্তি হিচাপে গঢ়ি তোলাত সমর্থন আৰু প্রসাৰ কৰে।

মূল কার্য্যকলাপসমূহ	ইণ্টাৰনেট ছ'চাইটি: • প্রামাণিক, প্রট'কল, প্রশাসন, আৰু ইণ্টাৰনেটৰ কাৰিকৰী আন্তঃগাঁথনিৰ মুক্ত বিকাশৰ সুবিধা প্রদান কৰে। • বিশেষকৈ উন্নয়নশীল দেশসমূহত শিক্ষাৰ ক্ষেত্রখনক সহায় কৰে। • পেছাদাৰী বিকাশক প্রসাৰিত কৰে আৰু ইণ্টাৰনেটৰ বিৱর্তনৰ বাবে গুৰুত্বপূর্ণ ক্ষেত্রসমূহত অংশগ্রহণ আৰু নেতৃত্বক লাভান্বিত কৰিবলৈ সম্প্রদায় গঢ়ি তোলে। • ইণ্টাৰনেটৰ বিষয়ে নির্ভৰযোগ্য তথ্য প্রদান কৰে। • ইণ্টাৰনেটৰ বিৱর্তন, বিকাশ আৰু কাৰিকৰী, বাণিজ্যিক, সমাজ, আৰু অন্যান্য প্রসংগত ব্যৱহাৰক প্রভাৱিত কৰা বিষয়সমূহৰ আলোচনাৰ বাবে মঞ্চ প্রদান কৰে। • আন্তঃৰাষ্ট্রীয় সহযোগিতা, সম্প্রদায়, স্ব-নিয়ন্ত্রিত কাম-কাজৰ সংস্কৃতিৰ বাবে এক পৰিৱেশ গঢ়ি তোলে। • সমগ্র বিশ্বৰ সকলো লোকক উপকৃত কৰিব পৰাকৈ ইণ্টাৰনেটক ইতিবাচক আহিলা হিচাপে প্রচাৰৰ বাবে সহযোগিতামূলক প্রচেষ্টাৰ বাবে কেন্দ্রবিন্দু হিচাপে কাম কৰে। • মানৱীয়, শৈক্ষিক, সমাজ, আৰু অন্যান্য প্রসংগত কৌশলগত পদক্ষেপ আৰু আউটৰিচ প্রচেষ্টাৰ বাবে পৰিচালনা আৰু সমন্বয় প্রদান কৰে।

উৎস: https://www.internetsociety.org/

২.৪ সমাজত ইণ্টাৰনেটৰ গুৰুত্ব আৰু প্রভাৱ

ইণ্টাৰনেটে সমাজখনক কেইবাটাও দিশত গভীৰভাৱে প্রভাৱিত কৰিছে। সেইবোৰ হৈছে-

যোগাযোগ আৰু সংযোগ: ই যোগাযোগত বৈপ্লৱিক পৰিৱর্তন আনিছে, ইমেইল, ছ'চিয়েল মিডিয়া, আৰু তাৎক্ষণিক বার্তা প্রেৰণৰ দৰে প্লেটফর্মৰ জৰিয়তে তৎক্ষণাত আৰু বিশ্বব্যাপী পাৰস্পৰিক ক্রিয়া-কলাপ সহজ কৰি তুলিছে। ভিডিঅ' কনফাৰেন্সিং সঁজুলিসমূহে ভৌগোলিক ব্যৱধানসমূহ দূৰ কৰিছে, যাৰ ফলত একে সমতে সময়ৰ মুখামুখি পাৰস্পৰিক ক্রিয়াৰ সুবিধা হৈছে।

তথ্যৰ প্রৱেশ: ইণ্টাৰনেটে চার্চ ইঞ্জিন, অনলাইন লাইব্রেৰী, আৰু ডেটাবেছৰ সহায়ত জ্ঞানৰ প্রসাৰ সহজ কৰি তুলিছে। ই ব্যক্তিসকলক ইণ্টাৰনেট সংযোগৰ সৈতে যিকোনো ঠাইৰ পৰা সহজতেই বিভিন্ন বিষয়ৰ বিষয়ে জানিবলৈ সহায় কৰে।

ই-কমার্চ : অর্থনৈতিক বিকাশ যথেষ্ট বঢ়াই ইণ্টাৰনেটে নতুন উদ্যোগ আৰু চাকৰিৰ সুযোগ দিছে। আমাজন, আৰু ইবেৰ দৰে অনলাইন শ্বপিং প্লেটফর্মে সামগ্রীৰ বিশ্বব্যাপী প্ৰৱেশৰ সুবিধা প্রদান কৰি খুচুৰা বিক্রী সহজ কৰি তুলিছে। ডিজিটেল পেমেণ্ট আৰু অনলাইন বেংকিঙে বিত্তীয় লেনদেন অধিক কার্যক্ষম আৰু সুবিধাজনক কৰি তুলিছে।

শিক্ষা আৰু ই-লার্নিং : শিক্ষাৰ ক্ষেত্রত ইণ্টাৰনেটে অনলাইন পাঠ্যক্রম, ভার্চুৱেল শ্রেণীকোঠা, আৰু বিশ্বজুৰি সুলভ শিক্ষামূলক সম্পদৰ দ্বাৰা এক বিপ্লৱ কঢ়িয়াই আনিছে। Coursera, Khan Academy, আৰু edX আদি প্লেটফর্মে বিশ্বজুৰি শিক্ষার্থীসকলক প্রতিষ্ঠিত প্রতিষ্ঠানৰ পৰা পাঠ্যক্রম প্রদান কৰে।

মনোৰঞ্জন: অনলাইন গেমিং, ছ'চিয়েল মিডিয়া, আৰু ডিজিটেল কন্টেন্ট সৃষ্টিয়ে মনোৰঞ্জনৰ নতুন ৰূপ আৰু আত্মপ্রকাশৰ পথ মুকলি কৰিছে। নেটফ্লিক্স, ইউটিউব, আৰু স্পটিফাইৰ দৰে ষ্ট্রীমিং সেৱাই মানুহে কেনেকৈ মিডিয়া ব্যৱহাৰ কৰে তাত এক বৈপ্লৱিক পৰিৱর্তন আনিছে, তেওঁলোকৰ হাতৰ মুঠিতে ভিন্ন সমাহাৰ দাঙি ধৰিছে।

সামাজিক প্রভাৱঃ ইণ্টাৰনেটে সমূহীয়া মতা গঠন, ঐক্য বৃদ্ধি কৰি ছ'চিয়েল মিডিয়া প্লেটফর্মৰ জৰিয়তে মতামত আৰু প্রচাৰৰ সুবিধা কৰি ৰাজহুৱা বিচাৰ-বিবেচনা, সামাজিক আন্দোলনক সক্রিয় কৰিছে। ই বিশ্বব্যাপী সামাজিক পৰিৱর্তন আৰু সামজুৱা সংযোগৰ বাবে এক শক্তিশালী আহিলাত পৰিণত হৈছে।

ইণ্টাৰনেটৰ বিকাশিত নতুন ৰূপ- ইণ্টাৰনেট অৱ থিংছ (IoT), ৫জি প্রযুক্তি, আৰু কৃত্রিম বুদ্ধিমত্তা (AI)ৰ দৰে নব্য প্রযুক্তিয়ে আমাৰ জীৱনক আৰু অধিক ৰূপান্তৰিত কৰিবলৈ সাজু হৈছে।

২.৫ প্রত্যাহ্বান আৰু উদ্বেগ

ইণ্টাৰনেটৰ সুবিধা যিদৰে আছে, তেনেকৈ প্রত্যাহ্বানো আছে। ইয়াৰে কিছুমান হ'ল-

গোপনীয়তা: এটা চিন্তাকৰিবলগীয়া বিষয় হৈছে গোপনীয়তা। কোম্পানী আৰু চৰকাৰে সংগ্রহ কৰা ব্যক্তিগত তথ্য আৰু ইয়াৰ সম্ভাব্য অপব্যৱহাৰে গুৰুত্বপূর্ণ নৈতিক আৰু আইনী সমস্যাৰ সৃষ্টি কৰে।

নিৰাপত্তা : চাইবাৰ নিৰাপত্তা এটা জটিল বিষয় হৈয়ে আছে- হেকিং, মেলৱেৰ, আৰু ফিছিঙৰ দৰে ভাবুকিয়ে ব্যক্তি আৰু সংস্থাৰ নিৰাপত্তাৰ প্রতি ভাবুকি কঢ়িয়াই আনিছে।

ডিজিটেল বিভাজন: "ডিজিটেল বিভাজন" হৈছে আধুনিক তথ্য আৰু যোগাযোগ প্রযুক্তি (আইচিটি) সম্পদ, যেনে ইণ্টাৰনেট আৰু ডিজিটেল ডিভাইচৰ সুবিধা থকা ব্যক্তি আৰু নথকা

ব্যক্তি, তেওঁলোকৰ মাজৰ ব্যৱধান। এই বৈষম্যৰ ফলত পাবলগীয়া সুবিধাবোৰৰ পৰা বঞ্চিত হ'ব লগা হয়। ডিজিটেল উন্নতিৰ পৰা সকলোৱে সমানে লাভৱান হ'বও নোৱাৰে।

ভুল তথ্যঃ ভুল তথ্য আৰু ভুৱা বাতৰিৰ প্ৰসাৰৰ ফলত সমাজত ভয়াৱহ পৰিস্থিতি হ'ব পাৰে। এই প্ৰত্যাহ্বানসমূহৰ সৈতে মোকাবিলা কৰিবলৈ নীতি, শিক্ষা, আৰু প্ৰযুক্তিগত উদ্ভাৱনৰ ক্ষেত্ৰত নিৰাপদ, বিশ্বাসযোগ্য অনলাইন পৰিৱেশৰ প্ৰসাৰৰ বাবে প্ৰচেষ্টাৰ প্ৰয়োজন।

২.৬ চাইবাৰস্পেচত নিয়ন্ত্ৰণ

চাইবাৰস্পেচ, যিয়ে সমগ্ৰ বিশ্বজুৰি বিস্তৃত হৈ আছে, কোনো একক সংস্থা, ব্যক্তি বা চৰকাৰৰ মালিকীস্বত্ব বা নিয়ন্ত্ৰণ নথকাৰ বাবে কোনো নিৰ্দিষ্ট চৌহদৰ ভিতৰত কাম নকৰে। ফলত, চাইবাৰস্পেচ নিয়ন্ত্ৰণ কৰাৰ প্ৰত্যাহ্বান ক্ৰমে বৃদ্ধি পাই আহিছে।

চাইবাৰস্পেচত নিয়মাৱলী গুৰুত্বপূৰ্ণ, কিয়নো ইয়াৰ জৰিয়তে ব্যৱহাৰকাৰী আৰু সংস্থাসমূহক চাইবাৰ বিপদৰ পৰা ৰক্ষা কৰা হয়। এই নিয়মাৱলী বিভিন্ন চৰকাৰী আৰু আন্তঃৰাষ্ট্ৰীয় সংস্থাই ব্যক্তিগত ডেটাৰ সু�ৰক্ষা, গোপনীয়তা ৰক্ষা আৰু ডিজিটেল পৰিৱেশ সুৰক্ষিত কৰিবলৈ প্ৰণয়ন কৰে। চৰকাৰ আৰু আন্তঃৰাষ্ট্ৰীয় সংস্থাই একেলগে কাম কৰি বিকশিত হৈ থকা চাইবাৰ বিপদসমূহৰ সৈতে মোকাবিলা কৰিব পৰা নীতি প্ৰস্তুত কৰে।

প্ৰতিখন দেশৰ ভৌতিক ব্যৱসায়িক লেনদেন নিয়ন্ত্ৰণ কৰা আইনসমূহ অনলাইন লেনদেন নিয়ন্ত্ৰণ কৰা আইনৰ পৰা বহু পৰিমাণে পৃথক। প্ৰযুক্তিৰ অগ্ৰগতিৰ লগে লগে চাইবাৰস্পেচত মানুহৰ আচৰণ নিয়ন্ত্ৰণ কৰাটো এক গুৰুত্বপূৰ্ণ প্ৰয়োজনীয়তালৈ ৰূপান্তৰিত হৈছে। চাইবাৰ আইনসমূহ দায়িত্বশীল প্ৰযুক্তিৰ ব্যৱহাৰ উৎসাহিত কৰিবলৈ প্ৰণয়ন কৰা হৈছে। চাইবাৰস্পেচত ব্যক্তিৰ অধিকাৰৰ ওপৰত যিকোনো প্ৰকাৰৰ উলংঘাই চাইবাৰ উলংঘন বুলি গণ্য কৰা হয় আৰু এই আইনৰ অধীনত ইয়াৰ বাবে শাস্তিৰ ব্যৱস্থা কৰা হয়।

নিয়ন্ত্ৰণ পৰিকাঠামো

চাইবাৰ বিপদসমূহ সঘনাই সীমান্ত অতিক্ৰম কৰে, যাৰ বাবে আন্তঃৰাষ্ট্ৰীয় সহযোগিতা অতি গুৰুত্বপূৰ্ণ হৈ পৰে। উদাহৰণস্বৰূপে,

- সাধাৰণ তথ্য নিৰাপত্তা নিয়ন্ত্ৰণ (GDPR) হৈছে বিশ্বজুৰি আটাইতকৈ কঠোৰ গোপনীয়তা আৰু নিৰাপত্তা আইন। এয়া যদিও ইউৰোপীয় সংঘই (EU) সৃষ্টি কৰিছে, ইউৰোপীয় সংঘৰ লোকসকলক লক্ষ্য কৰি বা তথ্য সংগ্ৰহ কৰা বিশ্বৰ যিকোনো সংস্থাৰ ক্ষেত্ৰত ই প্ৰযোজ্য।

- নেচনেল ইনষ্টিটিউট অৱ ষ্টেণ্ডার্ডছ এণ্ড টেকন'লজি (এনআইএছটি) চাইবাৰ নিৰাপত্তা কাঠামোৰে চাইবাৰ নিৰাপত্তাৰ বিপদ ব্যৱস্থাপনা উন্নত কৰাৰ বাবে নির্দেশনা প্রদান কৰে।
- ভাৰতত জটিল তথ্যৰ আন্তঃগাঁথনি সুৰক্ষিত, চাইবাৰ নিৰাপত্তা বৃদ্ধি, আৰু ব্যক্তিগত তথ্য সুৰক্ষিত কৰাৰ বাবে কেইবাটাও নিয়ন্ত্রণ ব্যৱস্থা আছে। তথ্য প্রযুক্তি আইন, ২০০০ৰ সংশোধনে চাইবাৰ নিৰাপত্তাৰ মূল বিধান প্রৱর্তন কৰে।

চাইবাৰ স্পেচ আমাৰ জীৱনৰ অধিক অবিচ্ছেদ্য অংগ হৈ পৰাৰ লগে লগে ব্যক্তি, ব্যৱসায় আৰু সমাজক চাইবাৰ ভাবুকি আৰু অপব্যৱহাৰৰ পৰা ৰক্ষা কৰিবলৈ নিয়ন্ত্রণৰ প্রয়োজনীয়তা ক্রমান্বয়ে জটিল হৈ পৰে। চাইবাৰ স্পেচ নিয়ন্ত্রণ কৰাটো প্রয়োজনীয়, কাৰণ-

- ক্রমাৎ বৃদ্ধি পোৱা চাইবাৰ আক্রমণ
- ডিজিটেল ব্যৱহাৰ বৃদ্ধি
- ব্যৱসায়ৰ ওপৰত প্রভাৱ
- ব্যক্তিৰ ওপৰত প্রভাৱ

এই আক্রমণৰ বিষয়ে অতি চমুকৈ আলোচনা কৰা যাওক।

১. ক্রমাৎ বৃদ্ধি পোৱা চাইবাৰ আক্রমণ: আমি দেখিছোঁ যে, দিনে দিনে চাইইবাৰ আক্রমণ আৰু চাইবাৰ অপৰাধ বাঢ়িব ধৰিছে। ভাৰততো আন বহু দেশৰ দৰে চাইবাৰ অপৰাধ দ্রুতগতিত বৃদ্ধি পাইছে। দৈনন্দিন জীৱনৰ অবিচ্ছেদ্য অংগ হৈ পৰাৰ লগে লগে মানুহে বজাৰ কৰা, গেমিং, অনলাইন শিক্ষা, ছ'চিয়েল নেটৱর্কিঙৰ দৰে কাম-কাজৰ বাবে ইণ্টাৰনেটৰ ওপৰত ক্রমান্বয়ে নির্ভৰশীল হৈ পৰিছে। চাইবাৰ অপৰাধীয়ে ইণ্টাৰনেটে প্রদান কৰা গতি, সুবিধা আৰু নাম উপস্থিতহীন অপৰাধ যেনে ফিছিং, ক্রেডিট কার্ড জালিয়াতি, বেংক ডকাইতি, ভাইৰাছ বিতৰণ আদি সংঘটিত কৰে।

ভাৰতৰ ৰাষ্ট্রীয় অপৰাধ অভিলেখ ব্যুৰোৱে (NCRB) অপৰাধ আৰু অপৰাধমূলক ন্যায়ৰ সৈতে জড়িত তথ্য সংগ্রহ, বিশ্লেষণ আৰু প্রচাৰৰ ক্ষেত্রত গুৰুত্বপূর্ণ ভূমিকা পালন কৰে। এন চি আৰ বিয়ে সমগ্র দেশতে ৰিপ'র্ট কৰা বিভিন্ন ধৰণৰ অপৰাধৰ তথ্য সংগ্রহ কৰে। ইয়াৰ ভিতৰত চুৰি, হত্যা, আক্রমণৰ দৰে গতানুগতিক অপৰাধৰ লগতে চাইবাৰ অপৰাধ আৰু অর্থনৈতিক অপৰাধৰ দৰে আধুনিক অপৰাধ দুয়োটাকে অন্তর্ভুক্ত কৰা হৈছে। ব্যুৰোৱে কেন্দ্রীয় ৰাষ্ট্রীয় অপৰাধ তথ্যকোষ ৰক্ষণাবেক্ষণ কৰে, যিয়ে অপৰাধ সম্পর্কীয় তথ্যৰ ভঁৰাল হিচাপে কাম কৰে। শেহতীয়া বছৰবোৰত এনচিআৰবিয়ে চাইবাৰ অপৰাধ নিৰীক্ষণ আৰু প্রতিবেদনক সামৰি লোৱাৰ দিশত নিজৰ মনোযোগ সম্প্রসাৰিত কৰিছে। ই ডেটা ভংগ, অনলাইন জালিয়াতি,

চাইবাৰ-আক্ৰমণ, আৰু অন্যান্য ডিজিটেল অপৰাধকে ধৰি চাইবাৰ অপৰাধৰ কাণ্ডসমূহ অনুসৰণ আৰু প্ৰতিবেদন কৰে।

২. ডিজিটেল ব্যৱহাৰ বৃদ্ধি: বিত্তীয় সেৱা, বেংকিং, শক্তি, উৎপাদন, আৰু পাৰমাণৱিক শক্তি কেন্দ্ৰৰ দৰে বহু খণ্ড দ্ৰুতগতিত ডিজিটেল হৈ পৰিছে। মানুহে এতিয়া কাম, শিক্ষা, মনোৰঞ্জন, ব্যৱসায়ৰ বাবে অনলাইনত বহু সময় কটায়। ইণ্টাৰনেটে বিশ্বজুৰি মানুহক সংযোগ কৰে, যাৰ ফলত প্ৰতিদিনে লাখ লাখ লোকে তথ্য ভাগ-বতৰা আৰু সেইবোৰত প্ৰৱেশ কৰিব পাৰে। কিন্তু ডিজিটেল ডেটা প্ৰায়ে বিভিন্ন ঠাইত সংৰক্ষণ কৰা হয়, আৰু ব্যৱহাৰকাৰীয়ে হয়তো নাজানে যে তেওঁলোকৰ তথ্য ক'ত ৰখা হয় বা কোনবোৰ আইন প্ৰযোজ্য। এই ব্যক্তি উপস্থিতিহীন সুবিধাই মানুহক নিজৰ পৰিচয় প্ৰকাশ নকৰাকৈ অনলাইনত কামবোৰ কৰিবলৈ দিয়ে, যাৰ ফলত অপব্যৱহাৰ হ'ব পাৰে আৰু ইয়াৰ বাবে তদাৰকী আৰু নিয়ন্ত্ৰণৰ প্ৰয়োজন হয়।

৩. ব্যৱসায়ৰ ওপৰত প্ৰভাৱ: ইণ্টাৰনেটৰ দ্ৰুত আৰু দক্ষ ডেটা প্ৰেৰণে বিশ্বব্যাপী বাণিজ্যক সলনি কৰিছে। ই কাগজবিহীন লেনদেন সম্ভৱ কৰি তুলিছে আৰু কাৰ্যক্ষমতা উন্নত কৰিছে। অনলাইন বেংকিং আৰু ডিজিটেল পেমেণ্ট প্লেটফৰ্ম যেনে Google Pay আৰু PhonePe-য়ে বিত্তীয় লেনদেন অতি সহজ আৰু সাধাৰণ কৰি তুলিছে।

৪) ব্যক্তিৰ ওপৰত প্ৰভাৱ: ইণ্টাৰনেটে ব্যক্তিৰ ফটো, সংগীত, ভিডিঅ' আৰু ই-বুকৰ দৰে ডিজিটেল সামগ্ৰী বিতৰণ আৰু গ্ৰহণ কৰিবলৈ সুবিধা দিয়ে। শিশুসকলে স্মাৰ্টফোন আৰু লেপটপৰ জৰিয়তে গেম আৰু ভিডিঅ' চাবলৈ দক্ষ হৈ পৰিছে। ডিজিটেল জগতে অন্তৰ্মুখী, লাজকুৰীয়া ব্যক্তিসকলক নিজকে প্ৰকাশ কৰাৰ এক সুযোগ দিয়ে, কিন্তু ইয়াৰ লগতে ইয়াৰ কিছু বিপদো আছে। চ'চিয়েল মিডিয়াত শ্বেয়াৰ কৰা ব্যক্তিগত তথ্য অপব্যৱহাৰ হ'ব পাৰে, যাৰ ফলত গুৰুতৰ সমস্যাৰ সৃষ্টি হ'ব পাৰে। শিশু আৰু বয়স্ক লোকসকল, যিসকলে অনলাইন বিপদবোৰ চিনাক্ত কৰিব নোৱাৰে, তেওঁলোক বিশেষকৈ বেছি বিপদত পৰাৰ অৱকাশ থাকে। গতিকে, অনলাইনত ব্যক্তিগত তথ্য আৰু বিত্তীয় একাউণ্ট সুৰক্ষিত কৰাটো ভৌতিক সম্পদ ৰক্ষা কৰাৰ দৰেই গুৰুত্বপূৰ্ণ।

সকলো ব্যৱহাৰকাৰীৰ বাবে এক সুৰক্ষিত ডিজিটেল পৰিৱেশ গঢ়ি তুলিবলৈ সজাগতা, শিক্ষা আৰু কঠোৰ আইন অতি প্ৰয়োজনীয়।

২.৭ চাইবাৰ নিৰাপত্তাৰ ধাৰণা

ইণ্টাৰনেটৰ যোগেদি যোগাযোগৰ বাবে বিভিন্ন প্ৰকাৰৰ ছফ্টৱেৰ, হার্ডৱেৰ, যোগাযোগ চেনেল আৰু মাধ্যমসমূহ আন্তঃসংযোগ কৰি তথ্য বিনিময় আৰু বিতৰণ সহজ কৰা হয়। এই

আন্তঃসংযুক্ত ব্যৱস্থাসমূহত অনুমোদনহীন প্ৰৱেশৰ পৰা তথ্য সু�ৰক্ষিত কৰিবলৈ সু�ৰক্ষা ব্যৱস্থা গ্ৰহণ কৰাটো অতি গুৰুত্বপূৰ্ণ। চাইবাৰ সু�ৰক্ষা হৈছে এই ব্যৱস্থাসমূহক চাইবাৰ বিপদৰ পৰা ৰক্ষা কৰাৰ এক প্ৰক্ৰিয়া।

আধুনিক প্ৰযুক্তিয়ে মানুহৰ জীৱনশৈলী সলনি কৰি পেলাইছে, ফলত চাইবাৰস্পেচত বিত্তীয় লেনদেন আৰু ক্ৰয়-বিক্ৰয়ৰ বাবে প্ৰযুক্তিৰ ব্যৱহাৰ বৃদ্ধি পাইছে। চচিয়েল মিডিয়াৰ ব্যাপক বিস্তাৰৰ লগে লগে অনলাইন অপৰাধ বা চাইবাৰ অপৰাধো বৃদ্ধি পাইছে। আমি যিদৰে বাহ্যিক জগতত সাৱধানতা অৱলম্বন কৰোঁ–যেনে ঘৰ, গাড়ী, আৰু অফিচ লক কৰা, আৰু মূল্যৱান কাগজ-পত্ৰ বেংকৰ চেফটি ডিপজিট বক্সত ৰখা–ঠিক তেনেদৰে ডিজিটেল জগততো আমি নিজকে সুৰক্ষিত কৰিব লাগে। ইমেইল আৰু ৱৰ্ল্ড ৱাইড ৱেবৰ জৰিয়তে কাম আৰু সামাজিক জীৱনত ইণ্টাৰনেটৰ ওপৰত নিৰ্ভৰ কৰি থকা সত্ত্বেও, আমি প্ৰায়ে অনলাইন সুৰক্ষাক উপেক্ষা কৰোঁ। ভাৰ্চুৱেল জগতখন বাস্তৱ জগততকৈ সুৰক্ষিত বা নিৰাপদ বুলি ভবা এক ভুল ধাৰণা। নতুন প্ৰযুক্তিৰ যুগত অনলাইনত তথ্য শ্বেয়াৰ কৰোঁতে আমাৰ ডেটা আৰু তথ্য সুৰক্ষিত কৰাটো অগ্ৰাধিকাৰ হিচাপে গ্ৰহণ কৰিব লাগে।

তথ্য সুৰক্ষা আজিৰ দিনত এক ডাঙৰ প্ৰত্যাহ্বান হৈ পৰিছে। চাইবাৰ সুৰক্ষাই বিভিন্ন প্ৰকাৰৰ প্ৰযুক্তি, প্ৰক্ৰিয়া আৰু ব্যৱস্থা সামৰি লয়, যি চাইবাৰ আক্ৰমণৰ শংকা হ্ৰাস কৰি ব্যক্তি আৰু সংস্থাসমূহক কম্পিউটাৰ-ভিত্তিক বিপদৰ পৰা ৰক্ষা কৰে। চাইবাৰ আক্ৰমণত কম্পিউটাৰ চিষ্টেমত গুৰুতৰ ক্ষতি সাধন কৰিব পাৰে বা গুৰুত্বপূৰ্ণ তথ্য চুৰি হ'ব পাৰে। চাইবাৰস্পেচত টকাৰ জালিয়াতি কৰা আৰু পৰিচয় চুৰিৰ দৰে সমস্যাই চাইবাৰ সুৰক্ষা বৃদ্ধি কৰাৰ প্ৰয়োজনীয়তাক অধিক গুৰুত্বপূৰ্ণ কৰি তুলিছে। চাইবাৰ অপৰাধ, যত কম্পিউটাৰ বা নেটৱৰ্কক অপৰাধ কৰাৰ সঁজুলি বা লক্ষ্য হিচাপে ব্যৱহাৰ কৰা হয়, সেয়া উদ্বেগৰ বিষয়। চৰকাৰ আৰু ব্যৱসায়িক প্ৰতিষ্ঠানে এই ধৰণৰ অপৰাধৰ বিৰুদ্ধে যুঁজ দিবলৈ বিভিন্ন পদক্ষেপ গ্ৰহণ কৰিছে। ব্যৱহাৰকাৰীসকলক সুৰক্ষিত কৰিবলৈ চৰকাৰে কেইবাখনো চাইবাৰ আইন প্ৰৱৰ্তন কৰিছে, যাতে প্ৰযুক্তি দায়িত্বশীলভাৱে ব্যৱহাৰ কৰা হয় আৰু ইয়াৰ অপব্যৱহাৰ নহয়। এই পাঠ্যক্ৰমৰ পৰৱৰ্তী অধ্যায়সমূহত আমি চাইবাৰ অপৰাধ আৰু চাইবাৰ আইনৰ দৰে মূল ধাৰণাসমূহৰ বিষয়ে বিস্তৃত আলোচনা কৰিম।

২.৫.১ চাইবাৰ নিৰাপত্তাৰ বিষয় আৰু প্ৰত্যাহ্বানসমূহ

ব্যক্তি, ব্যৱসায়, চৰকাৰকে ধৰি সকলোৰে বাবে চাইবাৰ নিৰাপত্তা এক গুৰুত্বপূৰ্ণ বিষয় হৈ পৰিছে। যিহেতু ফটো, ভিডিঅ', ভ্ৰমণৰ বিতং তথ্য, আৰু বিত্তীয় তথ্যৰ দৰে অধিক ব্যক্তিগত

আৰু স্পৰ্শকাতৰ তথ্য অনলাইনত শ্বেয়াৰ কৰা হয়, ইয়াৰ নিৰাপত্তা নিশ্চিত কৰাটো অতি গুৰুত্বপূৰ্ণ। বিশেষকৈ মহামাৰীৰ পাছত ডিজিটেল প্ৰযুক্তিৰ ওপৰত ক্ৰমাৎ নিৰ্ভৰশীলতাই চাইবাৰ আক্ৰমণৰ ভয়াৱহতা বৃদ্ধি কৰিছে। অনলাইন ভাবুকিৰ এই বৃদ্ধিয়ে চাইবাৰ নিৰাপত্তাক শীৰ্ষ অগ্ৰাধিকাৰ হিচাপে লৈছে।

এই খণ্ডত আমি আজি বহু উদ্যোগ আৰু সংস্থা, ব্যক্তিয়ে সন্মুখীন হোৱা কিছুমান গুৰুত্বপূৰ্ণ চাইবাৰ নিৰাপত্তা প্ৰত্যাহ্বানৰ বিষয়ে আলোচনা কৰিম।

- ৰেনছমৱেৰ আক্ৰমণ
- ক্লাউড আক্ৰমণ
- IoT আক্ৰমণ
- ফিছিং আক্ৰমণ
- ক্ৰিপ্টোকাৰেন্সী আক্ৰমণ
- মোবাইল বেংকিং মেলৱেৰ
- AI আক্ৰমণ
- আভ্যন্তৰীণ আক্ৰমণ
- সামাজিক অভিযান্ত্ৰিক আক্ৰমণ
- মেন-ইন-দ্য-মিডল এটেক

ৰেনছমৱেৰ আক্ৰমণ: ৰেনছমৱেৰ হৈছে চাইবাৰ নিৰাপত্তাৰ অন্যতম ডাঙৰ প্ৰত্যাহ্বান। ৰেনছমৱেৰ হৈছে এক প্ৰকাৰৰ ক্ষতিকাৰক চফ্টৱেৰ (মেলৱেৰ) যিটো ব্যৱহাৰকাৰীক ফাইল আৰু সুৰক্ষিত ডেটাকে ধৰি তেওঁলোকক কম্পিউটাৰ চিষ্টেমত যেতিয়ালৈকে ৰেনচমৰ ধন হেকাৰক পৰিশোধ নকৰে তেতিয়ালৈকে প্ৰৱেশৰ পৰা বঞ্চিত কৰিবলৈ ডিজাইন কৰা হৈছে। ভুক্তভোগীয়ে আক্ৰমণকাৰীক ধন নিদিয়ালৈকে ডেটা বা কম্পিউটাৰ চিষ্টেমৰ প্ৰৱেশ কৰাত বাধা দিয়ে। ২০২১-২০২২ চনত Covid মহামাৰীৰ পিছত বাঢ়ি অহা ডিজিটেল ব্যৱহাৰৰ বাবে, বিপুল সংখ্যক ৰেনছমৱেৰ আক্ৰমণ সংঘটিত হৈছিল। ২০২১ চনত ২০% তকৈ অধিক চাইবাৰ আক্ৰমণক ৰেনছমৱেৰ হিচাপে শ্ৰেণীভুক্ত কৰা হৈছিল। ৰেনছমৱেৰ আক্ৰমণৰ কিছু শতাংশ ৰিপৰ্ট কৰা হোৱা নাছিল।

ক্লাউড আক্রমণ : ক্লাউড কম্পিউটিং শেহতীয়া বছৰবোৰত ক্রমান্বয়ে জনপ্রিয় হৈ পৰিছে। ই ভৌতিক চার্ভাৰৰ পৰা ভার্চুৱেল প্লেটফর্মলৈ ডেটা সংৰক্ষণত বৈপ্লৱিক পৰিৱর্তন আনিছে। প্রথমতে বেকআপ সংৰক্ষণৰ বাবে ব্যৱহৃত, ক্লাউড কম্পিউটিঙে এটা জনপ্রিয় কম্পিউটিং প্লেটফর্মলৈ ৰূপান্তৰিত হৈছে। কিন্তু, ক্লাউড নিৰাপত্তাৰ দুর্বলতা, যেনে অপর্যাপ্ত ডেটা ইনক্রিপচণ, দুর্বল প্রমাণীকৰণ পদ্ধতি, আৰু অনুচিত চিস্টেম বিন্যাস, বহু বিপদৰ সৃষ্টি কৰে। Distributed Denial-of-Service (DDoS) ৰ দৰে ক্লাউড প্লেটফর্মত আক্রমণ বৃদ্ধি পাইছে, ই চার্ভাৰ আৰু নেটৱর্কসমূহক ট্রেফিক সৃষ্টি কৰি সমস্যাত পেলায়, সেৱাসমূহ বিঘ্নিত কৰে আৰু বৈধ ব্যৱহাৰকাৰীৰ প্রৱেশত বাধা দিয়ে। উদাহৰণস্বৰূপে, Azure Networking এ ২০২১ চনৰ আৰম্ভণিতে পূর্বৰ বছৰৰ তুলনাত অধিক DDoS আক্রমণৰ ৰিপর্ট দিছিল।

IoT আক্রমণ: ইণ্টাৰনেট অৱ থিংছ (IoT) এ স্মার্ট ঘৰুৱা সঁজুলিৰ পৰা আৰম্ভ কৰি ঔদ্যোগিক যন্ত্রপাতিলৈকে বহুতো ডিভাইচক ইণ্টাৰনেটৰ সৈতে সংযোগ কৰে। এই সংযোগে সুবিধা কৰি দিয়ে ঠিকেই, কিন্তু সমস্যাও সৃষ্টি কৰে। IoT ডিভাইচসমূহত প্রায়ে শক্তিশালী নিৰাপত্তা বৈশিষ্ট্যৰ অভাৱ হয়, যাৰ ফলত এইবিলাক চাইবাৰ অপৰাধীৰ লক্ষ্য হৈ পৰে। IoT ডিভাইচসমূহত আক্রমণে ডেটা ভংগ, ডিভাইচসমূহৰ ওপৰত নিয়ন্ত্রণ হেৰুৱা, আৰু আনকি জটিল আন্তঃগাঁথনি, ভৌতিক ক্ষতি কৰিব পাৰে।

ফিছিং আক্রমণ: ফিছিং চাইবাৰ আক্রমণৰ অন্যতম সাধাৰণ আৰু কার্যকৰী পদ্ধতি হৈয়েই আছে। আক্রমণকাৰীয়ে ব্যক্তিক পাছৱর্ড, ক্রেডিট কার্ড নম্বৰ বা ব্যক্তিগত তথ্যৰ দৰে স্পর্শকাতৰ তথ্য প্রকাশ কৰিবলৈ প্রতাৰণামূলক ইমেইল, বার্তা বা ৱেবছাইট ব্যৱহাৰ কৰে। ফিছিং আক্রমণে পৰিচয় চুৰি, আর্থিক ক্ষতি, আৰু চিস্টেমসমূহত অবৈধ প্রৱেশ সৃষ্টি কৰিব পাৰে।

ক্রিপ্টোকাৰেন্সী আক্রমণ : ক্রিপ্টোকাৰেন্সী আৰু ব্লকচেইন প্রযুক্তিৰ উত্থানে নতুন নিৰাপত্তাজনিত প্রত্যাহ্বানৰ সৃষ্টি কৰিছে। চাইবাৰ অপৰাধীয়ে ক্রিপ্টোকাৰেন্সী এক্সচেঞ্জ আৰু ৱালেটক লক্ষ্য কৰি লয়, আৰু ডিজিটেল সম্পত্তি চুৰি কৰে।

মোবাইল বেংকিং মেলৱেৰ : বেংকিং আৰু বিত্তীয় লেনদেনৰ বাবে মোবাইল ডিভাইচৰ ব্যৱহাৰ বৃদ্ধি পোৱাৰ লগে লগে মোবাইল বেংকিং মেলৱেৰ এক উল্লেখযোগ্য ভাবুকি হৈ পৰিছে। এই ক্ষতিকাৰক প্রগ্রেমসমূহে মোবাইল এপসমূহক লক্ষ্য কৰি স্পর্শকাতৰ তথ্য চুৰি কৰিবলৈ, যোগাযোগ বাধাগ্রস্ত কৰিবলৈ বা লেনদেনত বিধি পথালি দিবলৈ লক্ষ্য কৰে। ব্যৱহাৰকাৰীয়ে অজানিতে ক্ষতিকাৰক এপ বা লিংকৰ জৰিয়তে মেলৱেৰ ডাউনলোড কৰিব পাৰে, যাৰ ফলত আর্থিক লোকচান হয়।

AI Attacks : কৃত্রিম বুদ্ধিমত্তাই (AI) বিভিন্ন উদ্যোগক নতুন ৰূপ দিছে সঁচা, কিন্তু ই চাইবাৰ নিৰাপত্তাৰ নতুন প্রত্যাহ্বানো সৃষ্টি কৰিছে। আক্রমণকাৰীয়ে অত্যাধুনিক মেলৱেৰ বিকশিত

কৰিবলৈ, আক্রমণ স্বয়ংক্রিয় কৰিবলৈ, আৰু দুর্বলতা চিনাক্ত কৰিবলৈ AI ব্যৱহাৰ কৰিব পাৰে। ইয়াৰ বিপৰীতে এআইয়ে ভাবুকি ধৰা পেলোৱা আৰু সঁহাৰিৰ উন্নতি সাধন কৰিও নিৰাপত্তা বৃদ্ধি কৰিব পাৰে। এআইৰ দ্বৈত ব্যৱহাৰৰ প্রকৃতিৰ বাবে চাইবাৰ অপৰাধীৰ অপব্যৱহাৰ ৰোধ কৰিবলৈ সাৱধানে পৰিচালনাৰ কৰাৰ প্রয়োজন আছে।

আভ্যন্তৰীন আক্রমণ : ইনচাইডাৰ থ্রেট বা অভ্যন্তৰীণ বিপদবোৰ কোম্পানীৰ কর্মচাৰী, চুক্তিবদ্ধ কর্মী বা ব্যৱসায়িক অংশীদাৰৰ পৰা আহে, যিসকলৰ সংস্থাৰ ব্যৱস্থা আৰু ডেটালৈ প্রৱেশাধিকাৰ থাকে। এই ব্যক্তিসকলে ইচ্ছাকৃতভাৱে বা অনিচ্ছাকৃতভাৱে গুৰুত্বপূর্ণ ক্ষতি কৰিব পাৰে, যেনে— গোপন তথ্য লিক কৰা, ব্যৱস্থাসমূহ নষ্ট কৰা বা বাহ্যিক আক্রমণত সহায় কৰা। ইনচাইডাৰ আক্রমণসমূহ চিনাক্ত কৰা আৰু প্রতিৰোধ কৰাটো এক প্রত্যাহ্বান, কিয়নো ইয়াত জড়িত ব্যক্তিসকল প্রায়ে বিশ্বাসৰ ভিত্তিত কাম কৰে।

সামাজিক অভিযান্ত্রিক আক্রমণ : চ'চিয়েল ইঞ্জিনিয়াৰিং হৈছে মানৱ মনোবিজ্ঞানৰ অপব্যৱহাৰ কৰি ব্যক্তিক কোনো কাম কৰাবলৈ বা গোপন তথ্য প্রকাশ কৰাবলৈ প্রভাৱিত কৰা এক পদ্ধতি। ইয়াত প্রিটেক্সিটং, বেইটিং, টেইলগেটিংৰ দৰে কৌশল ব্যৱহাৰ কৰি ব্যৱস্থা বা ডেটালৈ অননুমোদিত প্রৱেশ কৰা হয়। চ'চিয়েল ইঞ্জিনিয়াৰিং আক্রমণবোৰ বিশেষকৈ ফলপ্রসূ হয়, কিয়নো ই মানৱীয় দিশটো লক্ষ্য কৰি প্রযুক্তিগত সু�ৰক্ষা ব্যৱস্থাক পাৰ কৰি যায়।

The Man-in-the-Middle Attack : মেন-ইন-দ্য-মিডল (MitM) আক্রমণত আক্রমণকাৰীয়ে দুটা পক্ষৰ মাজৰ যোগাযোগ গোপনে বাধা দি সেইবোৰ পুনৰ প্রেৰণ কৰে। এই ধৰণৰ আক্রমণ অসুৰক্ষিত নেটৱর্কত হ'ব পাৰে, য'ত আক্রমণকাৰীয়ে তথ্য চোৱাংকৈ শুনিব পাৰে, সলনি কৰিব পাৰে বা চুৰি কৰিব পাৰে। মেন-ইন-দ্য-মিডল আক্রমণে বিত্তীয় লেনদেন, যোগাযোগ আৰু গোপন তথ্যৰ বাবে গুৰুতৰ বিপদৰ সৃষ্টি কৰে।

কিছুমান বিশেষ কাৰকৰ ওপৰত এই প্রত্যাহ্বানসমূহ নির্ভৰশীল। ইয়াৰে কিছুমান হ'ল-

- **প্রক্রিয়াগত নিয়মৰ অভাৱ:** বিভিন্ন উদ্যোগ আৰু অঞ্চলত চাইবাৰ সুৰক্ষাৰ বাবে বিশেষ প্রক্রিয়া আৰু নিয়মাৱলীৰ অভাৱে সুৰক্ষাৰ স্তৰত অসামঞ্জস্য আৰু সুৰক্ষা ব্যৱস্থাত ফাঁকৰ সৃষ্টি কৰে।
- **প্রযুক্তিগত কর্মীৰ অভাৱ:** বিশ্বব্যাপী দক্ষ চাইবাৰ সুৰক্ষা পেছাদাৰীৰ অভাৱ আছে, যাৰ ফলত সংস্থাসমূহে চাইবাৰ বিপদৰ সৈতে ফলপ্রসূভাৱে যুঁজ দিবলৈ অসুবিধাৰ সন্মুখীন হয়।
- **অনুষ্ঠানিক ব্যৱস্থাৰ অভাৱ:** চাইবাৰ সুৰক্ষাৰ অনুষ্ঠানিক ব্যৱস্থা আৰু পৰীক্ষাগাৰলৈ অপর্যাপ্ত বিনিয়োগে দৃঢ় সুৰক্ষা ব্যৱস্থাৰ বিকাশ আৰু পৰীক্ষণত বাধাৰ সৃষ্টি কৰে।

- **স্থানীয়কৰণৰ প্ৰয়োজন:** বিভিন্ন অঞ্চলৰ চাইবাৰ সুৰক্ষাৰ আৱশ্যকতা আৰু বিপদবোৰ বেলেগ বেলেগ। এই বিশেষ প্ৰত্যাহ্বানসমূহ সমাধান কৰিবলৈ স্থানীয়কৰণ কৰা কৌশল আৰু সমাধানৰ প্ৰয়োজন।

এই চাইবাৰ নিৰাপত্তা প্ৰত্যাহ্বানসমূহ মোকাবিলা কৰিবলৈ এক ব্যাপক পদ্ধতিৰ প্ৰয়োজন যিয়ে শক্তিশালী কাৰিকৰী প্ৰতিৰক্ষা, নিয়মীয়া প্ৰশিক্ষণ আৰু সজাগতা কাৰ্যসূচী, চাইবাৰ নিৰাপত্তা আন্তঃগাঁথনিত বিনিয়োগ, আৰু প্ৰামাণিক পদ্ধতি আৰু নিয়মৰ বিকাশ আদি অন্তৰ্ভুক্ত কৰে।



আপোনাৰ অগ্ৰগতি পৰীক্ষা কৰক

প্ৰশ্ন ১. শুদ্ধ উত্তৰ বাচি উলিয়াওক

ক) ইণ্টাৰনেটৰ বীজ ৰোপণ কৰা প্ৰথমটো নেটৱৰ্ক আছিল:

a) NFSNET b) ARPANET

c) Telnet d) ARPA

খ) ইণ্টাৰনেটে ব্যৱহাৰ কৰা যোগাযোগ প্ৰট'কলসমূহ হ'ল...

a) TCP/IP b) HTTP

c) SMTP d) WWW

গ) ইণ্টাৰনেটৰ প্ৰৱেশ কৰিবলৈ, ব্যৱহাৰকাৰীজন এজনৰ সৈতে সংযুক্ত হ'ব লাগে-

a) ইণ্টাৰনেট সেৱা প্ৰদানকাৰী (ISP) b) চাৰ্ভাৰ

c) DNS d) এটাও নহয়

ঘ) ইণ্টাৰনেট হৈছে

a) জটিল ব্যৱস্থা b) গতিশীল ব্যৱস্থা

c) বিকেন্দ্ৰীকৃত ব্যৱস্থা d) এই সকলোবোৰ।

প্ৰশ্ন ২। ARPANET কি?

প্ৰশ্ন ৩। খালী ঠাই পূৰণ কৰক:

i) _____ হৈছে বৃহৎ পৰিমাণৰ ফাইবাৰ অপ্টিক কেবল, যিবোৰ সাগৰৰ তলত পতা হয় আৰু মহাদেশসমূহ সংযোগ কৰি গোলকীয় ডেটা স্থানান্তৰ সম্ভৱ কৰে।

ii) _____ হৈছে ইণ্টাৰনেটৰ সুচল কাৰ্যকলাপৰ ভেটি, যিয়ে নিৰ্ভৰযোগ্য আৰু সুৰক্ষিত যোগাযোগ নিশ্চিত কৰে।

iii) _____হৈছে ৱৰ্ল্ড ৱাইড ৱেবত ডেটা যোগাযোগৰ মূল প্ৰটোকল, আৰু ইয়াৰ সুৰক্ষিত সংস্কৰণ _____এ এনক্ৰিপশন যন্ত্ৰ যোগ কৰে।

iv) _____ ডেটা প্রচেছিং আৰু সংৰক্ষণৰ বাবে প্রয়োজনীয় ভৌতিক স্থান আৰু শক্তিৰ যোগান ধৰে, যিয়ে ইণ্টাৰনেটৰ পৰি কাঠামোৰ মূল ভেটি গঠন কৰে।

v) _____ হৈছে এক প্রকাৰৰ দূর্ভাৱনামূলক ছফ্টৱেৰ, যিয়ে হেকাৰক এটা মুক্তিপণ দিয়া নহ'লে ব্যৱহাৰকাৰীক তেওঁলোকৰ কম্পিউটাৰ ব্যৱস্থাত প্রৱেশ কৰিবলৈ অস্বীকাৰ কৰে।

vi) ক্লাউড সুৰক্ষাৰ দুর্বলতাসমূহৰ ভিতৰত আছে অপর্যাপ্ত_____, দুর্বল প্রমাণীকৰণ পদ্ধতি আৰু অনুচিত ব্যৱস্থাপনাৰ কনফিগাৰেচন।

vii) ফিছিং আক্রমণৰ লক্ষ্য হৈছে ব্যক্তিক সংবেদনশীল তথ্য যেনে_____বা ব্যক্তিগত ডেটা প্রকাশ কৰাবলৈ প্রভাৱিত কৰা।

viii) চাইবাৰ অপৰাধীসকলে ক্রিপ্টকাৰেন্সি এক্সচেঞ্জ আৰু ৱালেটৰ দুর্বলতাসমূহৰ সুযোগ লৈ _____ চুৰি কৰে।

ix) মেন-ইন-দ্য-মিডল আক্রমণত, আক্রমণকাৰীয়ে দুটা পক্ষৰ মাজৰ _____ গোপনে বাধা দি সেইবোৰ পুনৰ প্রেৰণ কৰে।

x) আক্রমণকাৰীসকলে AI ব্যৱহাৰ কৰি অত্যাধুনিক_____ বিকশিত কৰিব পাৰে আৰু চাইবাৰ আক্রমণ স্বয়ংক্রিয় কৰিব পাৰে।



২.৮ অধ্যায়টিৰ পৰা আমি কি কি শিকিলোঁ

- ইণ্টাৰনেট হৈছে বিশ্বজুৰি কম্পিউটাৰ আৰু ডিভাইচসমূহ সংযোগ কৰা এক বিশ্বব্যাপী নেটৱর্ক।
- ই প্রামাণিককৃত প্রটোকলসমূহৰ জৰিয়তে যোগাযোগ আৰু তথ্য বিনিময় সক্ষম কৰে।
- ১৯৬০ চনত আমেৰিকাৰ প্রতিৰক্ষা বিভাগে নির্মাণ কৰা ARPANET ৰ লক্ষ্য আছিল এক স্থিতিস্থাপক যোগাযোগ ব্যৱস্থা সৃষ্টি কৰা।
- ১৯৭০ চনত TCP/IP প্রটোকল গ্রহণে ARPANET ৰ ক্ষমতাসমূহ সম্প্রসাৰিত কৰে।
- ১৯৮০ চনৰ আ�ৰম্ভণিতে আর্পানেটে বিশ্বজুৰি শৈক্ষিক আৰু গৱেষণা প্রতিষ্ঠানসমূহক সংযোগ কৰিছিল।
- ১৯৮৯ চনত টিম বার্নার্ছ-লীয়ে ৱর্ল্ড ৱাইড ৱেব আৱিষ্কাৰে ইণ্টাৰনেটত বৈপ্লৱিক পৰিৱর্তন আনি বাণিজ্যিক ব্যৱহাৰ আৰু বিশ্বব্যাপী নেটৱর্ক সংযোগৰ সুবিধা প্রদান কৰে।
- ইন্টাৰনেট আন্তঃগাঁথনিয়ে ভৌতিক হার্ডৱেৰ, তথ্য স্থানান্তৰ প্রটোকলসমূহ (যেনে, TCP/IP, HTTP), আৰু ডেটা কেন্দ্রসমূহ অন্তর্ভুক্ত কৰে।

- এই উপাদানসমূহে তথ্য নিৰাপত্তাৰ বাবে নিয়ন্ত্রণমূলক প্রামাণিকসমূহ মানি চলি দক্ষ, নির্ভৰযোগ্য, আৰু সুৰক্ষিত তথ্য সংক্রমণ নিশ্চিত কৰে।
- ইণ্টাৰনেট ছ'চাইটিয়ে বিশ্বব্যাপী তথ্য বিনিময়ক প্রসাৰিত কৰে আৰু ইণ্টাৰনেটক বিশ্বব্যাপী কাৰিকৰী আন্তঃগাঁথনি হিচাপে বিকাশত সহায় কৰে।
- ইয়াৰ লক্ষ্য হৈছে সার্বজনীন ইণ্টাৰনেটৰ ব্যৱহাৰ আৰু ব্যৱহাৰৰ জৰিয়তে মানুহৰ জীৱন সমৃদ্ধ কৰা।
- ডিজিটেল প্রযুক্তিৰ ওপৰত নির্ভৰশীলতা বৃদ্ধিয়ে ব্যক্তি, ব্যৱসায় আৰু চৰকাৰৰ বাবে চাইবাৰ নিৰাপত্তাৰ উদ্বেগ বৃদ্ধি কৰে।
- মূল প্রত্যাহ্বানসমূহৰ ভিতৰত আছে ৰেনছমৱেৰ, ক্লাউড আক্রমণ, IoT দুর্বলতা, ফিছিং, ক্রিপ্টোকাৰেন্সী আক্রমণ, মোবাইল বেংকিং মেলৱেৰ, এআই ভাবুকি, ভিতৰৰ আক্রমণ, আৰু ছ'চিয়েল ইঞ্জিনিয়াৰিং।
- প্রতিৰক্ষা, দক্ষ চাইবাৰ নিৰাপত্তা পেছাদাৰী, পর্যাপ্ত আন্তঃগাঁথনি, আৰু বিপদসমূহ ফলপ্রসূভাৱে হ্রাস কৰিবলৈ প্রামাণিক নিয়মৰ প্রয়োজন ।

২.৯ অগ্রগতিৰ খতিয়ান

১ নং প্রশ্নৰ উত্তৰঃ

ক) ARPANET খ) TCP/IP গ) ইণ্টাৰনেট সেৱা প্রদানকাৰী (ISP) ঘ) এই সকলোবোৰ

প্রশ্ন নং ২ৰ উত্তৰঃ

উন্নত গৱেষণা প্রকল্প সংস্থা নেটৱর্ক (ARPANET) হৈছে ইণ্টাৰনেটৰ পূর্বসূৰী। ৬০ৰ দশকৰ শেষৰ ফালে আৰু ৭০ৰ দশকৰ আৰম্ভণিতে আমেৰিকাৰ প্রতিৰক্ষা বিভাগৰ এডভান্সড ৰিচার্চ প্রজেক্ট এজেন্সীয়ে (ARPA) ইয়াক WAN ৰ পৰীক্ষা হিচাপে প্রতিষ্ঠা কৰিছিল যাতে বিভিন্ন ব্যৱস্থা চলোৱা কম্পিউটাৰক একেলগে সংযোগ কৰিব পাৰি যাতে এটা স্থানৰ মানুহে আন এটা স্থানৰ পৰা কম্পিউটিং সম্পদ ব্যৱহাৰ কৰিব পাৰে। ARPANET আছিল TCP/IP প্রটোকল চুইট প্রণয়ন কৰা প্রথম নে'টৱর্কসমূহৰ এটা।

৩ নং প্রশ্নৰ উত্তৰঃ

i) *ছাবমেৰিন*

ii) *TCP/IP*

iii) *HTTP*

iv) *ডেটা কেন্দ্রসমূহে*

v) *ৰেনছমৱেৰ*

vi) *ডেটা এনক্রিপশন*

vii) *পাছৱর্ড*

viii) *ডিজিটেল সম্পদ*

ix) *যোগাযোগ*

x) *মেলৱেৰ*



২.১০ অধিক জানিবলৈ

1) Forouzan, B., & Fegan, S. (2006). Data Communication and Networking, Special Indian Edition *Tata McGraw Hill Education Private Limited*.
2) Internet Society Mission and Vision - Internet Society
3) https://www.legalserviceindia.com/legal/article-2548-need-of-regulation-in-cyberspace.html
4) https://legaldesire.com/laws-applicable-in-cyberspace-in-india/
5) https://increditools.com/ransomware-statistics/
6) https://www.thesagenext.com/blog/emerging-cybersecurity-challenges
7) https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050
8) https://gdpr.eu/
9) https://www.researchgate.net/publication/347373943_Cyber_Security_Challenges_and_its_Emerging_Trends_on_Latest_Technologies

২.১১ আৰ্হি প্রশ্ন

প্রশ্ন ১। ইণ্টাৰনেট কি?

প্রশ্ন ২। চাইবাৰ নিৰাপত্তা কি?

প্রশ্ন ৩। ডিজিটেল ডিভাইড বুলিলে কি বুজায়?

প্রশ্ন ৪। "চাইবাৰস্পেচ"ৰ অর্থ কি?

প্রশ্ন ৫। প্রকৃত স্থান চাইবাৰ স্থানৰ পৰা কেনেকৈ পৃথক?

প্রশ্ন ৬। ইণ্টাৰনেটক কিয় নেটৱর্কৰ নেটৱর্ক বুলি কোৱা হয়?

প্ৰশ্ন ৭। সমাজত ইণ্টাৰনেটৰ কিছুমান নেতিবাচক প্ৰভাৱ কি কি, আৰু সেইবোৰ কেনেকৈ লাঘৱ কৰিব পাৰি?

প্ৰশ্ন ৮। ইণ্টাৰনেট ছ'চাইটিৰ মিছন আৰু দৃষ্টিভংগী কি?

প্ৰশ্ন ৯। ইণ্টাৰনেট ছ'চাইটিয়ে পৰিচালনা কৰা পাঁচটা কাম কি কি?

প্ৰশ্ন ১০। চাইবাৰ নিৰাপত্তাৰ মূল বিষয় আৰু প্ৰত্যাহ্বানসমূহ কি কি? বৰ্ণনা কৰক।

প্ৰশ্ন ১১। চাইবাৰ স্পেচৰ বাবে নিয়ম কিয় প্ৰয়োজনীয়?

প্ৰশ্ন ১২। ইণ্টাৰনেটৰ আগমনে বিশ্বজুৰি যোগাযোগ আৰু সংযোগক কেনেদৰে ৰূপান্তৰিত কৰিছে?

প্ৰশ্ন ১৩। ব্যক্তি আৰু সংস্থাসমূহৰ ওপৰত ৰেনছমৱেৰ আক্ৰমণৰ প্ৰভাৱৰ বিষয়ে চমুকৈ আলোচনা কৰক।

প্ৰশ্ন ১৪। ইণ্টাৰনেটে বিশ্বজুৰি যোগাযোগ আৰু সংযোগত কেনেদৰে বৈপ্লৱিক পৰিৱৰ্তন আনিছে সেই বিষয়ে ব্যাখ্যা কৰক।

****

অধ্যায় ৩: চাইবাৰ অপৰাধ (প্ৰথম খণ্ড)

অধ্যায় গাঁথনি

৩.১ উদ্দেশ্য
৩.২ পৰিচয়
৩.৩ চাইবাৰ অপৰাধ
৩.৪ চাইবাৰ অপৰাধৰ শ্ৰেণীবিভাজন
৩.৫ সাধাৰণ চাইবাৰ অপৰাধ
৩.৫.১ কম্পিউটাৰ আৰু মোবাইল ডিভাইচক লক্ষ্য কৰি চাইবাৰ অপৰাধ
৩.৫.২ ব্যক্তিৰ বিৰুদ্ধে চাইবাৰ অপৰাধ
৩.৫.৩ মহিলা আৰু শিশুৰ বিৰুদ্ধে চাইবাৰ অপৰাধ
৩.৬ অধ্যায়টিৰ পৰা আমি কি কি শিকিলোঁ
৩.৭ অগ্ৰগতিৰ খতিয়ান
৩.৮ অধিক জানিবলৈ
৩.৯ আৰ্হি প্ৰশ্ন

৩.১ উদ্দেশ্য

এই অধ্যায়ৰ আলোচনাৰ পৰা আপুনি-

- চাইবাৰ অপৰাধৰ সংজ্ঞা দিব পাৰিব
- বিভিন্ন ধৰণৰ চাইবাৰ অপৰাধৰ শ্ৰেণীবিভাজন কৰিব পাৰিব
- সাধাৰণ চাইবাৰ অপৰাধৰ তালিকা প্ৰস্তুত কৰিব পাৰিব
- কম্পিউটাৰ আৰু মোবাইলক লক্ষ্য কৰি ঘটা চাইবাৰ অপৰাধৰ বৰ্ণনা কৰিব পাৰিব
- ব্যক্তিৰ বিৰুদ্ধে চাইবাৰ অপৰাধৰ বৰ্ণনা কৰিব পাৰিব
- মহিলা আৰু শিশুৰ বিৰুদ্ধে সংঘতিত চাইবাৰ অপৰাধৰ বৰ্ণনা কৰিব পাৰিব

৩.২ পৰিচয়

আগৰ অধ্যায়ত আমি ইণ্টাৰনেট আৰু ইণ্টাৰনেটৰ সৈতে জড়িত ধাৰণা যেনে তথ্য স্থানান্তৰ আৰু শাসনৰ বাবে ইণ্টাৰনেট আন্তঃগাঁথনিৰ বিষয়ে জানিলোঁ । চাইবাৰ স্পেচৰ নিয়ন্ত্ৰণ, চাইবাৰ সুৰক্ষাৰ ধাৰণা, ইয়াৰ সমস্যা আৰু ইয়াৰ প্ৰত্যাহ্বানসমূহৰ বিষয়েও আমি বিতংভাৱে জানিলোঁ। এই অধ্যায়ত আমি বিভিন্ন ধৰণৰ চাইবাৰ অপৰাধৰ সৈতে পৰিচিত হ'ম।

চাইবাৰ অপৰাধৰ শ্ৰেণীসমূহৰ বিষয়েও আমি জানিব পাৰিম। কম্পিউটাৰ আৰু মোবাইলক লক্ষ্য কৰি সংঘটিত চাইবাৰ অপৰাধৰ বিষয়ে এই অধ্যায়ত বিতংভাৱে আলোচনা কৰা হৈছে। ইয়াৰ উপৰিও ব্যক্তিৰ বিৰুদ্ধে আৰু বিশেষভাৱে মহিলা আৰু শিশুৰ বিৰুদ্ধে হোৱা চাইবাৰ অপৰাধৰ বিষয়েও এই অধ্যায়ত বিতংভাৱে আলোচনা কৰা হৈছে। পৰৱৰ্তী অধ্যায়ত আমি বিভিন্ন ধৰণৰ বিত্তীয় জালিয়াতি আৰু সামাজিক অভিযান্ত্রিক আক্ৰমণৰ বিষয়ে জানিব পাৰিম। আমি পৰৱৰ্তী অধ্যায়ত বিভিন্ন ধৰণৰ মেলৱেৰৰ বিষয়েও জানিব পাৰিম।

৩.৩ চাইবাৰ অপৰাধ

কম্পিউটাৰ আৰু ইলেক্ট্ৰনিক ডিভাইচসমূহ আমাৰ দৈনন্দিন জীৱনৰ অবিচ্ছেদ্য অংগ হৈ পৰিছে, যোগাযোগ আৰু মনোৰঞ্জনৰ পৰা আৰম্ভ কৰি বেংকিং আৰু শিক্ষালৈকে বিভিন্ন কাৰ্য্যকলাপৰ সুবিধাজনক হৈ পৰিছে। এই ব্যাপক ব্যৱহাৰে একেসময়তে ইণ্টাৰনেট ব্যৱহাৰকাৰীৰ পৰিসংখ্যা বৃদ্ধিত প্ৰেৰণা যোগাইছে, বিশ্বজুৰি কোটি কোটি লোকক সংযোগ কৰিছে। ইণ্টাৰনেট আৰু ডিজিটেল প্ৰযুক্তিয়ে নিঃসন্দেহে জীৱনৰ বহু দিশ সৰল কৰি তুলিছে, অৱশ্যে এই ডিজিটেল বিপ্লৱৰ ফলত অপৰাধৰ এক নতুন শ্ৰেণী—চাইবাৰ অপৰাধৰ উত্থান ঘটিছে।

ভাৰতীয় ৰাষ্ট্ৰীয় চাইবাৰ অপৰাধ প্ৰতিবেদন পৰ্টেলত চাইবাৰ অপৰাধৰ সংজ্ঞা দাঙি ধৰিছে এনেদৰে-

"কম্পিউটাৰ বা যোগাযোগ যন্ত্ৰ বা কম্পিউটাৰ নেটৱৰ্ক ব্যৱহাৰ কৰি অপৰাধ সংঘটিত কৰা যিকোনো অবৈধ কাৰ্য্যই চাইবাৰ অপৰাধ।"

চাইবাৰ অপৰাধক কম্পিউটাৰ আৰু নেটৱৰ্ক ব্যৱহাৰ কৰি সঁজুলি হিচাপে বা লক্ষ্য হিচাপে কৰা যিকোনো অপৰাধ বুলি সংজ্ঞায়িত কৰিব পাৰি। এই সংজ্ঞাই চাইবাৰ অপৰাধত প্ৰযুক্তিয়ে ল'ব পৰা দ্বৈত ভূমিকাক আলোকপাত কৰে—পৰম্পৰাগত অপৰাধ সংঘটিত কৰাৰ মাধ্যম (যেনে প্ৰৱঞ্চনা বা হাৰাশাস্তি) আৰু নিজৰ লক্ষ্য ভিত্তিত (যেনে হেকিঙৰ ক্ষেত্ৰত) দুয়োটা হিচাপে।

৩.৪ চাইবাৰ অপৰাধৰ শ্ৰেণীবিভাজন

চাইবাৰ অপৰাধৰ প্ৰকাৰৰ ওপৰত নিৰ্ভৰ কৰি ইয়াক বিভিন্ন গোটত ভাগ কৰিব পাৰি। সাধাৰণতে চাইবাৰ অপৰাধৰ শ্ৰেণীবিভাজন চাইবাৰ অপৰাধৰ লক্ষ্যৰ ওপৰত ভিত্তি কৰি কৰা হয়।

চাইবাৰ অপৰাধৰ লক্ষ্যৰ ওপৰত ভিত্তি কৰি তলত দিয়া শ্ৰেণীসমূহ হ'লঃ

১. প্ৰতিষ্ঠান আৰু চৰকাৰ কেন্দ্ৰিক অপৰাধঃ যেতিয়া চাইবাৰ অপৰাধীয়ে কম্পিউটাৰ চিষ্টেম হেক কৰে বা কোনো লক্ষ্য সংস্থা বা জাতিৰ কম্পিউটাৰ চিষ্টেমত মেলৱেৰ ইনষ্টল কৰিবলৈ সক্ষম হয় তেতিয়া এই চাইবাৰ অপৰাধক সংস্থা বা চৰকাৰ আৰু দেশৰ বিৰুদ্ধে অপৰাধ বুলি গণ্য কৰা হয়। চৰকাৰৰ বিৰুদ্ধে অপৰাধৰ কিছুমান উদাহৰণ হ'ল চাইবাৰ সন্ত্ৰাসবাদ, স্পাইৱেৰ ইনষ্টল কৰা ইত্যাদি।

২. ব্যক্তি কেন্দ্ৰিক অপৰাধ : যেতিয়া চাইবাৰ অপৰাধীয়ে কোনো ব্যক্তিক তেওঁলোকৰ কম্পিউটাৰ চিষ্টেমত হেক কৰি বা তেওঁলোকৰ চিষ্টেমত মেলৱেৰ ইনষ্টল কৰি লক্ষ্য কৰি লয় তেতিয়া এই চাইবাৰ অপৰাধক ব্যক্তি কেন্দ্ৰিক অপৰাধ বুলি গণ্য কৰা হয়। এই শ্ৰেণীৰ অপৰাধৰ কিছুমান উদাহৰণ হ'ল আৰ্থিক প্ৰৱঞ্চনা, কম্পিউটাৰ বা মোবাইল ডিভাইচ হেক কৰা ইত্যাদি।

৩. সম্পত্তি কেন্দ্ৰিক অপৰাধ: যেতিয়া চাইবাৰ অপৰাধীয়ে বৌদ্ধিক সম্পত্তি আৰু ডিজিটেল সম্পত্তিক লক্ষ্য কৰি অধিকাৰ উলংঘা কৰে আৰু যথেষ্ট আৰ্থিক লোকচানৰ সৃষ্টি কৰে তেতিয়া এই চাইবাৰ অপৰাধক সম্পত্তি কেন্দ্ৰিক অপৰাধ বুলি গণ্য কৰা হয়।

৪. সমাজ কেন্দ্ৰিক অপৰাধ : সমাজ কেন্দ্ৰিক অপৰাধ হৈছে বৃহৎ পৰিসৰৰ চাইবাৰ অপৰাধ যিবোৰৰ লক্ষ্য হৈছে সমাজৰ নীতি-নিয়ম বিঘ্নিত কৰা আৰু জনকল্যাণক বিপদত পেলোৱা। ইয়াৰ ভিতৰত মানৱ সৰবৰাহৰ বাবে কম্পিউটাৰ ব্যৱস্থা ব্যৱহাৰ কৰা, শিশু পৰ্ণগ্ৰাফী বিয়পোৱা আৰু মুদ্ৰাৰ ডিজিটেল জালিয়াতিৰ দৰে কাম-কাজ অন্যতম।

অপৰাধ সংঘটিত কৰাত কম্পিউটাৰ কেনেকৈ ব্যৱহাৰ কৰা হয় তাৰ ওপৰতো চাইবাৰ অপৰাধক দুটা ভাগত ভাগ কৰিব পাৰি:

১. কম্পিউটাৰক লক্ষ্য কৰি: এই শ্ৰেণী অপৰাধত কম্পিউটাৰটোৱেই প্ৰধান লক্ষ্য। এই শ্ৰেণীৰ উদাহৰণ হ'ল হেকিং, মেলৱেৰ আক্ৰমণ আৰু সেৱা অস্বীকাৰ কৰা আক্ৰমণ।

২. কম্পিউটাৰক মাধ্যম হিচাপে ব্যৱহাৰ কৰা: এই শ্ৰেণীত অপৰাধৰ সুবিধাৰ বাবে কম্পিউটাৰক মাধ্যম হিচাপে ব্যৱহাৰ কৰা হয়। এই শ্ৰেণীৰ উদাহৰণ হ'ল চাইবাৰষ্টাকিং, চাইবাৰ বুলিং, আৰু বিভিন্ন ধৰণৰ অনলাইন জালিয়াতি আৰু পৰিচয় চুৰি।



অগ্ৰগতি নিৰীক্ষণ কৰক

Q1. চাইবাৰ অপৰাধ কি? বুজাই লিখক ।

Q2. উদ্দেশ্য অনুসৰি চাইবাৰ অপৰাধৰ ভাগবোৰ কি কি লিখক ?

৩.৫ সাধাৰণ চাইবাৰ অপৰাধ

এই খণ্ডত আমি কিছুমান সাধাৰণ চাইবাৰ অপৰাধৰ বিষয়ে চাম। এই সাধাৰণ চাইবাৰ অপৰাধসমূহক তলত দিয়া শ্ৰেণীত ভাগ কৰা হয়:

- কম্পিউটাৰ আৰু মোবাইল ডিভাইচক লক্ষ্য কৰি সংঘটিত হোৱা চাইবাৰ অপৰাধ
- ব্যক্তি কেন্দ্ৰিক চাইবাৰ অপৰাধ
- মহিলা আৰু শিশু কেন্দ্ৰিক চাইবাৰ অপৰাধ

৩.৫.১ কম্পিউটাৰ আৰু মোবাইল ডিভাইচসমূহক লক্ষ্য কৰি সংঘটিত হোৱা চাইবাৰ অপৰাধ

কম্পিউটাৰ আৰু মোবাইল ডিভাইচক লক্ষ্য কৰি বিভিন্ন ধৰণৰ চাইবাৰ অপৰাধৰ সংঘটিত হয় । সেইবোৰ তলত আলোচনা কৰা হ'ল-

১. হেকিং:

হেকিং হৈছে অন্যতম সাধাৰণ চাইবাৰ অপৰাধ। হেকিঙৰ অৰ্থ হ'ল অনুমতি অবিহনে আৰু অবৈধ উপায়েৰে আন এজন ব্যক্তিৰ কম্পিউটাৰ চিষ্টেম বা মোবাইল ডিভাইচত প্ৰৱেশ কৰা। হেকিঙক আন ব্যক্তিৰ কম্পিউটাৰ চিষ্টেম বা নেটৱৰ্কত অবৈধ অনুপ্ৰৱেশ বুলিও ক'ব কৰিব পাৰি। ইয়াক কম্পিউটাৰ চিষ্টেম আৰু কম্পিউটাৰ নেটৱৰ্কত দুৰ্বলতা বিচাৰি উলিওৱা আৰু এই দুৰ্বলতাসমূহৰ সুযোগ লৈ তথ্য আৰু ডিভাইচত প্ৰৱেশ লাভ কৰাৰ কাৰ্য্যকলাপ বুলিব পাৰি।

হেকাৰ, চিষ্টেমটো হেক কৰা অপৰাধী হয়তো কোনো ব্যক্তি, বা কোনো দল বা সংস্থাৰ অন্তৰ্গত। হেকাৰক সাধাৰণতে তিনিটা ভাগত ভাগ কৰা হয়:

ক) হুৱাইট হেট হেকাৰ: হুৱাইট হেট হেকাৰ হৈছে নৈতিক হেকাৰ যিসকলক সাধাৰণতে সংস্থাসমূহে তেওঁলোকৰ চিষ্টেমৰ সুৰক্ষা পৰীক্ষা কৰিবলৈ নিয়োগ কৰে। তেওঁলোকে ব্যৱস্থাটোৰ ত্ৰুটি বিচাৰি ব্যৱস্থাটোক সুৰক্ষিত কৰিবলৈ চেষ্টা কৰে যাতে এই ত্ৰুটিবোৰ সমাধান কৰিব পৰা যায়। হুৱাইট হেট হেকাৰ নৈতিক হেকাৰ বুলিও কোৱা হয় কাৰণ তেওঁলোকে ভৱিষ্যতে হেক হোৱাৰ পৰা চিষ্টেমটোক সুৰক্ষিত কৰাৰ উদ্দেশ্যেৰে হেক কৰে।

খ) ব্লেক হেট হেকাৰ: ব্লেক হেট হেকাৰ হুৱাইট হেট হেকাৰৰ বিপৰীত। তেওঁলোকে চিষ্টেমৰ মালিকৰ অনুমতি অবিহনে কম্পিউটাৰ চিষ্টেম আৰু নেটৱৰ্কত অবৈধভাৱে হেক কৰে। তেওঁলোকৰ প্ৰধান উদ্দেশ্য হৈছে ব্যক্তিগত লাভৰ বাবে দুৰ্বলতাসমূহৰ সুবিধা লোৱা, আৰ্থিক চুৰি, ডাটা নষ্ট কৰা আৰু মেলৱেৰ বিয়পোৱা আদি এনে কাম হ'ব পাৰে।

গ) গ্ৰে হেট হেকাৰঃ গ্ৰে হেট হেকাৰ হৈছে এনে হেকাৰ যিয়ে কম্পিউটাৰ চিষ্টেম আৰু নেটৱৰ্কত চিষ্টেমৰ মালিকৰ অনুমতি অবিহনে হেক কৰে, কিন্তু বেয়া উদ্দেশ্যেৰে বা আৰ্থিক লাভৰ বাবে নকৰে। বেছিভাগ সময়তে সিহঁতে চিষ্টেমত হেক কৰে চিষ্টেমসমূহৰ সুৰক্ষা আৰু সুৰক্ষা স্তৰ পৰীক্ষা কৰিবলৈ আৰু সেই চিষ্টেমসমূহৰ প্ৰশাসকক চিষ্টেমৰ দুৰ্বলতাৰ বিষয়ে অৱগত কৰিবলৈ এই কাম কৰে।

২ চফ্টৱেৰ পাইৰেচি:

চফট্ ৱেৰ পাইৰেচিক কপিৰাইটযুক্ত চফ্টৱেৰৰ অবৈধ কপি আৰু অবৈধ বিতৰণ বুলিব পাৰি। যেতিয়া কোনো কপিৰাইটযুক্ত চফট্ ৱেৰ অবৈধভাৱে বিতৰণ কৰা হয়, তেতিয়া চফট্ ৱেৰৰ মালিকসকলে সেই চফট্ ৱেৰৰ বাবে ৰাজহ নাপায়। ইয়াৰ ফলত বৈধ ব্যৱহাৰকাৰীৰ বাবে চফট্ ৱেৰৰ মূল্যও বৃদ্ধি পাব পাৰে। ইয়াৰ বিৰুদ্ধে যুঁজিবলৈ বহুতো চফ্টৱেৰ কোম্পানীয়ে "পাইৰেচি বিৰোধী" অভিযান চলায় বা বেছিভাগ চফ্টৱেৰে এটা শেষ ব্যৱহাৰকাৰী অনুজ্ঞাপত্ৰ চুক্তি (EULA) পাইৰেচি প্ৰতিৰোধ কৰিবলৈ চফ্টৱেৰ ব্যৱহাৰৰ চৰ্তসমূহ অন্তৰ্ভুক্ত কৰে যিটো ব্যৱহাৰকাৰীয়ে সন্মত হ'ব লাগিব-

এতিয়া চফটৱেৰ পাইৰেচিৰ বিভিন্ন শ্ৰেণীসমূহ চাওঁ আহক-

ক) চফ্টলিফটিং : চফ্টলিফটিং তেতিয়া হয় যেতিয়া অনুজ্ঞাপত্ৰ চুক্তিৰ অধীনত ইয়াক ব্যৱহাৰ কৰিবলৈ অনুমোদিত নহয় কিন্তু কোনো প্ৰগ্ৰেম কোনোবা এজনৰ সৈতে শ্বেয়াৰ কৰা হয়। এনে অপৰাধৰ এটা সাধাৰণ উদাহৰণ হ'ল চফ্টৱেৰৰ এটা কপি ক্ৰয় কৰি অতিৰিক্ত অনুজ্ঞাপত্ৰ অবিহনে একাধিক কম্পিউটাৰত ইনষ্টল কৰা।

খ) OEM আনবাণ্ডলিং: OEM আনবাণ্ডলিঙত এটা নিৰ্দিষ্ট হাৰ্ডৱেৰৰ সৈতে মিলাই চফ্টৱেৰ বাণ্ডিলৰ অংশ হিচাপে বিক্ৰী কৰাৰ উদ্দেশ্য প্ৰস্তুত কৰা চফ্টৱেৰ অবৈধ ভাৱে পৃথকীকৰণ আৰু বিক্ৰী কৰা হয়। এই ব্যৱস্থাই অনুজ্ঞাপত্ৰৰ চুক্তিসমূহ উলংঘা কৰে আৰু উদ্দেশ্য প্ৰণোদিত ব্যৱহাৰকাৰী অভিজ্ঞতাক অধিক ফলপ্ৰসূ কৰি তুলিব নোৱাৰে।

গ) ইণ্টাৰনেট পাইৰেচি: ইণ্টাৰনেট পাইৰেচি বা অনলাইন পাইৰেচিৰ লগত ইণ্টাৰনেটৰ জৰিয়তে কপিৰাইটযুক্ত চফ্টৱেৰৰ অকৰ্তৃত্বশীল বিতৰণ জড়িত হৈ থাকে। ইয়াৰ ভিতৰত ৱেবছাইটসমূহত পাইৰেটেড চফ্টৱেৰ হ'ষ্ট কৰা, ইয়াক Peer-to-peer নেটৱৰ্কৰ জৰিয়তে শ্বেয়াৰ কৰা, বা প্ৰত্যক্ষ ডাউনলোড লিংক প্ৰদান কৰা আদি অন্তৰ্ভুক্ত হ'ব পাৰে।

ঘ) চফ্টৱেৰ নকল: চফ্টৱেৰ নকল হৈছে কপিৰাইটযুক্ত চফ্টৱেৰৰ অবৈধ নকল, বিতৰণ আৰু বিক্ৰী। মাইক্ৰ'ছফ্টৰ উইণ্ড'জ আৰু অফিচৰ দৰে সামগ্ৰীৰ চাহিদা বেছি হোৱাৰ বাবে সাধাৰণতে নকল কৰা হয়।

ঙ) **হাৰ্ড ডিস্ক লোডিং :** হাৰ্ড ডিস্ক লোডিং হয় যেতিয়া হাৰ্ডৱেৰৰ বিক্ৰেতাসকলে তেওঁলোকে বিক্ৰী কৰা কম্পিউটাৰত চফ্টৱেৰৰ অকৰ্তৃত্বশীল কপি ইনষ্টল কৰে, যাৰ ফলত তেওঁলোকৰ সামগ্ৰীসমূহ ক্ৰেতাৰ বাবে অধিক আকৰ্ষণীয় কৰি তোলে।

চ) ভাড়া দিয়া: ভাড়া লৈ অনুজ্ঞাপত্ৰপ্ৰাপ্ত চফট্ ৱেৰ অস্থায়ীভাৱে বিতৰণ কৰা হয়, অথচ যিসকলৰ ইয়াক ব্যৱহাৰ কৰাৰ সঠিক অনুজ্ঞাপত্ৰ নাই, তেওঁলোককো ইয়াক ব্যৱহাৰ কতিবলৈ দিয়া হয়। এই ব্যৱস্থাই বেছিভাগ চফ্টৱেৰৰ ভাড়া, লিজ, বা ঋণ দিয়া অনুজ্ঞাপত্ৰৰ চৰ্তসমূহ উলংঘা কৰে।

৩.৫.২ ব্যক্তি কেন্দ্ৰিক চাইবাৰ অপৰাধ

১. ডিজিটেল জালিয়াতি:

এনে জালিয়াতি হ'ল কোনো নথি ভুলকৈ বনোৱা আৰু পৰিৱৰ্তন কৰা বা আনকি জাল নথি ৰখাৰ প্ৰক্ৰিয়া। ডিজিটেল মাধ্যম ব্যৱহাৰ কৰি নথিপত্ৰ জাল কৰা প্ৰক্ৰিয়াকেই ডিজিটেল জালিয়াতি বুলিব পাৰি। ডিজিটেল জালিয়াতিৰ কিছুমান সাধাৰণ উদাহৰণ হ'ল স্বাক্ষৰ, নকল মুদ্ৰাৰ নোট, নকল মার্ক শ্বীট আদি। প্ৰিণ্টাৰ, কপিয়াৰ আৰু ইমেজ স্কেনাৰ আদি ডিজিটেল প্ৰযুক্তিৰ সহায়ত চাইবাৰ অপৰাধীয়ে পৰিচয় প্ৰমাণ, পাছপ'ৰ্ট আদি জাল নথি-পত্ৰ তৈয়াৰ কৰে।

ডিজিটেল জালিয়াতিৰ কিছুমান ভাগ চাওঁ আহক-

ক) নথিপত্ৰ জালিয়াতি: নথিপত্ৰ জালিয়াতিৰ লগত আইনী নথিপত্ৰৰ ওপৰত সংযোগ বিয়োগ, মেনিপুলেচন কৰা বা প্ৰতিলিপি কৰাটো জড়িত হৈ থাকে। সাধাৰণ উদাহৰণসমূহ হ'ল- জাল মার্ক শ্বীট, প্ৰমাণপত্ৰ, আৰু ৰাজহ ষ্টাম্প ইত্যাদি প্ৰস্তুত কৰা।

খ) নকল ধন জালিয়াতি: নকল ধন জালিয়াতিৰ লগত নোটৰ ডিজিটেল প্ৰতিলিপি কৰাটো সোমাই থাকে। অপৰাধীয়ে হাই-ৰিজ'লিউচন স্কেনাৰ আৰু প্ৰিণ্টাৰ ব্যৱহাৰ কৰি প্ৰকৃত আইনী টেণ্ডাৰৰ দৰে ভুৱা নোট প্ৰস্তুত কৰে।

গ) ডিজিটেল স্বাক্ষৰ জালিয়াতি: ডিজিটেল স্বাক্ষৰ জালিয়াতিৰ লগত ডিজিটেল মাধ্যম ব্যৱহাৰ কৰি ব্যক্তিৰ স্বাক্ষৰৰ অবৈধ প্ৰতিলিপি কৰাটো জড়িত হৈ থাকে। ইয়াত এটা প্ৰকৃত স্বাক্ষৰ স্কেন কৰি চফ্টৱেৰ ব্যৱহাৰ কৰি পিছত ইয়াক অন্য নথিপত্ৰত কপি কৰি, বা মূলৰ সৈতে মিল থকা স্বাক্ষৰ সৃষ্টি কৰা হয়।

ঘ) কলা জালিয়াতি: ডিজিটেল ক্ষেত্ৰত কলা জালিয়াতিৰ ভিতৰত শিল্পকর্মৰ প্ৰতিলিপি বা কোনো শিল্পকর্মৰ ওপৰত শিল্পীৰ স্বাক্ষৰ মিছা নমুনা লগোৱা কৰা হয়। চাইবাৰ অপৰাধীয়ে ডিজিটেল সঁজুলি ব্যৱহাৰ কৰি বিখ্যাত চিত্ৰকলাৰ পতিয়ন যোগ্য প্ৰতিৰূপ তৈয়াৰ কৰিব পাৰে বা কম পৰিচিত বা ভুৱা শিল্পকর্মত কোনো সুপৰিচিত শিল্পীৰ স্বাক্ষৰ যোগ কৰি ইয়াৰ মূল্য বৃদ্ধি কৰিব পাৰে।

২. চাইবাৰ সন্ত্ৰাসবাদ:

চাইবাৰ সন্ত্ৰাসবাদক কম্পিউটাৰ আৰু নেটৱর্ক ব্যৱহাৰ কৰি কৰা সন্ত্ৰাসবাদৰ কার্য্য বুলিব পাৰি। মূলতঃ ৰাজনৈতিক বা মতাদর্শগত লাভৰ বাবে আৰু ভুক্তভোগীক ভাবুকি আৰু

ভয় দেখুৱাবলৈ চাইবাৰ সন্ত্ৰাসবাদীয়ে এনে অপৰাধ কৰে। চাইবাৰ সন্ত্ৰাসবাদৰ ফলত সম্পদ, সম্পত্তি আৰু বহু সময়ত আনকি জীৱন হেৰুৱাবলগীয়াও হ'ব পাৰে। চাইবাৰ সন্ত্ৰাসবাদীয়েও এই সেৱাসমূহক বিশেষভাৱে লক্ষ্য কৰি চৰকাৰী সেৱাসমূহৰ বিফলতা সৃষ্টি কৰিবলৈ চেষ্টা কৰে। উদাহৰণ স্বৰূপে চিকিৎসা সেৱা, বৈদ্যুতিক আৰু সৌৰশক্তি কেন্দ্ৰ, বিমান আৰু ৰেল যাতায়ত নিয়ন্ত্ৰণ ব্যৱস্থা, আৰক্ষী আৰু সামৰিক সেৱা, যিকোনো অত্যাৱশ্যকীয় সেৱা আদি বেছিভাগ সময়তে চাইবাৰ সন্ত্ৰাসবাদীৰ মূল লক্ষ্য হৈ পৰে। চাইবাৰ সন্ত্ৰাসবাদৰ অন্যতম উদাহৰণ হৈছে ১৯৯৮ চনত সংঘটিত তামিল গেৰিলাই দুসপ্তাহৰ ভিতৰত প্ৰতিদিনে ৮০০টা ইমেইল প্ৰেৰণ কৰি শ্ৰীলংকাৰ দূতাবাসৰ বিৰুদ্ধে আক্ৰমণ চলাইছিল।

জানি থওক

চাইবাৰ ৰাৰফেয়াএ এটা জাতি বা ৰাষ্ট্ৰৰ বিৰুদ্ধে কম্পিউটাৰ প্ৰণালী আৰু নেটৱৰ্ক ব্যৱহাৰ কৰি এটা জাতি বা ৰাষ্ট্ৰৰ ক্ষতি কৰা বা কাৰু-কাৰ্য বিঘ্নিত কৰাৰ বুজায়। ইয়াক অৰ্থনৈতিক যুদ্ধ, গুপ্তচৰবৃত্তি, ধ্বংসাত্মক কাৰ্য, প্ৰচাৰ আৰু হস্তক্ষেপৰ দৰে বহুতো উদ্দেশ্যৰে কৰে।

৩. চাইবাৰ মানহানি:

মানহানিৰ সংজ্ঞা হ'ল কাৰোবাৰ বিষয়ে বেয়া বা মিছা কথা কৈ বা লিখি সুনাম ক্ষতি কৰা। যেতিয়া কোনো ব্যক্তিক চাইবাৰ স্পেচত বদনাম কৰা হয় তেতিয়া ইয়াক চাইবাৰ ডিফেমেচন বুলি কোৱা হয়। চাইবাৰ মানহানি কম্পিউটাৰ ব্যৱস্থা আৰু ইণ্টাৰনেট ব্যৱহাৰ কৰি কৰা মানহানি বুলি সংজ্ঞায়িত কৰিব পাৰি। উদাহৰণস্বৰূপে, যেতিয়া কোনো ব্যক্তিয়ে কোনো ৰেবছাইটত কাৰোবাৰ বিষয়ে মানহানিকাৰক বিষয় প্ৰকাশ কৰে তেতিয়া সেয়া হৈছে চাইবাৰ মানহানি। মানহানি মৌখিকভাৱে (নিন্দা) আৰু লিখিত ৰূপত (মানহানি) দুয়োটা দিশতে হ'ব পাৰে।

চাইবাৰ মানহানি নিয়ন্ত্ৰণ কৰিবলৈ দুটা উপায় আছে।

১) Cease and desist **পত্ৰ**: যি ক্ষেত্ৰত ব্যক্তিজনৰ বিৰুদ্ধে কোনো গুৰুতৰ ক্ষোভ নাথাকে, তেনে ক্ষেত্ৰত ডিজিটেল মাধ্যমৰ পৰা মানহানিকাৰক বার্তা আঁতৰোৱাৰ বাবে Cease and desist পত্ৰ পঠিয়াব পাৰে। এই পত্ৰখনে মানহানিকাৰক বিষয়বস্তু আঁতৰাই আৰু অধিক মানহানিকাৰক কার্য্য বন্ধ কৰাৰ বাবে দাবী জনায়।

২) **আইনী আশ্ৰয়:** যেতিয়া মানহানি ক্ষতি কৰাৰ গুৰুতৰ উদ্দেশ্যেৰে কৰা হয়, তেতিয়া আইনী আশ্ৰয় লোৱাৰ প্ৰয়োজন হ'ব পাৰে। অপৰাধীক শাস্তি দিবলৈ আইন ব্যৱহাৰ কৰিব পাৰে।

চাইবাৰ মানহানিয়ে ব্যক্তিজনৰ সুনামৰ ক্ষতি কৰাই নহয়, বিশেষকৈ ব্যক্তিজনে বিশিষ্ট পদবীত থাকিলে তেওঁলোকৰ পৰিয়াল, সংগঠন, আনকি জাতিটোকো নেতিবাচক প্ৰভাৱ পেলাব পাৰে। ভাৰতত মানহানিৰ বাবে দুই ধৰণৰ দায়বদ্ধতা আছে। প্ৰথম শ্ৰেণীত মানহানিকাৰক বাৰ্তা লিখা বা প্ৰকাশ কৰা ব্যক্তিসকল দায়ী। দ্বিতীয় শ্ৰেণীত মানহানিকাৰক বাৰ্তা প্ৰকাশৰ অনুমোদন দিয়া ইণ্টাৰনেট সেৱা প্ৰদানকাৰী আৰু অনুৰূপ সেৱা প্ৰদানকাৰীসকলো দায়ী।

১৩.৫.৩ মহিলা আৰু শিশুৰ বিৰুদ্ধে চাইবাৰ অপৰাধ

ডিজিটেল যুগত মহিলা আৰু শিশু কেন্দ্ৰিক চাইবাৰ অপৰাধ এক আতংকজনক বিষয় হৈ পৰিছে। ডিজিটেল ডিভাইচ আৰু অনলাইন প্লেটফৰ্মৰ উত্থানে অপৰাধীসকলৰ বাবে দুৰ্বল ব্যক্তিক লক্ষ্য কৰি লোৱাৰ নতুন সুযোগ সৃষ্টি কৰিছে, আৰু ই ভয়ংকৰ ৰূপ লৈছে। মহিলা আৰু শিশুৰসৈতে সংঘটিত হোৱা বিভিন্ন ধৰণৰ চাইবাৰ অপৰাধবোৰ চাওঁ আহক।

১. চাইবাৰ ষ্টাকিং:

ষ্টাকিং হৈছে ভুক্তভোগীক হাৰাশাস্তি কৰা কাৰ্য্য। ষ্টাকিংৰ ভিতৰত ভুক্তভোগীক অনুসৰণ কৰা, হাৰাশাস্তি কৰা ফোন কল কৰা, ভুক্তভোগীৰ সম্পত্তি ভাঙি পেলোৱা, ভুক্তভোগীয়ে বিচাৰি পোৱাৰ বাবে লিখিত বাৰ্তা বা বস্তু এৰি দিয়া আদি বিভিন্ন কাৰ্য্য অন্তৰ্ভুক্ত। যদিও যিকোনো ব্যক্তি চাইবাৰ ষ্টাকিঙৰ বলি হ'ব পাৰে, তথাপিও সাধাৰণতে মহিলাসকল চাইবাৰ ষ্টাকিঙৰ লক্ষ্য হৈ পৰে।

চাইবাৰ ষ্ট'কিঙৰ বহু ক্ষেত্ৰত ষ্ট'কাৰে বাৰে বাৰে অনলাইন মেছেজ আৰু ইমেইল প্ৰেৰণ কৰি হাৰাশাস্তি কৰি আহিছে। চাইবাৰ অপৰাধীয়ে গ্ৰুপ আৰু আলোচনা মঞ্চত বাৰ্তা প্ৰেৰণ কৰিও ভুক্তভোগীক হাৰাশাস্তি কৰে। অপৰাধীয়ে ফেচবুক, ইনষ্টাগ্ৰাম, টুইটাৰ আদি ছ'চিয়েল মিডিয়া এপ্লিকেচনৰ সহায়ত ভুক্তভোগীৰ দৈনন্দিন ৰুটিন ট্ৰেক কৰিবলৈ চেষ্টা কৰে। বেছিভাগ ভুক্তভোগীয়ে নিজৰ দৈনন্দিন ৰুটিন, ভ্ৰমণ কৰা ঠাই আৰু অংশগ্ৰহণ কৰা অনুষ্ঠানৰ লগতে লাইভ লকেচন ছ'চিয়েল মিডিয়াত আজিকালি শ্বেয়াৰ কৰে। এইটোৱে চাইবাৰ ষ্টাকাৰসকলৰ বাবে অনলাইন আৰু অফলাইন দুয়োটাতে ভুক্তভোগীক ষ্টাক কৰাটো অত্যন্ত সহজ কৰি তোলে। বহু সময়ত অনলাইন ষ্টাকাৰসকলেও অনলাইন ষ্টাকিঙৰ উপৰিও অফলাইন ষ্টাকিংৰ আশ্ৰয় লয়।

২. চাইবাৰ হাৰাশাস্তি:

চাইবাৰ হাৰাশাস্তি হৈছে ইণ্টাৰনেট আৰু ইলেক্ট্ৰনিক মাধ্যমৰ ব্যৱহাৰ কৰি কোনো শিশু, প্ৰাপ্তবয়স্ক, ব্যৱসায় বা গোটক প্ৰত্যক্ষ বা অন্তৰ্নিহিত শাৰীৰিক ক্ষতিৰ ভাবুকি নোহোৱাকৈ হাৰাশাস্তি, নিয়ন্ত্ৰণ, হেতালি খেলা। চাইবাৰ হাৰাশাস্তিৰ বাবে আইচিটিৰ ব্যৱহাৰ আৰু হয়তো কোনো ব্যক্তি, গোট বা সংস্থাৰ মৌখিক, যৌন, আৱেগিক বা সামাজিক নিৰ্যাতনৰ প্ৰয়োজন হয়। চাইবাৰ হাৰাশাস্তিৰ প্ৰধান লক্ষ্য হৈছে লক্ষ্য ভুক্তভোগীৰ ওপৰত ক্ষমতা আৰু নিয়ন্ত্ৰণ প্ৰয়োগ কৰা।

৩. চাইবাৰ গুণ্ডাগিৰি

চাইবাৰ গুণ্ডাগিৰি, অনলাইন পদ্ধতি বা ইলেক্ট্ৰনিক মাধ্যমেৰে বিশেষকৈ কিশোৰ-কিশোৰী আৰু শিশুৰ মাজত গুণ্ডাগিৰি কৰা কাৰ্য্য। ইয়াক "ছ'চিয়েল মিডিয়া, ইমেইল, টেক্সট মেছেজ আদিত বার্তা দি কাৰোবাক ভয় খুওৱা বা বিচলিত কৰা ক্ৰিয়া কলাপ" বুলি সংজ্ঞায়িত কৰিব পাৰি। চাইবাৰ গুণ্ডাগিৰিক অনলাইন গুণ্ডাগিৰি বুলিও কোৱা হয়।

ক'ভিড-১৯ মহামাৰীৰ পিছত আৰু ক'ভিড-১৯ মহামাৰীৰ সময়ত ছাত্ৰ-ছাত্ৰীসকলে অনলাইন শিক্ষণলৈ স্থানান্তৰিত হৈ পৰ্দাৰ সময় আৰু শিক্ষা আৰু সামাজিক যোগাযোগৰ বাবে ডিজিটেল প্লেটফৰ্মৰ ওপৰত নিৰ্ভৰশীলতাই চাইবাৰ দাদাগিৰিক ইন্ধন যোগাইছে। প্ৰায়ে সময়ত, ভুক্তভোগীসকলক অনলাইন গেমিং বা অন্যান্য জনপ্ৰিয় ছ'চিয়েল মিডিয়া চাইটৰ বাবে অনলাইন কমিউনিটি ফ'ৰামত ট্ৰ'ল কৰি প্ৰতিক্ৰিয়া আনিবলৈ বা কেতিয়াবা কেৱল চাইবাৰ গুণ্ডাগিৰি কৰাজনৰ আনন্দৰ বাবে কৰা হয়। বেছিভাগ ক্ষেত্ৰতে চাইবাৰ গুণ্ডাগিৰি কৰা ভুক্তভোগীয়ে অফলাইন জগতখনত কেতিয়াবা শাৰীৰিকভাৱেও গুণ্ডাগিৰিৰ সন্মুখীন হ'ব পাৰে। ভুক্তভোগীসকলে প্ৰায়ে আত্মসন্মান লাঘৱ হোৱা, মানসিক চাপৰ মাত্ৰা বৃদ্ধি আৰু গুৰুতৰ হতাশাত ভুগিবলগীয়া হয়।

৪. অনলাইন গ্ৰেডেচন:

অনলাইন গ্ৰেডেচন হৈছে এক প্ৰকাৰৰ চাইবাৰ অপৰাধ, য'ত বিভিন্ন অনলাইন প্লেটফৰ্মৰ জৰিয়তে দুৰ্বল ব্যক্তি, বিশেষকৈ শিশুক লক্ষ্য কৰা হয়। অপৰাধীসকলে প্ৰায়ে ইন্টাৰনেটৰ বেনামী আৰু সহজলভ্যতাৰ সুবিধা লৈ শোষণ আৰু পৰিচালনা কৰি তেওঁলোকৰ চিকাৰক যৌন শোষণ বা অন্যান্য ক্ষতিকৰ উদ্দেশ্যৰ বাবে ব্যৱহাৰ কৰে। তেওঁলোকে সামাজিক মাধ্যম, চেট ৰুম, অনলাইন গেমিং প্লেটফৰ্ম, বা মেছেজিং এপৰ জৰিয়তে নাবালকৰ সৈতে মিছা অজুহাতত

সম্পৰ্ক স্থাপন কৰে, আৰু ক্ৰমে তেওঁলোকৰ বিশ্বাস আৰু আত্মবিশ্বাস অৰ্জন কৰে। এই পৰিচালনাত প্ৰৱঞ্চনামূলক কৌশল ব্যৱহাৰ কৰা হব পাৰে, যেনে চিকাৰীজনৰ চিনাকি ব্যক্তি হিচাপে ভাও লোৱা বা মনোযোগ, উপহাৰ, বা মৰমৰ প্ৰতিশ্ৰুতি দিয়া। এবাৰ বিশ্বাস স্থাপন হ'লে, অপৰাধীসকলে তেওঁলোকৰ আচৰণ সলনি কৰে, চিকাৰক যৌন কাৰ্যত লিপ্ত হ'বলৈ, ছবি বা ভিডিঅ শ্বেয়াৰ কৰিবলৈ, বা ব্যক্তিগতভাৱে লগ হ'বলৈ বাধ্য কৰিব পাৰে।

৫. চাইবাৰ পৰ্ণগ্ৰাফী:

চাইবাৰ পৰ্ণোগ্ৰাফি মানে অনলাইনত যৌন বিষয়বস্তু সৃষ্টি কৰা, শ্বেয়াৰ কৰা বা পোষ্ট কৰা। এই বিষয়বস্তুত স্পষ্ট যৌন কাৰ্য্য দেখুওৱা ভিডিঅ', ছবি বা চলচ্চিত্ৰ আদি অন্তৰ্ভুক্ত থাকে, যিবোৰ বেছিভাগ মানুহে অনুচিত বুলি গণ্য কৰে। ইন্টাৰনেট আৰু আধুনিক প্ৰযুক্তিৰ বাবে এনে বিষয়বস্তু প্ৰৱেশ কৰা আৰু শ্বেয়াৰ কৰা বেছি সহজ হৈ পৰিছে। ইয়াৰ ফলত সমাজ, নৈতিকতা আৰু আইনৰ ওপৰত পৰা প্ৰভাৱ সম্পৰ্কে বহুতো উদ্বেগৰ সৃষ্টি হৈছে।

৬. যৌন নিৰ্যাতন:

"Sextortion" শব্দটো "sex" (যৌন) আৰু "extortion" (অতিশয্য) এই দুটা শব্দৰ মিশ্ৰণ। চেক্সটৰ্চন হৈছে এক প্ৰকাৰৰ চাইবাৰ অপৰাধ, য'ত অপৰাধীসকলে পীড়িতক তেওঁলোকৰ পৰা যৌন অনুগ্ৰহ বা অন্য কিছু দাবী আদায় কৰে। বহু ক্ষেত্ৰত, চেক্সটৰ্চনত অপৰাধীসকলে যদি তেওঁলোকৰ দাবীসমূহ পূৰণ নহয় তেতিয়া ব্যক্তিগত ছবি, ভিডিঅ' বা যৌন বিষয়বস্তু অনলাইনত শ্বেয়াৰ কৰাৰ ভাবুকি দিয়ে । বেছিভাগ ক্ষেত্ৰত, অপৰাধীসকলে যৌন অনুগ্ৰহ বা টকা দাবী কৰে। যদিও যিকোনো ব্যক্তিয়েই চেক্সটৰ্চনৰ বলি হ'ব পাৰে, কিন্তু সাধাৰণতে মহিলা আৰু শিশুবোৰক লক্ষ্য কৰি এই অপৰাধ সংঘটিত কৰা হয়।

৭. এআইয়ে সৃষ্টি কৰা ভাবুকি: ডিপ ফেকচ

অতি সম্প্ৰতি আটাইতকৈ উদ্বেগজনক বিকাশবোৰৰ ভিতৰত ডীপ ফেকৰ উত্থান অন্যতম। ডীপ ফেক হৈছে কৃত্ৰিম কিন্তু অতি বাস্তৱসম্মত অডিঅ', ছবি বা ভিডিঅ', যিবোৰ ডীপ লাৰ্নিং নামৰ উন্নত কম্পিউটাৰ প্ৰযুক্তিৰ সহায়ত সৃষ্টি কৰা হয়। এই প্ৰযুক্তিয়ে নিউৰেল নেটৱৰ্ক, বিশেষকৈ জেনেৰেটিভ এডভাৰচেৰিয়েল নেটৱৰ্ক (GANs) ব্যৱহাৰ কৰি ডিজিটেল বিষয়বস্তু সৃষ্টি বা সলনি কৰে। এই নেটৱৰ্কবোৰে বহু ছবি, ভিডিঅ' বা অডিঅ' অধ্যয়ন কৰি মানুহৰ চেহেৰা, মাত আৰু আচৰণৰ নমুনা শিকে। ইয়াৰ ফলত সিহঁতে বাস্তৱৰ লোকৰ অতি বিশ্বাসযোগ্য কিন্তু

মিছা ভিডিঅ' বা অডিঅ' সৃষ্টি কৰিব পাৰে। অপৰাধীসকলে ডীপ ফেক ব্যৱহাৰ কৰি মানুহক প্ৰতাৰণা কৰিব পাৰে, মিছা তথ্য বিয়পাব পাৰে বা বিভিন্ন ধৰণৰ ঠগবাজি আৰু সামাজিক ক্ষেত্ৰত আক্ৰমণ চলাব পাৰে। উদাহৰণস্বৰূপে, সিহঁতে এজন ব্যক্তিৰ মিছা ভিডিঅ' বনাব পাৰে, য'ত তেওঁ কেতিয়াও নকৰা কথা কোৱা বা কাম কৰা দেখুওৱা হয়। ইয়াৰ দ্বাৰা তেওঁৰ সুনাম নষ্ট কৰিব পাৰে বা আনক প্ৰতাৰণা কৰিব পাৰে।

৮. চাইবাৰ দাসত্ব:

চাইবাৰ দাসত্ব, যাক অনলাইন শোষণ বা ডিজিটেল দাসত্ব বুলিও কোৱা হয়, এয়া হৈছে ডিজিটেল প্ৰযুক্তি, বিশেষকৈ ইন্টাৰনেটৰ জৰিয়তে ব্যক্তিক জোৰদাৰী শ্ৰম, যৌন শোষণ বা আধুনিক দাসত্বৰ অন্যান্য ৰূপত শোষণ কৰা। চাইবাৰ দাসত্বৰ এটা সাধাৰণ ৰূপ হৈছে অনলাইন মানৱ অবৈধ সৰবৰাহ। সৰবৰহীসকলে ইন্টাৰনেটৰ বেনামী আৰু ব্যাপক প্ৰভাৱৰ সুবিধা লৈ দুৰ্বল ব্যক্তি, বিশেষকৈ মহিলা আৰু শিশুক প্ৰতাৰণা কৰি জোৰদাৰী শ্ৰম বা যৌন শোষণত ঠেলি দিয়ে। তেওঁলোকে চাকৰি, শিক্ষা বা প্ৰেমৰ মিছা প্ৰতিশ্ৰুতিৰ জৰিয়তে আকৰ্ষণ কৰে, কিন্তু শেষত তেওঁলোকক নিয়ন্ত্ৰণ, পৰিচালনা আৰু নিপীড়নৰ পৰিস্থিতিত আৱদ্ধ কৰি ৰাখে।

৯. চাইবাৰ অপহৰণ:

চাইবাৰ কিডনেপিং, যাক ভাৰ্চুৱেল কিডনেপিং বা অনলাইন কিডনেপিং বুলিও কোৱা হয়, হৈছে এক প্ৰকাৰৰ ধন দাবী য'ত অপৰাধীয়ে প্ৰতাৰণা আৰু মানসিক হেতালি খেলি ভুক্তভোগীক শোষণ কৰি মুক্তিপণৰ ধন উলিয়ায়। ব্যক্তিক শাৰীৰিকভাৱে অপহৰণ কৰাৰ দৰে ই নহয়, চাইবাৰ অপহৰণ সম্পূৰ্ণৰূপে অনলাইনত সংঘটিত হয় আৰু উদ্দেশ্যৰ বাবে ভাবুকি আৰু জোৰ-জবৰদস্তি কৰে। এটা সাধাৰণ চাইবাৰ অপহৰণ আঁচনিত অপৰাধীয়ে তেওঁলোকৰ ভুক্তভোগীক লক্ষ্য কৰি বিভিন্ন পদ্ধতি ব্যৱহাৰ কৰে, যেনে ফিছিং ইমেইল, ছ'চিয়েল ইঞ্জিনিয়াৰিং কৌশল, বা মেলৱেৰৰ সংক্ৰমণ। তেওঁলোকে প্ৰায়ে এনে ব্যক্তিক চিকাৰ কৰে যিসকল দুৰ্বল বা সহজে প্ৰতাৰিত হয়, যেনে সন্তান থকা পিতৃ-মাতৃ বা অকলে বাস কৰা বৃদ্ধ ব্যক্তি।



অগ্ৰগতি নিৰীক্ষণ কৰক

Q3. হুৱাইট, ব্লেক আৰু গ্ৰে হেট হেকাৰচ কি?

Q4. চাইবাৰ ষ্টাকিং কি বুজাই লিখক।

Q5. অনলাইন প্ৰেডেচন কি লিখক ।

Q6. ডিপ ফেকচ কি বুজাই লিখক।



৩.৬ অধ্যায়টিৰ পৰা আমি কি কি শিকিলোঁ

- চাইবাৰ অপৰাধক কম্পিউটাৰ আৰু নেটৱৰ্ক ব্যৱহাৰ কৰি সংঘটিত কৰা যিকোনো অপৰাধ বুলি সংজ্ঞায়িত কৰিব পাৰি।
- হেকিঙক আন ব্যক্তিৰ কম্পিউটাৰ চিষ্টেম বা নেটৱৰ্কত অবৈধ অনুপ্ৰৱেশ বুলিব পাৰি।
- ডিজিটেল মাধ্যম ব্যৱহাৰ কৰি নথিপত্ৰ জাল কৰা প্ৰক্ৰিয়াক ডিজিটেল জালিয়াতি বোলা হয়।
- চফট্ ৱেৰ পাইৰেচি হৈছে কপিৰাইটযুক্ত চফ্টৱেৰৰ অবৈধ কপি আৰু অবৈধ বিতৰণ।
- চাইবাৰ সন্ত্ৰাসবাদক কম্পিউটাৰ আৰু নেটৱৰ্ক ব্যৱহাৰ কৰি কৰা সন্ত্ৰাসবাদৰ কার্য্য বুলিব পাৰি।
- চাইবাৰ মানহানি হৈছে কম্পিউটাৰ ব্যৱস্থা আৰু ইণ্টাৰনেট ব্যৱহাৰ কৰি কৰা মানহানি।
- চাইবাৰষ্টাকিংক ইণ্টাৰনেট আৰু অনলাইন প্ৰযুক্তি ব্যৱহাৰ কৰি কৰা ষ্টাকিংৰ কার্য্য বুলি সংজ্ঞায়িত কৰিব পাৰি।
- চাইবাৰ হাৰাশাস্তি হৈছে ইণ্টাৰনেট আৰু ইলেক্ট্ৰনিক মাধ্যমৰ ব্যৱহাৰ কৰি কোনো শিশু, প্ৰাপ্তবয়স্ক, ব্যৱসায় বা গোটক প্ৰত্যক্ষ বা অন্তর্নিহিত শাৰীৰিক ক্ষতিৰ ভাবুকি নোহোৱাকৈ হাৰাশাস্তি, নিয়ন্ত্ৰণ, হেতালি খেলা বা অভ্যাসগতভাৱে অৱজ্ঞা কৰা।
- অনলাইন পদ্ধতি বা ইলেক্ট্ৰনিক মাধ্যমেৰে কৰা গুণ্ডাগিৰিৰ কার্য্যক চাইবাৰ বুলিং বোলে।
- চাইবাৰ পর্ণগ্ৰাফী মানে চাইবাৰ স্পেচ ব্যৱহাৰ কৰি পর্ণগ্ৰাফী প্ৰকাশ, বিতৰণ বা ডিজাইন কৰা।
- অনলাইন চিকাৰ হৈছে বিভিন্ন অনলাইন প্লেটফর্মৰ জৰিয়তে দুর্বল ব্যক্তি বিশেষকৈ শিশুক লক্ষ্য কৰি চাইবাৰ অপৰাধৰ এক প্ৰকাৰ।
- অপৰাধীয়ে ভুক্তভোগীক ভাবুকি দিয়া আৰু বিনিময়ত ভুক্তভোগীৰ পৰা যৌন অনুকূল ধন দাবী কৰা চাইবাৰ অপৰাধ।
- গভীৰ নকলত অতি বাস্তৱসন্মত, কিন্তু সম্পূর্ণৰূপে নির্মিত, অডিঅ', ছবি বা ভিডিঅ' বিষয়বস্তু সৃষ্টি কৰা জড়িত যিবোৰ ব্যক্তিক প্ৰতাৰণা বা হেঁচা মাৰি ধৰিব পৰা যায়।
- শ্ৰম , যৌন শোষণ বা অন্যান্য ধৰণৰ আধুনিক দাসত্বৰ বাবে শোষণ কৰিবলৈ ডিজিটেল প্ৰযুক্তি, বিশেষকৈ ইণ্টাৰনেটৰ ব্যৱহাৰক বুজায়।

- চাইবাৰ কিডনেপিং, যাক ভাৰ্চুৱেল কিডনেপিং বা অনলাইন কিডনেপিং বুলিও কোৱা হয়, হৈছে এক প্ৰকাৰৰ ধন দাবী য'ত অপৰাধীয়ে প্ৰতাৰণা আৰু মানসিক হেতালি খেলি ভুক্তভোগীক শোষণ কৰি মুক্তিপণৰ ধন উলিয়ায়।

৩.৭ অগ্ৰগতিৰ খতিয়ান

প্ৰশ্ন ১ ৰ উত্তৰ: চাইবাৰ অপৰাধক এনে এক অবৈধ কাৰ্য্য বুলি ধৰা হয় য'ত কম্পিউটাৰ বা যোগাযোগ যন্ত্ৰ বা কম্পিউটাৰ নেটৱৰ্ক ব্যৱহাৰ কৰি অপৰাধ সংঘটিত কৰা বা সংঘটিত কৰাত সহায় কৰা হয়।

প্ৰশ্ন ২ৰ উত্তৰ: লক্ষ্যৰ ওপৰত ভিত্তি কৰি চাইবাৰ অপৰাধৰ শ্ৰেণীসমূহ হ'ল-

- প্ৰতিষ্ঠান বা চৰকাৰৰ বিৰুদ্ধে অপৰাধ
- ব্যক্তিৰ বিৰুদ্ধে অপৰাধ
- সম্পত্তিৰ বিৰুদ্ধে অপৰাধ
- সমাজৰ বিৰুদ্ধে অপৰাধ

প্ৰশ্ন ৩ৰ উত্তৰঃ সাধাৰণতে লক্ষ্য ব্যৱস্থাৰ মালিকে নিজৰ কম্পিউটাৰ চিষ্টেম আৰু নেটৱৰ্কত দুৰ্বলতা বিচাৰিবলৈ নিয়োগ কৰা হেকাৰক হুৱাইট হেট হেকাৰ বোলা হয়। অবৈধভাৱে কম্পিউটাৰ চিষ্টেম আৰু নেটৱৰ্কত হেক কৰা হেকাৰক ব্লেক হেট হেকাৰ বুলি কোৱা হয়। গ্ৰে হেট হেকাৰ হ'ল এনে হেকাৰ যিয়ে চিষ্টেমৰ মালিকৰ অনুমতি অবিহনে কম্পিউটাৰ চিষ্টেম আৰু নেটৱৰ্কত হেক কৰে কিন্তু বেয়া উদ্দেশ্যেৰে বা আৰ্থিক লাভৰ বাবে তেনে নকৰে।

প্ৰশ্ন ৪ৰ উত্তৰ: চাইবাৰষ্টাকিঙক ইণ্টাৰনেট আৰু অনলাইন প্ৰযুক্তি ব্যৱহাৰ কৰি কৰা ষ্টাকিঙৰ কাৰ্য্য বুলিব পাৰি। চাইবাৰষ্টাকিঙক ইণ্টাৰনেট বা অন্যান্য ইলেক্ট্ৰনিক মাধ্যমৰ ব্যৱহাৰ কৰি ভুক্তভোগীক ভয় খুৱাই হাৰাশাস্তি কৰা হয়।

প্ৰশ্ন ৫ৰ উত্তৰ: অনলাইন চিকাৰ হৈছে বিভিন্ন অনলাইন প্লেটফৰ্মৰ জৰিয়তে দুৰ্বল ব্যক্তি বিশেষকৈ শিশুক লক্ষ্য কৰি কৰা চাইবাৰ অপৰাধ।

প্ৰশ্ন ৬ ৰ উত্তৰঃ ডিপ ফেকত অতি বাস্তৱসন্মত, অডিঅ', ছবি বা ভিডিঅ' বিষয়বস্তু সৃষ্টি কৰা জড়িত যিবোৰ ব্যক্তিক প্ৰতাৰণা বা অতিশৰ্য্য কৰা হয়।



৩.৮ অধিক জানিবলৈ

1) https://en.wikiversity.org/wiki/Digital_Media_Concepts/Cyber_Crimes
2) https://www.javatpoint.com/types-of-hackers
3) https://www.legalservicesindia.com/article/365/Historical-Perspective-of-Terrorism-&-Cyber-Terrorism.html
4) https://blog.ccasociety.com/cyber-defamation/
5) https://cs.stanford.edu/people/eroberts/cs181/projects/1999-00/software-piracy/types.html
6) https://ipredator.co/cyber-harassment/
7) https://en.wikipedia.org/wiki/Cyberbullying
8) https://www.oxfordlearnersdictionaries.com/definition/english/cyberbullying?q=cyberbullying
9) https://blog.ipleaders.in/cyber-pornography/



৩.৯ আৰ্হি প্ৰশ্ন

প্ৰশ্ন ১। চাইবাৰ অপৰাধৰ সংজ্ঞা দিয়ক। চাইবাৰ অপৰাধৰ শ্ৰেণীসমূহ বৰ্ণনা কৰক।

প্ৰশ্ন ২। মহিলা আৰু শিশুৰসৈতে সংঘটিত হোৱা চাইবাৰ অপৰাধৰ বৰ্ণনা কৰক।

প্ৰশ্ন ৩। কম্পিউটাৰ আৰু মোবাইলক লক্ষ্য সংঘটিত হোৱা চাইবাৰ অপৰাধৰ বৰ্ণনা কৰক।

প্ৰশ্ন ৪। বিভিন্ন ধৰণৰ চফটৱেৰ পাইৰেচিৰ বিষয়ে ব্যাখ্যা কৰক।

প্ৰশ্ন ৫। ডিজিটেল জালিয়াতিৰ বিভিন্ন ধৰণৰ বিষয়ে ব্যাখ্যা কৰা।

প্ৰশ্ন ৬। চাইবাৰ সন্ত্ৰাসবাদ আৰু চাইবাৰ যুদ্ধৰ সহায়ত এখন দেশক কেনেকৈ আক্ৰমণ কৰা হয় বুজাই লিখক।

প্ৰশ্ন ৭। হেকিঙৰ সংজ্ঞা দিয়ক। বিভিন্ন ধৰণৰ হেকিং কি কি?

প্ৰশ্ন ৮। চাইবাৰ হাৰাশাস্তি আৰু চাইবাৰ গুণ্ডাগিৰিৰে কিদৰে মহিলা আৰু শিশুক ভাবুকি দিয়া হয়?

প্ৰশ্ন ৯। মহিলাক লক্ষ্য কৰি কেনেকৈ ডিপ ফেক ব্যৱহাৰ কৰা হয় বুজাই দিয়ক।

প্ৰশ্ন ১০। চাইবাৰ দাসত্ব আৰু চাইবাৰ অপহৰণ কি?

****

অধ্যায় ৪: চাইবাৰ অপৰাধ (দ্বিতীয় খণ্ড)

অধ্যায় গাঁথনি

৪.১ উদ্দেশ্য

৪.২ পৰিচয়

৪.৩ আর্থিক প্ৰৱঞ্চনা

- ৪.৩.১ পৰিচয় জালিয়াতি
- ৪.৩.২ বিনিয়োগ জালিয়াতি
- ৪.৩.৩ গণ বিপণন জালিয়াতি
- ৪.৩.৪ ইণ্টাৰনেট বেংকিং জালিয়াতি
- ৪.৩.৫ ইউপিআই পেমেণ্ট গেটৱে জালিয়াতি
- ৪.৩.৬ এটিএম ক্লনিং
- ৪.৩.৭ চিম ক্লনিং

৪.৪ চচিয়েল ইঞ্জনীয়াৰিং আক্ৰমণ

- ৪.৪.১ ফিছিং
- ৪.৪.২ বেইটিং
- ৪.৪.৩ ৰাটাৰ হলিং
- ৪.৪. ৪ অজুহাত
- ৪.৪.৫ কুইড প্ৰ' ক্যু
- ৪.৪.৬ টেইলগেটিং
- ৪.৪.৭ অনুকৰণ

৪.৫ মেলৱেৰ

৪.৬ জিৰ' ডে আক্ৰমণ

৪.৭ জিৰ' ক্লিক আক্ৰমণ

৪.৮ অধ্যায়টিৰ পৰা আমি কি কি শিকিলোঁ

৪.৯ অগ্ৰগতিৰ খতিয়ান

৪.১০ অধিক জানিবলৈ

৪.১১ আৰ্হি প্ৰশ্ন

৪.১ উদ্দেশ্য

এই অধ্যায়ৰ আলোচনাৰ পাছত আপুনি –

- বিত্তীয় জালিয়াতি আৰু চচিয়েল ইঞ্জনীয়াৰিং আক্রমণৰ সংজ্ঞা দিব পাৰিব
- বিভিন্ন আর্থিক প্ররঞ্চনাৰ বর্ণনা কৰিব পাৰিব
- বিভিন্ন চচিয়েল ইঞ্জনীয়াৰিং আক্রমণৰ বর্ণনা কৰিব
- মেলৱেৰ আৰু ইয়াৰ বিভিন্ন শ্রেণীসমূহ বুজিব পাৰিব
- জিৰ' ডে আক্রমণে কেনেকৈ কাম কৰে বর্ণনা কৰিব পাৰিব
- জিৰ' ক্লিক আক্রমণ কি বুজিব পাৰিব

৪.২ পৰিচয়

পূর্বৰ অধ্যায়টোত আমি চাইবাৰ অপৰাধৰ বিষয়ে জানিব পাৰিছো আৰু চাইবাৰ অপৰাধৰ বিভিন্ন শ্রেণীৰ বিষয়ে বুজিব পাৰিছোঁ। ব্যক্তিক লক্ষ্য কৰি বিশেষভাৱে মহিলা আৰু শিশুক লক্ষ্য কৰি লোৱা বহুতো ভিন্ন ধৰণৰ চাইবাৰ অপৰাধৰ যেনে চাইবাৰ ষ্টাকিং, চাইবাৰ গুণ্ডাগিৰি আদিৰ বিষয়ে জানিব পাৰিছো। একেদৰে আমাৰ কম্পিউটাৰ আৰু মোবাইল ফোন হেক কৰা বিভিন্ন ধৰণৰ চাইবাৰ অপৰাধৰ বিষয়েও আমি জানিব পাৰিছো।

এই অধ্যায়ত আমি বিভিন্ন বিত্তীয় প্ররঞ্চনাৰ বিষয়ে জানিব পাৰিম। আমি বিভিন্ন চচিয়েল ইঞ্জনীয়াৰিং আক্রমণৰ বিষয়েও জানিব পাৰিম। এই অধ্যায়ত বিভিন্ন ধৰণৰ মেলৱেৰৰ বিষয়েও বিতংভাৱে আলোচনা কৰা হৈছে। জিৰ' দিনৰ আক্রমণ আৰু জিৰ' ক্লিক আক্রমণৰ দৰে চাইবাৰ অপৰাধৰ বিষয়েও এই অধ্যায়ত আলোচনা কৰা হৈছে। পৰৱর্তী অধ্যায়ত আমি বিভিন্ন চাইবাৰ অপৰাধৰ সৈতে মোকাবিলা কৰিবলৈ ব্যৱহাৰ কৰিব পৰা চাইবাৰ আইনসমূহৰ বিষয়ে জানিব পাৰিম।

৪.৩ আর্থিক প্ররঞ্চনা

যেতিয়া ব্যক্তি বা সংস্থাই প্রতাৰণামূলক, বিভ্রান্তিকৰ আৰু অবৈধ কার্য্যৰ জৰিয়তে আমাৰ ধনৰ পৰা বঞ্চিত কৰে বা আমাৰ আর্থিক ক্ষতি কৰে তাকেই **আর্থিক প্ররঞ্চনা** বুলি কোৱা হয়। আমি বিভিন্ন ধৰণৰ আর্থিক প্ররঞ্চনাৰ বিষয়ে জানিব লাগিব যাতে আমি এই অপৰাধৰ পৰা নিজকে বচাই চলিব পাৰো।

আর্থিক জালিয়াতিৰ কিছুমান উপায় হ'ল-

- পৰিচয় জালিয়াতি
- বিনিয়োগ জালিয়াতি
- গণ বিপণন জালিয়াতি
- ইণ্টাৰনেট বেংকিং জালিয়াতি
- ইউপিআই পেমেণ্ট গেটৱে জালিয়াতি
- এটিএম ক্লু'নিং
- চিম ক্লু'নিং

এই আর্থিক প্ৰৱঞ্চনাৰ প্ৰতিটোকে বিতংভাৱে চাওঁ আহক।

৪.৩.১ পৰিচয় জালিয়াতি

পৰিচয় জালিয়াতি হৈছে কোনো অপৰাধীয়ে আন ব্যক্তিৰ ব্যক্তিগত তথ্য চুৰি বা ব্যৱহাৰ কৰি তেওঁলোকৰ অনুমতি অবিহনে আর্থিক জালিয়াতি কৰা অপৰাধ। অপৰাধীয়ে সাধাৰণতে ধন, ঋণ বা আন কোনো আর্থিক সুবিধা লাভৰ বাবে ভুক্তভোগীৰ পৰিচয় ব্যৱহাৰ কৰে।

বেছিভাগেই চুৰি হোৱা তথ্য আর্থিক বিষয়ৰ লগত সংযুক্ত- যেনে বেংক একাউণ্ট নম্বৰ আৰু সবিশেষ, ক্ৰেডিট কার্ড, ডেবিট কার্ড, ডিজিটেল পেমেণ্টৰ তথ্য, এটিএম পিন আদি ভুক্তভোগীৰ বেংক একাউণ্টৰ পৰা জালিয়াতিৰে উলিওৱাৰ বাবে। চুৰি হোৱা তথ্যসমূহ অনন্য বা চিনাক্তকৰণকাৰী ব্যক্তিগত তথ্য যেনে পেন, আধাৰ নম্বৰ আদিও হ'ব পাৰে। এই তথ্যৰ সহায়ত নতুন বেংক বা ক্ৰেডিট কার্ড একাউণ্ট খুলিব পাৰে আৰু সকলো চার্জৰ বাবে ভুক্তভোগীক জগৰীয়া কৰিব পাৰে। পৰিচয় জালিয়াতিৰ ফলত চিবিআইএল স্ক'ৰ বা ক্ৰেডিট স্ক'ৰ কম হ'ব পাৰে যিয়ে ভুক্তভোগীৰ আর্থিক সমস্যাত পেলাব পাৰে।

৪.৩.২ বিনিয়োগ জালিয়াতি

বিনিয়োগ জালিয়াতি হৈছে এনে এটা অপৰাধ য'ত অপৰাধীয়ে মানুহক একেবাৰে সম্ভাৱনা শূন্য বা কেতিয়াও অস্তিত্বও নথকা আঁচনিত বিনিয়োগ কৰিবলৈ পতিয়ন নিয়ায় । অপৰাধীয়ে সাধাৰণতে ভুক্তভোগীক এই আঁচনিবোৰ ভুৱা আৰু বিভ্ৰান্তিকৰ তথ্যৰে বিক্ৰী কৰে যাৰ ফলত বহুত বেছি লাভ কৰে। বেছিভাগ ক্ষেত্ৰতে বিনিয়োগ কৰাৰ লগে লগেই অপৰাধীয়ে ভুক্তভোগীৰ সৈতে যোগাযোগ বন্ধ কৰি দিয়ে।

বিনিয়োগৰ সাধাৰণ প্ৰৱঞ্চনাৰ কিছুমান হ'ল-

- **পঞ্জি আঁচনি:** এই ধৰণৰ বিনিয়োগ জালিয়াতিত অপৰাধীয়ে নতুন বিনিয়োগকাৰীৰ পৰা ধন সংগ্ৰহ কৰি বৰ্তমানৰ বিনিয়োগকাৰীক ধন সংগ্ৰহ কৰে। আঁচনিখনৰ অন্ত পৰে যেতিয়া কোনো নতুন বিনিয়োগকাৰীয়ে যোগদান নকৰে আৰু আঁচনিকাৰে পুৰণি বিনিয়োগকাৰীক ঘূৰাই নিদিয়াকৈ বাকী থকা ধন ৰাখে।
- **পিৰামিড আঁচনি:** পিৰামিড আঁচনিসমূহে পূৰ্বৰ বিনিয়োগকাৰীৰ বাবে লাভৰ সৃষ্টি কৰিবলৈ নতুন অংশগ্ৰহণকাৰী নিযুক্তিৰ ওপৰত নিৰ্ভৰ কৰে, সম্ভাব্য নিযুক্তিৰ পুল শেষ হোৱাৰ বাবে আঁচনিখন অৱশেষত বিফল হয়।
- **অগ্ৰিম মাচুল জালিয়াতি:** এই আঁচনিত ভুক্তভোগীক আগতীয়া ধনৰ বিনিময়ত বৃহৎ পৰিমাণৰ ধন বা অন্যান্য উচ্চ মূল্যৰ সামগ্ৰী দিয়াৰ প্ৰতিশ্ৰুতি দিয়া হয়। প্ৰাৰম্ভিক মাচুলক প্ৰায়ে প্ৰক্ৰিয়াকৰণ মাচুল, কৰ বা আন কোনো অজুহাত হিচাপে ব্যাখ্যা কৰা হয়।
- **পাম্প এণ্ড ডাম্প জালিয়াতি:** বিনিয়োগকাৰীয়ে আজিকালি ইণ্টাৰনেট আৰু ছ'চিয়েল মিডিয়া ব্যৱহাৰ কৰি কিছুমান ষ্টকক অধিক লাভজনক যেন দেখুৱাই কোনটো ষ্টক কিনিব আৰু নিজৰ ধন ক'ত বিনিয়োগ কৰিব সেই সিদ্ধান্তক প্ৰভাৱিত কৰে। ইয়াৰ লগত মিছা বা বিভ্ৰান্তিকৰ বক্তব্যৰ জৰিয়তে ষ্টকৰ মূল্য বৃদ্ধি কৰাটো জড়িত হৈ থাকে।

৪.৩.৩ গণ বিপণন জালিয়াতি

গণ বিপণন জালিয়াতি হৈছে এক প্ৰকাৰৰ আৰ্থিক অপৰাধ যিয়ে গণসংযোগ মাধ্যম, যেনে ইমেইল, ছ'চিয়েল মিডিয়া, টেলিমাৰ্কেটিং, অনলাইন বিজ্ঞাপন আদিৰ জৰিয়তে বৃহৎ সংখ্যক সম্ভাব্য ভুক্তভোগীক লক্ষ্য কৰি লয়।

গণ বিপণন জালিয়াতিৰ কিছুমান সাধাৰণ প্ৰকাৰ হ'ল-

- **লটাৰী জালিয়াতি:** এই ধৰণৰ প্ৰৱঞ্চনাত ভুক্তভোগীক জনোৱা হয় যে তেওঁলোকে (কেতিয়াও প্ৰৱেশ নকৰা) লটাৰীত জয়ী হৈছে। পুৰস্কাৰ দাবী কৰিবলৈ তেওঁলোকক আগতেই মাচুল বা কৰ দিবলৈ নিৰ্দেশ দিয়া হয় কিন্তু এবাৰ ধন পৰিশোধ কৰিলে পুৰস্কাৰ কেতিয়াও নিদিয়ে।
- **ৰোমাঞ্চ কেলেংকাৰী:** এই কেলেংকাৰীত প্ৰৱঞ্চকে ডেটিং চাইট বা ছ'চিয়েল মিডিয়াত ভুৱা প্ৰফাইল সৃষ্টি কৰি ভুক্তভোগীৰ সৈতে ৰোমান্টিক সম্পৰ্ক স্থাপন কৰি ভুক্তভোগীক

অতিশার্য্য কৰি ৰচনা কৰা জৰুৰীকালীন বা ভ্ৰমণ খৰচৰ বাবে ধন প্ৰেৰণ কৰিবলৈ বাধ্য কৰে।

- **অনলাইন শ্বপিং আৰু নিলাম জালিয়াতি :** এই জালিয়াতিত প্ৰৱঞ্চকে অস্তিত্বহীন বা ভুলকৈ উপস্থাপন কৰা সামগ্ৰীৰ বাবে ভুৱা অনলাইন ষ্ট'ৰ বা নিলামৰ তালিকা সৃষ্টি কৰে। কেতিয়াও ডেলিভাৰী নোহোৱা বা বিজ্ঞাপনত দিয়াতকৈ কম মূল্যৰ সামগ্ৰীৰ বাবে ভুক্তভোগীয়ে ধন দিয়ে।
- **চেৰিটি জালিয়াতি:** এই প্ৰৱঞ্চনাত ব্যক্তিসকলৰ সদিচ্ছা প্ৰৱঞ্চকে ভুৱা চেৰিটি সংস্থাৰ বাবে অনুদান লৈ শোষণ কৰে যদিও ধনখিনি আৰ্তজনৰ ওচৰলৈ নহয়, পোনপটীয়াকৈ স্কেমাৰৰ হাতলৈ যায়।

৪.৩.৪ ইণ্টাৰনেট বেংকিং জালিয়াতি

ইণ্টাৰনেট বেংকিং আধুনিক বিত্তীয় লেনদেনৰ এক অবিচ্ছেদ্য অংগ হৈ পৰিছে, বিল পৰিশোধ, সামগ্ৰী ক্ৰয় আৰু ধন স্থানান্তৰ কৰাৰ সুবিধাজনক উপায় প্ৰদান কৰিছে। ইয়াৰ সহজ ব্যৱহাৰ আৰু সময় ৰাহি কৰা বৈশিষ্ট্যই ইয়াক বহুতৰে বাবে পছন্দৰ পদ্ধতি কৰি তুলিছে, যাৰ ফলত বেংকলৈ সশৰীৰে যোৱাৰ প্ৰয়োজনীয়তা নাইকিয়া হৈছে। কিন্তু ইণ্টাৰনেট বেংকিঙৰ ওপৰত ক্ৰমাৎ নিৰ্ভৰশীলতা বৃদ্ধি পোৱাৰ ফলত অনলাইন বেংকিঙৰ জালিয়াতিও বৃদ্ধি পাইছে।

ইণ্টাৰনেট বেংকিং জালিয়াতি বা অনলাইন বেংকিং জালিয়াতিত অপৰাধীয়ে ভুক্তভোগীক প্ৰতাৰণা কৰিবলৈ ইণ্টাৰনেট বা অনলাইন প্ৰযুক্তি ব্যৱহাৰ কৰে। ইয়াৰ লগত ভুক্তভোগীৰ অনুমতি অবিহনে ভুক্তভোগীৰ ধন বিভিন্ন বেংক একাউণ্টলৈ স্থানান্তৰ কৰে। অনলাইন বেংকিং জালিয়াতিৰ পৰা ৰক্ষা পোৱাৰ অন্যতম পদ্ধতি হ'ল বেংকসমূহে তেওঁলোকৰ অনলাইন বেংকিং পৰ্টেলত প্ৰদান কৰা ভাৰ্চুৱেল কিবৰ্ড ব্যৱহাৰ কৰা।

৪.৩.৪ ইউপিআই পেমেণ্ট গেটৱে জালিয়াতি

ইউপিআই আটাইতকৈ বেছি ব্যৱহৃত পেমেণ্ট পদ্ধতি হিচাপে পৰিগণিত হৈ পৰিছে। UPI ঠিকনা হৈছে এজন ব্যৱহাৰকাৰীক দিয়া এটা অনন্য ভাৰ্চুৱেল চিনাক্তকৰণ ঠিকনা। ই ব্যৱহাৰকাৰীৰ নাম @bank ৰ প্ৰাথমিক নাম অনুসৰি দিয়ে । ইউজাৰনেম কোনো ব্যক্তিৰ নাম বা তেওঁলোকৰ মোবাইল ফোন নম্বৰ হ'ব পাৰে। উদাহৰণস্বৰূপে, 94351xxxxx@icici য়ে 94351xxxxxx মোবাইল নম্বৰৰ এজন ব্যৱহাৰকাৰীক বুজায় যাৰ আইচিআইচিআই বেংকত একাউণ্ট আছে।

ইউপিআইৰ কিছুমান সাধাৰণ জালিয়াতি চাওঁ আহক:

QR ক'ড স্কেনিং কেলেংকাৰী: এই কেলেংকাৰীত প্ৰৱঞ্চকে ভুৱা QR ক'ড সৃষ্টি কৰে আৰু ভুক্তভোগীক ছলনাৰে স্কেনিং কৰায়, যাৰ ফলত মিছাকৈ ধন পৰিশোধ কৰোৱায়।

ভুৱা পেমেণ্ট চাইট: এই কেলেংকাৰীত ভুক্তভোগীক বৈধ পেমেণ্ট পৰ্টেল অনুকৰণ কৰা ভুৱা ৱেবছাইটলৈ প্ৰলোভিত কৰা হয়, যাৰ ফলত ব্যৱহাৰকাৰীয়ে তেওঁলোকৰ ইউপিআই আইডি দিবলৈ বাধ্য কৰায়।

দূ�ৰৱর্তী প্ৰৱেশ জালিয়াতি: দূৰৱর্তী প্ৰৱেশ জালিয়াতিত ভুক্তভোগীসকলে দূৰৱর্তী নিয়ন্ত্ৰণ এপ্লিকেচন ডাউনলোড কৰিবলৈ পতিয়ন নিয়ায় যাৰু প্ৰৱঞ্চকে ভুক্তভোগীৰ মোবাইল ডিভাইচত প্ৰৱেশ লাভ কৰে। এপটো ইনষ্টল হ'লেই প্ৰৱঞ্চকে ভুক্তভোগীৰ ডিভাইচটো দূৰৈৰ পৰা নিয়ন্ত্ৰণ কৰিব পাৰে, য'ত ইউপিআই এপসমূহত প্ৰৱেশ কৰা আৰু ভুক্তভোগীৰ অজ্ঞাতে লেনদেনৰ অনুমোদন দিয়া আদি সম্ভৱপৰ হৈ পৰে।

৪.৩.৫ এটিএম ক্লে'নিং

এটিএম ক্লে'নিঙত অপৰাধীয়ে ভুক্তভোগীৰ এটিএম কার্ড ক্লে'ন কৰিবলৈ চেষ্টা কৰে। এটিএম কার্ডৰ ক্লে'ন কৰিবলৈ এটিএম কার্ডৰ মেগনেটিক ষ্ট্ৰাইপ স্কেন কৰিবলৈ বিভিন্ন ধৰণৰ মেচিন সংলগ্ন কৰা হয়। ভুক্তভোগীৰ এটিএম কার্ডৰ পিন লাভ কৰিবলৈ এটিএমৰ প্ৰকৃত কিপেডৰ ওপৰতো ভুৱা কিপেড ব্যৱহাৰ কৰা হয়। এই সকলোবোৰ কৰিবলৈ অপৰাধীসকলে এ টি এম কার্ডৰ মেগনেটিক ষ্ট্ৰাইপ স্কেনিং আৰু কপি কৰাৰ বাবে মেচিন আৰু ব্যৱহাৰকাৰীৰ পিন ধৰি ৰখাৰ বাবে কেমেৰা আৰু ভুক্তভোগীৰ সকলো তথ্য সংৰক্ষণ কৰিবলৈ মেম'ৰী কার্ড ব্যৱহাৰ কৰে।

৪.৩.৬ চিম ক্লে'নিং

চিম ক্লে'নিং হৈছে আন এক প্ৰকাৰৰ চাইবাৰ অপৰাধ য'ত ভুক্তভোগীৰ চিম কার্ড ক্লে'ন কৰি আর্থিক জালিয়াতি কৰা হয়। এই ধৰণৰ প্ৰৱঞ্চনাত মূল চিম কার্ডখন ডুপ্লিকেট চিম কার্ড পাবলৈ কপি কৰা হয়। ফিছিং আদিৰ দৰে ছ'চিয়েল ইঞ্জিনিয়াৰিঙৰ আক্ৰমণ ব্যৱহাৰ কৰি এই কাম কৰিব পাৰি। চিম কার্ডখন সফলভাৱে ক্লে'ন কৰিলেই অপৰাধীয়ে ভুক্তভোগীৰ ব্যক্তিগত

তথ্য আৰু বেংক একাউণ্টৰ সবিশেষত প্ৰৱেশ কৰি পাছৱৰ্ড আৰু পিন ৰিছেট কৰি ভুক্তভোগীৰ পৰা ধন লাভ কৰিব পাৰে।

৪.৪ চচিয়েল ইঞ্জনীয়াৰিং আক্ৰমণ

চচিয়েল ইঞ্জনীয়াৰিং আক্ৰমণত মানুহৰ পাৰস্পৰিক ক্ৰিয়া-কলাপ আৰু আৱেগৰ সৈতে হেতালি খেলা জড়িত ক্ষতিকাৰক কার্য্য জড়িত হৈ থাকে। ইয়াত সাধাৰণতে ভুক্তভোগীক ভুল কৰিবলৈ বা স্পৰ্শকাতৰ তথ্য প্ৰকাশ কৰিবলৈ প্ৰতাৰণা কৰা হয়। বহু ক্ষেত্ৰত ভুক্তভোগীক গোপনীয় তথ্য প্ৰকাশৰ বাবে ছলনা কৰা হয় বা জৰুৰীকালীনতা, ভয় আদি আৱেগ জগাই তুলি ক্ষতিকাৰক লিংক ক্লিক কৰা বা ক্ষতিকাৰক ফাইল খোলাৰ বাবে ছলনা কৰা হয়। ছ'চিয়েল ইঞ্জিনিয়াৰিঙৰ আক্ৰমণ প্ৰতিৰোধ কৰাটো কঠিন যিহেতু ইয়াত মানৱীয় উপাদান জড়িত হৈ থাকে।

চচিয়েল ইঞ্জনীয়াৰিংত হোৱা কিছুমান সাধাৰণ আক্ৰমণ হ'ল-

- ফিছিং
- বেটিং
- ৱাটাৰ হলিং
- অজুহাত
- কুইড প্ৰ' ক্যু
- টেইলগেটিং
- অনুকৰণ

এই ছ'চিয়েল ইঞ্জিনিয়াৰিঙৰ প্ৰতিটো আক্ৰমণৰ বিষয়ে বিতংভাৱে চাওঁ আহক।

৪.৪.১ ফিছিং

ফিছিং হৈছে ছ'চিয়েল ইঞ্জিনিয়াৰিঙৰ অন্যতম সাধাৰণ আক্ৰমণ। ফিছিঙক এনে এটা অপৰাধ বুলি সংজ্ঞায়িত কৰিব পাৰি য'ত অপৰাধীয়ে ইমেইল ব্যৱহাৰ কৰি ভুক্তভোগীক তেওঁলোকৰ ব্যক্তিগত আৰু আর্থিক তথ্য ল'বলৈ চেষ্টা কৰে। প্ৰৱঞ্চকসকলে প্ৰেৰণ কৰা ইমেইলবোৰ বেংক আৰু সংস্থাৰ পৰা অহা বৈধ উৎসৰ হুবহু ইমেইলৰ দৰে দেখা যায়। ভুক্তভোগীক লিংকত ক্লিক কৰা বা ইমেইলৰ পৰা ফাইল ডাউনলোড কৰিবলৈ প্ৰলোভিত কৰা হয় ।

অপৰাধীয়ে ভইচ কলৰ জৰিয়তে ভুক্তভোগীৰ পৰা ব্যক্তিগত আৰু স্পর্শকাতৰ তথ্য আহৰণ কৰাৰ চেষ্টা কৰাটো **vishing** বুলি কোৱা হয়। এছএমএছ ফিছিং বা **স্মিছিং** হৈছে ফিছিঙৰ এটা ভাগ য'ত প্ৰৱঞ্চকে ভুক্তভোগীৰ মোবাইল ফোনলৈ প্ৰতাৰণামূলক টেক্সট বার্তা প্ৰেৰণ কৰি তেওঁলোকক স্পর্শকাতৰ তথ্য প্ৰকাশ কৰিবলৈ বা ক্ষতিকাৰক লিংকত ক্লিক কৰিবলৈ উদ্যত কৰে।

৪.৪.২ বেইটিং

বেইটিং হৈছে এটা চাইবাৰ অপৰাধ য'ত সাধাৰণতে ইউএছবিৰ দৰে ভৌতিক মাধ্যমৰ ডিভাইচ ব্যৱহাৰ কৰি ভুক্তভোগীৰ কম্পিউটাৰ চিষ্টেমলৈ মেলৱেৰ বিয়পাই দিয়া হয়। সাধাৰণতে অপৰাধীয়ে কর্মচাৰীসকলক এই ইউএছবি ডিভাইচসমূহ বাছি ল'বলৈ আৰু ব্যৱহাৰ কৰিবলৈ বাধ্য কৰিবলৈ চতুৰ টেগৰে লক্ষ্যণীয় ঠাইত ইউএছবি ডিভাইচসমূহক বেইট হিচাপে এৰি দিয়ে। যেতিয়া ভুক্তভোগীয়ে এই সংক্রমিত ইউএছবিসমূহ ব্যৱহাৰ কৰে, তেতিয়া তেওঁলোকে নিজৰ কম্পিউটাৰ চিষ্টেমত মেলৱেৰটো ইনষ্টল কৰে।

৪.৪.৩ ৰাটাৰ হলিং

ৰাটাৰ হলিং হৈছে এক চাইবাৰ আক্রমণ য'ত আক্রমণকাৰীয়ে লক্ষ্য ব্যক্তি বা লক্ষ্য প্রতিষ্ঠানৰ কর্মচাৰীয়ে ভ্রমণ কৰা ৱেবছাইটসমূহ পর্যবেক্ষণ কৰে। তাৰ পিছত আক্রমণকাৰীয়ে সেই ৱেবছাইটসমূহক মেলৱেৰৰ দ্বাৰা সংক্রমিত কৰে যে যেতিয়া লক্ষ্য ব্যক্তিজনে সেই ৱেবছাইটসমূহলৈ যায় তেতিয়া তেওঁলোকে ক্ষতিকাৰক লিংকসমূহত ক্লিক কৰে বা তেওঁলোকৰ চিষ্টেমত মেলৱেৰ ডাউনলোড কৰে। "পানীৰ গাঁত" শব্দটো প্রাকৃতিক জগতৰ পৰা অহা, য'ত চিকাৰীয়ে চিকাৰ ধৰিবলৈ প্রায়ে পানী থকা গাঁতৰ ওচৰত অপেক্ষা কৰে । একেদৰে আক্রমণকাৰীয়ে তেওঁলোকৰ লক্ষ্য লোকজনে চলনা কৰা ৱেবছাইটলৈ যোৱাৰ বাবে অপেক্ষা কৰে, য'ত তেওঁলোকে তাৰ পিছত নিজৰ চাইবাৰ আক্রমণ আৰম্ভ কৰিব পাৰে।

৪.৪.৪ প্রিটেক্সিং

প্রিটেক্সিং কৰা হৈছে এক চাইবাৰ অপৰাধ য'ত অপৰাধীয়ে কোনো অজুহাত বা উদ্ভাৱন কৰা পৰিস্থিতিৰ ভিত্তিত ভুক্তভোগীক গোপন আৰু গোপনীয় তথ্য প্রকাশৰ বাবে প্রলোভিত কৰিবলৈ চেষ্টা কৰে। বহু সময়ত অপৰাধীয়ে প্রায়ে আৰম্ভণিতে আৰক্ষী কর্মীৰ দৰে জন সুৰক্ষা কর্তৃপক্ষৰ লোক বুলি কৈ ভুক্তভোগীৰ সৈতে বিশ্বাস স্থাপন কৰিবলৈ চেষ্টা কৰে আৰু এটা জটিল কাম সম্পূর্ণ কৰিবলৈ তেওঁলোকক স্পর্শকাতৰ তথ্যৰ প্রয়োজন বুলি কয়।

৪.৪.৫ কুইড প্র' ক'

কুইড প্ৰ' কু' হৈছে সামাজিক অভিযান্ত্রিকতাৰ এক পদ্ধতি, যি মানুহৰ পৰস্পৰ উপকাৰৰ প্ৰতি থকা সাধাৰণ ইচ্ছাক অপব্যৱহাৰ কৰে। "কুইড প্ৰ' ক' "ৰ অৰ্থ হৈছে " এটাৰ বিনিময়ত আন এটা"। এই ধৰণৰ আক্ৰমণত, আক্ৰমণকাৰীয়ে এজন ব্যক্তিক কিবা উপকাৰ বা মূল্যৱান বস্তু আগবঢ়ায়, যাতে সেই ব্যক্তিয়ে তেওঁলোকক কিবা প্ৰতিদান দিবলৈ উদ্যত হয়। এই "কিবা" হ'ল সচৰাচৰ গোপন তথ্য বা চিস্টেমলৈ প্ৰৱেশ কৰাৰ অধিকাৰ। আক্ৰমণকাৰীয়ে ব্যক্তিৰ এই প্ৰতিদানৰ সুযোগ লৈ নিজৰ উদ্দেশ্য সাধন কৰে।

৪.৪.৬ টেইলগেটিং

টেইলগেটিং, যাক পিগিবেকিং বুলিও কোৱা হয়, হৈছে এক শাৰীৰিক সুৰক্ষা ভংগ কৰা পদ্ধতি যিটো সামাজিক অভিযান্ত্রিকতাৰ আক্ৰমণত ব্যৱহাৰ কৰা হয়। ইয়াত এক অননুমোদিত ব্যক্তিয়ে বৈধ প্ৰৱেশাধিকাৰ থকা এজন ব্যক্তিৰ পিছে পিছে গৈ এটা সুৰক্ষিত বা নিষিদ্ধ অঞ্চলত প্ৰৱেশ কৰে। এটা উদাহৰণ হ' ল য' ত আক্ৰমণকাৰীয়ে সুৰক্ষিত অঞ্চলত প্ৰৱেশ কৰিবলৈ অনুমতি থকা ব্যক্তিৰ পিছে পিছে গৈ ফোনত কথা পাতি থকাৰ ভাও ধৰে, আৰু যিজন ব্যক্তিৰ প্ৰৱেশাধিকাৰ আছে সি সৌজন্যত সেই সুৰক্ষিত দুৱাৰ খুলি দিয়ে।

৪.৪.৭ অনুকৰণ

অনুকৰণ হৈছে এটা প্ৰতাৰণামূলক কৌশল য'ত কোনো ব্যক্তি বা সত্তাই লক্ষ্যক অতিশয়্য বা প্ৰতাৰণা কৰিবলৈ আন কাৰোবাৰ, সাধাৰণতে বিশ্বাসযোগ্য বা কৰ্তৃত্বশীল ব্যক্তিৰ অভিনয় কৰে। আক্ৰমণকাৰীয়ে কিছুমান বিশেষ ভূমিকা বা পদত ৰখা আস্থাক শোষণ কৰি নিজৰ প্ৰতাৰণামূলক কাৰ্য্যকলাপ সম্পন্ন কৰে, লক্ষ্যই চিনাকি বা কৰ্তৃত্বশীল উৎসৰ পৰা অহা যোগাযোগ বা অনুৰোধৰ প্ৰতি কম সন্দেহযুক্ত বুলি ধাৰণা কিৰ লয়। উদাহৰণস্বৰূপে, অনুকৰণকাৰীয়ে এটা সংস্থাৰ ভিতৰত উচ্চ পদস্থ ব্যক্তিৰ অনুকৰণ কৰিব পাৰে, কৰ্মচাৰীসকলক প্ৰৱঞ্চনামূলক অনুৰোধ মানি চলিবলৈ বাধ্য কৰিব পাৰে।



অগ্ৰগতি নিৰীক্ষণ

Q1. ফিশ্বিং, ৰিশ্বিং আৰু স্মিশ্বিং কি ?

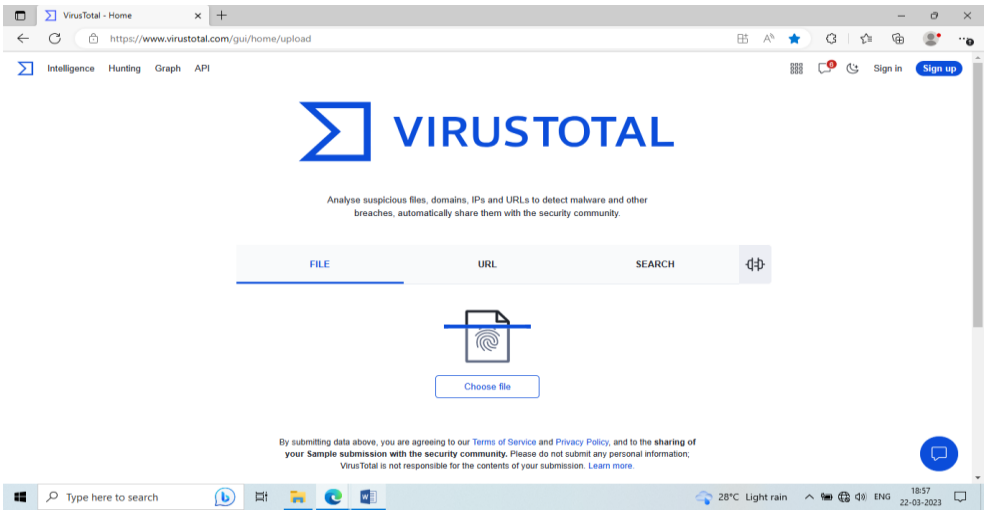
Q2. পঞ্জী আচনি কি ?

৪.৫ মেলৱেৰ

মেলৱেৰ হৈছে "মেলিচিয়াচ চফ্টৱেৰ" শব্দটোৰ সৰল ৰূপ। মেলৱেৰে যিকোনো চফ্টৱেৰ সামৰি লয় যিয়ে ইচ্ছাকৃতভাৱে ব্যৱহাৰকাৰীৰ কম্পিউটাৰ, নেটৱৰ্ক বা চাৰ্ভাৰৰ কাম-কাজ আৰু ইয়াৰ সুৰক্ষা দিশসমূহৰ ক্ষতি কৰিবলৈ, প্ৰৱেশ লাভ কৰিবলৈ, নেটৱৰ্কত ব্যাঘাত জন্মাবলৈ বা বাধা দিবলৈ চেষ্টা কৰে। ই ভাইৰাছ, ৱৰ্মচ, ট্ৰ'জান হৰ্চেচ, ৰেনছমৱেৰ, স্পাইৱেৰ, এডৱেৰ, আদিকে ধৰি বহুতো ক্ষতিকাৰক চফ্টৱেৰৰ প্ৰকাৰ সামৰি লয়। মেলৱেৰসমূহক সাধাৰণতে তলত দিয়া নিম্নলিখিত গোটসমূহৰ এটাত শ্ৰেণীভুক্ত কৰা হয়:

১. ভাইৰাছ:

কম্পিউটাৰ ভাইৰাছ শব্দটো জৈৱিক 'ভাইৰাছ'ৰ পৰা উদ্ভৱ হৈছে। ভাইৰাছে ব্যৱস্থাটোক কেনেকৈ সংক্ৰমিত কৰে সেয়া ইয়াৰ দ্বাৰা বুজোৱা হৈছে। কম্পিউটাৰ ভাইৰাছ হৈছে এনে এটা কম্পিউটাৰ প্ৰগ্ৰেম যিয়ে নিজকে প্ৰতিলিপি কৰি আন কম্পিউটাৰ প্ৰগ্ৰেমবোৰ পৰিৱৰ্তন কৰি ভাইৰাছ ক'ড এক্সিকিউট হ'লে সেই প্ৰগ্ৰেমবোৰত নিজৰ ক'ড সুমুৱাই দিয়ে। ২০০০ চনত ILOVEYOU ভাইৰাছে লাখ লাখ কম্পিউটাৰত প্ৰভাৱ পেলাইছিল। এনে ভাবুকিৰ পৰা সুৰক্ষা দিবলৈ ব্যৱহাৰকাৰীয়ে VirusTotal ৱেবছাইটৰ দৰে অনলাইন সঁজুলি ব্যৱহাৰ কৰিব পাৰে, যিটো URL https://www.virustotal.com/gui/home/upload ত প্ৰৱেশ কৰিব পাৰি , য'ত ব্যৱহাৰকাৰীয়ে ফাইল আপলোড কৰিব পাৰে বা ভাইৰাছৰ বাবে স্কেন কৰিবলৈ URL জমা দিব পাৰে।



চিত্ৰ 4.1: কোনো ফাইল বা URLত ভাইৰাছ আছে নে নাই পৰীক্ষা কৰিবলৈ Virustotal ৱেবছাইট

২. ৰৰ্মচঃ

কম্পিউটাৰ ৰৰ্ম হৈছে এক মেলৰেৰ যি কম্পিউটাৰ নেটৰৰ্ক ব্যৱহাৰ কৰি আৰু নিজকে প্ৰতিলিপি কৰি কম্পিউটাৰ চিস্টেমবোৰত বিয়পি পৰে। যেতিয়া এটা ৰৰ্ম এটা চিস্টেমত প্ৰৰেশ কৰে, ই সেই চিস্টেমক হোস্ট হিচাপে ব্যৱহাৰ কৰি নেটৰৰ্কৰ ভিতৰত থকা অন্যান্য দুৰ্বল মেচিনবোৰ স্কেন আৰু চিনাক্ত কৰে। তাৰ পিছত ৰৰ্মটোৱে এই সংযুক্ত চিস্টেমবোৰক সংক্ৰমিত কৰাৰ চেষ্টা কৰে আৰু নেটৰৰ্ক জুৰি বিয়পি যাবলৈ থাকে। SQL Slammer আছিল এক দ্ৰুতগতিত বিয়পি যোৱা ৰৰ্ম যিয়ে ২০০৩ চনত Microsoftৰ SQL Server ছফ্টৱেৰক সংক্ৰমিত কৰিছিল আৰু হাজাৰ হাজাৰ চাৰ্ভাৰৰ ওপৰত প্ৰভাৱ পেলাইছিল।

৩. ট্ৰ'জান হৰ্চেচ

"ট্ৰ'জান হৰ্চেচ" শব্দটোৰ উৎপত্তি প্ৰাচীন গ্ৰীক কাহিনীৰ পৰা হৈছে য'ত গ্ৰীক সৈন্যই প্ৰতাৰণামূলক কাঠৰ ঘোঁৰা ব্যৱহাৰ কৰি ট্ৰয় চহৰত অনুপ্ৰৰেশ কৰিছিল আৰু শেষত জয় লাভ কৰিছিল। চাইবাৰ সুৰক্ষাৰ প্ৰসংগত, এটা ট্ৰ'জান হৰ্চ বা কেৱল "ট্ৰ'জান"- নিজকে বৈধ, উপযোগী চফ্টৱেৰ এপ্লিকেচনৰ বেশত থাকি একে কৌশল অনুকৰণ কৰে। কিন্তু এবাৰ ইনষ্টল কৰিলে ইয়াৰ প্ৰকৃত ক্ষতিকাৰক প্ৰকৃতি প্ৰকাশ পায়, ব্যৱহাৰকাৰীৰ অজ্ঞাতে ক্ষতিকাৰক কাৰ্য্যকলাপ সম্পন্ন কৰে। ট্ৰ'জানৰ এটা উদাহৰণ হ'ল জিউছ ট্ৰ'জান, যিটো প্ৰথমবাৰৰ বাবে ২০০৭ চনত ধৰা পৰিছিল যিয়ে মাইক্ৰ'ছফ্ট উইণ্ড'জ চিষ্টেমক লক্ষ্য কৰি বেংকিং প্ৰমাণপত্ৰ আৰু বিত্তীয় তথ্য চুৰি কৰিছিল।

৪. ৰেনছমৱেৰ:

"ৰেনছমৱেৰ" শব্দটো বাস্তৱ জগতত মুক্তিপণৰ ধাৰণাটোৰ পৰা উদ্ভৱ হৈছে, য'ত অপহৰণকাৰীয়ে পণবন্দীক মুকলি কৰি দিবলৈ ধন দাবী কৰে। একেদৰে ৰেনছমৱেৰ হৈছে চাইবাৰ অপৰাধীয়ে ব্যৱহাৰ কৰা এক প্ৰকাৰৰ ক্ষতিকাৰক চফ্ট্ ৱেৰ, যাৰ সহায়ত ভুক্তভোগীৰ তথ্য এনক্ৰিপ্ট কৰি ধন আদায় কৰে আৰু ইয়াক ডিক্ৰিপ্ট কৰি প্ৰৰেশ পুনৰুদ্ধাৰ কৰিবলৈ মুক্তিপণৰ দাবী কৰে। এই দুৰ্নীতিপৰায়ণ কাৰ্য্যই মূলতঃ ধন পৰিশোধ কৰাৰ পিছত ইয়াক ঘূৰাই দিয়াৰ প্ৰতিশ্ৰুতিৰে ভুক্তভোগীৰ তথ্যক পণবন্দী কৰি ৰাখে। ৰেনছমৱেৰ আক্ৰমণৰ এটা উদাহৰণ আছিল WannaCry প্ৰাদুৰ্ভাৰ।

৫. স্পাইৱেৰ:

স্পাইৱেৰ হৈছে এনে এটা মেলৱেৰ যিয়ে ব্যৱহাৰকাৰীৰ অজ্ঞাতে ডিভাইচ আৰু ব্যৱহাৰকাৰীৰ তথ্য সংগ্রহ কৰে। এই স্পাইৱেৰটো ব্যৱহাৰকাৰীৰ কার্যকলাপৰ ওপৰত চো�ৰাংচো�ৰাগিৰি কৰি পাছৱর্ডৰ দৰে স্পর্শকাতৰ আৰু গোপনীয় তথ্যৰ প্ৰৱেশ লাভ কৰিবলৈ বা ব্যৱহাৰকাৰীৰ ইণ্টাৰনেট কার্যকলাপ অনুসৰণ কৰিবলৈ ব্যৱহাৰ কৰা হয়। ডার্কহোটেল হৈছে এটা স্পাইৱেৰ যিয়ে হোটেলৰ ৱাই-ফাই নেটৱর্ক চিষ্টেমৰ দুর্বলতা ব্যৱহাৰ কৰি বিশেষভাৱে লক্ষ্য কৰি হোটেলৰ অতিথিসকলক চোৰাংচোৰাগিৰি কৰে।

৬. কী-লগাৰ :

কী-লগাৰ হৈছে ব্যৱহাৰকাৰীয়ে কৰা প্রতিটো কিষ্ট্র'ক তেওঁলোকৰ কম্পিউটাৰত ৰেকর্ড কৰিবলৈ ডিজাইন কৰা এক প্রকাৰৰ মেলৱেৰ। এই ক্ষতিকাৰক চফ্টৱেৰে টাইপ কৰা ইমেইল, পাছৱর্ড, ক্রেডিট কার্ড নম্বৰ, আৰু অন্যান্য স্পর্শকাতৰ তথ্যকে ধৰি বিতং তথ্য ধৰি ৰাখে। তাৰ পিছত ধৰা পৰা তথ্য আক্রমণকাৰীলৈ প্রেৰণ কৰা হয়, প্রায়ে ব্যৱহাৰকাৰীৰ অজ্ঞাতে, যাৰ ফলত গোপনীয়তা যথেষ্ট ভংগ হয়। অলিম্পিক ভিজন হৈছে এটা কী-লগাৰ মেলৱেৰ যিটো বিজনেছ ইমেইল কম্প্রমাইজ (BEC) অভিযানৰ সৈতে জড়িত আছিল যিয়ে বিশ্বৰ বহু কোম্পানীক লক্ষ্য কৰি লৈছিল।

৭. এডৱেৰ:

এডৱেৰ বা বিজ্ঞাপন সমর্থিত চফ্টৱেৰ হৈছে এটা মেলৱেৰ যিয়ে আপোনাৰ কম্পিউটাৰত বিজ্ঞাপনসমূহ পপ-আপৰ আকাৰত প্রদর্শন কৰে কিন্তু প্রকৃততে পটভূমিত ব্যৱহাৰকাৰীসকলৰ তথ্য সংগ্রহ কৰে। এডৱেৰে ব্যৱহাৰকাৰীসকলে ব্রাউজিং ইতিহাস অনুসৰণ কৰি বেংকিং ডাটা বা গোপনীয় ডাটা সংগ্রহ কৰে যাতে ইয়াক হয় ক্ষতিকাৰক উদ্দেশ্যত ব্যৱহাৰ কৰিব পাৰে বা তৃতীয় পক্ষক বিক্রী কৰিব পাৰে। ফায়াৰবল হৈছে এটা ব্রাউজাৰ হাইজেকাৰ মেলৱেৰ যিয়ে ব্যৱহাৰকাৰীৰ ব্রাউজাৰত ছেটিংছ পৰিৱর্তন কৰে আৰু ইয়াক সলনি বা পুনৰুদ্ধাৰ কৰাৰ প্রচেষ্টাক বাধা দিয়ে।

৮. বট আৰু বটনেট:

বটনেট হৈছে ইণ্টাৰনেট সংযুক্ত ডিভাইচসমূহৰ এটা গোট যিয়ে এটা বা ততোধিক বট চলায়। বটনেট হৈছে চাইবাৰ অপৰাধীয়ে বিভিন্ন ধৰণৰ চাইবাৰ আক্রমণ আৰু

কেলেংকাৰী কৰিবলৈ ডিভাইচ আৰু কম্পিউটাৰ চিষ্টেমত প্ৰৱেশ কৰিবলৈ ব্যৱহাৰ কৰা মেলৱেৰ। বটনেটসমূহ হয় বিতৰণ কৰা সেৱা অস্বীকাৰ (DDoS) আক্ৰমণ কৰিবলৈ, ৰেবকেম বা কিষ্ট্ৰ'ক ব্যৱহাৰ কৰি কার্য্যকলাপ ৰেকর্ড কৰিবলৈ, ডিভাইচৰ পৰা ফিছিং ইমেইল প্ৰেৰণ কৰিবলৈ বা চাইবাৰ অপৰাধীসকলক ডিভাইচৰ দূৰৱর্তী নিয়ন্ত্ৰণ দিবলৈ ব্যৱহাৰ কৰিব পাৰি। মিৰাই হৈছে এটা মেলৱেৰ যিয়ে লিনাক্স ব্যৱহাৰ কৰা নেটৱর্কযুক্ত ডিভাইচসমূহক দূৰৱর্তীভাৱে নিয়ন্ত্ৰিত বটলৈ আৰু এটা বৃহৎ পৰিসৰৰ বটনেটৰ অংশ হিচাপে ৰূপান্তৰিত কৰিছিল য'ত বেছিভাগ লক্ষ্য ডিভাইচ আছিল ইণ্টাৰনেট প্ৰট'কল কেমেৰা আৰু ঘৰুৱা ৰাউটাৰ।

৯. ৰুটকিটসমূহ:

ৰুটকিট হৈছে এনে এটা মেলৱেৰ যিয়ে ব্যৱহাৰকাৰীৰ অজ্ঞাতে চাইবাৰ আক্ৰমণকাৰীক কম্পিউটাৰ চিষ্টেম নিয়ন্ত্ৰণ কৰে। ৰুটকিটসমূহ ফিছিং আৰু ক্ষতিকাৰক ডাউনলোডৰ জৰিয়তে বিয়পি পৰে আৰু চিস্টেমত অন্য মেলৱেৰ ইনষ্টল কৰিবলৈ সুবিধা কৰি দিয়ে। Zacinlo হৈছে এটা ৰুটকিট চষ্টৱেৰ যিয়ে অপাৰেটিং চিষ্টেম আৰু এণ্টি-মেলৱেৰ চষ্টৱেৰসমূহক অতিশর্য্য কৰে যাতে ব্যৱহাৰকাৰীয়ে চিষ্টেমত ৰুটকিটৰ উপস্থিতিৰ বিষয়ে অজ্ঞাত থাকে।

১০. ফাইলবিহীন মেলৱেৰ:

ফাইললেছ মেলৱেৰ হৈছে এটা ধৰণৰ মেলৱেৰ যিয়ে ক্ষতিকাৰক কার্য্যকলাপ ইনষ্টল আৰু এক্সিকিউট কৰিবলৈ ইতিমধ্যে বিল্ট-ইন বা ডিভাইচ অপাৰেটিং চিষ্টেমৰ স্থানীয় চষ্টৱেৰ, এপ্লিকেচন, আৰু প্ৰটোকল ব্যৱহাৰ কৰে। পৰম্পৰাগত মেলৱেৰৰ দৰে ইয়াত ফাইল ডাউনলোড কৰাৰ প্ৰয়োজন নাই, যাৰ বাবে ইয়াক ধৰা পেলোৱাটো ব্যতিক্ৰমীভাৱে কঠিন হৈ পৰে। ফাইললেছ মেলৱেৰৰ উদাহৰণ হ'ল Astaroth মেলৱেৰ যিয়ে সংক্ৰমিত মেচিনত লুকাই থাকিবলৈ ফাইললেছ কৌশল ব্যৱহাৰ কৰে।

১১. বিজ্ঞাপন

মেলভাৰটাইজিং হৈছে এক প্ৰকাৰৰ মেলৱেৰ যিয়ে অনলাইন বিজ্ঞাপন ব্যৱহাৰ কৰি মেলৱেৰ বিয়পাই দিয়ে। ইয়াৰ লগত বৈধ অনলাইন ৰেবছাইট আৰু ৰেবপেজত ক্ষতিকাৰক ডিজিটেল বিজ্ঞাপন ইনজেকচন কৰাটো জড়িত হৈ থাকে। মেলভাৰটাইজিং এডৱেৰৰ পৰা পৃথক এই অর্থত যে এডৱেৰ হৈছে ইতিমধ্যে কম্পিউটাৰ চিষ্টেমত

থকা এটা প্ৰগ্ৰেম আৰু ইয়াক ব্যৱহাৰকাৰীৰ ৰেব কার্যকলাপ অনুসৰণ কৰিবলৈ ব্যৱহাৰ কৰা হয় আনহাতে মেলভাৰটাইজিংত আক্ৰমণ সংক্ৰমিত বিজ্ঞাপনৰ জৰিয়তে অনলাইনত কৰা হয়।

১২. ৰাইপাৰ:

ৰাইপাৰ হৈছে এটা মেলৱেৰ যিটো ই সংক্ৰমিত কম্পিউটাৰ চিষ্টেমৰ ব্যৱহাৰকাৰী বা চিষ্টেমৰ ডাটা পুনৰ উদ্ধাৰ কৰিব নোৱাৰাকৈ মচি পেলাবলৈ ব্যৱহাৰ কৰা হয় যাতে ইয়াক। চাইবাৰ অপৰাধীয়ে নেটৱৰ্কত থকা কম্পিউটাৰসমূহক লক্ষ্য কৰি সেই চিষ্টেমসমূহত সংৰক্ষিত তথ্য মচি পেলাবলৈ আৰু আন কোনো মেলৱেৰ আক্ৰমণৰ পিছত অনুপ্ৰৱেশৰ লেখ-জোখ আঁতৰাবলৈ ৰাইপাৰ ব্যৱহাৰ কৰে। WhisperGate হৈছে কম্পিউটাৰ চিষ্টেমত ডাটা মচি পেলাবলৈ ব্যৱহাৰ কৰা ৰাইপাৰৰ উদাহৰণ।

১৩. স্কেয়াৰৱেৰ:

স্কেয়াৰৱেৰ হৈছে এক প্ৰকাৰৰ মেলৱেৰ য'ত চাইবাৰ অপৰাধীয়ে ছ'চিয়েল ইঞ্জিনিয়াৰিঙৰ সহায়ত ব্যৱহাৰকাৰীক আক্ৰমণ কৰি অবাঞ্ছিত চফট্ ৱেৰ ক্ৰয় কৰায়। স্কেয়াৰৱেৰ আক্ৰমণত ব্যৱহাৰকাৰীসকলক প্ৰতাৰিত কৰি তেওঁলোকৰ কম্পিউটাৰ চিষ্টেমটো ভাইৰাছৰ দ্বাৰা সংক্ৰমিত বুলি বিশ্বাস কৰা হয় আৰু তাৰ পিছত তেওঁলোকৰ চিষ্টেমৰ পৰা ভাইৰাছটো আঁতৰাই পেলোৱা এন্টিভাইৰাছ চফটৱেৰ এটাৰ পৰামৰ্শ দিয়ে। বেছিভাগ সময়তে ব্যৱহাৰকাৰীয়ে এন্টিভাইৰাছৰ বাবে ধন দিব লাগে আৰু যদি চফট্ ৱেৰটো বিনামূলীয়া হয় তেন্তে এন্টিভাইৰাছ চফট্ ৱেৰটো অকার্য্যকৰী বা ই কোনো ধৰণৰ মেলৱেৰ।

৪.৬ জিৰ' দে আক্ৰমণ

চফ্টৱেৰ প্ৰগ্ৰেমসমূহ মুকলি কৰাৰ সময়ত প্ৰায়ে প্ৰগ্ৰেমসমূহত ত্ৰুটি বা দুৰ্বলতা থাকে যাৰ সুবিধা এজন চাইবাৰ অপৰাধীয়ে ল'ব পাৰে। চফ্টৱেৰ ডেভেলপাৰসকলে চফ্টৱেৰটো মুকলি কৰাৰ লগে লগে প্ৰায়ে এই দুৰ্বলতাসমূহ বিচাৰি উলিয়াবলৈ চেষ্টা কৰে। গতিকে তেওঁলোকে ক'ডটো বিশ্লেষণ কৰে আৰু ত্ৰুটিসমূহ সমাধানৰ বাবে পেটচ যোগ কৰে। কিন্তু যেতিয়া কোনো আক্ৰমণকাৰীয়ে এই অনাকাংক্ষিত ত্ৰুটিবোৰৰ ধৰা পেলায় চফ্টৱেৰ ডেভেলপাৰ বা কোম্পানীয়ে এই ত্ৰুটিবোৰ ঠিক কৰাৰ আগতেই চিষ্টেমটোক আক্ৰমণ কৰে, তেতিয়া ইয়াক 'জিৰ' ডে'

আক্রমণ বুলি কোৱা হয়। এই আক্রমণৰ শব্দটো 'শূন্য' দিন' হিচাপে দিয়া হৈছে যিহেতু চফট্ ৱেৰটোৰ ত্রুটিবোৰ সমাধান কৰিবলৈ দিনৰ সংখ্যা জিৰ'।

এজন চাইবাৰ অপৰাধীয়ে বিভিন্ন চিষ্টেমৰ দুর্বলতা যেনে অপাৰেটিং চিষ্টেম, ৱেব ব্রাউজাৰ, এপ্লিকেচন চফ্টৱেৰ, হার্ডৱেৰ আৰু ফার্মৱেৰ কম্পোনেণ্ট আদিৰ শোষণ কৰিব পাৰে। চাইবাৰ অপৰাধীয়ে ছ'চিয়েল ইঞ্জিনিয়াৰিং পদ্ধতিকে ধৰি দুর্বল চিষ্টেমটোক আক্রমণ কৰিবলৈ বিভিন্ন ধৰণৰ আক্রমণ কৰে। আক্রমণকাৰীয়ে ইমেইল আৰু বার্তা ব্যৱহাৰ কৰি ব্যৱহাৰকাৰীক ক্ষতিকাৰক লিংকত ক্লিক কৰিবলৈ প্রলোভিত কৰিবলৈ চেষ্টা কৰে আৰু এবাৰ ভুক্তভোগীয়ে মেলৱেৰটো ডাউনলোড কৰিলে তেতিয়া আক্রমণকাৰীয়ে চিষ্টেমত অনুপ্রৱেশ কৰি দুর্বলতাৰ সুযোগ লৈ আক্রমণ কৰিব পাৰে। চফট্ ৱেৰ ডেভেলপাৰসকলে এবাৰ এই দুর্বলতা জানিব পাৰিলে, তেওঁলোকে পেটচ তৈয়াৰ কৰি কৰি ক'ডটো ঠিক কৰিবলৈ চেষ্টা কৰে। কিন্তু, এই পেটচ ক'ডসমূহ বিকশিত কৰিবলৈ সময় লাগে। কেতিয়াবা ত্রুটিটো আৱিষ্কাৰ কৰিবলৈ আৰু সেই ত্রুটিবোৰ সমাধান কৰিবলৈ ক'ড লিখিবলৈ দিন, সপ্তাহ বা মাহ সময় লাগিব পাৰে। এই সময়ছোৱাত যিকোনো চাইবাৰ অপৰাধীয়ে এই ত্রুটিৰ শোষণ কৰি ব্যৱস্থাটোক আক্রমণ কৰিবলৈ সুবিধাজনক হৈ থাকে। আনকি যেতিয়া পেচসমূহ ব্যৱহাৰকাৰীসকলৰ বাবে মুকলি কৰা হয়, বহুতে এই আপডেইটসমূহ দ্রুতভাৱে প্রণয়ন নকৰে যিয়ে চিস্টেমক এই আক্রমণসমূহৰ বাবে দুর্বল কৰি তোলে। শূন্য দিনৰ আক্রমণ বিপজ্জনক কাৰণ আক্রমণকাৰীয়েহে ইয়াৰ বিষয়ে জানে আৰু বেছিভাগ সময়তে চাইবাৰ আক্রমণকাৰীয়ে আক্রমণ কঢ়িয়াই নিবলৈ আটাইতকৈ সুবিধাজনক সময়ৰ বাবে অপেক্ষা কৰে। জিৰ' দিনৰ আক্রমণৰ এটা ক্ষেত্র আছিল ভিডিঅ' কনফা�ৰেন্সিং এপ্লিকেচন জুমত য'ত আক্রমণকাৰীয়ে উইণ্ড'জ ৭ বা উইণ্ড'জৰ পুৰণি সংস্কৰণ ব্যৱহাৰকাৰীৰ চিষ্টেমত দূৰৈৰ পৰা প্রৱেশ কৰিব পাৰিছিল।

চফ্টৱেৰ বিকাশকসকলে তেওঁলোকৰ নিজৰ চফ্টৱেৰত দুর্বলতাসমূহ বিচাৰে আৰু তাৰ পিছত সেই দুর্বলতাসমূহ সমাধান কৰিবলে পেচসমূহ মুকলি কৰে যাতে চিস্টেমসমূহ আক্রমণ কৰা নহয়। জিৰ' দিনৰ আক্রমণ প্রতিৰোধৰ এটা উত্তম উপায় হ'ল চফট্ ৱেৰটো আপডেট কৰি ৰখা।

৪.৭ জিৰ' ক্লিক আক্রমণ

জিৰ'-ক্লিক আক্রমণ হৈছে এনে এটা আক্রমণ য'ত ব্যৱহাৰকাৰীৰ হস্তক্ষেপৰ প্রয়োজন নাই। ব্যৱহাৰকাৰীয়ে কোনো লিংকত ক্লিক কৰাৰ প্রয়োজন নোহোৱাকৈ বা মেলৱেৰ থকা কোনো

ফাইল ডাউনলোড কৰাৰ প্ৰয়োজন নোহোৱাকৈ আক্ৰমণকাৰীয়ে মেলৱেৰ ইনষ্টল কৰিব পাৰে বা অন্য কোনো ক্ষতিকাৰক আক্ৰমণ কৰিব পাৰে । সাধাৰণতে, বেছিভাগ মেলৱেৰ ব্যৱহাৰকাৰীক ক্ষতিকাৰক লিংক ক্লিক কৰিবলৈ ছলনা কৰি ব্যৱহাৰকাৰীৰ মোবাইল ফোন বা চিষ্টেমত ডাউনলোড কৰা হয়। কিন্তু জিৰ' ক্লিক আক্ৰমণৰ ক্ষেত্ৰত চাইবাৰ অপৰাধীয়ে ব্যৱহাৰকাৰীয়ে মেলৱেৰ ইনষ্টল কৰাৰ বাবে কোনো লিংকত ক্লিক কৰাৰ প্ৰয়োজন নাই। এই বৈশিষ্ট্যই জিৰ' ক্লিক আক্ৰমণক অত্যন্ত বিপজ্জনক কৰি তোলে।

বিশেষকৈ স্মাৰ্টফোনৰ ব্যৱহাৰ বৃদ্ধি আৰু বিস্তৃত ব্যক্তিগত তথ্য সংৰক্ষণৰ লগে লগে জিৰ' ক্লিক আক্ৰমণ ক্ৰমান্বয়ে বৃদ্ধি পাইছে। এই শোষণসমূহে অবিশ্বাস্য ডাটা নিয়ন্ত্ৰণ কৰা এপ্লিকেচনসমূহৰ দুৰ্বলতাসমূহৰ সুযোগ লয়, যেনে এছএমএছ, বাৰ্তা প্ৰেৰণ এপসমূহ, ইমেইল ক্লায়েন্টসমূহ, আৰু ফোন এপ্লিকেচনসমূহ। যিহেতু নটিফিকেশন ব্যৱহাৰকাৰীৰ পাৰস্পৰিক ক্ৰিয়াৰ অবিহনে বাৰ্তাৰ বিষয়বস্তু প্ৰদৰ্শন কৰে, ভালদৰে নিৰ্মিত ক্ষতিকাৰক বাৰ্তাই এই দুৰ্বলতাসমূহ ব্যৱহাৰ কৰি মেলৱেৰ ইনষ্টল কৰিব পাৰে বা ডিভাইচত অন্য ক্ষতিকাৰক কাৰ্য্যকলাপসমূহ কৰিব পাৰে।



অগ্ৰগতি নিৰীক্ষণ

Q3. কম্পিউটাৰ ভাইৰাচ আৰু ৱৰ্মৰ মাজৰ পাৰ্থক্য কি ?

Q4. ৰাইপাৰ মেলৱেৰ কি লিখক।



৪.৮ অধ্যায়টিৰ আমি কি কি শিকিলোঁ

- **আৰ্থিক প্ৰৱঞ্চনা** হৈছে- ব্যক্তি বা সংস্থাই প্ৰতাৰণামূলক, বিভ্ৰান্তিকৰ আৰু অবৈধ কাৰ্য্যৰ জৰিয়তে আমাৰ ধনৰ পৰা বঞ্চিত কৰা বা আৰ্থিক ক্ষতি কৰা।
- কোনো অপৰাধীয়ে আন ব্যক্তিৰ ব্যক্তিগত তথ্য চুৰি বা ব্যৱহাৰ কৰি তেওঁলোকৰ অনুমতি অবিহনে আৰ্থিক জালিয়াতি কৰা এক অপৰাধ।
- বিনিয়োগ জালিয়াতি হৈছে এনে এটা অপৰাধ যিটো অপৰাধীয়ে মানুহক এনে আঁচনিত বিনিয়োগ কৰিবলৈ পতিয়ন নিয়ায় যিবোৰৰ সম্ভাৱনা নাই বা কেতিয়াবা অস্তিত্বও নাই।

- ইণ্টাৰনেট বেংকিং জালিয়াতি বা অনলাইন বেংকিং জালিয়াতিত অপৰাধীয়ে নিজৰ ধনৰ ভুক্তভোগীক প্ৰতাৰণা কৰিবলৈ ইণ্টাৰনেট বা অনলাইন প্ৰযুক্তি ব্যৱহাৰ কৰে। ইয়াৰ লগত ভুক্তভোগীৰ অনুমতি অবিহনে ভুক্তভোগীৰ ধন বিভিন্ন বেংক একাউণ্টলৈ স্থানান্তৰ কৰে।
- **চচিয়েল ইঞ্জনীয়াৰিং আক্ৰমণত** মানুহৰ পাৰস্পৰিক ক্ৰিয়া-কলাপ আৰু আৱেগৰ সৈতে হেতালি খেলাধৰনৰ ক্ষতিকাৰক কাৰ্য্য জড়িত হৈ থাকে। সাধাৰণতে ভুক্তভোগীক ভুল কৰিবলৈ বা স্পৰ্শকাতৰ তথ্য প্ৰকাশ কৰিবলৈ প্ৰতাৰণা কৰা হয়।
- ফিছিঙক এনে এটা অপৰাধ বুলি সংজ্ঞায়িত কৰিব পাৰি য'ত অপৰাধীয়ে ইমেইল ব্যৱহাৰ কৰি ভুক্তভোগীক তেওঁলোকৰ ব্যক্তিগত আৰু আৰ্থিক তথ্য লাভ কৰিবলৈ চেষ্টা কৰে।
- বেইটিং হৈছে এটা চাইবাৰ অপৰাধ য'ত সাধাৰণতে ইউএছবিৰ দৰে ভৌতিক মাধ্যমৰ ডিভাইচ ব্যৱহাৰ কৰি ভুক্তভোগীৰ কম্পিউটাৰ চিষ্টেমলৈ মেলৱেৰ বিয়পাই দিয়া হয়।
- প্ৰিটেক্সিং হৈছে এক চাইবাৰ অপৰাধ য'ত অপৰাধীয়ে কোনো অজুহাত বা উদ্ভাৱন কৰা পৰিস্থিতিৰ ভিত্তিত ভুক্তভোগীক গোপন আৰু গোপনীয় তথ্য প্ৰকাশৰ বাবে প্ৰলোভিত কৰিবলৈ চেষ্টা কৰে।
- টেইলগেটিঙত আক্ৰমণকাৰীয়ে এজন ব্যক্তিক অনুসৰণ কৰি নিৰাপদ নিষিদ্ধ অঞ্চললৈ যায়, য'ত আক্ৰমণকাৰীৰ কোনো বৈধ প্ৰৱেশ নাই।
- **মেলৱেৰ** হৈছে "মেলিচিয়াচ চফ্টৱেৰ" শব্দটোৰ সৰলৰূপ। মেলৱেৰে ইচ্ছাকৃতভাৱে ব্যৱহাৰকাৰীৰ কম্পিউটাৰ, নেটৱৰ্ক বা চাৰ্ভাৰৰ কাম-কাজ আৰু ইয়াৰ সুৰক্ষা দিশসমূহৰ ক্ষতি কৰিবলৈ, প্ৰৱেশ লাভ কৰিবলৈ, নেটৱৰ্কত ব্যাঘাত জন্মাবলৈ বা বাধা দিবলৈ চেষ্টা কৰা যিকোনো চফ্টৱেৰক সামৰি লয় ।
- কম্পিউটাৰ ভাইৰাছ হৈছে এনে এটা কম্পিউটাৰ প্ৰগ্ৰেম যিয়ে নিজকে প্ৰতিলিপি কৰি আন কম্পিউটাৰ প্ৰগ্ৰেমবোৰ পৰিৱৰ্তন কৰি ভাইৰাছ ক'ড এক্সিকিউট হ'লে সেই প্ৰগ্ৰেমবোৰত নিজৰ ক'ড সুমুৱাই দিয়ে।
- কম্পিউটাৰ ৱৰ্ম হৈছে কম্পিউটাৰ নেটৱৰ্ক ব্যৱহাৰ কৰি আৰু নিজৰ প্ৰতিলিপি কৰি কম্পিউটাৰ চিষ্টেমৰ মাজেৰে বিয়পি পৰা এটা মেলৱেৰ।
- ট্ৰ'জান হৰ্চ হৈছে এনে এক আক্ৰমণ য'ত চফট্ ৱেৰটো ব্যৱহাৰকাৰীৰ বাবে বৈধ উপযোগী চফট্ ৱেৰ প্ৰগ্ৰেম যেন লাগে কিন্তু এবাৰ ইনষ্টল হ'লে চফট্ ৱেৰটোৱে ইয়াৰ ক্ষতিকাৰক কাৰ্য্যসমূহ লোড কৰে।

- ৰেনছমৱেৰ আক্রমণত চাইবাৰ অপৰাধীয়ে ব্যৱহাৰকাৰীৰ কম্পিউটাৰ চিষ্টেমত সংক্রমিত কৰি গোটেই বা অংশটো ডাটা এনক্রিপ্ট কৰে আৰু ডিভাইচটোৰ প্রৱেশ ডিক্রিপ্ট কৰি ব্যৱহাৰকাৰীলৈ ঘূৰাই আনিবলৈ ধন দাবী কৰে।
- যেতিয়া কোনো আক্রমণকাৰীয়ে এই অনাকাংক্ষিত ত্রুটিসমূহৰ শোষণ কৰি চষ্টৱেৰ ডেভেলপাৰ বা কোম্পানীয়ে এই ত্রুটিসমূহ সমাধান কৰাৰ আগতেই চিষ্টেমটোক আক্রমণ কৰে, তেতিয়া ইয়াক 'জিৰ' দে' আক্রমণ বোলা হয়।
- জিৰ'-ক্লিক আক্রমণ হৈছে এনে এটা আক্রমণ য'ত ব্যৱহাৰকাৰীৰ হস্তক্ষেপৰ প্রয়োজন নাই।

৪.৯ অগ্রগতিৰ খতিয়ান

প্রশ্ন ১ ৰ উত্তৰ: ফিছিঙক এনে এটা অপৰাধ বুলি সংজ্ঞায়িত কৰিব পাৰি য'ত অপৰাধীয়ে ইমেইল ব্যৱহাৰ কৰি ভুক্তভোগীক তেওঁলোকৰ ব্যক্তিগত আৰু আর্থিক তথ্য প্রকাশ কৰিবলৈ চেষ্টা কৰে। স্মিছিং বা এছএমএছ ফিছিং হৈছে এক প্রকাৰৰ ফিছিং য'ত অপৰাধীয়ে চেল ফোন বা স্মার্টফোনৰ পৰা টেক্সট মেছেজ ব্যৱহাৰ কৰি ভুক্তভোগীক বেইট কৰিবলৈ চেষ্টা কৰে। ভইচ ফিছিং বা ভিছিং হৈছে এনে এক অপৰাধ যিটো অপৰাধীয়ে ভইচ কল ব্যৱহাৰ কৰি ভুক্তভোগীক ব্যক্তিগত আৰু গোপনীয় তথ্য লাভ কৰিবলৈ চেষ্টা কৰে।

প্রশ্ন ২ ৰ উত্তৰ: পঞ্জী আঁচনিত অপৰাধীয়ে নতুন বিনিয়োগকাৰীৰ পৰা ধন সংগ্রহ কৰি বর্তমানৰ বিনিয়োগকাৰীক ধন সংগ্রহ কৰে। আঁচনিখনৰ অন্ত পৰে যেতিয়া কোনো নতুন বিনিয়োগকাৰীয়ে যোগদান নকৰে আৰু আঁচনিকাৰে পুৰণি বিনিয়োগকাৰীক ৰিটার্ণ নিদিয়াকৈ বাকী থকা ধন ৰাখে।

প্রশ্ন ৩ৰ উত্তৰ: কম্পিউটাৰ ভাইৰাছ আৰু কম্পিউটাৰ ৱর্মৰ মাজত পার্থক্যটো হ'ল ইহঁতে প্রতিলিপি কৰাৰ ধৰণ। ভাইৰাছে সেই প্রগ্রেমটো এক্সিকিউট কৰিবলৈ এটা হ'ষ্ট প্রগ্রেম আৰু এজন ব্যৱহাৰকাৰীৰ প্রয়োজন হয় আনহাতে এটা ৱর্ম এ স্ব-প্রতিলিপি কৰিব পাৰে আৰু স্বাধীন হ'ব পাৰে।

Q4 ৰ উত্তৰ: ৰাইপাৰ হৈছে এটা মেলৱেৰ যিটো সংক্রমিত কম্পিউটাৰ চিষ্টেমৰ ব্যৱহাৰকাৰী বা চিষ্টেম ডাটা মচি পেলাবলৈ ব্যৱহাৰ কৰা হয় যাতে ইয়াক পুনৰ উদ্ধাৰ কৰিব নোৱাৰি।



৪ .১০ অধিক জানিবলৈ

1) https://en.wikipedia.org
2) https://www.justice.gov/criminal-fraud/mass-marketing-fraud
3) https://www.kaspersky.co.in/resource-center/definitions/zero-day-exploit
4) https://www.forbes.com/sites/daveywinder/2020/07/10/zoom-confirms-zero-day-security-vulnerability-for-windows-7-users/ ?sh=6ca797c0753d
5) https://www.kaspersky.com/resource-center/definitions/what-is-zero-click-malware
6) https://www.checkpoint.com/cyber-hub/cyber-security/what-is-a-zero-click-attack/



৪.১১ আৰ্হি প্ৰশ্ন

প্রশ্ন ১। বিভিন্ন ধৰণৰ আর্থিক প্রৱঞ্চনাৰ বর্ণনা কৰক।

প্রশ্ন ২। চচিয়েল ইঞ্জনীয়াৰিং আক্রমণৰ বিভিন্ন ধৰণৰ বর্ণনা কৰক।

প্রশ্ন ৩। যিকোনো পাঁচটা ভিন্ন ধৰণৰ মেলৱেৰৰ বর্ণনা কৰক ।

প্রশ্ন ৪। জিৰ' দে আক্রমণ কি? জিৰ' দেৰ আক্রমণ আমি কেনেকৈ ৰোধ কৰিব পাৰো?

প্রশ্ন ৫। জিৰ'-ক্লিক আক্রমণে কেনেকৈ কাম কৰে বুজাৰি লিখক।

প্রশ্ন ৬। এডৱেৰ, স্কেয়াৰৱেৰ আৰু স্পাইৱেৰৰ মাজৰ পার্থক্য কি লিখক।

প্রশ্ন ৭। ৰেনছমৱেৰ আক্রমণ কি? ই কেনেকৈ সংঘটিত হয়?

প্রশ্ন ৮। কী-লগাৰ মেলৱেৰে কেনেকৈ কাম কৰে বুজাই লিখক।

প্রশ্ন ৯। ইউপিআই পেমেণ্ট গেটৱে জালিয়াতি কেনেকৈ হয় বুজাওক।

প্রশ্ন ১০। ৰাটাৰ হলিং কৰা আক্রমণে কেনেকৈ কাম কৰে বুজাই দিয়া।

****

অধ্যায় ৫ – চাইবাৰ আইন

অধ্যায় গাঁথনি

৫.১ উদ্দেশ্য

৫.২ পৰিচয়

৫.৩ চাইবাৰ অপৰাধী মডাছ-অপাৰাণ্ডি

৫.৪ চাইবাৰ অপৰাধৰ ৰিপৰ্ট

৫.৫ প্রতিকাৰ আৰু প্রশমনৰ ব্যৱস্থা

৫.৬ চাইবাৰ অপৰাধৰ আইনী দৃষ্টিভংগী

- ৫.৬.১ আই টি আইন ২০০০
- ৫.৬.২ এটা সংশোধনী
- ৫.৬.৩ আই টি আইনৰ অধীনত চাইবাৰ অপৰাধ

৫.৭ ভাৰতত চাইবাৰ অপৰাধ আৰু চাইবাৰ সুৰক্ষাৰ সৈতে মোকাবিলা কৰা সংস্থা

৫.৮ কেছ ষ্টাডিজ

৫.৯ অধ্যায়টিৰ পৰা আমি কি কি শিকিলোঁ

৫.১০ অগ্রগতি নিৰীক্ষণ

৫.১১ অধিক জানিবলৈ

৫.১২ আৰ্হি প্রশ্ন

৫.১ উদ্দেশ্য

এই অধ্যায়পৰা আপোনালোকে নিম্নোক্ত বিষয়ে জ্ঞাত হ'ব-

- চাইবাৰ অপৰাধীৰ মডাছ-অপাৰাণ্ডি কি বুজি উঠিব
- চাইবাৰ অপৰাধৰ ৰিপৰ্ট কেনেকৈ দিব লাগে সেই বিষয়ে জানিব
- আইনী প্রতিকাৰ আৰু প্রশমন ব্যৱস্থাৰ বর্ণনা কৰিব পাৰিব
- আই টি আইন ২০০০ আৰু ইয়াৰ সংশোধনীৰ অধীনত অহা বিভিন্ন আইনসমূহৰ বিষয়ে জানিব পাৰিব
- ভাৰতত চাইবাৰ অপৰাধ আৰু চাইবাৰ সুৰক্ষাৰ সৈতে জড়িত সংস্থাসমূহৰ তালিকা প্রস্তুত কৰিব পাৰিব।

৫.২ পৰিচয়

পূৰ্বৰ অধ্যায়ত আমি আৰ্থিক প্ৰৱঞ্চনা আৰু ছ'চিয়েল ইঞ্জিনিয়াৰিঙৰ আক্ৰমণৰ সন্মুখীন হোৱা বিভিন্ন চাইবাৰ অপৰাধৰ বিষয়ে জানিব পাৰিছো। ভাইৰাছ, ৱৰ্মচ, ৰেনছমৱেৰ আদিকে ধৰি বিভিন্ন ধৰণৰ মেলৱেৰৰ বিষয়েও আমি জানিব পাৰিছো। জিৰ'-ডে আক্ৰমণ আৰু জিৰ' ক্লিক আক্ৰমণৰ বিষয়েও পূৰ্বৰ অধ্যায়ত বিতংভাৱে আলোচনা কৰা হৈছে।

এই অধ্যায়ত আমি অপৰাধৰ আঁৰৰ চাইবাৰ অপৰাধীৰ মোডাছ-অপাৰাণ্ডিৰ বিষয়ে জানিব পাৰিম। ভাৱতত চাইবাৰ অপৰাধৰ ৰিপৰ্ট কেনেকৈ আৰু ক'ত কৰিব লাগে সেই বিষয়েও আমি জানিব পাৰিম। এই অধ্যায়ত প্ৰতিকাৰ আৰু প্ৰশমন ব্যৱস্থাৰ বিষয়েও আলোচনা কৰা হৈছে। আই টি আইন ২০০০ আৰু ইয়াৰ বিভিন্ন সংশোধনীৰ বিষয়েও এই অধ্যায়ত বিতংভাৱে আলোচনা কৰা হৈছে। পৰৱৰ্তী অধ্যায়ত আপোনাক বিভিন্ন ছ'চিয়েল মিডিয়া প্লেটফৰ্মৰ সৈতে পৰিচয় কৰাই দিয়া হ'ব।

৫.৩ চাইবাৰ অপৰাধৰ ধৰণ-কাৰ্য্য

Modus-operandi হৈছে লেটিন ভাষাৰ এটা শব্দ যাৰ অৰ্থ হৈছে "কাৰ্য্যৰ ধৰণ"। অপৰাধৰ বিষয়ে আলোচনা কৰাৰ সময়ত আৰু অপৰাধীয়ে ব্যৱহাৰ কৰা পদ্ধতিৰ উল্লেখ কৰাৰ সময়ত মডাছ-অপাৰাণ্ডি শব্দটো বেছিভাগেই ব্যৱহাৰ কৰা হয়। চাইবাৰ অপৰাধীৰ মডাছ-অপাৰাণ্ডি হৈছে এটা চিনাক্তকৰণ বৈশিষ্ট্য বা আচৰণৰ আৰ্হি যিটো ব্যৱহাৰ কৰি অপৰাধীয়ে অপৰাধ সংঘটিত কৰিছিল আৰু এতিয়া ইয়াক অপৰাধীক চিনাক্ত কৰিবলৈ ব্যৱহাৰ কৰিব পাৰি।

পূৰ্বৰ দুটা অধ্যায়ত আমি বহুতো চাইবাৰ অপৰাধ আৰু এই অপৰাধসমূহ কেনেকৈ সংঘটিত হয় সেই বিষয়ে আলোচনা কৰিছো। চাইবাৰ অপৰাধৰ ওপৰত নিৰ্ভৰ কৰি লক্ষ্য আৰু চাইবাৰ অপৰাধীৰ পদ্ধতিও ভিন্ন হয়। উদাহৰণস্বৰূপে, হেকিঙৰ দৰে চাইবাৰ অপৰাধৰ বাবে যি মোডাছ-অপাৰাণ্ডি ব্যৱহাৰ কৰা হ'ব, সেয়া চাইবাৰ বুলিঙৰ বাবে প্ৰয়োগ কৰা হ'বলগীয়া মোডাছ-অপাৰেণ্ডীতকৈ বহু বেলেগ হ'ব ।

চাইবাৰ অপৰাধীয়ে ব্যৱহাৰ কৰা কিছুমান সাধাৰণ পদ্ধতি হ'ল-

- বার্তা প্রেৰণ কৰা
- ফোন কল কৰা
- ইমেইল প্রেৰণ কৰা

- ছ'চিয়েল ইঞ্জিনিয়াৰিঙৰ আক্রমণ ব্যৱহাৰ কৰা

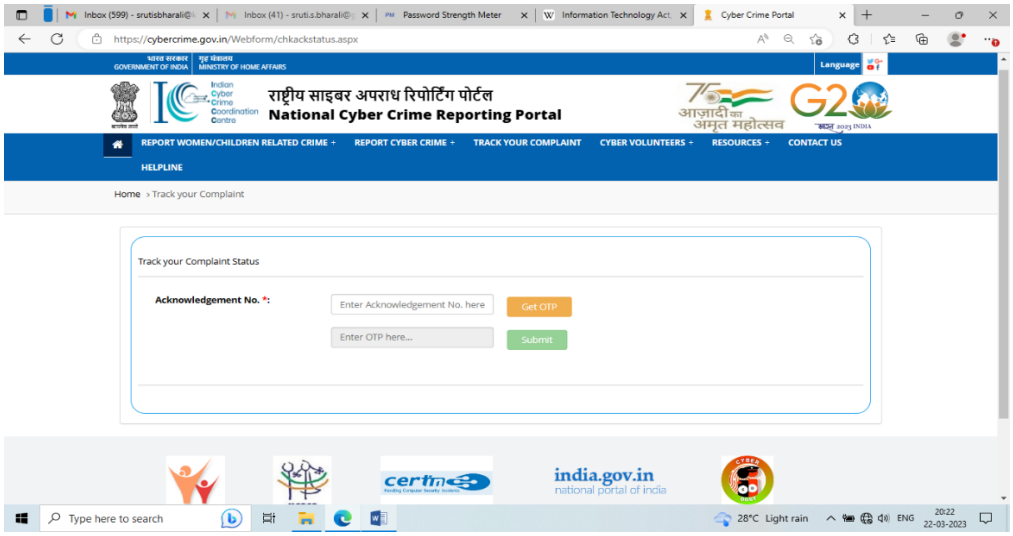
৫.৪ চাইবাৰ অপৰাধৰ প্ৰতিবেদন

https://cybercrime.gov.in/Default.aspx URL ব্যৱহাৰ কৰি "National Cyber Crime Reporting Portal" ৰ ৱেবছাইটত চাইবাৰ অপৰাধৰ ৰিপৰ্ট দিব পাৰি । এই পৰ্টেলটো ভাৰত চৰকাৰৰ এক পদক্ষেপ যাতে ভুক্তভোগী/অভিযোগকাৰীসকলে চাইবাৰ অপৰাধৰ অভিযোগ অনলাইনযোগে ৰিপৰ্ট কৰিব পাৰে। এই পৰ্টেলে মহিলা আৰু শিশুৰ বিৰুদ্ধে সংঘটিত হোৱা চাইবাৰ অপৰাধৰ ওপৰত বিশেষ গুৰুত্ব আৰোপ কৰিহে চাইবাৰ অপৰাধৰ অভিযোগৰ ব্যৱস্থা কৰে।



চিত্ৰ ৫.১: ৰাষ্ট্ৰীয় চাইবাৰ অপৰাধ প্ৰতিবেদন পৰ্টেলৰ ৱেবছাইট

আৰ্থিক প্ৰৱঞ্চনা আৰু আন বহুতো চাইবাৰ অপৰাধৰ বিৰুদ্ধে অভিযোগ ওপৰৰ ৱেবছাইটটো ব্যৱহাৰ কৰি ৰিপৰ্ট কৰিব পাৰি। অভিযোগসমূহ লোৱাৰ পিছত অভিযোগৰ বিৰুদ্ধে হোৱা অগ্ৰগতিও ৱেবছাইট ব্যৱহাৰ কৰি অনুসন্ধান কৰিব পাৰি। অভিযোগৰ ট্ৰেকিং তথ্য স্বীকৃতি নম্বৰ আৰু সেই স্বীকৃতি নম্বৰৰ বিপৰীতে সৃষ্টি হোৱা অ'টিপি দি লাভ কৰিব পাৰি। অপৰাধৰ ওপৰত নিৰ্ভৰ কৰি স্থানীয় আৰক্ষী থানাত এফআইআৰ দাখিল কৰিও চাইবাৰ অপৰাধৰ অভিযোগ উত্থাপন কৰিব পাৰি। এই ৱেবছাইটৰ উপৰিও "১৯৩০" হেল্পলাইন নম্বৰত ফোন কল ব্যৱহাৰ কৰিও চাইবাৰ অপৰাধ দাখিল কৰিব পাৰি।



চিত্র ৫.২: অভিযোগৰ অৱস্থা অনুসৰণ কৰা



চিত্র ৫.৩: চাইবাৰ অপৰাধৰ অভিযোগৰ বাবে হেল্পলাইন নম্বৰ

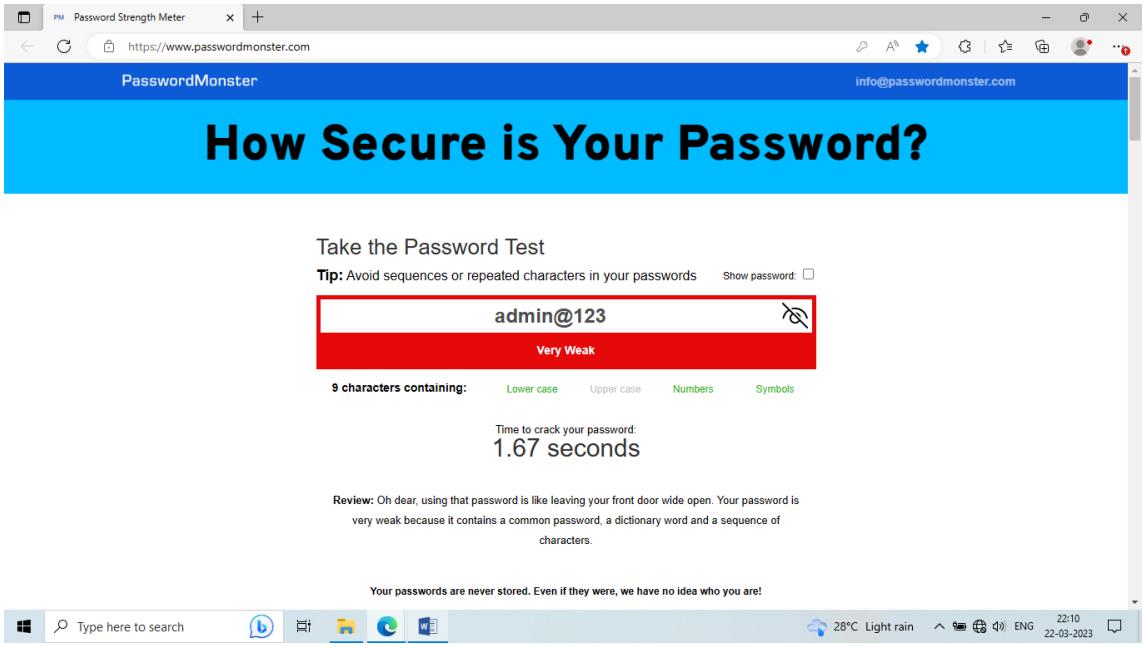
৫.৫ প্রতিকাৰ আৰু প্রশমনৰ ব্যৱস্থা

আমাৰ কম্পিউটাৰ আৰু মোবাইল ডিভাইচসমূহক চাইবাৰ অপৰাধৰ পৰা আমি বিভিন্ন উপায়ে�ৰে ৰক্ষা কৰিব পাৰো। চাইবাৰ অপৰাধৰ বিৰুদ্ধে ল'ব পৰা কিছুমান প্ৰতিকাৰ আৰু প্ৰশমনৰ ব্যৱস্থা চাওঁ আহক।

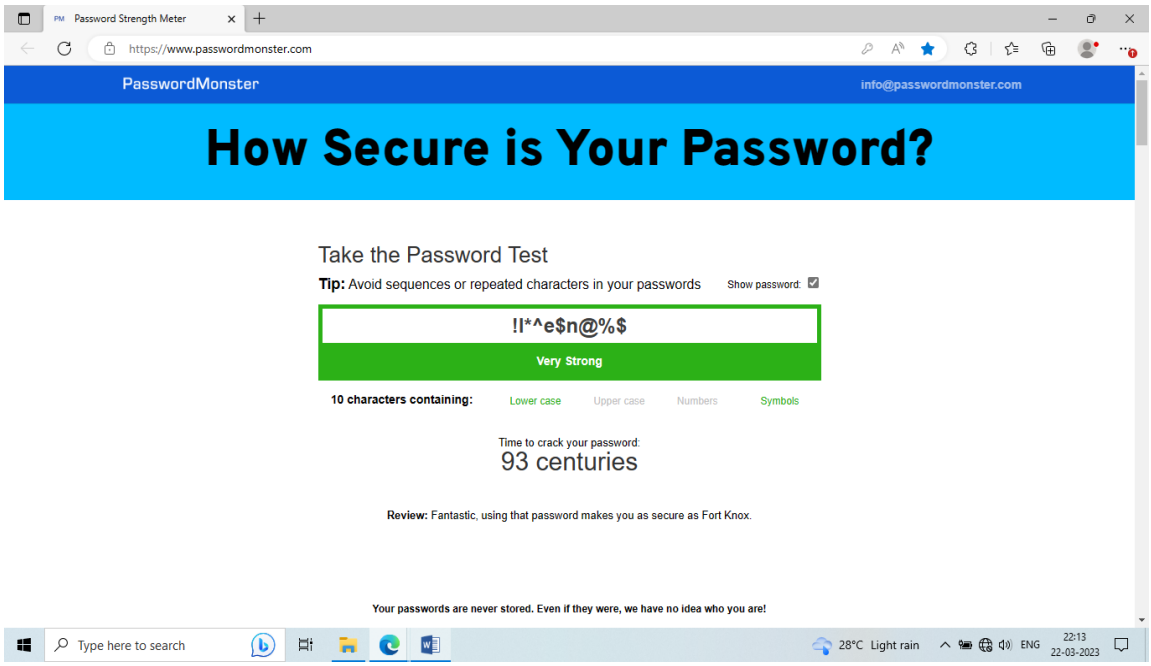
- **চফ্‌ট্ ৱেৰ আপডেট আৰু উন্নীতকৰণ:** আমি ব্যৱহাৰ কৰা বিভিন্ন চফ্‌ট্ ৱেৰসমূহ সেই চফ্‌ট্ ৱেৰৰ নতুন সংস্কৰণ উপলব্ধ হ'লে সময়ে সময়ে আপডেট কৰা উচিত। নতুন চফ্‌ট্ ৱেৰ সংস্কৰণত কেৱল নতুন বৈশিষ্ট্যই নহয়, ক'ডৰ পেচো থাকে য'ত বিভিন্ন ভাইৰাছ আৰু মেলৱেৰ আক্ৰমণৰ পৰা সুৰক্ষাৰ ব্যৱস্থা থাকে।

- **এণ্টি-ভাইৰাছ আৰু এণ্টি-মেলৱেৰ চফ্‌ট্ ৱেৰ ইনষ্টল কৰা:** এণ্টি-ভাইৰাছ আৰু এণ্টি-মেলৱেৰ চফ্‌ট্ ৱেৰ ইনষ্টল আৰু আপডেট কৰি আমাৰ ইলেক্ট্ৰনিক ডিভাইচসমূহ সুৰক্ষিত কৰাটো ভাল অভ্যাস। এণ্টিভাইৰাছ আৰু এণ্টি-মেলৱেৰ চফ্টৱেৰে বহুতো চাইবাৰ অপৰাধৰ বিৰুদ্ধে আমাৰ ডিভাইচসমূহক অতিৰিক্ত স্তৰৰ সুৰক্ষা প্ৰদান কৰে।

- **শক্তিশালী পাছৱৰ্ড ব্যৱহাৰ কৰা:** আমি আমাৰ অনলাইন একাউণ্টৰ মূলতঃ ইণ্টাৰনেট বেংকিং, ব্যক্তিগত মেইল ঠিকনা, কৰ্মৰ মেইল ঠিকনা আদিৰ বাবে সদায় শক্তিশালী পাছৱৰ্ড ব্যৱহাৰ কৰা উচিত। আমাৰ বেছিভাগেই বহু একাউণ্টৰ বাবে একেটা পাছৱৰ্ড কৰোঁ। কিন্তু যেতিয়া এই পাছৱৰ্ডটো যথেষ্ট শক্তিশালী নহয় তেতিয়া চাইবাৰ অপৰাধীসকলে ইয়াক আক্ৰমন কৰিবলৈ আৰু আমাৰ বিত্তীয় আৰু আমাৰ গোপনীয় তথ্যৰ অপব্যৱহাৰ কৰিবলৈ বেছি সময় নালাগে। আমাৰ পাছৱৰ্ড কিমান শক্তিশালী পৰীক্ষা কৰাৰ এটা উপায় হ'ল https://www.passwordmonster.com/ URL ত পাছৱৰ্ড মনষ্টাৰ ৱেবছাইটত দিয়া সঁজুলি ব্যৱহাৰ কৰি পৰীক্ষা কৰা । উদাহৰণস্বৰূপে, "admin@123" ৰ দৰে পাছৱৰ্ড ১.৬৭ ছেকেণ্ডতে আক্ৰমণ কৰিব পাৰে আনহাতে "!l *^ e$n @%$" ৰ দৰে শক্তিশালী পাছৱৰ্ড লাভ কৰিবলৈ বহু শতিকাৰ প্ৰয়োজন হ'ব।



চিত্ৰ 5.4: দুৰ্বল গুপ্তশব্দৰ পৰীক্ষা



চিত্ৰ 5.5: শক্তিশালী গুপ্তশব্দৰ পৰীক্ষা

- **ব্যক্তিগত তথ্য কাকো নিদিয়া:** ব্যক্তিগত বা বিত্তীয় তথ্য ভাগ-বতৰা কৰাৰ সময়ত আমি সদায় অতি সাৱধান হোৱা উচিত। এই গোপনীয় তথ্যসমূহ আকস্মিকভাৱে বার্তা প্ৰেৰণ, আড্ডা বা ফোন কলত এৰাব নোৱাৰা ব্যক্তি বা বেংকিং বিষয়া বা গুৰুত্বপূৰ্ণ চৰকাৰী বিষয়াৰ ৰূপ লোৱা লোকক শ্বেয়াৰ কৰা উচিত নহয়।

৫.৬ চাইবাৰ অপৰাধৰ আইনী দৃষ্টিভংগী

ভাৰতত চাইবাৰ অপৰাধসমূহ ২০২০ চনৰ তথ্য প্ৰযুক্তি (আই টি) আইনৰ অধীনত সামৰি লোৱা হৈছে। ২০২০ চনৰ পৰা এই আইনখন একাধিকবাৰ সংশোধন কৰা হৈছে আৰু নতুন চাইবাৰ অপৰাধসমূহ আইনৰ অধীনত অন্তৰ্ভুক্ত কৰা হৈছে।

৫.৬.১ তথ্য প্ৰযুক্তি আইন ২০০০

তথ্য প্ৰযুক্তি (আই টি) আইন, ২০০০ হৈছে তথ্য প্ৰযুক্তিৰ বাণিজ্যিক ব্যৱহাৰৰ বাবে এক সক্ষম পৰিৱেশ সৃষ্টি কৰাৰ প্ৰধান উদ্দেশ্যেৰে প্ৰণয়ন কৰা ভাৰতীয় সংসদৰ আইন। আই টি আইনখনে ভাৰতত চাইবাৰ অপৰাধ আৰু ইলেক্ট্ৰনিক কমাৰ্চৰ সন্দৰ্ভত আইনৰ দ্বাৰা শাস্তিযোগ্য কাৰ্য্যসমূহ নিৰ্দিষ্ট কৰিছে। ১৮৬০ চনৰ ভাৰতীয় দণ্ডবিধিৰ (আই পি চি), ১৮৭২ চনৰ ভাৰতীয় প্ৰমাণ আইন, ১৮৯১ চনৰ বেংকাৰছ বুক অৰ এভিডেন্স এক্ট আৰু ১৯৩৪ চনৰ ৰিভাৰ্ছ বেংক অৰ ইণ্ডিয়া আইনৰ বিভিন্ন ধাৰা সংশোধন কৰি নতুন প্ৰযুক্তি ব্যৱহাৰ কৰি কৰা চাইবাৰ অপৰাধসমূহ অন্তৰ্ভুক্ত কৰা হৈছে।

৫.৬.২ সংশোধনী

২০০৮ চনত আই টি আইনখনৰ এটা ডাঙৰ সংশোধন কৰা হয়। ২০০৮ চনত ৬৬এৰ আপত্তিজনক বাৰ্তা প্ৰেৰণৰ বাবে শাস্তি প্ৰদান ধাৰা প্ৰৱৰ্তন কৰা হয়। কৰ্তৃপক্ষক "যিকোনো কম্পিউটাৰ সম্পদৰ জৰিয়তে যিকোনো তথ্য আটক বা নিৰীক্ষণ বা ডিক্ৰিপচন" কৰাৰ ক্ষমতা প্ৰদান কৰা ৬৯ নং ধাৰাও প্ৰৱৰ্তন কৰা হয়। সংশোধনীত পৰ্ণগ্ৰাফী, শিশু পৰ্ণ, চাইবাৰ সন্ত্ৰাসবাদ আৰু ভয়ৰিজমৰ (voyeurism) সৈতে জড়িত সমস্যাসমূহ সমাধানৰ ব্যৱস্থাও অন্তৰ্ভুক্ত কৰা হয়। ২০১৩ চনত চাইবাৰ ষ্টাকিংৰ অপৰাধ অন্তৰ্ভুক্ত কৰিবলৈ আন এটা সংশোধনী কৰা হয়।

৫.৬.৩ আই টি আইনৰ অধীনত চাইবাৰ অপৰাধ

এতিয়া আই টি আইনৰ অধীনত বিভিন্ন ধাৰাত শাস্তিযোগ্য কৰি তোলা বিভিন্ন অপৰাধৰ কথা চাওঁ আহক।

শাখা	অপৰাধ
ধাৰা ৬৫	কম্পিউটাৰৰ উৎস নথিপত্ৰত হাত দিয়া
ধাৰা ৬৬	কম্পিউটাৰ সম্পৰ্কীয় অপৰাধ

ধাৰা ৬৬এ	যোগাযোগ সেৱা আদিৰ জৰিয়তে আপত্তিজনক বার্তা প্রেৰণ কৰাৰ শাস্তি।
ধাৰা ৬৬বি	চুৰি হোৱা কম্পিউটাৰৰ সম্পদ বা যোগাযোগৰ যন্ত্র অসৎভাৱে লাভ কৰাৰ শাস্তি।
ধাৰা ৬৬চি	পৰিচয় চুৰিৰ শাস্তি।
ধাৰা ৬৬ডি	কম্পিউটাৰ সম্পদ ব্যৱহাৰ কৰি ব্যক্তিত্ব প্রতাৰণা কৰাৰ শাস্তি।
ধাৰা ৬৬ই	গোপনীয়তা উলংঘা কৰাৰ শাস্তি।
ধাৰা ৬৬এফ	চাইবাৰ সন্ত্রাসবাদৰ শাস্তি।
ধাৰা ৬৭	ইলেক্ট্রনিক ৰূপত অশ্লীল সামগ্রী প্রকাশ বা প্রেৰণ কৰাৰ শাস্তি।
ধাৰা ৬৭এ	ইলেক্ট্রনিক ৰূপত যৌন সম্পর্কীয় কার্য্য আদি থকা সামগ্রী প্রকাশ বা প্রেৰণৰ শাস্তি।
ধাৰা ৬৭বি	ইলেক্ট্রনিক ৰূপত শিশুক যৌন সম্পর্কীয় কার্য্য আদিত চিত্রিত কৰা সামগ্রী প্রকাশ বা প্রেৰণৰ শাস্তি।
ধাৰা ৬৭চি	মধ্যস্থতাকাৰীৰ দ্বাৰা তথ্য সংৰক্ষণ আৰু ধৰি ৰখা।
ধাৰা ৬৮	নির্দেশনা দিবলৈ নিয়ন্ত্রকৰ ক্ষমতা।
ধাৰা ৬৯	যিকোনো কম্পিউটাৰ সম্পদৰ জৰিয়তে যিকোনো তথ্যৰ বাধা বা নিৰীক্ষণ বা ডিক্রিপচনৰ বাবে নির্দেশনা জাৰি কৰাৰ ক্ষমতা।
ধাৰা ৬৯এ	যিকোনো কম্পিউটাৰ সম্পদৰ জৰিয়তে যিকোনো তথ্যৰ ৰাজহুৱা প্ররেশৰ বাবে বাধা দিয়াৰ বাবে নির্দেশনা জাৰি কৰাৰ ক্ষমতা।
ধাৰা ৬৯বি	চাইবাৰ সুৰক্ষাৰ বাবে যিকোনো কম্পিউটাৰ সম্পদৰ জৰিয়তে ট্রেফিক ডেটা বা তথ্য নিৰীক্ষণ আৰু সংগ্রহ কৰিবলৈ অনুমোদন দিয়াৰ ক্ষমতা।
ধাৰা ৭০	সুৰক্ষিত ব্যৱস্থাপ্রণালী।
ধাৰা ৭১	ভুল বর্ণনাৰ শাস্তি।
ধাৰা ৭২	গোপনীয়তা আৰু গোপনীয়তা ভংগ কৰাৰ বাবে শাস্তি।
ধাৰা ৭২এ	বৈধ চুক্তি ভংগ কৰি তথ্য প্রকাশ কৰাৰ শাস্তি।
ধাৰা ৭৩	কিছুমান বিশেষ তথ্যত প্রমাণপত্রত ভুৱা ইলেক্ট্রনিক স্বাক্ষৰ প্রকাশ কৰাৰ বাবে শাস্তি।

ধাৰা ৭৪	প্ৰৱঞ্চনামূলক উদ্দেশ্যত প্ৰকাশ।
ধাৰা ৭৫	ভাৰতৰ বাহিৰত সংঘটিত অপৰাধ বা উলংঘাৰ বাবে আবেদন কৰিবলৈ আইন।
ধাৰা ৭৬	বাজেয়াপ্ত কৰা।
ধাৰা ৭৭	অন্য শাস্তিত বাধা নিদিয়াৰ বাবে ক্ষতিপূৰণ, শাস্তি বা বাজেয়াপ্ত কৰা।
ধাৰা ৭৮	অপৰাধৰ তদন্তৰ ক্ষমতা।

আই পি চিৰ অধীনত হোৱা কিছুমান চাইবাৰ অপৰাধ তলত উল্লেখ কৰা হৈছে:

- ইমেইলৰ দ্বাৰা ভাবুকি বার্তা প্ৰেৰণ কৰা - Sec 503 IPC
- ইমেইলৰ দ্বাৰা মানহানিকাৰক বার্তা প্ৰেৰণ কৰা - Sec 499 IPC
- ইলেক্ট্ৰনিক ৰেকর্ডৰ জাল - ধাৰা ৪৬৩ আইপিচি
- ইমেইল স্পুফিং - Sec 463 IPC
- ভুৱা ৰেবছাইট, চাইবাৰ জালিয়াতি - Sec 420 IPC
- ৰেব-জেকিং - Sec. 383 আইপিচি
- ই-মেইলৰ অপব্যৱহাৰ - Sec. 500 IPC

৫.৭ ভাৰতত চাইবাৰ অপৰাধ আৰু চাইবাৰ সুৰক্ষাৰ সৈতে জড়িত সংস্থা

চাইবাৰ অপৰাধৰ বিৰুদ্ধে যুঁজিবলৈ ভাৰত চৰকাৰৰ অন্যতম পদক্ষেপ হৈছে ভাৰতীয় চাইবাৰ অপৰাধ সমন্বয় কেন্দ্ৰ (I4C)। এই চৰকাৰী পদক্ষেপৰ লক্ষ্য হৈছে ভাৰতত চাইবাৰ অপৰাধক সমন্বিত আৰু ফলপ্ৰসূভাৱে মোকাবিলা কৰা। ই গৃহ পৰিক্ৰমা মন্ত্ৰালয় (এম এইচ এ)ৰ সৈতে জড়িত। চাইবাৰ অপৰাধৰ বিৰুদ্ধে যুঁজত ইয়াক মূল হিচাপে প্ৰতিষ্ঠা কৰা হৈছিল। I4C এ কেইবাটাও মূল ক্ষেত্ৰত গুৰুত্ব আৰোপ কৰে, সেইবোৰ হৈছে-

- আইন প্ৰয়োগকাৰী সংস্থাসমূহৰ গৱেষণা সমস্যা আৰু প্ৰয়োজনীয়তাসমূহ চিনাক্ত কৰা আৰু ভাৰত আৰু বিদেশৰ শিক্ষানুষ্ঠান আৰু গৱেষণা প্ৰতিষ্ঠানসমূহৰ সৈতে সহযোগিতাত নতুন প্ৰযুক্তি আৰু ফৰেনছিক সঁজুলি বিকশিত কৰিবলৈ গৱেষণা আৰু বিকাশ কার্য্যকলাপ হাতত লোৱা।

- চাইবাৰস্পেচক চৰমপন্থী আৰু সন্ত্রাসবাদী গোটসমূহে অপব্যৱহাৰ কৰাৰ পৰা ৰক্ষা কৰা।
- দ্রুত পৰিৱর্তনশীল প্রযুক্তিৰ লগত খাপ খুৱাবলৈ চাইবাৰ আইনত প্রয়োজনীয় সংশোধনীৰ পৰামর্শ দিয়া আৰু আন্তঃৰাষ্ট্রীয় সহযোগিতা বৃদ্ধি কৰা।
- MHA-ৰ সংশ্লিষ্ট নোডেল প্রাধিকৰণৰ সৈতে সহযোগিতা কৰি চাইবাৰ অপৰাধৰ সৈতে জড়িত অন্যান্য দেশসমূহৰ সৈতে Mutual Legal Assistance Treaties (MLAT) ৰ কার্য্যকৰীকৰণৰ সৈতে জড়িত কার্য্যকলাপসমূহ সম্পাদন কৰা।

ভাৰতীয় চাইবাৰ অপৰাধ সমন্বয় কেন্দ্রত চাইবাৰ অপৰাধৰ বিভিন্ন সমস্যাৰ সৈতে মোকাবিলা কৰাৰ বাবে সাতটা গুৰুত্বপূর্ণ উপাদান সংগঠন আছে। এই উপাদানসমূহ তলত তালিকাভুক্ত কৰা হৈছে -

১. ৰাষ্ট্রীয় চাইবাৰ অপৰাধ প্রত্যাশা বিশ্লেষণ ইউনিট (TAU) National Cyber Crime Threat Analytics Unit (TAU):: এই ইউনিটে ভাবুকি বুদ্ধিমত্তাৰ প্রতিবেদন সৃষ্টি কৰে আৰু নির্দিষ্ট চাইবাৰ অপৰাধৰ ওপৰত পর্যায়ক্রমিক আলোচনাৰ সুবিধা প্রদান কৰে, যিয়ে আইন প্রয়োগকাৰী বিশেষজ্ঞ আৰু উদ্যোগৰ বিশেষজ্ঞসকলক একত্রিত কৰি সুচল পৰিৱেশ সৃষ্টি কৰে।

২. ৰাষ্ট্রীয় চাইবাৰ অপৰাধ প্রতিবেদন পর্টেলঃ National Cyber Crime Reporting Portal এই পর্টেলে সকলো প্রকাৰৰ চাইবাৰ অপৰাধৰ ঘটনাৰ প্রতিবেদন সাব্যস্ত কৰে, বিশেষকৈ মহিলা আৰু শিশুৰ বিৰুদ্ধে অপৰাধৰ ওপৰত গুৰুত্ব আৰোপ কৰে। ই স্বয়ংক্রিয়ভাৱে প্রতিবেদনসমূহ সংশ্লিষ্ট ৰাজ্য/কেন্দ্রশাসিত অঞ্চললৈ প্রেৰণ কৰে।

৩. ৰাষ্ট্রীয় চাইবাৰ অপৰাধ প্রশিক্ষণ কেন্দ্রঃ National Cyber Crime Training Centre এই কেন্দ্রই মুখ্য চাইবাৰ অপৰাধৰ ভাবুকিৰ বিৰুদ্ধে বুদ্ধিমত্তা-প্রণালীগত ব্যৱস্থা কৰে। ই চাইবাৰ অপৰাধৰ বিৰুদ্ধে বহু-আইনী ক্ষেত্র কার্য্যকৰীকৰণৰ বাবে চিনাক্তকৰণ, গুৰুত্ব নির্ণয়, তদন্ত প্রস্তুত কৰে।

৪. চাইবাৰ অপৰাধ ইকোচিষ্টেম পৰিচালনা ইউনিট Cyber Crime Ecosystem Management Unit:: এই সংগঠনে নতুন ডিজিটেল প্রযুক্তিৰ ব্যৱহাৰ কৰি চাইবাৰ অপৰাধৰ ফৰেনছিক বিশ্লেষণ আৰু গৱেষণাত সহায় কৰে।

৫. ৰাষ্ট্রীয় চাইবাৰ অপৰাধ গৱেষণা আৰু উদ্ভাৱন কেন্দ্র National Cyber Crime Research and Innovation Centre: এই কেন্দ্রই প্রভাৱ নিয়ন্ত্রণ আৰু গৱেষণাৰ ওপৰত গুৰুত্ব দি চাইবাৰ অপৰাধৰ ওপৰত পাঠ্যক্রম অনুমোদন কৰে। ই চাইবাৰ অপৰাধ চিনাক্তকৰণ, নিয়ন্ত্রণ, আৰু প্রতিবেদনৰ ওপৰত সিমুলেটেড পৰিৱেশত ব্যৱহাৰিক প্রশিক্ষণ প্রদান কৰে।

৬. ৰাষ্ট্ৰীয় চাইবাৰ অপৰাধ ফৰেনছিক লেবৰেটৰী (NCFL) ইকোচিষ্টেম National Cyber Crime Forensic Laboratory (NCFL) Ecosystem: এই ইকোচিষ্টেমে শিক্ষানুষ্ঠান, উদ্যোগ, আৰু চৰকাৰক একত্ৰিত কৰি চাইবাৰ অপৰাধৰ সচেতনতা বৃদ্ধি, সাধাৰণ মানবিশিষ্ট অপাৰেটিং প্ৰক্ৰিয়া স্থাপন, আৰু চাইবাৰ অপৰাধৰ প্ৰতি সঁহাৰি জনায়।

৭. যুটীয়া চাইবাৰ অপৰাধ গৱেষণা দলৰ প্লেটফৰ্ম Platform for Joint Cyber Crime Investigation Team: এই সংগঠনে উদীয়মান প্ৰযুক্তিগত উন্নয়ন চোৱা-চিতা কৰে, সম্ভাব্য দুৰ্বলতাসমূহৰ অনুমান কৰে, আৰু চাইবাৰ অপৰাধ, প্ৰভাৱ নিয়ন্ত্ৰণ, আৰু গৱেষণাৰ ক্ষেত্ৰত সহযোগিতা কৰে।

৫.৮ ক্ষেত্ৰ অধ্যয়ন

ভাৰতত চাইবাৰ অপৰাধৰ কিছুমান গুৰুত্বপূৰ্ণ ঘটনা চাওঁ আহক-

- **য়াহু বনাম আকাশ অৰোৰা গোচৰ:** এই গোচৰত প্ৰতিবাদী আকাশ অৰোৰাৰ বিৰুদ্ধে ট্ৰেডমাৰ্ক বা ডমেইন নাম 'yahooindia.com' ব্যৱহাৰ কৰাৰ অভিযোগ উত্থাপন হৈছিল। এই গোচৰটো ১৯৯৯ চনত ৰুজো হৈছিল আৰুষিয়ে ভাৰতত চাইবাৰ অপৰাধৰ প্ৰথম গোচৰ আছিল।

- **চাকৰি জালিয়াতিৰ গোচৰ:** এই ঘটনাত ভুক্তভোগীয়ে মাৰুতি চুজুকিৰ বুলি দাবী কৰি এটা ইমেইল পাইছিল, য'ত লিখা আছিল যে তেওঁলোকৰ বিজ্যুমক Monster.comৰ পৰা প্ৰতিমাহে ২.০ লাখ টকা দৰমহাৰে অভিযান্ত্ৰিক পদৰ বাবে চৰ্টলিষ্ট কৰা হৈছে । ইমেইলত ভুক্তভোগীক ৮,২০০ টকা এটা একাউণ্টত ভৰাই পে স্লিপখন লৈ সাক্ষাৎকাৰলৈ লৈ আহিবলৈ জনোৱা হৈছিল আৰু জনাইছিল যে সেই ধন ঘূৰাই দিয়া হ'ব। তদন্তত দেখা গ'ল যে ইমেইলবোৰ বিদেশৰ পৰা প্ৰেৰণ কৰা হৈছিল, বেংক একাউণ্টটো ভুৱা আছিল, আৰু ধনখিনি এটিএমৰ পৰা দ্ৰুতভাৱে উলিওৱা হৈছিল; অপৰাধীসকলে এছএমএছ আৰু ফোন কলৰ জৰিয়তেও ভুক্তভোগীৰ সৈতে যোগাযোগ কৰিছিল আৰু অৱশেষত মোবাইল কল ট্ৰেচিঙৰ জৰিয়তে গ্ৰেপ্তাৰ কৰা হৈছিল।

- **Baazee.com গোচৰঃ** দিল্লীৰ বজাৰৰ লগতে ৱেবছাইটত আপত্তিজনক সামগ্ৰীৰে এখন চিডি বিক্ৰী কৰাৰ অপৰাধত ২০০৪ চনৰ ডিচেম্বৰ মাহত Baazee.com ৰ চিইঅ'ক গ্ৰেপ্তাৰ কৰা হৈছিল। তেওঁক গ্ৰেপ্তাৰ কৰাৰ পিছত মুম্বাই আৰু দিল্লী আৰক্ষীয়ে ব্যৱস্থা গ্ৰহণ কৰে, আৰু পিছত চিইঅ'গৰাকীক জামিনত মুকলি কৰি দিয়া হয়। এই কাণ্ডই ইণ্টাৰনেট সেৱা প্ৰদানকাৰী আৰু বিষয়বস্তু প্ৰদানকাৰীৰ মাজত পাৰ্থক্য কৰাৰ

বিষয়ে প্ৰশ্ন উত্থাপন কৰিছিল আৰু চাইবাৰ অপৰাধৰ গোচৰসমূহ চম্ভালাৰ ক্ষেত্ৰত উন্নত শিক্ষাৰ প্ৰয়োজনীয়তাৰ ওপৰত আলোকপাত কৰিছিল।

- **নেচনেল এছ'চিয়েচন অৱ চফ্টৱেৰ এণ্ড চার্ভিচ কোম্পানী বনাম অজয় ছুদ এণ্ড অদার্ছ গোচৰ** - ২০০৫ চনৰ মার্চ মাহত, দিল্লী উচ্চ ন্যায়ালয়ে National Association of Software and Service Companies বনাম Ajay Sood & Others গোচৰত ফিচিঙক অবৈধ বুলি ঘোষণা কৰে। ফিচিঙক এটা অনলাইন প্ৰৱঞ্চনা বুলি সংজ্ঞায়িত কৰা হৈছিল, য'ত কোনো ব্যক্তিয়ে এটা বৈধ সংস্থা হিচাপে ভেশ ধৰি ব্যক্তিগত তথ্য যেনে পাছৱর্ড আদি চুৰ কৰে। ভাৰতত ফিচিঙৰ বাবে বিশেষ আইন নথকা স্বত্বেও, ন্যায়ালয়ে কৈছিল যে ইয়াত প্ৰৱঞ্চনা জড়িত থাকে আৰু ইয়ে গ্ৰাহক আৰু যি সংস্থাক অনুকৰণ কৰা হৈছে, দুয়োটাৰে ক্ষতি কৰে। ন্যায়ালয়ে ইয়াক সংস্থাৰ সুনাম নষ্ট কৰা বুলি গণ্য কৰিছিল। এই গোচৰত এটা নকল প্লেচমেণ্ট এজেন্সিয়ে নাছকম (Nasscom) হিচাপে ভেশ ধৰি ব্যক্তিগত তথ্য সংগ্ৰহ কৰিছিল। বিবাদীয় পক্ষই তেওঁলোকৰ কার্য্য স্বীকাৰ কৰিছিল, যিয়ে ভাৰতীয় ন্যায়পালিকাই বৌদ্ধিক সম্পত্তিৰ অধিকাৰ ৰক্ষা কৰাৰ প্ৰতি থকা সজাগতা দেখুৱাইছিল।



অগ্ৰগতি নিৰীক্ষণ

প্ৰশ্ন ১: ভাৰতত চাইবাৰ অপৰাধৰ গোচৰ কেনেকৈ দাখিল কৰিব পাৰি?

প্ৰশ্ন ২: ২০০০ চনৰ আইটি আইনত কৰা দুটা সংশোধনী কি কি?

প্ৰশ্ন ৩: I4C যোজনাৰ উপাদানসমূহ কি কি?

প্ৰশ্ন ৪: চাইবাৰ সন্ত্ৰাসবাদৰ বাবে কোনটো ধাৰা প্ৰযোজ্য?

ক্ৰিয়া-কলাপ

১. PasswordMonster ৱেবছাইটৰ সহায়ত আপোনাৰ পাছৱর্ডটো কিমান শক্তিশালী পৰীক্ষা কৰক। যদি আপোনাৰ পাছৱর্ডটো যথেষ্ট শক্তিশালী নহয়, তেন্তে ইয়াক সলনি কৰক আৰু ইয়াৰ ঠাইত এটা শক্তিশালী পাছৱর্ড ব্যৱহাৰ কৰক।



৫.৯ আমি কি কি শিকিলোঁ

- Modus-operandi হৈছে লেটিন ভাষাৰ এটা শব্দ যাৰ অর্থ হৈছে "কার্য্যৰ ধৰণ"।
- চাইবাৰ অপৰাধীৰ মডাছ-অপাৰাণ্ডি হৈছে এটা চিনাক্তকৰণ বৈশিষ্ট্য বা আচৰণৰ আর্হি যিটো ব্যৱহাৰ কৰি অপৰাধীয়ে অপৰাধ সংঘটিত কৰিছিল আৰু এতিয়া ইয়াক অপৰাধীক চিনাক্ত কৰিবলৈ ব্যৱহাৰ কৰিব পাৰি।
- https://cybercrime.gov.in/Default.aspx URL ব্যৱহাৰ কৰি "National Cyber Crime Reporting Portal" ৰ ৱেবছাইটত চাইবাৰ অপৰাধৰ গোচৰ দিব পাৰি ।
- "১৯৩০" হেল্পলাইন নম্বৰত ফোন কল ব্যৱহাৰ কৰিও চাইবাৰ অপৰাধৰ অভিযোগ দাখিল কৰিব পাৰি।
- তথ্য প্রযুক্তি (আই টি) আইন, ২০০০ হৈছে তথ্য প্রযুক্তিৰ বাণিজ্যিক ব্যৱহাৰৰ বাবে এক সক্ষম পৰিৱেশ সৃষ্টি কৰাৰ প্রধান উদ্দেশ্যেৰে প্রণয়ন কৰা ভাৰতীয় সংসদৰ আইন।
- আই টি আইনখনে ভাৰতত চাইবাৰ অপৰাধ আৰু ইলেক্ট্রনিক কমার্চৰ সন্দর্ভত আইনৰ দ্বাৰা শাস্তিযোগ্য কৰি তোলা কার্য্যসমূহ নির্দিষ্ট কৰিছে।
- ২০০৮ চনত আই টি আইনখনৰ এটা ডাঙৰ সংশোধন কৰা হয়। ২০০৮ চনত ৬৬এ ধাৰা প্রৱর্তন কৰা হয় যিয়ে আপত্তিজনক বার্তা প্রেৰণৰ বাবে শাস্তি প্রদান কৰে।
- ৬৯ নং ধাৰাও প্রৱর্তন কৰা হৈছিল যিয়ে কর্তৃপক্ষক "যিকোনো কম্পিউটাৰ সম্পদৰ জৰিয়তে যিকোনো তথ্যক বাধা বা নিৰীক্ষণ বা ডিক্রিপচন" কৰাৰ ক্ষমতা প্রদান কৰিছিল।
- ভাৰতৰ চাইবাৰ অপৰাধ সমন্বয় কেন্দ্র (I4C) হৈছে ভাৰতৰ চাইবাৰ অপৰাধৰ সৈতে সমন্বয় আৰু ফলপ্রসূভাৱে মোকাবিলা কৰাৰ বাবে চৰকাৰী পদক্ষেপ।
- ভাৰতীয় চাইবাৰ অপৰাধ সমন্বয় কেন্দ্রত চাইবাৰ অপৰাধৰ বিভিন্ন সমস্যাৰ সৈতে মোকাবিলা কৰাৰ বাবে সাতটা গুৰুত্বপূর্ণ সংগঠন আছে।

৫.১০ অগ্রগতিৰ খতিয়ান

প্ৰশ্ন ১ ৰ উত্তৰঃ ভাৰতত " https://cybercrime.gov.in/Default.aspx " URL ব্যৱহাৰ কৰি "National Cyber Crime Reporting Portal" ৰ ৱেবছাইটত চাইবাৰ অপৰাধৰ ৰিপৰ্ট দিব পাৰি ।

প্ৰশ্ন ২ ৰ উত্তৰ : সংশোধনীৰ এটা ২০০৮ চনত ৬৬এ ধাৰাত প্ৰৱৰ্তন কৰা হৈছিল যিয়ে আপত্তিজনক বাৰ্তা প্ৰেৰণৰ বাবে শাস্তি প্ৰদান কৰিছিল। ৬৯ নং ধাৰাত আন এটা সংশোধনীও উত্থাপন কৰা হৈছিল যিয়ে কৰ্তৃপক্ষক "যিকোনো কম্পিউটাৰ সম্পদৰ জৰিয়তে যিকোনো তথ্যক বাধা বা নিৰীক্ষণ বা ডিক্ৰিপচন" কৰাৰ ক্ষমতা প্ৰদান কৰিছিল।

প্ৰশ্ন ৩ ৰ উত্তৰঃ ভাৰতীয় চাইবাৰ অপৰাধ সমন্বয় কেন্দ্ৰত সাতটা গুৰুত্বপূৰ্ণ উপাদান সংস্থা আছে যিবোৰ হ'ল- ৰাষ্ট্ৰীয় চাইবাৰ অপৰাধ ভাবুকি বিশ্লেষণ অধ্যায় (টি এ ইউ), ৰাষ্ট্ৰীয় চাইবাৰ অপৰাধ প্ৰতিবেদন পৰ্টেল, ৰাষ্ট্ৰীয় চাইবাৰ অপৰাধ প্ৰশিক্ষণ কেন্দ্ৰ, চাইবাৰ অপৰাধ পৰিৱেশ তন্ত্ৰ ব্যৱস্থাপনা অধ্যায় , ৰাষ্ট্ৰীয় চাইবাৰ অপৰাধ গৱেষণা আৰু উদ্ভাৱন কেন্দ্ৰ, ৰাষ্ট্ৰীয় চাইবাৰ অপৰাধ ফৰেনছিক পৰীক্ষাগাৰ (এন চি এফ এল) পৰিৱেশ তন্ত্ৰ, আৰু যৌথ চাইবাৰ অপৰাধ অনুসন্ধান দলৰ বাবে মঞ্চ।

Q4 ৰ উত্তৰ: চাইবাৰ সন্ত্ৰাসবাদক সামৰি লোৱা ধাৰাটো হৈছে ধাৰা 66F।



৫.১১ অধিক জানিবলৈ

1) https://www.soolegal.com/rc/what-are-remedies-available-for-cyber-crimes-and-cyber-defamation-under-law-
2) https://cybercrime.gov.in/Default.aspx
3) https://www.meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf
4) https://www.indiacode.nic.in/handle/123456789/1999
5) https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html
6) https://www.legalserviceindia.com/legal/article-797-an-analysis-on-cyber-crime-in-india.html
7) https://i4c.mha.gov.in/
8) https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme
9) https://gurgaon.haryanapolice.gov.in/job-froud

10) https://www.indiancybersecurity.com/case_stuty_bazee.com_case.php
11) https://www.indiancybersecurity.com/case_study_nasscom_ajay_sood.php
12) https://www.cyberralegalservices.com/detail-casestudies.php



৫.১২ আৰ্হি প্ৰশ্ন

প্ৰশ্ন ১. মডাছ-অপাৰাণ্ডি কি?

প্ৰশ্ন ২। ভাৰতত চাইবাৰ অপৰাধৰ ৰিপৰ্ট দিব পৰা বিভিন্ন উপায়বোৰ কি কি?

প্ৰশ্ন ৩। I4C ৰ উদ্দেশ্যসমূহ বৰ্ণনা কৰক।

প্ৰশ্ন ৪। ভাৰতত চাইবাৰ অপৰাধৰ যিকোনো দুটা কেছ বৰ্ণণা কৰক।

প্ৰশ্ন ৫। আই টি আইন ২০০০ৰ অধীনত থকা বিভিন্ন আইনী বিধানৰ বৰ্ণনা কৰক।

প্ৰশ্ন ৬। চাইবাৰ অপৰাধৰ বিৰুদ্ধে ব্যৱহাৰ কৰিব পৰা কিছুমান প্ৰতিকাৰ আৰু প্ৰশমন ব্যৱস্থাৰ বিষয়ে ব্যাখ্যা কৰক।

প্ৰশ্ন ৭। ভাৰতীয় আইনৰ আই পি চিৰ অধীনত অহা চাইবাৰ অপৰাধবোৰ কি কি?

প্ৰশ্ন ৮। আই টি আইন ২০০০ৰ বৰ্ণনা কৰক। আইনত কৰা সংশোধনীৰ বিষয়ে চমুকৈ বৰ্ণনা কৰক।

প্ৰশ্ন ৯। ৰাষ্ট্ৰীয় চাইবাৰ অপৰাধ গৱেষণা আৰু উদ্ভাৱন কেন্দ্ৰৰ উদ্দেশ্য কি ?

প্ৰশ্ন ১০। ভাৰতীয় চাইবাৰ অপৰাধ সমন্বয় কেন্দ্ৰৰ বিভিন্ন উপাদানসমূহ ব্যাখ্যা কৰক।

****

অধ্যায় ৬: সামাজিক মাধ্যমৰ পৰিচয়

অধ্যায় গাঁথনি

৬.১ উদ্দেশ্য

৬.২ সামাজিক নেটৱৰ্কৰ পৰিচয়

৬.৩ সামাজিক মাধ্যমৰ প্ৰকাৰ

৬.৪ সামাজিক মাধ্যম প্লেটফৰ্ম

৬.৫ অধ্যায়টিৰ পৰা আমি কি কি শিকিলোঁ

৬.৬ অধিক জানিবলৈ

৬.৭ অগ্ৰগতিৰ খতিয়ান

৬.৮ আৰ্হি প্ৰশ্ন

৬.১ উদ্দেশ্য

এই অধ্যায়টোৰ আলোচনাৰ পৰা আপোনালোকে নিম্নোক্ত বিষয়বোৰ জানিব পাৰিব-

- বিভিন্ন সামাজিক মাধ্যম নেটৱৰ্কিং চাইটসমূহ
- বিভিন্ন ধৰণৰ ছ'চিয়েল নেটৱৰ্কিং ষ্টাইজ
- বিভিন্ন ছ'চিয়েল নেটৱৰ্কিং প্লেটফৰ্ম

৬.২ সামাজিক নেটৱৰ্কৰ পৰিচয়

সামাজিক মাধ্যমে ব্যৱহাৰকাৰীক তথ্য আদান প্ৰদান কৰিবলৈ, বিষয়বস্তু সৃষ্টি আৰু বিনিময় কৰিবলৈ, আৰু সেই ছ'চিয়েল নেটৱৰ্ক চাইটত অন্য জনসমাজৰ সৈতে সংযোগ স্থাপন কৰিবলৈ অনুমতি দিয়া ডিজিটেল প্লেটফৰ্ম আৰু সঁজুলিৰ সংকলনক বুজায়। কিছুমান জনপ্ৰিয় সামাজিক মাধ্যম প্লেটফৰ্মৰ ভিতৰত আছে ফেচবুক, টুইটাৰ, ইনষ্টাগ্ৰাম, টিকটক, লিংকডইন, আৰু স্নেপচ্যাট।

সামাজিক মাধ্যমে বিশ্বৰ মৌখিক যোগাযোগ, তথ্য বিনিময় আৰু আন জনসমাজৰ সৈতে সংযোগক এক নতুন উচ্চতালৈ লৈ গৈছে। সামাজিক মাধ্যমৰ জৰিয়তে ব্যৱহাৰকাৰীয়ে নিজৰ ডেটা যেনে ফটো, ভিডিঅ', আৰু লিখিত পোষ্ট তৈয়াৰ আৰু শ্বেয়াৰ কৰিব পাৰে। ইয়াৰ উপৰিও

ব্যৱহাৰকাৰীসকলে লাইক, ডিছলাইক আৰু শ্বেয়াৰৰ জৰিয়তে আনৰ শ্বেয়াৰ কৰা মিডিয়াৰ সৈতে জড়িত হ'ব পাৰে। ইয়াৰ উপৰিও ব্যৱহাৰকাৰীয়ে মন্তব্যৰ জৰিয়তে পোষ্টটোৰ ওপৰত নিজৰ মতামত শ্বেয়াৰ কৰিব পাৰে। সামগ্ৰীৰ প্ৰচাৰ, ৰাজনৈতিক সক্ৰিয়তা, সামাজিক ন্যায় জনমত, বিভিন্ন বিষয়ৰ সজাগতা বৃদ্ধিৰ বাবেও ইয়াক ব্যৱহাৰ কৰিব পাৰি।

কিন্তু সামাজিক মাধ্যমে মানসিক স্বাস্থ্যৰ ওপৰতো নেতিবাচক প্ৰভাৱ পেলাব পাৰে, কিয়নো ইয়াৰ ফলত নিসংগতা, উদ্বেগ, হতাশা অনুভৱ হ'ব পাৰে। ইয়াৰ উপৰিও সামাজিক মাধ্যম কেতিয়াবা ভুল তথ্য, চাইবাৰ বুলিং, অনলাইন হাৰাশাস্তিৰ উৎস হ'ব পাৰে। ব্যৱহাৰকাৰীসকলে নিৰাপদ আৰু দায়িত্বশীল অনলাইন আচৰণৰ অভ্যাস কৰাটো আৰু ইতিবাচক মানসিক স্বাস্থ্য আৰু সুস্থতাক প্ৰসাৰিত কৰা ধৰণে সামাজিক মাধ্যম ব্যৱহাৰ কৰাটো অধিক গুৰুত্বপূৰ্ণ বিষয়।

তলত এটা ভাল ছ'চিয়েল নেটৱৰ্কিং চাইটৰ কেইটামান বৈশিষ্ট্য উল্লেখ কৰা হ'ল-

1. **ব্যৱহাৰকাৰী প্ৰ'ফাইলসমূহ:** SNS ব্যৱহাৰকাৰীসকলক এটা প্ৰ'ফাইল সৃষ্টি কৰাৰ অনুমতি দিয়ে যিয়ে তেওঁলোকৰ তথ্য যেনে তেওঁলোকৰ নাম, বয়স, অৱস্থান, আগ্ৰহ, আৰু প্ৰ'ফাইল ছবি অন্তৰ্ভুক্ত কৰিবলৈ সুবিধা দিয়ে, ।

2. **সংযোগসমূহ:** ব্যৱহাৰকাৰীসকলে বন্ধুৰ অনুৰোধ প্ৰেৰণ কৰি বা ইজনে সিজনক অনুসৰণ কৰি অন্য ব্যৱহাৰকাৰীৰ সৈতে সংযোগ স্থাপন কৰিব পাৰে। এবাৰ সংযোগ স্থাপন হ'লে ব্যৱহাৰকাৰীয়ে তেওঁলোকৰ বন্ধুৰ পৰা আপডেট বা তেওঁলোকৰ নিউজ ফিডত সংযোগ চাব পাৰিব।

3. **নিউজ ফিড:** নিউজ ফিড হৈছে চাইটত ব্যৱহাৰকাৰীৰ সংযোগৰ কাৰ্যকলাপৰ দ্বাৰা সৃষ্টি হোৱা বিষয়বস্তুৰ এটা প্ৰবাহ। ইয়াত পোষ্ট, ফটো, ভিডিঅ', আৰু অন্যান্য আপডেট অন্তৰ্ভুক্ত থাকে।

4. **যোগাযোগ বৈশিষ্ট্যসমূহ:** এছএনএছে ব্যৱহাৰকাৰীসকলৰ বাবে ইজনে সিজনৰ সৈতে যোগাযোগ কৰাৰ সুবিধা কৰি দিয়ে, য'ত ব্যক্তিগত বার্তা প্ৰেৰণ, পোষ্টত মন্তব্য কৰা, আৰু গোটৰ আড্ডা আদি সোমাই থাকে।

5. **বিষয়বস্তু ভাগ-বতৰা:** ব্যৱহাৰকাৰীয়ে SNS ত বিভিন্ন ধৰণৰ বিষয়বস্তু, যেনে ফটো, ভিডিঅ', আৰু প্ৰবন্ধ বা ৱেবছাইটৰ লিংক শ্বেয়াৰ কৰিব পাৰে।

6. **গোপনীয়তা ছেটিং:** SNS-এ সাধাৰণতে ব্যৱহাৰকাৰীসকলক তেওঁলোকৰ গোপনীয়তা ছেটিং নিয়ন্ত্ৰণৰ কৰাৰ ক্ষমতা প্ৰদান কৰে, যিয়ে তেওঁলোকক

তেওঁলোকৰ প্ৰ'ফাইল আৰু বিষয়বস্তু কোনে চাব পাৰে নিৰ্বাচন কৰাৰ অনুমতি দিয়ে।

7. **মোবাইল এছেচিবিলিটি:** বহুতো এছএনএছত মোবাইল এপ্লিকেচন আছে, যাৰ ফলত ব্যৱহাৰকাৰীয়ে নিজৰ মোবাইল ডিভাইচত প্লেটফৰ্মত প্ৰৱেশ কৰিব পাৰে।

৬.৩ সামাজিক মাধ্যমৰ প্ৰকাৰ

সামাজিক মাধ্যম নেটৱৰ্কৰ ভিন্নতা আছে, প্ৰত্যেকৰে নিজস্ব বৈশিষ্ট্য, দৰ্শক আৰু উদ্দেশ্যও আছে। ইয়াত আমি কিছুমান জনপ্ৰিয় সামাজিক মাধ্যম নেটৱৰ্কৰ বিষয়ে আলোচনা কৰিম-

ফেচবুকঃ ফেচবুক হৈছে আমেৰিকাৰ কোম্পানী মেটা প্লেটফৰ্মছৰ মালিকানাধীন অনলাইন সামাজিক মাধ্যম আৰু ছ'চিয়েল নেটৱৰ্কিং সেৱা। ২০০৪ চনত মাৰ্ক জুকাৰবাৰ্গে প্ৰতিষ্ঠা কৰা এই নেটৱৰ্ক হৈছে মাহিলী ২.৮ বিলিয়নতকৈ অধিক সক্ৰিয় ব্যৱহাৰকাৰীৰ সৈতে সৰ্ববৃহৎ সামাজিক মাধ্যম নেটৱৰ্ক। ই ব্যৱহাৰকাৰীসকলক বন্ধু-বান্ধৱ আৰু পৰিয়ালৰ সৈতে সংযোগ স্থাপন, গোট আৰু সম্প্ৰদায়ত যোগদান, আৰু ফটো আৰু ভিডিঅ' শ্বেয়াৰ কৰাৰ অনুমতি দিয়ে। ইণ্টাৰনেট সংযোগ থকা যিকোনো ডিভাইচ, যেনে ব্যক্তিগত কম্পিউটাৰ, টেবলেট আৰু স্মাৰ্টফোনৰ পৰা ফেচবুক ব্যৱহাৰ কৰিব পাৰি। নতুন ব্যৱহাৰকাৰীয়ে ফেচবুক ব্যৱহাৰ কৰিবলৈ প্ৰথমে নিজৰ মৌলিক তথ্য দি ফেচবুকত পঞ্জীয়ন কৰিব লাগে। পঞ্জীয়ন কৰাৰ পিছত ব্যৱহাৰকাৰীয়ে প্ৰফাইল তৈয়াৰ কৰিব পাৰে যিয়ে নিজৰ মৌলিক তথ্য ৰাখে। ফেচবুকত ব্যৱহাৰকাৰীয়ে ফটো, ভিডিঅ' আৰু টেক্সট পোষ্ট কৰিব পাৰে যিবোৰ মূলতঃ বিভিন্ন গোপনীয়তা ছেটিংছৰ ওপৰত নিৰ্ভৰ কৰি ফেচবুকৰ আন ব্যৱহাৰকাৰীসকলে দেখা পায়। ব্যৱহাৰকাৰীয়ে মেচেঞ্জাৰৰ জৰিয়তেও ফেচবুকত ইজনে সিজনৰ সৈতে পোনপটীয়াকৈ যোগাযোগ কৰিব পাৰে। লগতে ব্যৱহাৰকাৰীয়ে সাধাৰণ স্বাৰ্থৰ গোটত যোগদান কৰি তেওঁলোকৰ মাজত মতামত, বাতৰি আদি ভাগ-বতৰা কৰিব পাৰে। ইয়াৰ উপৰিও ব্যৱহাৰকাৰীয়ে ফেচবুকত তেওঁলোকৰ কাৰ্য্যকলাপ আৰু তেওঁলোকে অনুসৰণ কৰা পেজৰ বিষয়ে জাননী লাভ কৰে।

Facebook-ক সদায়ে ব্যৱহাৰকাৰীৰ গোপনীয়তা, ৰাজনৈতিক হস্তক্ষেপ, আৰু mass surveillance আদিৰ সৈতে মোকাবিলা কৰাৰ বাবে সমালোচিত হৈ আহিছে। ইয়াৰ উপৰিও Facebook-এ মানসিক প্ৰভাৱ যেনে আসক্তি আৰু আত্ম-সন্মান কমোৱা, আৰু বিভিন্ন বিতৰ্ক

যেনে ভুৱা বাতৰি, ষড়যন্ত্ৰ, কপিৰাইট ভংগ, আৰু ঘৃণামূলক বক্তব্য আদিৰ বাবে সমালোচনাৰ সন্মুখীন হৈছে।

ইনষ্টাগ্ৰাম: এই প্লেটফৰ্মটোৱে দৃশ্যগত বিষয়বস্তু, যেনে ফটো আৰু ভিডিঅ'ৰ ওপৰত গুৰুত্ব আৰোপ কৰে আৰু ইয়াৰ মাহিলী ১ বিলিয়নতকৈ অধিক সক্ৰিয় ব্যৱহাৰকাৰী আছে। ইয়াৰ মালিক আছিল আমেৰিকাৰ কোম্পানী মেটা প্লেটফৰ্মছ। প্ৰভাৱশালী, ব্ৰেণ্ড, ব্যৱসায়ীসকলৰ মাজত ই অধিক জনপ্ৰিয়। ইয়াৰ দ্বাৰা মূলতঃ ব্যৱহাৰকাৰীয়ে ফটো আৰু ভিডিঅ' শ্বেয়াৰ কৰাৰ লগতে লাইক, কমেণ্ট আৰু অধিক মাধ্যমেৰে আন ব্যৱহাৰকাৰীৰ সৈতে মত বিনিময় কৰিব পাৰে। ২০১০ চনত আৰম্ভ হোৱা ইনষ্টাগ্ৰাম পিছত ই বিশ্বৰ অন্যতম জনপ্ৰিয় সামাজিক মাধ্যম প্লেটফৰ্মলৈ পৰিণত হৈছে। ইয়াত ব্যৱহাৰকাৰীসকলে এটা ব্যক্তিগত প্ৰফাইল সৃষ্টি কৰিব পাৰে, তেওঁলোকৰ ফিডত বিষয়বস্তু পোষ্ট কৰিব পাৰে, আৰু তেওঁলোকৰ নিজৰ ফিডত তেওঁলোকৰ বিষয়বস্তু চাবলৈ অন্য ব্যৱহাৰকাৰীসকলক অনুসৰণ কৰিব পাৰে। ইনষ্টাগ্ৰামত ষ্ট'ৰী, ৰিল আদিৰ দৰে বৈশিষ্ট্যও আছে, যিয়ে ব্যৱহাৰকাৰীক চুটি ৰূপৰ ভিডিঅ' আৰু অন্যান্য ধৰণৰ বিষয়বস্তু শ্বেয়াৰ কৰিবলৈ অনুমতি দিয়ে। ইনষ্টাগ্ৰাম iOS আৰু Android ডিভাইচৰ বাবে মোবাইল এপ হিচাপে উপলব্ধ, লগতে ডেস্কটপ ৱেবছাইটো আছে।

টুইটাৰ: এইটো এটা মাইক্ৰ'ব্লগিং প্লেটফৰ্ম। ইয়াত ব্যৱহাৰকাৰীয়ে নিজৰ অনুগামীৰ সৈতে টুইট নামেৰে জনা চুটি বাৰ্তা শ্বেয়াৰ কৰিব পাৰে। ইয়াৰ মাহেকীয়া সক্ৰিয় ব্যৱহাৰকাৰী ৩৩ কোটিতকৈ অধিক আৰু ইয়াক প্ৰায়ে বাতৰি আৰু সাম্প্ৰতিক পৰিঘটনাৰ বাবে ব্যৱহাৰ কৰা হয়। ইয়াৰ মালিক আৰু পৰিচালক আমেৰিকান কোম্পানী Twitter Inc.। টুইটত লিখা, ফটো, ভিডিঅ', আৰু অন্য ৱেবছাইটৰ লিংক থাকিব পাৰে। বেছিভাগ ক্ষেত্ৰতে এটা টুইটৰ টেক্সট কন্টেন্টত ২৮০টা আখৰলৈকে থাকিব পাৰে। ২০০৬ চনত আৰম্ভ হোৱা টুইটাৰ বাতৰি, ৰাজনীতি, মনোৰঞ্জনৰ জনপ্ৰিয় মঞ্চত পৰিণত হৈছে। ব্যৱহাৰকাৰীয়ে ব্যক্তিগত প্ৰফাইল তৈয়াৰ কৰিব পাৰে, তেওঁলোকৰ নিজৰ ফিডত তেওঁলোকৰ টুইট চাবলৈ আন ব্যৱহাৰকাৰীক অনুসৰণ কৰিব পাৰে, আৰু তেওঁলোকৰ টুইটৰ লাইক, ৰিটুইট আৰু উত্তৰ দি অন্য ব্যৱহাৰকাৰীৰ সৈতে যোগাযোগ কৰিব পাৰে। টুইটাৰে হেচটেগৰ দৰে সুবিধাও আছে, যাৰ ফলত ব্যৱহাৰকাৰীয়ে তেওঁলোকৰ টুইটসমূহ শ্ৰেণীভুক্ত কৰিব পাৰে আৰু আন ব্যৱহাৰকাৰীৰ বাবে বিচাৰি উলিয়াবৰ বাবে সহজ কৰি তোলে। টুইটাৰ আই অ' এছ আৰু এণ্ড্ৰইড ডিভাইচৰ বাবে মোবাইল এপ হিচাপে উপলব্ধ হোৱাৰ লগতে ডেস্কটপ ৱেবছাইট হিচাপেও উপলব্ধ।

লিংকডইন: এইটো এটা পেছাদাৰী নেটৱৰ্কিং প্লেটফৰ্ম যাৰ ৭৪ কোটিতকৈ অধিক ব্যৱহাৰকাৰী আছে। ইয়াক চাকৰি প্ৰাৰ্থী, নিয়োগকৰ্তা, আৰু পেছাদাৰীসকলৰ বাবে ডিজাইন কৰা হৈছে

যাতে তেওঁলোকে সংযোগ কৰিব পাৰে, কর্ম-সম্পর্কীয় বিষয়বস্তু ভাগ-বতৰা কৰিব পাৰে, আৰু কেৰিয়াৰৰ সুযোগ বিচাৰিব পাৰে। ইয়াক ২০০৩ চনত মুকলি কৰা হয় আৰু ই মাইক্ৰ'ছফ্টৰ মালিকানাধীন ৰেবছাইট আৰু মোবাইল এপৰ জৰিয়তে কাম পৰিচালনা কৰে। লিংকডইন ব্যৱহাৰকাৰীসকলক এটা পেছাদাৰী প্ৰফাইল সৃষ্টিৰ সুবিধা দিয়ে যিয়ে তেওঁলোকৰ কর্ম অভিজ্ঞতা, শিক্ষা, দক্ষতা, আৰু অন্যান্য প্ৰাসংগিক তথ্য অন্তর্ভুক্ত কৰে। ব্যৱহাৰকাৰীসকলে তেওঁলোকৰ ক্ষেত্ৰৰ অন্যান্য পেছাদাৰীসকলৰ সৈতে সংযোগ স্থাপন কৰিব পাৰে আৰু তথ্য আৰু ধাৰণাসমূহ ভাগ-বতৰা কৰিবলৈ গোটসমূহত যোগদান কৰিব পাৰে। কোম্পানীসমূহে নিজৰ সামগ্ৰী আৰু সেৱাসমূহ প্ৰদর্শন কৰিবলৈ আৰু সম্ভাব্য কর্মচাৰীৰ সৈতে সংযোগ স্থাপন কৰিবলৈ লিংকডইনত পৃষ্ঠাও সৃষ্টি কৰিব পাৰে। চাকৰীৰ বিজ্ঞাপন দিয়াৰ লগতে ব্যৱহাৰকাৰীসকলে তেওঁলোকৰ উদ্যোগ বা পেছাৰ সৈতে জড়িত প্ৰবন্ধ আৰু অন্যান্য বিষয়বস্তুও ইয়াত শ্বেয়াৰ কৰিব পাৰে।

টিকটক: টিকটক, আৰু ইয়াৰ চীনা কাউণ্টাৰপার্ট ডৌইন হৈছে চীনা কোম্পানী বাইটডান্সৰ মালিকানাধীন এটা চুটি ভিডিঅ' হ'ষ্টিং চাইট। ইয়াত ব্যৱহাৰকাৰীসকলক সংগীতত ছেট কৰা চুটি-ফর্মৰ ভিডিঅ' সৃষ্টি আৰু শ্বেয়াৰ কৰাৰ সুবিধা দিয়া হৈছে। ইয়াৰ মাহেকীয়া ১ বিলিয়নতকৈ অধিক সক্ৰিয় ব্যৱহাৰকাৰী আছে আৰু ই কম বয়সীয়া দর্শকৰ মাজত অধিক জনপ্ৰিয়। ২০১৬ চনৰ ছেপ্টেম্বৰ মাহত চীনত মুক্তি পোৱা টিকটক এপটো ২০১৭ চনৰ ছেপ্টেম্বৰ মাহত আন্তঃৰাষ্ট্ৰীয় বজাৰত মুকলি কৰা হৈছিল। ২০১৯ চনৰ জানুৱাৰী মাহত টিকটকে ব্যৱসায়ীসকলক ভিডিঅ'সমূহত বিক্ৰীৰ লিংক যোগ কৰাৰ অনুমতি দিছিল। ২০২২ চনৰ অক্টোবৰ মাহত আমেৰিকাৰ ই-কমার্চ বজাৰত টিকট প্ৰসাৰ কৰা হয়।

উল্লখযোগ্য যে- ২০২০ চনৰ ২৯ জুনত চীনৰ দ্বাৰা নির্মিত আন ৫৮টা এপৰ সৈতে টিকটক ভাৰতত ৰাষ্ট্ৰীয় নিৰাপত্তাজনিত সমস্যাক লৈ ভাৰতত সম্পূর্ণৰূপে নিষিদ্ধ কৰিছিল।

ইউটিউব: এইটো এটা ভিডিঅ' শ্বেয়াৰিং প্লেটফর্ম । ইয়াৰ মাহিলী ২ বিলিয়নতকৈ অধিক সক্ৰিয় ব্যৱহাৰকাৰী আছে। ইয়াৰ মুখ্য কার্যালয় কেলিফর্ণিয়াৰ ছান ব্রুনোত। ২০০৫ চনৰ ১৪ ফেব্রুৱাৰীত ষ্টিভ চেন, চাড হার্লি আৰু জাৱেদ কৰিমে ইয়াক মুকলি কৰে। গুগলৰ মালিকানাধীন আৰু গুগল চার্চৰ পিছতে দ্বিতীয় সর্বাধিক ব্যৱহাৰ কৰা কৰা ৰেবছাইট ইউটিউব। ইয়াক মনোৰঞ্জন, শিক্ষা, তথ্য বিনিময়ৰ বাবে ব্যৱহাৰ কৰা হয়। ইউটিউবে সৃষ্টিকর্তাসকলৰ বাবে বিশেষ সুবিধাও প্ৰদান কৰে, অর্থিক লাভৰ সুবিধা, লাইভ ষ্ট্ৰীমিং, আৰু সম্প্ৰদায় নির্মাণ সঁজুলি। ব্যৱহাৰকাৰীৰ দ্বাৰা সৃষ্ট বিষয়বস্তুৰ উপৰিও, YouTube-এ মিডিয়া কোম্পানী, বাতৰি সংস্থা, আৰু ব্যক্তিগত সৃষ্টিকর্তাৰ বিষয়বস্তুৰ সুবিধাও প্ৰদান কৰে। এই বিষয়বস্তু বিনামূলীয়াকৈ

চাব পাৰে যদিও ইউটিউবে ইউটিউব প্রিমিয়াম নামৰ প্রিমিয়াম চাবস্ক্রিপচন সেৱাও আগবঢ়ায়, যিয়ে ব্যৱহাৰকাৰীক বিজ্ঞাপন অবিহনে ভিডিঅ' চাবলৈ আৰু বিশেষ কিছু বিষয়বস্তুত প্রৱেশ কৰিবলৈ অনুমতি দিয়ে। ইউটিউবেও বিজ্ঞাপন ব্যৱহাৰৰ সুবিধাও দিয়ে অথবা ইউটিউবৰ পৰাই বিজ্ঞাপন দিয়ে।

স্নেপচ্যাট: স্নেপচ্যাট হৈছে ২০১১ চনত ইভান স্পিগেল, ববি মার্ফি, আৰু ৰেগি ব্রাউনে আৰম্ভ কৰা এটা সামাজিক মাধ্যম প্লেটফর্ম। এই প্লেটফর্মৰ জৰিয়তে ব্যৱহাৰকাৰীয়ে কেইছেকেণ্ডমানৰ পৰা ২৪ ঘণ্টালৈকে নির্দিষ্ট সময়ৰ পিছত নোহোৱা হোৱা ফটো আৰু ভিডিঅ' প্রেৰণ আৰু গ্রহণ কৰিব পাৰে। এপটোত বিভিন্ন ফিল্টাৰ, লেন্স, আৰু অন্যান্য বৈশিষ্ট্যও আছে যিয়ে ব্যৱহাৰকাৰীয়ে নিজৰ স্নেপ ব্যক্তিগতকৰণ কৰিবলৈ সুবিধা দিয়ে। ইয়াৰ মাহেকীয়া সক্রিয় ব্যৱহাৰকাৰী ৩০ কোটিতকৈ অধিক আৰু কম বয়সীয়া দর্শকৰ মাজত ই অধিক জনপ্রিয়।

ক্ষণস্থায়ী বিষয়বস্তুৰ ওপৰত গুৰুত্ব দিয়া আৰু ঘনিষ্ঠ বন্ধুৰ সৈতে যোগাযোগৰ ওপৰত গুৰুত্ব দিয়াৰ বাবে স্নেপচ্যাট নৱ প্রজন্মৰ মাজত জনপ্রিয় হৈ পৰিছে। স্নেপ প্রেৰণ কৰাৰ উপৰিও ব্যৱহাৰকাৰীয়ে Stories পোষ্ট কৰিব পাৰে।

স্নেপচ্যাটে নিজৰ অফাৰসমূহো সম্প্রসাৰিত কৰি বিভিন্ন সুবিধা দিয়ে যেনেঃ স্নেপ মেপ, ব্যৱহাৰকাৰীসকলক তেওঁলোকৰ বন্ধুসকলৰ অৱস্থান মেপত চাবলৈ অনুমতি দিয়ে, আৰু ডিস্কভাৰ, মিডিয়া কোম্পানী, চেলিব্রিটি আৰু অন্যান্য উৎসৰ পৰা কিউৰেট কৰা কন্টেন্ট সুবিধা দিয়ে। এই প্লেটফর্মত বিজ্ঞাপনৰ সুবিধাও আছে, যাৰ ফলত ব্রেণ্ডসমূহে স্নেপচ্যাটৰ বৃহৎ ব্যৱহাৰকাৰী সৈতে সম্পর্কিত হ'ব পাৰে।

Pinterest: Pinterest হৈছে এটা সামাজিক মাধ্যম প্লেটফর্ম যিয়ে ব্যৱহাৰকাৰীক ছবি আৰু ভিডিঅ'ৰ জৰিয়তে , সংৰক্ষণ আৰু ভাগ-বতৰা কৰিবলৈ অনুমতি দিয়ে, যাক পিন বুলি জনা যায়। ব্যৱহাৰকাৰীসকলে থিম বা বিষয়ৰ ওপৰত ভিত্তি কৰি তেওঁলোকৰ পিনসমূহ সংগঠিত কৰিবলৈ ভার্চুৱেল বর্ড সৃষ্টি কৰিব পাৰে, যেনে ৰেচিপি, ঘৰ সজ্জা, ভ্রমণ, আৰু ফেশ্বন। বেন ছিলবাৰমেন, পল স্কিয়াৰা আৰু ইভান শ্বার্পে এই চাইটটো সৃষ্টি কৰিছিল আৰু ইয়াৰ প্র'ট'টাইপটো ২০১১ চনৰ মার্চ মাহত লেন্স কৰা হৈছিল।

Pinterest ৰ মাহিলী ৪০ কোটিতকৈ অধিক সক্রিয় ব্যৱহাৰকাৰী আছে আৰু ই ৩০ টাতকৈও অধিক ভাষাত উপলব্ধ। ইয়াক ব্যক্তিসকলে ব্যক্তিগত আগ্রহ আৰু চখৰ বাবে ব্যৱহাৰ কৰে, লগতে ব্যৱসায়ী আৰু বিক্রেতাসকলে নিজৰ সামগ্রী আৰু সেৱাৰ প্রচাৰৰ বাবে ব্যৱহাৰ কৰে। Pinterestৰ এলগৰিদমে মেচিন লার্নিং ব্যৱহাৰ কৰি ব্যৱহাৰকাৰীসকলক প্লেটফর্মত

তেওঁলোকৰ কার্য্যকলাপ, আগ্রহ আৰু আচৰণৰ ওপৰত ভিত্তি কৰি ব্যক্তিগতকৃত পৰামর্শ প্রদান কৰে। ব্যৱহাৰকাৰীসকলে কীৱর্ড ব্যৱহাৰ কৰি পিন আৰু বর্ডৰ বাবেও সন্ধান কৰিব পাৰে বা শ্রেণী আৰু বিষয়সমূহৰ মাজেৰে ব্রাউজ কৰিব পাৰে।

Pinterestৰ দৃশ্য আৰু ব্যৱহাৰকাৰী-বন্ধুত্বপূর্ণ ডিজাইনৰ বাবে প্রশংসা কৰা হৈছে, লগতে নতুন ধাৰণা আৰু ট্রেণ্ড আৱিষ্কাৰৰ বাবে এক মঞ্চ হিচাপে কাম কৰাৰ ক্ষমতাৰ বাবেও প্রশংসা কৰা হৈছে। কিন্তু ভুল তথ্য বিয়পোৱা আৰু অবাস্তৱ বা ক্ষতিকাৰক সৌন্দর্য্যৰ মানদণ্ডৰ প্রচাৰৰ সম্ভাৱনা আদি বিষয়ক লৈও ই সমালোচনাৰ সন্মুখীন হৈছে।

আন আন সামাজিক মাধ্যম নেটৱর্কসমূহৰ ভিতৰত আছে Reddit, Tumblr, আৰু বহুতো। প্রতিটো মঞ্চৰ নিজস্ব দর্শক আৰু উদ্দেশ্য থাকে, আৰু আমাৰ প্রয়োজন আৰু লক্ষ্যৰ বাবে সঠিক মঞ্চ বাছি লোৱাটো গুৰুত্বপূর্ণ বিষয়।

৬.৪ সামাজিক মাধ্যম প্লেটফর্ম

সামাজিক মাধ্যম বিভিন্ন প্রকাৰৰ। প্রত্যেকৰে নিজস্ব বৈশিষ্ট্য আৰু উদ্দেশ্য আছে। সামাজিক মাধ্যমৰ কিছুমান সাধাৰণ প্রকাৰৰ বিষয়ে উল্লেখ কৰা হ'ল:

ছ'চিয়েল নেটৱর্কিং চাইট : ছ'চিয়েল নেটৱর্কিং চাইট হৈছে এনে অনলাইন প্লেটফর্ম যিয়ে ব্যৱহাৰকাৰীক একে ধৰণৰ আগ্রহ, পটভূমি বা কার্য্যকলাপৰ আনৰ সৈতে সংযোগ আৰু যোগাযোগ কৰিবলৈ সুবিধা দিয়ে। এই চাইটসমূহে সাধাৰণতে ব্যৱহাৰকাৰীসকলক এটা প্রফাইল সৃষ্টি কৰিবলৈ, তথ্য শ্বেয়াৰ কৰিবলৈ, বার্তা প্রেৰণ, মন্তব্য, বা আড্ডাৰ জৰিয়তে অন্য ব্যৱহাৰকাৰীৰ সৈতে যোগাযোগ কৰিবলৈ, আৰু গোট বা সম্প্রদায়ত যোগদান বা সৃষ্টি কৰিবলৈ সুবিধা কৰি দিয়ে। কিছুমান জনপ্রিয় ছ'চিয়েল নেটৱর্কিং চাইটৰ ভিতৰত ফেচবুক, টুইটাৰ, লিংকডইন, ইনষ্টাগ্রাম, স্নেপচ্যাট, টিকটক আদি অন্যতম। প্রতিটো প্লেটফর্মৰ নিজস্ব বৈশিষ্ট্য আৰু লক্ষ্য গ্রাহক আছে। উদাহৰণস্বৰূপে, ফেচবুক ব্যক্তিগত আৰু পেছাদাৰী দুয়োটা নেটৱর্কিঙৰ বাবে বহু লোকে ব্যৱহাৰ কৰে, আনহাতে টিকটক মূলতঃ নৱ প্রজন্মই চুটি ৰূপৰ ভিডিঅ' কন্টেন্টৰ বাবে ব্যৱহাৰ কৰে। ছ'চিয়েল নেটৱর্কিং চাইটে মানুহৰ ইজনে সিজনৰ লগত যোগাযোগ কৰাৰ ধৰণ আৰু তেওঁলোকে কেনেকৈ তথ্য লাভ কৰে আৰু ভাগ-বতৰা কৰে তাত এক বৈপ্লৱিক পৰিৱর্তন আনিছে। কিন্তু ছ'চিয়েল নেটৱর্কিং চাইটসমূহক গোপনীয়তাৰ চিন্তা, চাইবাৰ বুলিং, নিচা, ভুৱা বাতৰি আৰু ভুল তথ্যৰ প্রচাৰ আদি বিষয়ৰ বাবেও সমালোচনা কৰা হয়।

মাইক্ৰ'ব্লগিং প্লেটফৰ্ম: মাইক্ৰ'ব্লগিং প্লেটফৰ্ম হৈছে অনলাইন প্লেটফৰ্ম যিয়ে ব্যৱহাৰকাৰীক একে সময়ত লিখনী, ছবি বা ভিডিঅ'ৰে গঠিত চুটি-ফৰ্মৰ বিষয়বস্তু প্ৰকাশ কৰিবলৈ সুবিধা দিয়ে। মাইক্ৰ'ব্লগিং প্লেটফৰ্মত পোষ্ট কৰা বিষয়বস্তু সাধাৰণতে চমু আৰু সংক্ষিপ্ত হয়, প্ৰায়ে এটা নিৰ্দিষ্ট আখৰ বা শব্দৰ সংখ্যাত সীমাবদ্ধ থাকে, যেনে টুইটাৰৰ সীমা ২৮০ আখৰৰ। আন কিছুমান মাইক্ৰ'ব্লগিং চাইট হ'ল টাম্বলাৰ, আৰু ইনষ্টাগ্ৰাম। মাইক্ৰ'ব্লগিং প্লেটফৰ্মে ব্যৱহাৰকাৰীসকলক তেওঁলোকৰ অনুগামীসকলৰ সৈতে তথ্য আৰু ধাৰণাসমূহ ভাগ-বতৰা কৰাৰ আৰু একেধৰণৰ আগ্ৰহ থকা আনসকলৰ সৈতে সংযোগ স্থাপনৰ সুযোগ দিয়ে। ইয়াৰ উপৰিও পণ্য আৰু সেৱাৰ প্ৰচাৰৰ লগতে এংগেজমেণ্ট বৃদ্ধি আৰু ব্ৰেণ্ড সজাগতা বৃদ্ধিৰ বাবেও ব্যৱহাৰ কৰা হয়। কিন্তু মাইক্ৰ'ব্লগিং প্লেটফৰ্মসমূহক হাৰাশাস্তি, ভুৱা বাতৰি আৰু ভুল তথ্য বিয়পোৱা, চেঞ্চৰশ্বিপ আদি বিষয়ৰ বাবেও সমালোচনা কৰা হৈছে।

ফটো শ্বেয়াৰিং প্লেটফৰ্ম: ফটো শ্বেয়াৰিং প্লেটফৰ্ম হৈছে অনলাইন প্লেটফৰ্ম যিয়ে ব্যৱহাৰকাৰীক অন্য ব্যৱহাৰকাৰীৰ সৈতে ফটো আৰু ছবি আপলোড, শ্বেয়াৰ আৰু চাবলৈ সুবিধা দিয়ে। এই প্লেটফৰ্মসমূহ ব্যক্তিগত, সামাজিক বা বাণিজ্যিক উদ্দেশ্যত ব্যৱহাৰ কৰিব পাৰি, আৰু সাধাৰণতে ব্যৱহাৰকাৰীসকলক তেওঁলোকৰ ফটোসমূহ উন্নত আৰু সংগঠিত কৰাত সহায় কৰিবলৈ সম্পাদনা সঁজুলি, ফিল্টাৰ, আৰু টেগিং বিকল্পৰ দৰে বৈশিষ্ট্য প্ৰদান কৰে। কিছুমান জনপ্ৰিয় ফটো শ্বেয়াৰিং প্লেটফৰ্মৰ ভিতৰত আছে ইনষ্টাগ্ৰাম, ফ্লিকাৰ, আৰু গুগল ফটো। ফটো শ্বেয়াৰিং প্লেটফৰ্মে মানুহে ছবি জমা ৰখা আৰু শ্বেয়াৰ কৰাৰ ক্ষেত্ৰত এক বৈপ্লৱিক পৰিৱৰ্তন আনিছে, যাৰ ফলত যিকোনো ব্যক্তিয়েই বিশ্বব্যাপী দৰ্শকৰ সৈতে উচ্চমানৰ ফটো তুলিব আৰু শ্বেয়াৰ কৰিব পাৰে। ব্যৱসায়ী আৰু বজাৰকৰ্তাসকলেও তেওঁলোকৰ সামগ্ৰী আৰু সেৱাসমূহ প্ৰদৰ্শন কৰিবলৈ আৰু গ্ৰাহকৰ সৈতে জড়িত হ'বলৈ ব্যৱহাৰ কৰিছে।

ভিডিঅ' শ্বেয়াৰিং প্লেটফৰ্মসমূহ: ভিডিঅ' শ্বেয়াৰিং প্লেটফৰ্মসমূহ হৈছে অনলাইন প্লেটফৰ্ম যিয়ে ব্যৱহাৰকাৰীসকলক আনৰ সৈতে ভিডিঅ' আপলোড কৰা, চোৱা আৰু শ্বেয়াৰ কৰিবলৈ অনুমতি দিয়ে। এই প্লেটফৰ্মসমূহ ব্যক্তিগত, সামাজিক বা ব্যৱসায়িক উদ্দেশ্যত ব্যৱহাৰ কৰা হয় আৰু ভিডিঅ' সম্পাদনা আৰু উন্নত কৰাৰ সঁজুলি হিচাপেও ব্যৱহাৰ কৰা হয়। জনপ্ৰিয় ভিডিঅ' শ্বেয়াৰিং প্লেটফৰ্মসমূহৰ ভিতৰত আছে ইউটিউব, ভিমিঅ', আৰু টিকটক। প্ৰতিটো প্লেটফৰ্মৰ নিজস্ব বৈশিষ্ট্য আৰু লক্ষ্য গ্ৰাহক আছে। ভিডিঅ' শ্বেয়াৰিং প্লেটফৰ্মে মানুহে ভিডিঅ' কন্টেন্ট গ্ৰহণ আৰু সৃষ্টি কৰাৰ ক্ষেত্ৰত এক বৈপ্লৱিক পৰিৱৰ্তন আনিছে, যিয়ে যিকোনো ব্যক্তিক তেওঁলোকৰ ভিডিঅ' প্ৰস্তুত আৰু বিশ্বব্যাপী দৰ্শকৰ সৈতে শ্বেয়াৰ কৰাৰ সুবিধা দিছে।

ব্যৱসায়ী আৰু বজাৰকৰ্তাসকলেও নিজৰ সামগ্ৰী আৰু সেৱাৰ প্ৰচাৰ আৰু গ্ৰাহকৰ সৈতে জড়িত হোৱাৰ বাবে ইয়াক ব্যৱহাৰ কৰি আহিছে।

লাইভ ষ্ট্ৰীমিং প্লেটফৰ্ম: লাইভ ষ্ট্ৰীমিং তুলনামূলকভাৱে নতুন; ই মূলতঃ এটা অনলাইন প্লেটফৰ্ম যি ব্যৱহাৰকাৰীসকলক বাস্তৱ সময়ত দৰ্শকক লাইভ ভিডিঅ' বিষয়বস্তু সম্প্ৰচাৰ কৰিবলৈ সুবিধা দিয়ে। এই প্লেটফৰ্মসমূহ মনো�ৰঞ্জন, শিক্ষা, বাতৰি, ক্ৰীড়া, ব্যৱসায়কে ধৰি বিভিন্ন কামত ব্যৱহাৰ কৰিব পাৰি। কিছুমান জনপ্ৰিয় লাইভ ষ্ট্ৰীমিং প্লেটফৰ্ম হ'ল টুইচ, ইউটিউব লাইভ, ফেচবুক লাইভ, আৰু ইনষ্টাগ্ৰাম লাইভ। প্ৰতিটো প্লেটফৰ্মৰ নিজস্ব বৈশিষ্ট্য আৰু লক্ষ্য গ্ৰাহক আছে। উদাহৰণস্বৰূপে, টুইচ হৈছে ভিডিঅ' গেম আৰু ই-স্প'ৰ্টছৰ লাইভ ষ্ট্ৰীমিংৰ বাবে জনপ্ৰিয় প্লেটফৰ্ম, আনহাতে ফেচবুক লাইভ প্ৰায়ে ব্যক্তিগত আৰু সামূহিক অনুষ্ঠানৰ বাবে ব্যৱহাৰ কৰা হয়। লাইভ ষ্ট্ৰীমিং প্লেটফৰ্মে ব্যৱহাৰকাৰীসকলক তেওঁলোকৰ দৰ্শকৰ সৈতে বাস্তৱ সময়ত জড়িত হ'বলৈ সহায় কৰে। ব্যৱসায়ী আৰু বজাৰকৰ্তাসকলেও তেওঁলোকৰ সামগ্ৰী আৰু সেৱাৰ প্ৰচাৰ আৰু নতুন আৰু উদ্ভাৱনীমূলক পদ্ধতিৰে গ্ৰাহকৰ সৈতে সংযোগ স্থাপনৰ বাবে ব্যৱহাৰ কৰিছে।

আলোচনা মঞ্চ: আলোচনা মঞ্চ হৈছে কোনো বিষয়ৰ ওপৰত কথোপকথনৰ বাবে ব্যৱহাৰ কৰা অনলাইন প্লেটফৰ্ম। ইয়াত ব্যৱহাৰকাৰীসকলে বিভিন্ন বিষয়ৰ ওপৰত অন্য ব্যৱহাৰকাৰীৰ সৈতে আলোচনাত অংশগ্ৰহণ কৰে। এই প্লেটফৰ্মসমূহ ব্যক্তিগত, সামাজিক, শৈক্ষিক বা পেছাদাৰী উদ্দেশ্যত ব্যৱহাৰ কৰিব পাৰি, আৰু ব্যৱহাৰকাৰীসকলক প্ৰশ্ন সুধিবলৈ, ধাৰণাসমূহ ভাগ-বতৰা কৰিবলৈ, আৰু একে আগ্ৰহৰ অংশীদাৰসকলৰ সৈতে সংযোগ স্থাপন কৰিবলৈ সুবিধা প্ৰদান কৰে। কিছুমান জনপ্ৰিয় আলোচনা মঞ্চ প্লেটফৰ্মৰ ভিতৰত Reddit, Quora, আৰু Stack Overflow অন্তৰ্ভুক্ত। আলোচনা মঞ্চসমূহ ব্যৱহাৰকাৰীসকলৰ মাজত আনৰ সৈতে শিকিবলৈ, সংযোগ কৰিবলৈ আৰু সহযোগিতাৰ বাবে জনপ্ৰিয় হৈ পৰিছে। উদাহৰণস্বৰূপে, ষ্টেক অভাৰফ্লঃ' প্ৰগ্ৰেমাৰে তেওঁলোকৰ প্ৰগ্ৰেম ক'ডসমূহ শ্বেয়াৰ কৰিবলৈ আৰু প্ৰগ্ৰেমিংত সংঘটিত হোৱা বিভিন্ন ভুলৰ বিষয়ে আলোচনা কৰিবলৈ ব্যৱহাৰ কৰে।

সামাজিক বুকমাৰ্কিং চাইট: সামাজিক বুকমাৰ্কিং চাইট হৈছে এনে অনলাইন প্লেটফৰ্ম যিয়ে ব্যৱহাৰকাৰীক বুকমাৰ্ক বা ৱেব পৃষ্ঠা সংৰক্ষণ আৰু সংগঠিত কৰি আন ব্যৱহাৰকাৰীৰ সৈতে ভাগ-বতৰা কৰিবলৈ সুবিধা দিয়ে। এই প্লেটফৰ্মসমূহ ব্যক্তিগত বা পেছাদাৰী উদ্দেশ্যত ব্যৱহাৰ কৰিব পাৰি, আৰু ব্যৱহাৰকাৰীসকলক ৱেবৰ বিভিন্ন প্ৰান্তৰ পৰা বিষয়বস্তু আৱিষ্কাৰ আৰু কিউৰেট কৰাৰ সুবিধা প্ৰদান কৰে। কিছুমান জনপ্ৰিয় সামাজিক বুকমাৰ্কিং চাইটৰ ভিতৰত Pinterest, Pocket, আৰু Reddit আদি অন্তৰ্ভুক্ত। কিন্তু ভুল তথ্য আৰু স্পেমৰ বিস্তাৰ,

আৰু বিষাক্ত বা ক্ষতিকাৰক বিষয়বস্তুৰ প্ৰচাৰৰ সম্ভাৱনা আদি বিষয়ৰ বাবেও সামাজিক বুকমার্কিং চাইটসমূহে সমালোচনাৰ সম্মুখীন হৈ আহিছে।

ভার্চুৱেল ৰিয়েলিটি প্লেটফর্ম: ভার্চুৱেল ৰিয়েলিটি প্লেটফর্ম হৈছে অনলাইন প্লেটফর্ম যিয়ে ব্যৱহাৰকাৰীক ভার্চুৱেল ৰিয়েলিটি হেডছেট আৰু অন্যান্য ডিভাইচৰ ব্যৱহাৰৰ জৰিয়তে ইমার্চিভ, কম্পিউটাৰ-উৎপন্ন পৰিৱেশৰ অভিজ্ঞতা লাভ কৰিবলৈ সুবিধা দিয়ে। এই প্লেটফর্মসমূহ মনোৰঞ্জন, শিক্ষা, প্ৰশিক্ষণ, চিকিৎসা আদি বিভিন্ন কামত ব্যৱহাৰ কৰিব পাৰি। কিছুমান জনপ্ৰিয় ভার্চুৱেল ৰিয়েলিটি প্লেটফর্মৰ ভিতৰত আছে অকুলাছ, এইচটিচি ভাইভ, আৰু প্লেষ্টেচন ভিআৰ। প্ৰতিটো প্লেটফর্মৰ নিজস্ব বৈশিষ্ট্য আৰু লক্ষ্য গ্ৰাহক আছে। ভার্চুৱেল ৰিয়েলিটি প্লেটফর্মসমূহে নিচাযুক্ত আচৰণ প্ৰসাৰৰ সম্ভাৱনা, মচন চিকনেচৰ আশংকা, আৰু ব্যৱহাৰকাৰীসকলক বাস্তৱ জগতৰ পৰা বিচ্ছিন্ন কৰাৰ সম্ভাৱনা আদি সমালোচনাৰ সম্মুখীন হৈ আহিছে।

ব্লগিং প্লেটফর্ম: এই প্লেটফর্মসমূহে ব্যৱহাৰকাৰীসকলক নিজৰ লিখিত বিষয়বস্তু, যেনে প্ৰবন্ধ আৰু ৰচনা লিখা আৰু প্ৰকাশ কৰিবলৈ সুবিধা দিয়ে। উদাহৰণস্বৰূপে ৱর্ডপ্ৰেছ আৰু মিডিয়াম। এই প্লেটফর্মসমূহ ব্যক্তিগত বা পেছাদাৰী উদ্দেশ্যত ব্যৱহাৰ কৰিব পাৰি, আৰু ব্যৱহাৰকাৰীসকলক তেওঁলোকৰ ধাৰণা, মতামত আৰু অভিজ্ঞতাসমূহ বিশ্বব্যাপী থকা দর্শক পাঠকৰৰ সৈতে ভাগ-বতৰা কৰাৰ সুবিধা প্ৰদান কৰে। ব্লগিং প্লেটফর্মসমূহ বিষয়বস্তু সৃষ্টি আৰু বিতৰণৰ বাবে এক গুৰুত্বপূর্ণ আহিলাত পৰিণত হৈছে, ই মানুহক নিজৰ কাহিনী আৰু ধাৰণাসমূহ আনৰ সৈতে ভাগ-বতৰা কৰাৰ বাবে এক স্থান প্ৰদান কৰিছে। ব্যৱসায়ী আৰু বিক্ৰেতাসকলেও তেওঁলোকৰ সামগ্ৰী আৰু সেৱাৰ প্ৰচাৰ আৰু গ্ৰাহকৰ সৈতে অধিক ব্যক্তিগত আৰু আকর্ষণীয়ভাৱে সংযোগ স্থাপনৰ বাবে ব্যৱহাৰ কৰিছে।

আজিৰ দিনত উপলব্ধ বহু ধৰণৰ সামাজিক মাধ্যমৰ এয়া কেইটামান উদাহৰণহে মাত্ৰ। প্ৰত্যেক সামাজিক মাধ্যমে এক বেলেগ উদ্দেশ্য সাধন কৰে আৰু যোগাযোগ, সংযোগ, আৰু নিয়োগৰ বাবে অনন্য সুযোগ প্ৰদান কৰে।



অগ্ৰগতি নিৰীক্ষণ

১. “SNS” চমু নামটোৱে কি বুজায়?

a) Social Network System
b) Social Networking Site
c) Social Network Software
d) Social Network Sharing

২. তলৰ কোনটো সামাজিক মাধ্যম নেটৱৰ্কিং ছাইট নহয়?

a) Facebook b) LinkedIn

c) Instagram d) WhatsApp

৩. হেচটেগ কি?

a) এক প্ৰকাৰৰ সামাজিক মাধ্যম প্লেটফৰ্ম

b) সামাজিক মাধ্যমত বিষয়বস্তু টেগ আৰু শ্ৰেণীবদ্ধ কৰাৰ এক উপায়

c) এক প্ৰকাৰৰ ব্যক্তিগত বাৰ্তা প্ৰেৰণৰ সুবিধা

d) সামাজিক মাধ্যমত অন্যান্য ব্যৱহাৰকাৰীৰ সৈতে সংযোগ কৰাৰ এক উপায়

৪. টুইটাৰত এটা টুইটৰ বাবে কেইটা আখৰৰ সীমা আছে?

a) ১৪০ b) ২৮০

c) ৫০০ d) ১০০০

৫. কোনটো সামাজিক মাধ্যম প্লেটফৰ্ম মূলত চুটি ভিডিঅ' শ্বেয়াৰ কৰিবলৈ সজা হৈছে?

a) Facebook b) Twitter

c) TikTok d) LinkedIn

৬.৫ অধ্যায়টিৰ পৰা মি কি কি শিকিলোঁ

- সামাজিক মাধ্যমে অনলাইন প্লেটফৰ্ম আৰু সঁজুলিৰ সংকলনক বুজায় যিয়ে ব্যক্তি আৰু গোটসমূহক ইজনে সিজনৰ সৈতে তথ্য, ধাৰণা আৰু বিষয়বস্তু সৃষ্টি, ভাগ-বতৰা আৰু বিনিময় কৰিবলৈ সুবিধা কৰে। এই প্লেটফৰ্মসমূহৰ ভিতৰত আছে ফেচবুক, টুইটাৰ, ইনষ্টাগ্ৰাম, লিংকডইন, আৰু ইউটিউব আদি জনপ্ৰিয় ৱেবছাইটসমূহ।
- সামাজিক মাধ্যম আধুনিক সমাজৰ এক উল্লেখযোগ্য দিশ হৈ পৰিছে, যিয়ে যোগাযোগ, সংস্কৃতি, ৰাজনীতি, আৰু বাণিজ্যত প্ৰভাৱ পেলাইছে। ই ব্যক্তি আৰু গোটসমূহক ইজনে সিজনৰ সৈতে সংযোগ আৰু যোগাযোগ, বাতৰি আৰু তথ্য ভাগ-বতৰা আৰু

গ্রহণ, সম্পর্ক গঢ়ি তোলা আৰু বজাই ৰখা, আৰু সামাজিক আৰু ৰাজনৈতিক সক্রিয়তাত লিপ্ত হোৱাৰ সুবিধা প্রদান কৰে।

- ছ'চিয়েল মিডিয়া প্লেটফর্মসমূহে সাধাৰণতে ব্যৱহাৰকাৰীসকলক ব্যৱহাৰকাৰী প্র'ফাইল, অন্য ব্যৱহাৰকাৰীৰ সৈতে সংযোগ, বাতৰি ফিড, যোগাযোগ, বিষয়বস্তু অংশীদাৰী, গোপনীয়তা ছেটিংছ, আৰু এলগৰিদমি কিউৰেচনকে ধৰি বহুতো সুবিধা প্রদান কৰে।
- সামাজিক মাধ্যমে ব্যক্তি, সংস্থা আৰু সামগ্রিকভাৱে সমাজৰ বাবেও অসংখ্য সুযোগ আৰু প্রত্যাহ্বানৰ সৃষ্টি কৰে। ইয়াত গোপনীয়তা, তথ্য সুৰক্ষা, চাইবাৰ বুলিং, ভুৱা বাতৰি, আৰু ভুল তথ্যৰ সৈতে জড়িত বিষয়সমূহো অন্তর্ভুক্ত হৈ থাকে।
- ভিডিও শ্বেয়াৰিং চাইট, ফটো শ্বেয়াৰিং চাইট, চেটিং চাইট আদি বিভিন্ন সামাজিক মাধ্যম প্লেটফর্ম আছে।



৬.৬ অধিক জানিবলৈ

1) "The Social Media Bible: Tactics, Tools, and Strategies for Business Success" by Lon Safko and David K. Brake
2) "Social Media Marketing All-in-One for Dummies" by Jan Zimmerman and Deborah Ng
3) "Socialnomics: How Social Media Transforms the Way We Live and Do Business" by Erik Qualman
4) "The Art of Social Media: Power Tips for Power Users" by Guy Kawasaki and Peg Fitzpatrick
5) "Likeable Social Media: How to Delight Your Customers, Create an Irresistible Brand, and Be Amazing on Facebook, Twitter, LinkedIn, Instagram, Pinterest, and More" by Dave Kerpen



৬.৭ অগ্রগতিৰ খতিয়ান

প্রশ্ন ১ ৰ উত্তৰ : b) Social Networking Site

প্রশ্ন ২ৰ উত্তৰ: d) WhatsApp

প্রশ্ন ৩ৰ উত্তৰ b) সামাজিক মাধ্যমত বিষয়বস্তু টেগ আৰু শ্রেণীভুক্ত কৰাৰ এটা উপায়

প্রশ্ন ৪ৰ উত্তৰ: c) ২৮০

প্রশ্ন ৫ৰ উত্তৰ: d) টিকটক



আৰ্হি প্রশ্ন

প্রশ্ন ১. সামাজিক মাধ্যম কি, আৰু ই কেনেকৈ কাম কৰে?

প্রশ্ন ২। সামাজিক মাধ্যম ব্যৱহাৰ কৰাৰ সুবিধা আৰু অসুবিধা কি কি?

প্রশ্ন ৩। সামাজিক মাধ্যমে মানুহৰ ইজনে সিজনৰ লগত যোগাযোগ আৰু সংযোগৰ ধৰণ কেনেকৈ সলনি কৰিছে? লিখক।

প্রশ্ন ৪। ব্যৱসায়ীসকলে বিপণন আৰু নিয়োজিতাৰ বাবে সামাজিক মাধ্যম কেনেকৈ ব্যৱহাৰ কৰে?

প্রশ্ন ৫। বিভিন্ন সামাজিক মাধ্যম প্লেটফর্মবোৰৰ বিষয়ে এটা টোকা লিখক।

প্রশ্ন ৬। ফেচবুক আৰু ইনষ্টাগ্রামৰ বিষয়ে টোকা লিখক।

*****

অধ্যায় ৭: সামাজিক মাধ্যমৰ পৰিচয়

অধ্যায় গাঁথনি

৭.১ উদ্দেশ্য
৭.২ পৰিচয়
৭.৩ সামাজিক মাধ্যম নিৰীক্ষণ
৭.৪ সামাজিক মাধ্যমত হেচটেগ
৭.৫ ভাইৰেল কণ্টেণ্ট
৭.৬ সামাজিক মাধ্যমৰ মার্কেটিং
৭.৭ সামাজিক মাধ্যমৰ গোপনীয়তা
৭.৮ সামাজিক মাধ্যমৰ প্ৰত্যাহ্বান, সুযোগ আৰু ফান্দ
৭.৯ অধ্যায়টিৰ পৰা আমি কি কি শিকিলোঁ
৭.১০ অধিক জানিবলৈ
৭.১১ অগ্ৰগতিৰ খতিয়ান
৭.১২ আৰ্হি প্ৰশ্ন

৭.১ উদ্দেশ্য

এই অধ্যায়ৰ পৰা আপোনালোকে তলৰ বিষয়বোৰ জানিব পাৰিব-

- সামাজিক মাধ্যম নিৰীক্ষণ কি
- হেচটেগ আৰু ভাইৰেল কণ্টেণ্ট কি
- সামাজিক মাধ্যমত মার্কেটিং
- সামাজিক মাধ্যমৰ গোপনীয়তা, প্ৰত্যাহ্বান, সুযোগ আৰু ফান্দ

৭.২ পৰিচয়

এই অধ্যায়ত আমি সামাজিক মাধ্যমৰ মার্কেটিংৰ বিষয়ে আলোচনা কৰিম। সামাজিক মাধ্যমত ভাইৰেল কণ্টেণ্ট কি, ভাইৰেল হ'বলৈ সামাজিক মাধ্যমত সংঘটিত হোৱা মূল কথাবোৰ কি। সামাজিক মাধ্যমত কি কি গোপনীয়তাৰ সমস্যা, প্ৰত্যাহ্বান, সুযোগ আৰু ফান্দ আছে। সামাজিক মাধ্যম মার্কেটিং কি আৰু সামাজিক মাধ্যমে মার্কেটিঙৰ বাবে আমাৰ তথ্য কেনেকৈ সংগ্ৰহ কৰে এইবোৰৰ বিতং আলোচনা কৰিম।

৭.৩ সামাজিক মাধ্যম নিৰীক্ষণ

সামাজিক মাধ্যম নিৰীক্ষণৰ অর্থ হ'ল বিভিন্ন সামাজিক মাধ্যম প্লেটফর্মত বিষয়বস্তু, কথোপকথন, মতামত আদি অনুসৰণ আৰু বিশ্লেষণ কৰা। সামাজিক মাধ্যম নিৰীক্ষণৰ লক্ষ্য হৈছে ব্যৱহাৰকাৰীসকলৰ পৰা অন্তর্দৃষ্টি আৰু সবিশেষ সংগ্রহ কৰা। উদাহৰণস্বৰূপে, ব্যৱসায় সামগ্রী হ'লে ই গ্রাহকৰ আগ্রহ, ৰিভিউ সংগ্রহ কৰে, আনহাতে এটা ৰাজনৈতিক দলে ভোটাৰৰ পৰা আগ্রহ আৰু প্রয়োজনীয় ডেটা সংগ্রহ কৰিবলৈ আহে, এজন সংগীতজ্ঞই দর্শকৰ পছন্দ/অপছন্দৰ বিষয়ে নিৰীক্ষণ কৰিবলৈ আহে। এই ধৰণৰ তথ্যই নিজ নিজ ক্ষেত্রৰ বাবে সিদ্ধান্ত গ্রহণত যথেষ্ট সহায় কৰে।

সামাজিক মাধ্যম নিৰীক্ষণৰ কিছুমান মূল সুবিধা ইয়াত উল্লেখ কৰা হ'ল-

ব্রেণ্ডৰ সুনাম ব্যৱস্থাপনা: সামাজিক মাধ্যমৰ নিৰীক্ষণৰ দ্বাৰা ব্যৱসায়ীসকলে গ্রাহকৰ দ্বাৰা তেওঁলোকৰ ব্রেণ্ড বা সামগ্রীৰ মন্তব্য, পর্যালোচনা আৰু মতামত চাই তেওঁলোকৰ অনলাইন সুনাম অর্জন আৰু পৰিচালনা কৰিব পাৰে আৰু গ্রাহকৰ বাবে কৌশল তৈয়াৰ কৰিব পাৰে যাতে ব্রেণ্ডে অধিক গ্রাহকৰ মনোযোগ আকর্ষণ কৰিবলৈ সক্ষম হয়।

গ্রাহকৰ অন্তর্দৃষ্টি: সামাজিক মাধ্যম পর্যবেক্ষণ কৰি ব্যৱসায়ীসকলে গ্রাহকৰ আগ্রহৰ ক্ষেত্র, গ্রাহকৰ পছন্দ আৰু অপছন্দৰ বিষয়ে জানিব পাৰে। এই ধৰণৰ তথ্য সংগ্রহ কৰি ব্যৱসায়ে গ্রাহকৰ পছন্দসমূহ অন্তর্ভুক্ত কৰা, অপছন্দৰ দিশ বা আসোৱাহ- অসুবিধা দূৰ কৰা, গ্রাহকৰ মন বুজি পোৱা আৰু অধিক মতামত যোগ কৰাৰ বাবে প্রয়োজনীয় কামবোৰ সম্পাদন কৰিব পাৰে।

প্রতিযোগিতামূলক বিশ্লেষণ: সামাজিক মাধ্যমৰ তথ্য বিশ্লেষণ কৰি এজন ব্যৱসায়ীয়ে আন ব্যৱসায়ীসকলে কি কৰিছে সেই বিষয়ে জানিব পাৰে আৰু অন্য ব্যৱসায়ৰ সৈতে তুলনা কৰিব পাৰে, প্রতিযোগীসকলৰ সামাজিক মাধ্যমৰ কার্যকলাপ নিৰীক্ষণ কৰি বিপণন কৌশল আৰু গ্রাহকৰ সংযোগক আয়ত্ব কৰিব পাৰে।

সমস্যা ব্যৱস্থাপনা: সামাজিক মাধ্যম নিৰীক্ষণে ব্যৱসায়ীসকলক সম্ভাব্য সমস্যাৰ পৰিস্থিতি, যেনে গ্রাহকৰ নেতিবাচক মতামত আৰু অভিযোগ চিনাক্ত কৰি দ্রুতভাৱে সঁহাৰি জনাব পাৰে আৰু ব্যৱসায়ীসকলক এনে সমস্যা নাইকীয়া কৰিবলৈ দ্রুত পদক্ষেপ ল'বলৈ সুবিধা দিয়ে।

সামাজিক মাধ্যমত নিয়োজন: সামাজিক মাধ্যম নিৰীক্ষণে ব্যৱসায়ীসকলক তেওঁলোকৰ প্ৰশ্ন, মন্তব্য, আৰু মতামতৰ উত্তৰ দি তেওঁলোকৰ গ্ৰাহকৰ সৈতে জড়িত হৈ থাকিবলৈ সহায় কৰে আৰু ই গ্ৰাহকৰ সৈতে প্ৰত্যক্ষ যোগাযোগৰ বাবে এক উত্তম ব্যৱস্থা হৈ পৰে।

সামাজিক মাধ্যম নিৰীক্ষণৰ বাবে বহু সঁজুলি আৰু চফট্ ৱেৰ উপলব্ধ, যেনে Hootsuite, Sprout Social, আৰু Brandwatch। এই সঁজুলিসমূহে ব্যৱসায়ীসকলক একাধিক প্লেটফৰ্মত সামাজিক মাধ্যমৰ কাৰ্যকলাপ অনুসৰণ আৰু বিশ্লেষণ কৰিবলৈ, সতৰ্কবাণী আৰু জাননীসমূহ স্থাপন কৰিবলৈ, আৰু প্ৰতিবেদন আৰু অন্তৰ্দৃষ্টি সৃষ্টি কৰিবলৈ সুবিধা দিয়ে।

তলত কিছুমান জনপ্ৰিয় সামাজিক মাধ্যম নিৰীক্ষণ সঁজুলিৰ চমু বিৱৰণ দিয়া হ'ল:

Hootsuite - এটা জনপ্ৰিয় সামাজিক মাধ্যম ব্যৱস্থাপনা সঁজুলি যি সামাজিক মাধ্যম নিৰীক্ষণ, সময়সূচী, আৰু প্ৰতিবেদন সহ সুবিধাসমূহেৰে এটা চুইট প্ৰদান কৰে।

Sprout Social - এটা সামাজিম মাধ্যম ব্যৱস্থাপনা প্লেটফৰ্ম যিয়ে মাধ্যমবোৰ নিৰীক্ষণ, বিশ্লেষণ, প্ৰকাশন, আৰু ব্যৱহাৰকাৰীৰ নিয়োজনৰ সুবিধা প্ৰদান কৰে।

Mention- এটা বাস্তৱ সময়ৰ মিডিয়া নিৰীক্ষণ আৰু বিশ্লেষণ সঁজুলি যিয়ে ব্যৱহাৰকাৰীসকলক ছ'চিয়েল মিডিয়া, বাতৰি চাইট, আৰু ব্লগকে ধৰি বিভিন্ন চেনেলত তেওঁলোকৰ ব্ৰেণ্ড বা প্ৰতিযোগীৰ উল্লেখ অনুসৰণ কৰাৰ সুবিধা দিয়ে।

Brand24 - এটা সামাজিক মাধ্যম নিৰীক্ষণ সঁজুলি আৰু ই বিভিন্ন প্লেটফৰ্মত এটা ব্ৰেণ্ড বা নিৰ্দিষ্ট কীৱৰ্ডৰ উল্লেখবোৰ অনুসৰণ কৰে আৰু গুৰুত্ব, প্ৰসাৰ, আৰু নিয়োজনৰ ওপৰত আলোকপাত কৰে।

Awario - এটা সামাজিক মাধ্যম নিৰীক্ষণ সঁজুলি যিয়ে ছ'চিয়েল মিডিয়া, ব্লগ, আৰু নিউজ চাইটকে ধৰি বিভিন্ন চেনেলত এটা ব্ৰেণ্ড বা কীৱৰ্ডৰ উল্লেখ অনুসৰণ কৰে আৰু আৱেগ আৰু প্ৰসাৰ সম্পৰ্কে অন্তৰ্দৃষ্টি প্ৰদান কৰে।

Agora Pulse - এটা সামাজিক মাধ্যম ব্যৱস্থাপনা সঁজুলি যি মাধ্যমবোৰৰ নিৰীক্ষণ, সময়সূচী, প্ৰকাশন, আৰু বিশ্লেষণ সুবিধা কৰি দিয়ে।

Zoho Social - এটা সামাজিক মাধ্যম ব্যৱস্থাপনা সঁজুলি যি মাধ্যমবোৰৰ নিৰীক্ষণ, সময়সূচী, প্ৰকাশন, আৰু বিশ্লেষণ সুবিধা কৰি দিয়ে।.

Talkwalker - এটা সামাজিক মাধ্যম নিৰীক্ষণ আৰু বিশ্লেষণ সঁজুলি যিয়ে বিভিন্ন চেনেলত এটা ব্ৰেণ্ড বা কীৱৰ্ডৰ উল্লেখ অনুসৰণ কৰে আৰু প্ৰসাৰ, আৰু নিয়োজনত গুৰুত্ব দিয়ে।

Meltwater - এটা মাধ্যম বুদ্ধিমত্তা আৰু সামাজিক মাধ্যম নিৰীক্ষণ সঁজুলি যিয়ে বিভিন্ন চেনেলত এটা ব্ৰেণ্ড বা কীৱৰ্ডৰ উল্লেখ অনুসৰণ কৰে আৰু আৱেগ, প্ৰসাৰ, আৰু নিয়োজনৰ ওপৰত গুৰুত্ব দিয়ে।

Brandwatch - এটা সামাজিক মাধ্যমৰ নিৰীক্ষণ আৰু বিশ্লেষণ সঁজুলি যিয়ে সামাজিক মাধ্যম, বাতৰি চাইট, আৰু ফ'ৰামকে ধৰি বিভিন্ন চেনেলত এটা ব্ৰেণ্ড বা কীৱৰ্ডৰ উল্লেখ অনুসৰণ কৰে, প্ৰসাৰ ওপৰত অন্তৰ্দৃষ্টি প্ৰদান কৰে।

৭.৪ সামাজিক মাধ্যমত হেচটেগ

হেচটেগ হৈছে হেচ (#) চিহ্নৰ পাছত থকা শব্দ বা বাক্যাংশ যিটো সামাজিক মাধ্যম প্লেটফৰ্মত বিষয়বস্তুৰ শ্ৰেণীবিভাজন আৰু বিচাৰ আৰু অনুসৰণ কৰাত সহজ কৰি তোলা হয়। হেচটেগ হৈছে সামাজিক মাধ্যম মাৰ্কেটিং আৰু এংগেজমেণ্টৰ বাবে এক শক্তিশালী আহিলা, আৰু ইয়াক সাধাৰণতে টুইটাৰ, ইনষ্টাগ্ৰাম আৰু টিকটকৰ দৰে প্লেটফৰ্মত ব্যৱহাৰ কৰা হয়।

সামাজিক মাধ্যম ত হেচটেগ ব্যৱহাৰ কৰাৰ কিছুমান মূল উপায় হ'ল-

শ্ৰেণীবিভাজন: বিষয় আৰু পৰিঘটনা অনুসৰি বিষয়বস্তু শ্ৰেণীভুক্ত কৰিবলৈ হেচটেগ ব্যৱহাৰ কৰা হয়। উদাহৰণস্বৰূপে, নতুন ৰেষ্টুৰেণ্ট খোলাৰ বিষয়ে এটা পোষ্টত #foodie বা #newrestaurant বুলি হেচটেগ থাকিব পাৰে।

আৱিষ্কাৰ: কোনো বিশেষ বিষয়ৰ প্ৰতি আগ্ৰহী ব্যৱহাৰকাৰীসকলৰ বাবে বিষয়বস্তু অধিক আৱিষ্কাৰযোগ্য কৰিবলৈ হেচটেগ ব্যৱহাৰ কৰা হয়। ব্যৱহাৰকাৰীসকলে সেই বিষয়ৰ সৈতে জড়িত বিষয়বস্তু বিচাৰিবলৈ হেচটেগ সন্ধান কৰিব পাৰে। তেওঁলোকৰ ফিডত নতুন বিষয়বস্তু চাবলৈ হেচটেগ অনুসৰণ কৰিব পাৰে।

ব্ৰেণ্ডিং: হেচটেগক প্ৰায়ে কোনো ব্যৱসায়, সামগ্ৰী বা অভিযানৰ প্ৰচাৰৰ বাবে ব্ৰেণ্ডিং সঁজুলি হিচাপে ব্যৱহাৰ কৰা হয়। উদাহৰণস্বৰূপে, এটা কাপোৰৰ ব্ৰেণ্ডে নিজৰ শেহতীয়া সংগ্ৰহৰ প্ৰচাৰৰ বাবে #FashionForward হেচটেগ ব্যৱহাৰ কৰে।

সম্প্ৰদায় গঠন: হেচটেগসমূহৰ যোগেদি একে আগ্ৰহৰ সম্প্ৰদায় গঢ়ি তুলিবলৈ সুবিধা হয়। উদাহৰণস্বৰূপে, সামাজিক মতামত বা জনমত এটা গঢ় দিবলৈ, এটা সম্প্ৰদায় গঢ়ি

তুলিবলৈ #BlackLivesMatter, #WeWantJustice #Standwith(XYZ) হেচটেগ ব্যৱহাৰ কৰা দেখা যায়।

অভিযান অনুসৰণ: সামাজিক আন্দোলন বা চৰকাৰৰ বিৰুদ্ধে আন্দোলন প্ৰচাৰৰ বাবে হেচটেগ ব্যৱহাৰ কৰা হয় আদি অভিযানৰ সফলতা অনুসৰণ আৰু নিয়োজিততা জুখিবলৈও ব্যৱহাৰ কৰা হয়। উদাহৰণস্বৰূপে, এটা সামাজিক মাধ্যম অভিযানত এটা অনন্য হেচটেগ থাকিব পাৰে যাতে কিমান ব্যৱহাৰকাৰীয়ে অভিযানটোৰ সৈতে শ্বেয়াৰ আৰু জড়িত হৈ আছে সেইটো অনুসৰণ কৰিব পাৰে।

হেচটেগ ব্যৱহাৰ কৰাৰ সময়ত, শ্বেয়াৰ কৰা বিষয়বস্তুৰ সঠিক বৰ্ণনা কৰা প্ৰাসংগিক আৰু নিৰ্দিষ্ট কীৱৰ্ড বাছনি কৰাটো গুৰুত্বপূৰ্ণ। অত্যধিক হেচটেগ বা অপ্ৰাসংগিক হেচটেগ ব্যৱহাৰ কৰিলে পোষ্টবোৰ স্পেমী যেন লাগিব পাৰে আৰু নিয়োজিততা হ্ৰাস পাব পাৰে।

৭.৫ ভাই�ৰেল কণ্টেণ্ট

ভাইৰেল কণ্টেণ্ট হৈছে লাইক, শ্বেয়াৰ, আৰু কমেণ্টৰ জৰিয়তে সামাজিক মাধ্যম প্লেটফৰ্মত দ্ৰুত আৰু ব্যাপকভাৱে বিয়পি পৰা কণ্টেণ্ট। ভাইৰেল কণ্টেণ্ট যিকোনো হাস্যকৰ মিম বা ভিডিঅ'ৰ পৰা আৰম্ভ কৰি ব্ৰেকিং নিউজ ষ্ট'ৰী বা হৃদয়স্পৰ্শী মুহূৰ্তও হ'ব পাৰে। ভাইৰেল কণ্টেণ্টৰ মূল বৈশিষ্ট্য হ'ল ই বহু সংখ্যক লোকৰ মনত ঠাই পাই আৰু তেওঁলোকক আনৰ সৈতে শ্বেয়াৰ কৰিবলৈ অনুপ্ৰাণিত কৰে।

সামাজিক মাধ্যমত কণ্টেণ্ট ভাইৰেল হোৱাৰ কেইটামান মনকৰিবলগীয়া দিশঃ

আৱেগিক আবেদন: যিবোৰ বিষয়বস্তুৱে শক্তিশালী আৱেগ, যেনে সুখ, খং বা ভয়ৰ সৃষ্টি কৰে, সেইবোৰ ভাইৰেল হোৱাৰ সম্ভাৱনা বেছি। মানুহে সাধাৰণতে আৱেগিক সঁহাৰিৰ বিষয়বস্তু শ্বেয়াৰ কৰি ভাল পায়।

নতুনত্ব: অনন্য, অপ্ৰত্যাশিত, অন্বেষিত বা আচৰিত ধৰণৰ বিষয়বস্তুৱে মানুহৰ দৃষ্টি আকৰ্ষণ কৰাৰ সম্ভাৱনা বেছি আৰু আনৰ সৈতে ভাগ-বতৰা কৰিবলৈ উৎসাহিত কৰা সম্ভাবনা থাকে।

প্ৰাসংগিকতা: সাম্প্ৰতিক পৰিঘটনা, ধাৰা বা সাংস্কৃতিক মুহূৰ্তৰ সৈতে প্ৰাসংগিক বিষয়বস্তু ভাইৰেল হোৱাৰ সম্ভাৱনা বেছি। মানুহে সময়োপযোগী আৰু তেওঁলোকৰ আগ্ৰহৰ লগত প্ৰাসংগিক বিষয়বস্তু শ্বেয়াৰ কৰাৰ সম্ভাৱনা বেছি।

শ্বেয়াৰযোগ্যতা: সামাজিক মাধ্যম প্লেটফৰ্মত শ্বেয়াৰ আৰু বিতৰণ কৰাত সহজ বিষয়বস্তু ভাইৰেল হোৱাৰ সম্ভাৱনা বেছি। দৃশ্যগতভাৱে আকৰ্ষণীয়, স্পষ্ট বাৰ্তা থকা আৰু বুজিবলৈ সহজ বিষয়বস্তু শ্বেয়াৰ কৰাৰ সম্ভাৱনা বেছি।

প্ৰভাৱশালীতা: সামাজিক মাধ্যমৰ প্ৰভাৱশালী বা চেলিব্ৰিটিয়ে শ্বেয়াৰ কৰা বিষয়বস্তু ভাইৰেল হোৱাৰ সম্ভাৱনা বেছি। প্ৰভাৱশালীসকলৰ বৃহৎ অনুগামী থাকে আৰু ভাইৰেল বিষয়বস্তুৰ প্ৰসাৰ বৃদ্ধি কৰিব পাৰে।

ভাইৰেল কণ্টেণ্ট তৈয়াৰ কৰাটো কোনো বিশেষ বিজ্ঞান নহয়, কিন্তু সামাজিক মাধ্যমৰ কণ্টেণ্টৰ ভাইৰেলত কি কি কাৰকে অৱিহণা যোগায় সেই কথা বুজি পোৱাটোৱে ব্যৱসায় আৰু ব্যক্তিসকলক এনে কণ্টেণ্ট তৈয়াৰ কৰাত সহায় কৰিব পাৰে যিটো বহু দৰ্শকে শ্বেয়াৰ কৰা বা দেখাৰ সম্ভাৱনা অধিক।

৭.৬ সামাজিক মাধ্যমত মাৰ্কেটিং

সামাজিক মাধ্যমত মাৰ্কেটিং সামাজিক মাধ্যম প্লেটফৰ্ম ব্যৱহাৰ কৰি এই মাধ্যমৰ ব্যৱহাৰকাৰী আৰু সম্ভাব্য গ্ৰাহকৰ মাজত কোনো ব্ৰেণ্ড, প্ৰডাক্ট বা সেৱাৰ প্ৰচাৰ কৰিবলৈ ওলোৱাটোক সূচায়। সামাজিক মাধ্যমত মাৰ্কেটিং প্লেটফৰ্মত কণ্টেণ্ট সৃষ্টি আৰু শ্বেয়াৰ কৰা, লগতে মাৰ্কেটিং প্ৰচেষ্টা হিচাপ কৰিবলৈ আৰু অনুকূল কৰিবলৈ পেইড এডভাৰটাইজিং আৰু এনালাইটিক্স ব্যৱহাৰ কৰা এইবিলাক কথা জড়িত হৈ থাকে।

সামাজিক মাধ্যমত মাৰ্কেটিঙৰ মূল উপাদানসমূহ হৈছে

বিষয়বস্তু সৃষ্টি: সামাজিক মাধ্যম মাৰ্কেটিংৰ অন্তৰ্গত বিষয়বস্তু সৃষ্টি আৰু শ্বেয়াৰ কৰা, যেনে সামাজিক মাধ্যম প্লেটফৰ্মত ছবি, ভিডিঅ', আৰু ব্লগ পোষ্ট। বিষয়বস্তু আকৰ্ষণীয়, তথ্যসমৃদ্ধ আৰু লক্ষ্য গ্ৰাহকৰ বাবে প্ৰাসংগিক হ'ব লাগে।

দৰ্শকৰ সংযোগ: সামাজিক মাধ্যমত সামাজিক মাধ্যম মাৰ্কেটিংৰ মন্তব্য, বাৰ্তা আৰু অন্যান্য ধৰণৰ যোগাযোগৰ জৰিয়তে গ্ৰাহক আৰু সম্ভাব্য গ্ৰাহকৰ সৈতে সম্পৰ্কিত হৈ থাকে। ইয়াৰ ফলত সম্পৰ্ক গঢ়ি তোলাত সহায় হয় আৰু ব্ৰেণ্ডৰ আনুগত্য বৃদ্ধি পায়।

পেইড এডভাৰটাইজিং: সামাজিক মাধ্যমত মাৰ্কেটিঙ পেইড এডভাৰটাইজিঙ জড়িত হ'ব পাৰে, যেনে বৃহৎ দৰ্শকৰ মাজলৈ লৈ যোৱা আৰু নিৰ্দিষ্ট জনগাঁথনিক উদ্দেশ্য কৰি প্ৰচাৰ কৰা পোষ্ট বা পৃষ্ঠপোষকতা কৰা এড ইয়াৰ ভিতৰত থাকে।

বিশ্লেষণ আৰু অনুসৰণ: সামাজিক মাধ্যমত মাৰ্কেটিঙ বিপণনৰ সফলতা জুখিবলৈ আৰু তথ্য-চালিত সিদ্ধান্ত ল'বলৈ মেট্ৰিক্স, যেনে এংগেজমেণ্ট হাৰ আৰু ৰূপান্তৰ হাৰ অনুসৰণ আৰু বিশ্লেষণ কৰাৰ দিশবোৰ অন্তৰ্ভুক্ত হৈ থাকে।

মাৰ্কেটিঙৰ বাবে কিছুমান জনপ্ৰিয় সামাজিক মাধ্যম প্লেটফৰ্মৰ ভিতৰত আছে ফেচবুক, ইনষ্টাগ্ৰাম, টুইটাৰ, লিংকডইন, আৰু টিকটক। প্ৰতিটো প্লেটফৰ্মৰ নিজস্ব শক্তি আৰু দুৰ্বলতা

আছে, লগতে অনন্য সম্প্রদায় আছে, গতিকে ব্যৱসায়ীসকলৰ বাবে তেওঁলোকৰ বিপণন লক্ষ্য আৰু লক্ষ্য গ্রাহকৰ সৈতে মিল থকা প্লেটফর্মসমূহ বাছি লোৱাটো গুৰুত্বপূর্ণ বিষয়।

সামাজিক মাধ্যমত মার্কেটিং ব্যৱসায়ীসকলৰ বাবে গ্রাহকৰ সৈতে যোগাযোগ আৰু তেওঁলোকৰ সৈতে জড়িত হোৱাৰ, ব্রেণ্ড সজাগতা গঢ়ি তোলা, আৰু ৰূপান্তৰক আগুৱাই নিয়াৰ এক ফলপ্রসূ উপায় হ'ব পাৰে। কিন্তু বিপণন প্রচেষ্টা যাতে ফলপ্রসূ আৰু কার্যক্ষম হয় তাৰ বাবে লক্ষ্য গ্রাহক আৰু মেট্রিকৰ বিষয়ে স্পষ্ট কৌশল আৰু জ্ঞান থকাটো গুৰুত্বপূর্ণ।

৭.৭ সামাজিক মাধ্যম ত গোপনীয়তা

প্রায় সকলোৱেই কোনোবা নহয় কোনোবা ধৰণে সামাজিক মাধ্যম ব্যৱহাৰ কৰে। এতিয়া যুৱ প্রজন্মৰ বাবে এটা দিন যেন সামাজিক মাধ্যম অবিহনে জীৱনটো অসম্পূর্ণ, নহ'লে আমি ক'ব পাৰো যে আমি মানুহ খাদ্য, পানী, বায়ুৰ দৰেই সামাজিক মাধ্যমৰ ওপৰত নির্ভৰশীল হৈ পৰিছোঁ। জনসাধাৰণ ইমানেই নির্ভৰশীল যে সকলোৱে সামাজিক মাধ্যম প্লেটফর্মত প্রতিটো তথ্য শ্বেয়াৰ কৰাৰ প্রৱণতা থাকে। সামাজিক মাধ্যমৰ মূল ৰাজহৰ উৎস হ'ল বিজ্ঞাপন। তদুপৰি ফেচবুক, ইনষ্টাগ্রামৰ দৰে সামাজিক মাধ্যম চাইটত প্রতিজন ব্যৱহাৰকাৰীয়ে ইণ্টাৰনেটত কি ব্রাউজ কৰে ভাল আৰু অপছন্দৰ বিষয়ে চমু প্রফাইল যুগুত কৰে আৰু সেই অনুসৰি তেওঁলোকে বিজ্ঞাপন ফিডত আহে। আনকি কিছুমান সামাজিক মাধ্যম চাইটত ব্যৱহাৰকাৰীয়ে অফলাইনত থাকিলযো কি কৰি আছে সেই বিষয়ে তথ্য সংগ্রহ কৰে য'ত তেওঁলোকে কোনবোৰ দোকানলৈ যাবলৈ ভাল পায়, আগতে ব্যৱহাৰকাৰীৰ বন্ধুসকলে কি ভাল পায় আৰু কি বেয়া পায়, ক'ত ভ্রমণ কৰিছিল সকলো তথ্য আহৰণ কৰিব পাৰে।

সামাজিক মাধ্যমত গোপনীয়তাৰ কিছুমান মূল দিশ ইয়াত উল্লেখ কৰা হ'ল-

তথ্য সংগ্রহ: সামাজিক মাধ্যম প্লেটফর্মসমূহে ব্যক্তিগত তথ্য, ব্রাউজিং আচৰণ, আৰু অৱস্থানৰ ব্যৱহাৰকাৰীৰ পৰা তথ্য সংগ্রহ কৰে। এই তথ্য বিজ্ঞাপন আৰু অন্যান্য উদ্দেশ্যৰ বাবে ব্যৱহাৰ কৰে। গতিকে গোপনীয়তা ছেটিংছ বুজা, ইয়াক নিয়ন্ত্রণ কৰা, তথ্য সংগ্রহ কৰা আৰু ইয়াক ব্যৱহাৰ আৰু পৰিচালনাৰ কথাটো বুজি উঠাতো গুৰুত্বপূর্ণ।

গোপনীয়তা ছেটিংছ: সামাজিক মাধ্যম প্লেটফর্মসমূহে গোপনীয়তা ছেটিংছ প্রদান কৰে যিয়ে ব্যৱহাৰকাৰীসকলক তেওঁলোকৰ পোষ্ট, প্রফাইল তথ্য আৰু কার্য্যকলাপ কোনে চাব পাৰে নিয়ন্ত্রণ কৰিবলৈ অনুমতি দিয়ে। ব্যক্তিগত তথ্য কেৱল উদ্দেশ্যপ্রণোদিত দর্শকৰ বাবেহে দৃশ্যমান হোৱাটো নিশ্চিত কৰিবলৈ এই ছেটিংছসমূহ নিয়মিতভাৱে পর্যালোচনা আৰু সঠিক কৰাটো গুৰুত্বপূর্ণ।

তৃতীয় পক্ষৰ এপসমূহ: সামাজিক মাধ্যম প্লেটফৰ্মসমূহে প্ৰায়ে তৃতীয় পক্ষৰ এপ আৰু সেৱাসমূহৰ সৈতে একত্ৰিত হয়, যিয়ে ব্যৱহাৰকাৰীৰ তথ্য লাভ কৰিব পাৰে। ব্যক্তিগত তথ্যৰ প্ৰৱেশৰ অনুমতি দিয়াৰ আগতে এই এপ আৰু সেৱাসমূহৰ গোপনীয়তা নীতিসমূহ পৰ্যালোচনা কৰা আৰু বুজাটো গুৰুত্বপূৰ্ণ।

চাইবাৰ সুৰক্ষা: সামাজিক মাধ্যম প্লেটফৰ্মসমূহ হেকিং বা ফিছিং কেলেংকাৰীৰ দৰে চাইবাৰ আক্ৰমণৰ সন্মুখীন হ'ব পাৰে। ব্যক্তিগত তথ্যক অকৰ্তৃত্বশীল প্ৰৱেশৰ পৰা সুৰক্ষিত কৰিবলৈ শক্তিশালী পাছৱৰ্ড ব্যৱহাৰ কৰা আৰু টু ষ্টেপ প্ৰমাণীকৰণ কৰাত গুৰুত্ব দিব লাগে।

আইনী সমস্যা: সামাজিক মাধ্যম প্লেটফৰ্মসমূহ গোপনীয়তা আৰু তথ্য সুৰক্ষাৰ সৈতে জড়িত আইন আৰু নিয়মৰ অধীনত থাকে। এই আইন আৰু নিয়মসমূহৰ বিষয়ে সচেতন হোৱাটো প্ৰয়োজনীয় আৰু যিকোনো গোপনীয়তা উলংঘাৰ বিষয়ে উপযুক্ত কৰ্তৃপক্ষক জনোৱাটো গুৰুত্বপূৰ্ণ কথা।

সামগ্ৰিকভাৱে, সামাজিক মাধ্যম ব্যৱহাৰকাৰীসকলৰ বাবে এই প্লেটফৰ্মসমূহ ব্যৱহাৰ কৰাৰ গোপনীয়তাৰ প্ৰভাৱৰ বিষয়ে সচেতন হোৱাটো আৰু তেওঁলোকৰ ব্যক্তিগত তথ্য সুৰক্ষিত কৰাৰ বাবে পদক্ষেপ লোৱাটো মন কৰিবলগীয়া কথা। ইয়াৰ ভিতৰত গোপনীয়তা ছেটিংছ বুজি পোৱা আৰু পৰিচালনা কৰা, স্পৰ্শকাতৰ তথ্য অংশীদাৰী কৰাৰ ক্ষেত্ৰত সতৰ্ক হোৱা, আৰু শক্তিশালী চাইবাৰ সুৰক্ষা পদ্ধতিসমূহ ব্যৱহাৰ কৰা আদি দিশবোৰ জড়িত হৈ থাকে।

প্ৰতিটো তথ্য ব্যক্তিগত কৰি ৰখাৰ বাবে আপুনি সামাজিক মাধ্যমৰ গোপনীয়তা নীতি ভালদৰে পঢ়িব লাগিব। তলত কিছুমান উপায় দিয়া হ'ল-

১. ছ'চিয়েল নেটৱৰ্কিং চাইটৰ চর্ত আৰু নিয়মবোৰ ভালদৰে পঢ়ক।

২. প্ৰয়োজন অনুসৰি একাউণ্টৰ গোপনীয়তা ছেটিংছ ছেট কৰক।

৩. তৃতীয় পক্ষৰ লিংক যেনে "Check your Marriage Date", "Won prize" ইত্যাদি ক্লিক কৰাৰ পৰা বিৰত থাকিব।

৪. আপোনাৰ ডিভাইচসমূহৰ বাবে জনপ্ৰিয় এন্টিভাইৰাছ চফ্টৱেৰ ব্যৱহাৰ কৰক।

৫. প্ৰকৃত অৱস্থান অনবৰতে মুকলি কৰি নাৰাখিব । ইয়াক বন্ধ কৰক। কাৰণ কিছুমান চাইটে অফলাইন জগততো ব্যৱহাৰকাৰীৰ কার্যকলাপৰ তথ্যও ৰাখে।

৬. Security Answers ছেট কৰিবলৈ নাপাহৰিব।

৭. ৰাজহুৱা ডিভাইচৰ পৰা আপোনাৰ একাউণ্ট লগ ইন বা ব্ৰাউজ নকৰিব। আৰু ব্ৰাউজিং শেষ কৰিলে একাউণ্টৰ পৰা লগআউট কৰক।

৮. পোষ্ট কৰাৰ আগতে সদায় পোষ্টটো বিশ্লেষণ কৰক। সামাজিক মাধ্যমত ব্যক্তিগত তথ্য শ্বেয়াৰ নকৰিব।

৯. সদায় এটা শক্তিশালী পাছৱৰ্ড দিয়ক আৰু নিয়মীয়াকৈ যথা সময়ত সলনি কৰক। একাধিক চাইটৰ বাবে কেতিয়াও একে পাছৱৰ্ড নাৰাখিব।

৭.৮ সামাজিক মাধ্যমৰ প্রত্যাহ্বান, সুযোগ আৰু ফান্দ

সামাজিক মাধ্যমৰ প্রত্যাহ্বানসমূহ তলত উল্লেখ কৰা হ'ল-

গোপনীয়তাৰ চিন্তা: অনলাইন ছ'চিয়েল নেটৱৰ্কৰ ব্যৱহাৰকাৰীসকলে তেওঁলোকৰ ব্যক্তিগত তথ্য, ব্রাউজিং আচৰণ, আৰু অৱস্থান অনুসৰণ কৰিব পাৰে আৰু অন্যান্য উদ্দেশ্যৰ লগতে বিজ্ঞাপনৰ বাবে ব্যৱহাৰ কৰিব পাৰে। ইয়াৰ ফলত গোপনীয়তা আৰু তথ্য সুৰক্ষাৰ বিষয়ে চিন্তা হ'ব পাৰে।

চাইবাৰ বুলিং: অনলাইন ছ'চিয়েল নেটৱৰ্কে চাইবাৰ বুলিং আৰু হাৰাশাস্তিৰ বাবে এক মঞ্চ প্রদান কৰিব পাৰে, যাৰ ফলত ভুক্তভোগীৰ আৱেগিক আৰু মানসিক ক্ষতি হ'ব পাৰে।

ভুল তথ্য আৰু ভু�ৱা বাতৰিঃ অনলাইন ছ'চিয়েল নেটৱৰ্ক ভুল তথ্য আৰু ভুৱা বাতৰিৰ প্রকোপ বৃদ্ধিৰ এক ক্ষেত্র হ'ব পাৰে। এইবোৰ দ্রুতগতিত বিয়পিব পাৰে আৰু ব্যক্তি আৰু সমাজৰ ওপৰত গুৰুতৰ প্রভাৱ পেলাব পাৰে।

আসক্তিঃ অনলাইন ছ'চিয়েল নেটৱৰ্কত তথ্য আৰু জাননীৰ অহৰহ প্রবাহ আসক্তিলৈ পৰিণত হ'ব পাৰে, যাৰ ফলত মানসিক স্বাস্থ্য আৰু সুস্থতাৰ ওপৰত নেতিবাচক প্রভাৱ পৰিব পাৰে।

তলত সামাজিক মাধ্যম ৰ সুযোগসমূহ উল্লেখ কৰা হ'ল-

যোগাযোগ: অনলাইন ছ'চিয়েল নেটৱৰ্কে সমগ্র বিশ্বতে মানুহক ইজনে সিজনৰ সৈতে যোগাযোগ আৰু সংযোগ স্থাপনৰ এক সুবিধাজনক আৰু সুলভ উপায় হিচাপে কাম কৰিছে।

ব্যৱসায়িক সুযোগ: অনলাইন সামাজিক নেটৱৰ্কে ব্যৱসায়ীসকলক গ্রাহকৰ সৈতে যোগাযোগ আৰু তেওঁলোকৰ সৈতে জড়িত হোৱাৰ, ব্রেণ্ড সজাগতা গঢ়ি তোলা, আৰু ৰূপান্তৰক আগুৱাই নিয়াৰ সুবিধা প্রদান কৰে।

শিক্ষাঃ অনলাইন ছ'চিয়েল নেটৱৰ্কক শিক্ষাৰ আহিলা হিচাপে ব্যৱহাৰ কৰিব পাৰি, শৈক্ষিক সম্পদৰ সুবিধা প্রদান কৰিব পাৰি আৰু ছাত্র-ছাত্রী আৰু শিক্ষকৰ মাজত সহযোগিতাৰ সুবিধা প্রদান কৰিব পাৰি।

সামাজিক সক্রিয়তা: অনলাইন সামাজিক নেটৱৰ্ক সামাজিক সক্রিয়তাৰ বাবে এক শক্তিশালী আহিলা হ'ব পাৰে, যাৰ ফলত মানুহক সামাজিক আৰু ৰাজনৈতিক বিষয়সমূহৰ

বিষয়ে সজাগতা বৃদ্ধি আৰু তৃণমূল পর্যায়ৰ মতামতৰ মঞ্চ বা জনমত সংগঠিত কৰিব পৰা যায়।

সামাজিক মাধ্যম ৰ ফান্দসমূহ তলত উল্লেখ কৰা হ'লঃ

তথ্যৰ অতিৰিক্ত বোজা: সামাজিক মাধ্যমত তথ্যৰ নিৰৱচ্ছিন্ন প্রবাহ থাকে, ফলত তথ্যৰ অতিৰিক্ত বোজা আৰু জ্ঞানমূলক অতিৰিক্ত বোজাৰ সৃষ্টি হয়।

ফিল্টাৰ বাবল: অনলাইন ছ'চিয়েল নেটৱর্কে ফিল্টাৰ বাবল সৃষ্টি কৰিব পাৰে, য'ত ব্যৱহাৰকাৰীসকলে কেৱল তেওঁলোকৰ বর্তমানৰ বিশ্বাস নিশ্চিত কৰা তথ্য আৰু মতামতৰ সৈতে দেখা দেখি হৈ থাকিব পাৰে আৰু ফলত কেন্দ্রীকৰণ বা বিভাজনৰ সৃষ্টি হ'ব পাৰে।

আসক্তি: অনলাইন ছ'চিয়েল নেটৱর্কৰ আসক্তি স্বভাৱৰ বাবে মানসিক স্বাস্থ্য আৰু সুস্থতাৰ ওপৰত নেতিবাচক প্রভাৱ পৰিব পাৰে, য'ত হতাশা, উদ্বেগ, কম আত্মসন্মান আদিয়ে গা কৰি উঠিব পাৰে।

সময় ব্যৱস্থাপনাঃ অনলাইন ছ'চিয়েল নেটৱর্কত সময় অতিবাহিত কৰাৰ ফলত ফলপ্রসূভাৱে কাম সম্পাদন, পৰিচালনা কৰাত অসুবিধাৰ সৃষ্টি কৰিব পাৰে আৰু গুৰুত্বপূর্ণ কামত মনোনিৱেশ কৰিলৈ অসুবিধা হ'ব পাৰে।

সামগ্রিকভাৱে অনলাইন ছ'চিয়েল নেটৱর্কৰ সুযোগ আৰু প্রত্যাহ্বান দুয়োটাই মন কৰিবলগীয়া দিশ। ব্যক্তি আৰু সামগ্রিকভাৱে সমাজে এই প্রত্যাহ্বানসমূহৰ প্রতি সচেতন হোৱাটো গুৰুত্বপূর্ণ। অনলাইন ছ'চিয়েল নেটৱর্কে উপস্থাপন কৰা সুযোগসমূহ আকোৱালি লোৱাৰ লগতে এই প্রত্যাহ্বানসমূহৰ সমাধানৰ বাবে পদক্ষেপ লোৱাটো জৰুৰী।



অগ্রগতি নিৰীক্ষণ

তলে যুক্তিসমূহ সত্য নে অসত্য বিচাৰ কৰক।

১. ছ'চিয়েল মিডিয়া মনিটৰিংৰ দ্বাৰা ব্যক্তি, ব্রেণ্ড বা বিষয়বস্তু সম্পর্কে তথ্য সংগ্রহ কৰিবলৈ ছ'চিয়েল মিডিয়া প্লেটফর্মসমূহ ট্রেক আৰু বিশ্লেষণ কৰা হয়।

২. ছ'চিয়েল মিডিয়া মনিটৰিং বজাৰৰ গৱেষণা আৰু প্রতিযোগিতামূলক বিশ্লেষণৰ বাবে ব্যৱহাৰ কৰিব পাৰি।

৩. ছ'চিয়েল মিডিয়া মনিটৰিং সা-সৰঞ্জামে ব্রেণ্ডৰ উল্লেখ আৰু মূল শব্দৰ বাবে ৰিয়েল-টাইম সতর্কবাণী আৰু নটিফিকেশ্যন প্রদান কৰিব পাৰে।

৪. ছ'চিয়েল মিডিয়া মনিটৰিং কেৱল ডাঙৰ ছ'চিয়েল মিডিয়া উপস্থিতি থকা ব্যৱসায়ৰ বাহিৰেও সকলো ধৰণৰ ব্যৱসায়ৰ বাবে উপযোগী।

৫. ছ'চিয়েল মিডিয়া মনিটৰিং কেৱল গ্রাহকৰ অভিযোগ আৰু নেতিবাচক প্রতিক্রিয়া ট্রেক কৰাৰ বাবে নহয়, ইয়াৰ দ্বাৰা বহুতো কাম কৰিব পাৰি যেনে ব্রেণ্ডৰ প্রসাৰ, ট্রেণ্ড বিচাৰ আদি।

৭.৯ আধ্যায়টিৰ পৰা আমি কি কি শিকিলোঁ

- সামাজিক মাধ্যম নিৰীক্ষণ হৈছে ব্যক্তি, ব্ৰেণ্ড বা বিষয় সম্পৰ্কে অন্তৰ্দৃষ্টি লাভ কৰিবলৈ সামাজিক মাধ্যম প্লেটফৰ্মসমূহ অনুসৰণ আৰু বিশ্লেষণ কৰা প্ৰক্ৰিয়া।
- হেচটেগ হৈছে # চিহ্নলৰ পাছত থকা এটা মূল শব্দ বা বাক্যাংশ যিটো সামাজিক মাধ্যম প্লেটফৰ্মত কোনো নিৰ্দিষ্ট বিষয়ৰ সৈতে জড়িত বিষয়বস্তু শ্ৰেণীভুক্ত আৰু সংগঠিত কৰিবলৈ ব্যৱহাৰ কৰা হয়।
- ভাই�ৰেল বিষয়বস্তুৱে অনলাইন মাধ্যমক বুজায়, যেনে ভিডিঅ', ছবি বা প্ৰবন্ধ, যিয়ে সামাজিক মাধ্যমত শ্বেয়াৰিঙৰ জৰিয়তে দ্ৰুত আৰু ব্যাপকভাৱে বিয়পি পৰে, প্ৰায়ে বিষয়ে ব্যাপক জনপ্ৰিয়তা বা কুখ্যাতি লাভ কৰে।
- সামাজিক মাধ্যম ত গোপনীয়তাই ব্যক্তিৰ ব্যক্তিগত তথ্য আৰু সামাজিক মাধ্যম প্লেটফৰ্মত শ্বেয়াৰ কৰা তথ্য নিয়ন্ত্ৰণ আৰু পৰিচালনা কৰাৰ অধিকাৰক বুজায়।
- সামাজিক মাধ্যম মার্কেটিং হৈছে কোনো সামগ্ৰী বা সেৱাৰ প্ৰচাৰ আৰু গ্ৰাহকৰ সৈতে জড়িত হৈ ব্ৰেণ্ড গঢ়ি তোলা আৰু বিক্ৰী বৃদ্ধিৰ বাবে সামাজিক মাধ্যম প্লেটফৰ্মৰ ব্যৱহাৰ।
- সামাজিক মাধ্যমত সুযোগসমূহে সামাজিক মাধ্যম প্লেটফৰ্ম ব্যৱহাৰ কৰি লাভ কৰিব পৰা সম্ভাব্য সুবিধা আৰু সুবিধাসমূহ বুজায়, যেনে ব্ৰেণ্ডৰ দৃশ্যমানতা বৃদ্ধি, গ্ৰাহকৰ সংযোগ, আৰু নিৰ্দিষ্ট দৰ্শকক লক্ষ্য কৰি লোৱাৰ ক্ষমতা।
- সামাজিক মাধ্যমত প্ৰত্যাহ্বানসমূহে সামাজিক মাধ্যম ব্যৱহাৰৰ লগত জড়িত সম্ভাব্য বিপদ আৰু বাধাসমূহক বুজায়, যেনে অনলাইন সুনাম পৰিচালনা কৰা, নেতিবাচক প্ৰতিক্ৰিয়াৰ সৈতে মোকাবিলা কৰা, আৰু ব্যৱহাৰকাৰীৰ গোপনীয়তা সুৰক্ষিত কৰা।
- সামাজিক মাধ্যমত থকা ফান্দবোৰে সামাজিক মাধ্যম ব্যৱহাৰৰ লগত জড়িত সম্ভাব্য বিপদ আৰু অসুবিধা, যেনে চাইবাৰ বুলিং, আসক্তি, ভুল তথ্য, আৰু ভুৱা বাতৰিৰ প্ৰসাৰক বুজায়।



৭.১০ অধিক জানিবলৈ

1) "The Social Media Bible: Tactics, Tools, and Strategies for Business Success" by Lon Safko and David K. Brake

2) "Social Media Marketing All-in-One for Dummies" by Jan Zimmerman and Deborah Ng

3) "Socialnomics: How Social Media Transforms the Way We Live and Do Business" by Erik Qualman
4) "The Art of Social Media: Power Tips for Power Users" by Guy Kawasaki and Peg Fitzpatrick
5) "Likeable Social Media: How to Delight Your Customers, Create an Irresistible Brand, and Be Amazing on Facebook, Twitter, LinkedIn, Instagram, Pinterest, and More" by Dave Kerpen



৭.১০ অগ্ৰগতিৰ খতিয়ান

প্ৰশ্ন ১ৰ উত্তৰ: সঁচা

প্ৰশ্ন ২ৰ উত্তৰ: সঁচা

প্ৰশ্ন ৩ৰ উত্তৰ: সঁচা

প্ৰশ্ন ৫ ৰ উত্তৰ: মিছা

প্ৰশ্ন ৬ৰ উত্তৰ:: মিছা



৭.১২ আৰ্হি প্ৰশ্ন

প্ৰশ্ন ১। ব্যৱসায়ীসকলৰ বাবে সামাজিক মাধ্যমৰ নিৰীক্ষণৰ সুবিধা কি?

প্ৰশ্ন ২। সামাজিক মাধ্যমত হেচটেগ ব্যৱহাৰৰ বাবে কি কি পদ্ধতি আছে?

প্ৰশ্ন ৩। কণ্টেণ্টৰ মূল উপাদানবোৰ কি কি যিয়ে ইয়াক ভাইৰেল কৰি তুলিব পাৰে?

প্ৰশ্ন ৪। সামাজিক মাধ্যম ব্যৱহাৰৰ লগত জড়িত কিছুমান সাধাৰণ গোপনীয়তাৰ চিন্তা কি কি হ'ব পাৰে?

প্ৰশ্ন ৫। সামাজিক মাধ্যম প্লেটফৰ্মত ব্যক্তিয়ে নিজৰ গোপনীয়তা কেনেকৈ সুৰক্ষিত কৰিব পাৰে?

প্ৰশ্ন ৬। মাৰ্কেটিঙৰ বাবে সামাজিক মাধ্যম ব্যৱহাৰ কৰাৰ সময়ত ব্যৱসায়ীসকলে কি কি ডাঙৰ প্ৰত্যাহ্বানৰ সন্মুখীন হয়?

প্ৰশ্ন ৭। গ্ৰাহক সেৱাৰ বাবে সামাজিক মাধ্যম ব্যৱহাৰ কৰিলে কি কি লাভ হয়?

****

অধ্যায় ৮: ছ'চিয়েল মিডিয়াত নিৰাপত্তাৰ বিষয়

অধ্যায় গাঁথনি

৮.১ উদ্দেশ্য

৮.২ পৰিচয়

৮.৩ ছ'চিয়েল মিডিয়া সুৰক্ষাৰ সমস্যাসমূহ

৮.৪ আপত্তিজনক বিষয়বস্তু সম্পর্কে জাননী দিয়া আৰু তথ্য চিহ্নিত কৰা

৮.৫ আপত্তিজনক বিষয়বস্তু প্ৰকাশ নিয়ন্ত্ৰণ কৰা আইন

৮.৭ ছ'চিয়েল মিডিয়াৰ ব্যৱহাৰৰ বাবে উত্তম পদ্ধতি

৮.৮ কেছ ষ্টাডিজ

৮.৯ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ

৮.১০ অধিক জনিবলৈ

৮.১১ অগ্ৰগতিৰ খতিয়ান

৮.১২ আৰ্হি প্ৰশ্ন

৮.১ উদ্দেশ্য

এই অধ্যায়টি অধ্যয়ন কৰি আপুনি—

• ছ'চিয়েল মিডিয়া ব্যৱহাৰৰ সৈতে জড়িত সম্ভাব্য সুৰক্ষাৰ বিষয় সমূহ চিনাক্ত কৰিব পাৰিব।

• ছ'চিয়েল মিডিয়া প্লেটফৰ্মসমূহত গোপনীয়তা ছেটিংছৰ কাৰ্যকাৰিতা মূল্যায়ন কৰিব পাৰিব।

• ছ'চিয়েল মিডিয়া ব্যৱহাৰ কৰোতে ব্যক্তিগত তথ্য সুৰক্ষিত কৰি ৰাখিবলৈ কৌশল বিকাশ কৰিব পাৰিব।

• ব্যক্তিগত আৰু বৃত্তিমূলক সুনামৰ ওপৰত ছ'চিয়েল মিডিয়াৰ প্ৰভাৱ বিশ্লেষণ কৰিবলৈ শিকিব।

• নিৰাপত্তা ভংগ বা ছ'চিয়েল মিডিয়া একাউণ্টত অকৰ্তৃত্বশীল প্ৰৱেশৰ প্ৰতি সঁহাৰি জনাবলৈ পৰিকল্পনা তৈয়াৰ কৰিব পাৰিব।

৮.২ পৰিচয়

ছ'চিয়েল মিডিয়া আমাৰ জীৱনৰ এক অবিচ্ছেদ্য অংশ হৈ পৰিছে, এই মিডিয়াৰ জৰিয়তে কোটি কোটি লোকে বিভিন্ন প্লেটফৰ্ম ব্যৱহাৰ কৰি সংযোগ স্থাপন, তথ্যৰ ভাগ-বতৰা, আৰু নিজকে প্ৰকাশ কৰি আহিছে। ছ'চিয়েল মিডিয়াৰ বহু সুবিধা আছে যদিও ইয়াৰ নিৰাপত্তাজনিত বিপদো আছে, যাৰ বিষয়ে এই মিডিয়া ব্যৱহাৰকাৰীসকলে সচেতন হ'ব লাগিব। চাইবাৰ গুণ্ডাগিৰি আৰু অনলাইন হাৰাশাস্তিৰ পৰা আৰম্ভ কৰি তথ্য চুৰি আৰু

পৰিচয় চুৰিলৈকে ছ'চিয়েল মিডিয়াত নিৰাপত্তাজনিত সমস্যাই গুৰুতৰ সমস্যাৰ সৃষ্টি কৰিব পাৰে। ছ'চিয়েল মিডিয়া প্লেটফৰ্মত ব্যৱহাৰকাৰীসকলে নিজৰ গোপনীয়তা আৰু সুৰক্ষা সুৰক্ষিত কৰাৰ বাবে সক্রিয় ব্যৱস্থা গ্রহণ কৰাটো অতি প্রয়োজনীয়।
এই অধ্যায়টোত, প্রথমে আমি ছ'চিয়েল মিডিয়া সুৰক্ষাৰ সৈতে জড়িত সমস্যাসমূহ আলোচনা কৰিম। ইয়াৰ উপৰিও আমি চৰকাৰী নিয়মাৱলী আৰু আপত্তিজনক বিষয়সমূহ চিহ্নিত কৰাৰ বিষয়েও আলোচনা কৰিম। শেষত আমি ছ'চিয়েল মিডিয়াৰ সর্বোত্তম অনুশীলনসমূহৰ বিষয়ে শিকিম আৰু কেইটামান কেছ ষ্টাডি বুজিবলৈ চেষ্টা কৰিম।

৮.৩ ছ'চিয়েল মিডিয়া সুৰক্ষাৰ সমস্যাসমূহ

১) গোপনীয়তা: ছ'চিয়েল মিডিয়াৰ সুৰক্ষাৰ এটা ডাঙৰ সমস্যা হ'ল তথ্যৰ গোপনীয়তা। বহুতো ছ'চিয়েল মিডিয়া প্লেটফৰ্মে ব্যৱহাৰকাৰীৰ ব্যক্তিগত তথ্য সংগ্রহ কৰে, যিবোৰৰ লক্ষ্য বিজ্ঞাপন আৰু অন্যান্য উদ্দেশ্যত ব্যৱহাৰ কৰা। এই মিডিয়া ব্যৱহাৰকাৰীসকলে তেওঁলোকৰ তথ্যসমূহ কেনেকৈ সংগ্রহ আৰু ব্যৱহাৰ কৰা হৈছে সেই বিষয়ে সচেতন নহ'বও পাৰে, আৰু তেওঁলোকৰ ব্যক্তিগত তথ্য চুৰি বা অপব্যৱহাৰৰ বাবে ব্যৱহাৰ হ'ব পাৰে।

২) চাইবাৰ বুলিং: ছ'চিয়েল মিডিয়া ছিকিউৰিটিৰ আন এটা সমস্যা হ'ল চাইবাৰ বুলিং। ছ'চিয়েল মিডিয়াই ব্যক্তিসকলে অনলাইনত আনক হাৰাশাস্তি, ভয় বা ভাবুকি দিয়াৰ এক মঞ্চ প্রদান কৰে, প্রায়ে বেনামীভাৱে। চাইবাৰ বুলিঙে ইয়াৰ বলি হোৱা লোকসকলৰ বাবে ভয়াৱহ পৰিণতিৰ সৃষ্টি কৰিব পাৰে, য'ত হতাশা, উদ্বেগ, আনকি আত্মহত্যাও হ'ব পাৰে।

৩) পৰিচয় চুৰি: ছ'চিয়েল মিডিয়া প্লেটফৰ্মত ব্যৱহাৰকাৰীয়ে প্রায়ে ব্যক্তিগত তথ্য, যেনে তেওঁলোকৰ নাম, ইমেইল ঠিকনা, জন্ম তাৰিখ আদি দিব লাগে। এই তথ্য চাইবাৰ অপৰাধীয়ে সংগ্রহ কৰি ব্যৱহাৰকাৰীৰ পৰিচয় চুৰি কৰি জালিয়াতি কৰিব পাৰে।

৪) মেলৱেৰ: ছ'চিয়েল মিডিয়া প্লেটফৰ্মতো ব্যৱহাৰকাৰীসকল মেলৱেৰৰ আক্রমণৰ সন্মুখীন হ'বলগীয়া হয়। চাইবাৰ অপৰাধীয়ে ছ'চিয়েল মিডিয়া ব্যৱহাৰ কৰি ভুৱা লিংক আৰু ডাউনলোডৰ জৰিয়তে মেলৱেৰ বিয়পাব পাৰে, যাৰ ফলত ব্যৱহাৰকাৰীৰ ডিভাইচৰ সুৰক্ষাত সমস্যা হ'ব পাৰে।

৫) ভুৱা একাউণ্টঃ ছ'চিয়েল মিডিয়া প্লেটফৰ্মতো ভুৱা একাউণ্টৰ সন্মুখীন হ'বলগীয়া হয়। এই একাউণ্টসমূহৰ সহায়ত ভুল তথ্য, অপপ্রচাৰ আৰু অন্যান্য ধৰণৰ ক্ষতিকাৰক বিষয়বস্তু বিয়পাই দিব পাৰি।

এই সমস্যাসমূহৰ সমাধানৰ বাবে ছ'চিয়েল মিডিয়া প্লেটফর্মসমূহে দুটা কাৰক প্রমাণীকৰণ, গোপনীয়তা ছেটিংছ, আৰু বিষয়বস্তুৰ মডাৰেচনৰ দৰে সুৰক্ষা ব্যৱস্থা ৰূপায়ণ কৰিছে। কিন্তু ব্যৱহাৰকাৰীসকলে নিজৰ গোপনীয়তা আৰু সুৰক্ষা সুৰক্ষিত কৰাৰ বাবেও পদক্ষেপ ল'ব লাগে, যেনে শক্তিশালী পাছৱর্ড ব্যৱহাৰ কৰা, স্পর্শকাতৰ বিষয়বোৰ অনলাইনত ভাগ-বতৰা কৰাটো এৰাই চলা, আৰু অচিনাকি মানুহৰ পৰা বন্ধুত্বৰ অনুৰোধ গ্রহণ কৰাৰ ক্ষেত্রত সাৱধান হোৱা।

৮.৪ আপত্তিজনক বিষয়বস্তু সম্পর্কে জাননী দিয়া আৰু তথ্য চিহ্নিত কৰা

ছ'চিয়েল মিডিয়া ব্যৱহাৰকাৰীসকলে অনলাইন মাধ্যমত নিজকে সুৰক্ষিত আৰু অন্তর্ভুক্তিমূলক কৰি ৰাখিবলৈ আপত্তিজনক সামগ্রীসমূহৰ বিষয়ে জাননী দিয়া (ৰিপর্টিং) আৰু চিহ্নিত কৰা (ফ্লেগিং) কৰিব পাৰে। আপত্তিজনক সামগ্রীৰ বিভিন্ন ৰূপ থাকিব পাৰে, যেনে—হেট স্পীচ (ঘৃণামূলক ভাষণ), চাইবাৰ বুলিং আৰু গ্রাফিক বা হিংসাত্মক সামগ্রী। আপত্তিজনক সামগ্রী ৰিপর্ট বা ফ্লেগ কৰোতে বিবেচনা কৰিবলগীয়া কেইটামান মূল বিষয় তলত দিয়া হ'ল:

১. প্লেটফর্মৰ নীতিৰ বিষয়ে জ্ঞান লাভ কৰক:

ছ'চিয়েল মিডিয়া প্লেটফর্মসমূহৰ আপত্তিজনক বা অনুপযুক্ত সামগ্রীৰ বাবে ভিন্ন নীতি আৰু নির্দেশনা থাকে। সামগ্রী ৰিপর্ট বা ফ্লেগ কৰাৰ আগতে প্লেটফর্মটোৰ নীতি আৰু নির্দেশনাৰ সৈতে পৰিচিত হ'বলৈ চেষ্টা কৰক।

২. ততালিকে ৰিপর্ট কৰক:

আপত্তিজনক সামগ্রীৰ সন্মুখীন হ'লে ইয়াক সোনকালে ৰিপর্ট কৰাটো গুৰুত্বপূর্ণ। সামগ্রী ৰিপর্ট বা ফ্লেগ কৰিলে অন্যান্য ব্যক্তিক ক্ষতিকাৰক বা আপত্তিজনক সামগ্রীৰ পৰা ৰক্ষা কৰাত সহায় হয়।

৩. নির্দিষ্ট বিৱৰণ দিয়ক:

সামগ্রী ৰিপর্ট বা ফ্লেগ কৰোতে যিমান পাৰি সিমান নির্দিষ্ট বিৱৰণ দিয়ক, যেনে—সামগ্রীটোৰ অৱস্থান (যেনে—ইউআৰএল বা পোষ্ট আইডি), সামগ্রীৰ প্রকাৰ, আৰু ৰিপর্ট কৰাৰ কাৰণ।

৪. প্রতিহিংসামূলক আচৰণৰ পৰা বিৰত থাকক:

আপত্তিজনক সামগ্ৰীৰ সন্মুখীন হ'লে প্ৰতিহিংসামূলক আচৰণৰ পৰা বিৰত থাকিবলৈ চেষ্টা কৰক। আপত্তিজনক সামগ্ৰী বা ব্যৱহাৰকাৰীৰ সৈতে জড়িত হ'লে পৰিস্থিতি বেছি বেয়া হ'ব পাৰে আৰু অধিক ক্ষতি হ'ব পাৰে।

৫. সীমাবদ্ধতাসমূহ বুজি লওক:

যদিও আপত্তিজনক সামগ্ৰী ৰিপৰ্ট বা ফ্লেগ কৰাটো অনলাইন স্থানসমূহ সুৰক্ষিত ৰাখিবলৈ এক কাৰ্যকৰী উপায়, কিন্তু ইয়াৰ কিছুমান সীমাবদ্ধতা আছে বুলি বুজি ল'ব লাগে। ছ'চিয়েল মিডিয়া প্লেটফৰ্মসমূহে সদায় ৰিপৰ্ট কৰা সামগ্ৰীৰ বাবে কাৰ্য্যব্যৱস্থা ল'ব নোৱাৰিব পাৰে, আৰু এই প্ৰক্ৰিয়াটোত সময় লাগিব পাৰে।

এই পদক্ষেপসমূহ অনুসৰণ কৰি আপুনি ছ'চিয়েল মিডিয়াক অধিক সুৰক্ষিত আৰু শিষ্টাচাৰসম্পন্ন কৰাত অৰিহণা যোগাব পাৰে।



অগ্ৰগতি নিৰীক্ষণ

১. ছ'চিয়েল মিডিয়া সুৰক্ষাৰ মুখ্য সমস্যাসমূহ কি কি?

২. ছ'চিয়েল মিডিয়াত আপত্তিজনক সামগ্ৰী ৰিপৰ্ট বা চিহ্নিত কৰোতে গুৰুত্ব দিবলগীয়া মূল কথাবোৰ কি কি?

আপত্তিজনক বিষয়বস্তুৰ প্ৰতিবেদন বা ফ্লেগ কৰি ছ'চিয়েল মিডিয়া ব্যৱহাৰকাৰীসকলে এটা সুৰক্ষিত আৰু অধিক অন্তর্ভুক্ত অনলাইন সম্প্ৰদায় সৃষ্টি কৰাত সহায় কৰিব পাৰে। কিন্তু মনত ৰখা ভাল যে ৰিপৰ্ট কৰা আৰু ফ্লেগিং কৰাটো সমাধানৰ এটা অংশহে মাত্ৰ। সন্মানজনক আৰু ইতিবাচক অনলাইন যোগাযোগৰ প্ৰসাৰত আমাৰ সকলোৰে ভূমিকা আছে।

৮.৫ আপত্তিজনক বিষয়বস্তু প্ৰকাশ নিয়ন্ত্ৰণ কৰা আইন

ছ'চিয়েল মিডিয়া প্লেটফৰ্মত আপত্তিজনক সামগ্ৰী প্ৰকাশ কৰাটো এক জটিল বিষয়, আৰু ইয়াৰ বাবে প্ৰযোজ্য আইন দেশ বা ক্ষেত্ৰভেদে বেলেগ হ'ব পাৰে। আপত্তিজনক সামগ্ৰীত ঘৃণামূলক বক্তব্য (hate speech), মানহানি কৰা বিষয়বস্তু (defamatory content), বা যৌন বিষয়ক স্পষ্ট সামগ্ৰী (sexually explicit content) আদি অন্তর্ভুক্ত হ'ব পাৰে। ছ'চিয়েল মিডিয়াত আপত্তিজনক সামগ্ৰী প্ৰকাশৰ সৈতে জড়িত আইনৰ বিষয়ে কেইটামান সাধাৰণ দিশ তলত উল্লেখ কৰা হ'ল:

স্থানীয় আইন বুজি লওক : ছ'চিয়েল মিডিয়াত আপত্তিজনক সামগ্ৰী প্ৰকাশৰ বাবে বিভিন্ন দেশৰ বিভিন্ন আইন আছে। আপোনাৰ দেশ বা অঞ্চলৰ আইনী বিষয়সমূহ বুজি লোৱাটো গুৰুত্বপূৰ্ণ।

আপত্তিজনক সামগ্ৰীৰ সংজ্ঞা জানি লোৱা : ছ'চিয়েল মিডিয়াত কি কি সামগ্ৰীক আপত্তিজনক বুলি গণ্য কৰা হয়, সেই সম্পৰ্কে আইনত বিভিন্ন সংজ্ঞা থাকিব পাৰে। অনিচ্ছাকৃতভাৱে আইন ভংগ কৰাৰ পৰা বাচি থাকিবলৈ এই সংজ্ঞাসমূহৰ জ্ঞান থকা প্ৰয়োজন।

পৰিণামৰ বিষয়ে সচেতন হৈ থাকক : ছ'চিয়েল মিডিয়াত আপত্তিজনক সামগ্ৰী প্ৰকাশ কৰাৰ বাবে জৰিমনা, আইনী কাৰ্য্য বা কাৰাবাসৰ দৰে গুৰুতৰ পৰিণাম ভুগিব লগা হ'ব পাৰে।

অন্যান্যৰ ওপৰত প্ৰভাৱৰ কথা বিবেচনা কৰিব : ছ'চিয়েল মিডিয়াত আপত্তিজনক সামগ্ৰী প্ৰকাশ কৰাটোৱে বিশেষকৈ দুৰ্বল বা পৰিয়াল সমূহৰ ওপৰত নেতিবাচক প্ৰভাৱ পেলাব পাৰে। সেয়েহে, কোনো সামগ্ৰী পোষ্ট কৰাৰ আগতে ইয়াৰ সম্ভাব্য প্ৰভাৱ সম্পৰ্কে চিন্তা কৰিব।

আইনী পৰামৰ্শ ল'ব : যদি ছ'চিয়েল মিডিয়াত কোনো বিশেষ সামগ্ৰী প্ৰকাশ কৰাটো আইনসংগত হয় নে নহয় সেই সম্পৰ্কে সন্দেহ থাকে, তেন্তে স্থানীয় আইনৰ বিষয়ে জানিবলৈ বিশেষজ্ঞৰ পৰা আইনী পৰামৰ্শ লোৱাটো উচিত।

সাধাৰণতে, ছ'চিয়েল মিডিয়াত প্ৰকাশ কৰা সামগ্ৰীৰ বিষয়ে সচেতন হ'ব লাগে আৰু নিশ্চিত কৰিব লাগে যে ইয়াৰ দ্বাৰা কোনো আইন ভংগ বা আনৰ ক্ষতি নহয়। আইনী প্ৰক্ৰিয়াৰ বিষয়ে জ্ঞান ৰখা আৰু প্ৰয়োজন হ'লে আইনী পৰামৰ্শ লোৱাৰ দ্বাৰা আপুনি এটা দায়বদ্ধ আৰু সন্মানজনক অনলাইন উপস্থিতি নিশ্চিত কৰিব পাৰে।

ইয়াৰ উপৰিও, ছ'চিয়েল মিডিয়া কোম্পানীসমূহৰো নিজা সম্প্ৰদায় নিৰ্দেশিকা আৰু নীতি বলৱৎ কৰাৰ দায়িত্ব আছে, যাতে তেওঁলোকৰ প্লেটফৰ্মত আপত্তিজনক সামগ্ৰী প্ৰকাশৰ পৰা বাধা দিব পাৰি।

আন্তর্জাতিক আইন (International Laws):

ছ'চিয়েল মিডিয়াত আপত্তিজনক সামগ্ৰী প্ৰকাশৰ ওপৰত নিয়ন্ত্ৰণ কৰা আন্তঃৰাষ্ট্ৰীয় আইনসমূহ জটিল হ'ব পাৰে আৰু দেশ বা বিচাৰ ক্ষমতাৰ ওপৰত নিৰ্ভৰ কৰি ভিন্ন হ'ব পাৰে। কিন্তু কিছুমান আন্তঃৰাষ্ট্ৰীয় চুক্তি আৰু কাঠামো আছে যিয়ে এই ক্ষেত্ৰত পথ প্ৰদৰ্শন কৰিব পাৰে। বিবেচনা কৰিবলগীয়া কিছুমান মূল কথা ইয়াত উল্লেখ কৰা হ'ল:

১) মানৱ অধিকাৰৰ সাৰ্বজনীন ঘোষণা: মানৱ অধিকাৰৰ সাৰ্বজনীন ঘোষণা (UDHR) হৈছে মৌলিক মানৱ অধিকাৰৰ ৰূপৰেখা দাঙি ধৰা এক বিশ্বব্যাপী চুক্তি। ইউডিএইচআৰৰ ১৯ নং অনুচ্ছেদে মত প্ৰকাশৰ স্বাধীনতাৰ অধিকাৰ সুৰক্ষিত কৰে, কিন্তু এইটোও স্বীকাৰ কৰে যে এই

অধিকাৰ ৰাষ্ট্ৰীয় নিৰাপত্তা, ৰাজহুৱা শৃংখলা বা আনৰ অধিকাৰ সুৰক্ষাৰ বাবে বাধাৰ আওতাত থাকিব পাৰে।

২) নাগৰিক আৰু ৰাজনৈতিক অধিকাৰৰ আন্তঃৰাষ্ট্ৰীয় চুক্তি: নাগৰিক আৰু ৰাজনৈতিক অধিকাৰৰ আন্তঃৰাষ্ট্ৰীয় চুক্তি (ICCPR) হৈছে এক পৰিসৰৰ নাগৰিক আৰু ৰাজনৈতিক অধিকাৰ সুৰক্ষিত কৰা এখন সন্ধি। আইচিচিপিআৰৰ ১৯ নং অনুচ্ছেদে মত প্ৰকাশৰ স্বাধীনতাৰ অধিকাৰ সুৰক্ষিত কৰে, কিন্তু এইটোও স্বীকাৰ কৰে যে এই অধিকাৰ ৰাষ্ট্ৰীয় নিৰাপত্তা, ৰাজহুৱা শৃংখলা বা আনৰ অধিকাৰ সুৰক্ষাৰ বাবে বাধাৰ আওতাত থাকিব পাৰে।

৩) সকলো ধৰণৰ বৰ্ণ বৈষম্য দূৰীকৰণৰ আন্তঃৰাষ্ট্ৰীয় সন্ধি: সকলো ধৰণৰ বৰ্ণ বৈষম্য দূৰীকৰণৰ আন্তঃৰাষ্ট্ৰীয় সন্ধি (ICERD) হৈছে বৰ্ণ বৈষম্য নিষিদ্ধ কৰা আৰু বৰ্ণ সমতাক প্ৰসাৰিত কৰা এখন সন্ধি। আইচিইআৰডিৰ ৪ নং অনুচ্ছেদত ৰাষ্ট্ৰসমূহে বৈষম্য, শত্ৰুতা বা হিংসাৰ উচটনি দিয়া ঘৃণামূলক ভাষণক অপৰাধমূলক বুলি গণ্য কৰিব লাগিব।

৪) ইউৰোপীয় মানৱ অধিকাৰ সন্ধি: ইউৰোপীয় মানৱ অধিকাৰ সন্ধি (ECHR) হৈছে ইউৰোপৰ এক পৰিসৰৰ মানৱ অধিকাৰ সুৰক্ষিত কৰা এখন সন্ধি। ইচিএইচআৰৰ ১০ নং অনুচ্ছেদে মত প্ৰকাশৰ স্বাধীনতাৰ অধিকাৰ সুৰক্ষিত কৰে, কিন্তু এইটোও স্বীকাৰ কৰে যে এই অধিকাৰ ৰাষ্ট্ৰীয় নিৰাপত্তা, জনসাধাৰণৰ সুৰক্ষা বা আনৰ অধিকাৰৰ সুৰক্ষাৰ বাবে বাধাৰ আওতাত থাকিব পাৰে।

৫) ছ'চিয়েল মিডিয়া প্লেটফৰ্মৰ সেৱাৰ চর্ত: ছ'চিয়েল মিডিয়া প্লেটফৰ্মৰ প্ৰায়ে নিজস্ব সেৱাৰ চর্ত থাকে যিয়ে গ্ৰহণযোগ্য ব্যৱহাৰৰ নীতিৰ ৰূপৰেখা দাঙি ধৰে আৰু আপত্তিজনক সামগ্ৰী প্ৰকাশ কৰাত নিষেধাজ্ঞা আৰোপ কৰে। এই চর্তসমূহ উলংঘাৰ ফলত বিষয়বস্তু আঁতৰোৱা হ'ব পাৰে বা আনকি একাউণ্টসমূহ নিলম্বন বা বন্ধ কৰা হ'ব পাৰে।

ছ'চিয়েল মিডিয়াত আপত্তিজনক সামগ্ৰী প্ৰকাশৰ ওপৰত নিয়ন্ত্ৰণ কৰা আইনসমূহ জটিল আৰু বিচাৰ ক্ষমতাৰ ওপৰত নির্ভৰ কৰি ভিন্ন হ'ব পাৰে যদিও এই আইনসমূহৰ বিষয়ে সচেতন হোৱাটো গুৰুত্বপূর্ণ আৰু আপোনাৰ অনলাইন উপস্থিতি যাতে দায়বদ্ধ আৰু সন্মানজনক হয়। আপুনি অনলাইনত প্ৰকাশ কৰা বিষয়বস্তুৰ প্ৰতি সচেতন হৈ আৰু আনৰ অধিকাৰ আৰু মর্যাদাক সন্মান কৰি, আপুনি এটা সুৰক্ষিত আৰু অধিক অন্তর্ভুক্ত অনলাইন সম্প্ৰদায় সৃষ্টি কৰাত সহায় কৰিব পাৰে।

ভাৰতীয় আইন (Indian Laws):

ছ'চিয়েল মিডিয়াত আপত্তিজনক সামগ্ৰী প্ৰকাশৰ ওপৰত নিয়ন্ত্ৰণ কৰা আন্তঃৰাষ্ট্ৰীয় আইনসমূহ জটিল হ'ব পাৰে আৰু দেশ বা বিচাৰ ক্ষমতাৰ ওপৰত নির্ভৰ কৰি ভিন্ন হ'ব পাৰে। কিন্তু

কিছুমান আন্তঃৰাষ্ট্ৰীয় চুক্তি আৰু কাঠামো আছে যিয়ে এই ক্ষেত্ৰত পথ প্ৰদৰ্শন কৰিব পাৰে। বিবেচনা কৰিবলগীয়া কিছুমান মূল কথা ইয়াত উল্লেখ কৰা হ'ল:

১) মানৱ অধিকাৰৰ সাৰ্বজনীন ঘোষণা: মানৱ অধিকাৰৰ সাৰ্বজনীন ঘোষণা (UDHR) হৈছে মৌলিক মানৱ অধিকাৰৰ ৰূপৰেখা দাঙি ধৰা এক বিশ্বব্যাপী চুক্তি। ইউডিএইচআৰৰ ১৯ নং অনুচ্ছেদে মত প্ৰকাশৰ স্বাধীনতাৰ অধিকাৰ সুৰক্ষিত কৰে, কিন্তু এইটোও স্বীকাৰ কৰে যে এই অধিকাৰ ৰাষ্ট্ৰীয় নিৰাপত্তা, ৰাজহুৱা শৃংখলা বা আনৰ অধিকাৰ সুৰক্ষাৰ বাবে বাধাৰ আওতাত থাকিব পাৰে।

২) নাগৰিক আৰু ৰাজনৈতিক অধিকাৰৰ আন্তঃৰাষ্ট্ৰীয় চুক্তি: নাগৰিক আৰু ৰাজনৈতিক অধিকাৰৰ আন্তঃৰাষ্ট্ৰীয় চুক্তি (ICCPR) হৈছে এক পৰিসৰৰ নাগৰিক আৰু ৰাজনৈতিক অধিকাৰ সুৰক্ষিত কৰা এখন সন্ধি। আইচিচিপিআৰৰ ১৯ নং অনুচ্ছেদে মত প্ৰকাশৰ স্বাধীনতাৰ অধিকাৰ সুৰক্ষিত কৰে, কিন্তু এইটোও স্বীকাৰ কৰে যে এই অধিকাৰ ৰাষ্ট্ৰীয় নিৰাপত্তা, ৰাজহুৱা শৃংখলা বা আনৰ অধিকাৰ সুৰক্ষাৰ বাবে বাধাৰ আওতাত থাকিব পাৰে।

৩) সকলো ধৰণৰ বৰ্ণ বৈষম্য দূৰীকৰণৰ আন্তঃৰাষ্ট্ৰীয় সন্ধি: সকলো ধৰণৰ বৰ্ণ বৈষম্য দূৰীকৰণৰ আন্তঃৰাষ্ট্ৰীয় সন্ধি (ICERD) হৈছে বৰ্ণ বৈষম্য নিষিদ্ধ কৰা আৰু বৰ্ণ সমতাক প্ৰসাৰিত কৰা এখন সন্ধি। আইচিইআৰডিৰ ৪ নং অনুচ্ছেদত ৰাষ্ট্ৰসমূহে বৈষম্য, শত্ৰুতা বা হিংসাৰ উচটনি দিয়া ঘৃণামূলক ভাষণক অপৰাধমূলক বুলি গণ্য কৰিব লাগিব।

৪) ইউৰোপীয় মানৱ অধিকাৰ সন্ধি: ইউৰোপীয় মানৱ অধিকাৰ সন্ধি (ECHR) হৈছে ইউৰোপৰ এক পৰিসৰৰ মানৱ অধিকাৰ সুৰক্ষিত কৰা এখন সন্ধি। ইচিএইচআৰৰ ১০ নং অনুচ্ছেদে মত প্ৰকাশৰ স্বাধীনতাৰ অধিকাৰ সুৰক্ষিত কৰে, কিন্তু এইটোও স্বীকাৰ কৰে যে এই অধিকাৰ ৰাষ্ট্ৰীয় নিৰাপত্তা, জনসাধাৰণৰ সুৰক্ষা বা আনৰ অধিকাৰৰ সুৰক্ষাৰ বাবে বাধাৰ আওতাত থাকিব পাৰে।

৫) ছ'চিয়েল মিডিয়া প্লেটফৰ্মৰ সেৱাৰ চর্ত: ছ'চিয়েল মিডিয়া প্লেটফৰ্মৰ প্ৰায়ে নিজস্ব সেৱাৰ চর্ত থাকে যিয়ে গ্ৰহণযোগ্য ব্যৱহাৰৰ নীতিৰ ৰূপৰেখা দাঙি ধৰে আৰু আপত্তিজনক সামগ্ৰী প্ৰকাশ কৰাত নিষেধাজ্ঞা আৰোপ কৰে। এই চর্তসমূহ উলংঘাৰ ফলত বিষয়বস্তু আঁতৰোৱা হ'ব পাৰে বা আনকি একাউণ্টসমূহ নিলম্বন বা বন্ধ কৰা হ'ব পাৰে।

ছ'চিয়েল মিডিয়াত আপত্তিজনক সামগ্ৰী প্ৰকাশৰ ওপৰত নিয়ন্ত্ৰণ কৰা আইনসমূহ জটিল আৰু বিচাৰ ক্ষমতাৰ ওপৰত নির্ভৰ কৰি ভিন্ন হ'ব পাৰে যদিও এই আইনসমূহৰ বিষয়ে সচেতন হোৱাটো গুৰুত্বপূৰ্ণ আৰু আপোনাৰ অনলাইন উপস্থিতি যাতে দায়বদ্ধ আৰু সন্মানজনক হয়। আপুনি অনলাইনত প্ৰকাশ কৰা বিষয়বস্তুৰ প্ৰতি সচেতন হৈ আৰু আনৰ

অধিকাৰ আৰু মর্যাদাক সন্মান কৰি, আপুনি এটা সুৰক্ষিত আৰু অধিক অন্তর্ভুক্ত অনলাইন সম্প্রদায় সৃষ্টি কৰাত সহায় কৰিব পাৰে।



অগ্রগতি নিৰীক্ষণ

৩. ছ'চিয়েল মিডিয়াত আপত্তিজনক সামগ্রী প্রকাশ নিয়ন্ত্রণ কৰা আইন সম্পর্কে বিবেচনা কৰিবলগীয়া সাধাৰণ দিশসমূহ কি কি ?

৪. ছ'চিয়েল মিডিয়াত আপত্তিজনক সামগ্রী প্রকাশ নিয়ন্ত্রণ কৰা আইনৰ ক্ষেত্রত মার্গদর্শন কৰা আন্তর্জাতিক চুক্তি আৰু কাঠামোবোৰ কি কি ?

৮.৭ ছ'চিয়েল মিডিয়াৰ ব্যৱহাৰৰ বাবে উত্তম পদ্ধতি

ছ'চিয়েল মিডিয়া আমাৰ দৈনন্দিন জীৱনৰ এক অবিচ্ছেদ্য অংগ হৈ পৰিছে, আৰু ইয়াক দায়িত্বশীল আৰু ফলপ্রসূভাৱে ব্যৱহাৰ কৰাটো গুৰুত্বপূর্ণ। ছ'চিয়েল মিডিয়া ব্যৱহাৰৰ বাবে কিছুমান উত্তম পদ্ধতি আগবঢ়োৱা হ'ল:

১) আপোনাৰ দর্শকৰ প্রতি সচেতন হওক: আপোনাৰ উদ্দেশ্যপ্রণোদিত দর্শক কোন সেইটো বিবেচনা কৰক আৰু সেই অনুসৰি আপোনাৰ বিষয়বস্তু সালসলনি কৰক। এজন দর্শকৰ বাবে যিটো উপযুক্ত হ'ব পাৰে, সেয়া আন এজনৰ বাবে উপযুক্ত নহ'বও পাৰে।

২) পোষ্ট কৰাৰ আগতে চিন্তা কৰক: পোষ্ট কৰাৰ আগতে আপোনাৰ বিষয়বস্তুৰ সম্ভাব্য প্রভাৱৰ বিষয়ে বিবেচনা কৰিবলৈ অলপ সময় উলিয়াওক। নিজকে সুধিব যে ই আনৰ বাবে আপত্তিজনক বা ক্ষতিকাৰক হ'ব পাৰে নেকি, বা ইয়াৰ কোনো ধৰণে ভুল ব্যাখ্যা হ'ব পাৰে নেকি ?

৩) সন্মান প্রদর্শন কৰক: ছ'চিয়েল মিডিয়াত আনৰ লগত মতানৈক্য থাকিলেও আনৰ লগত সন্মান আৰু দয়ালু ব্যৱহাৰ কৰক। তর্ক বা নেতিবাচক পাৰস্পৰিক ক্রিয়া-কলাপত লিপ্ত হোৱাটো এৰক যিয়ে তীব্রতৰ হ'ব পাৰে।

৪) আপোনাৰ গোপনীয়তা সুৰক্ষিত কৰক: আপুনি ছ'চিয়েল মিডিয়াত শ্বেয়াৰ কৰা ব্যক্তিগত তথ্যৰ প্রতি সচেতন হওক, আৰু আপোনাৰ পোষ্ট আৰু ব্যক্তিগত বিৱৰণ কোনে চাব পাৰে সীমিত কৰিবলৈ আপোনাৰ গোপনীয়তা ছেটিংছ সামঞ্জস্য কৰক।

৫) নতুন ধ্যান-ধাৰণাৰ প্ৰতি সজাগ হৈ থাকক: ছ'চিয়েল মিডিয়াৰ শেহতীয়া ট্ৰেণ্ড আৰু আপডেটৰ সৈতে আপডেট হৈ থাকক, আৰু প্লেটফৰ্মৰ নীতি আৰু নিৰ্দেশনাত হোৱা যিকোনো পৰিৱৰ্তনৰ বিষয়ে সচেতন হওক।

৬) য'ত স্বীকৃতি দিব লাগে তাতেই দিয়ক: যদি আপুনি আনৰ দ্বাৰা সৃষ্টি কৰা বিষয়বস্তু শ্বেয়াৰ কৰে, তেন্তে য'ত সেই সম্পৰ্কে স্বীকৃতি দিব লাগে তাতেই স্বীকৃতি দিয়াটো নিশ্চিত কৰক। ইয়াৰ ভিতৰত সৃষ্টিকৰ্তাক টেগ কৰা বা বিষয়বস্তুৰ উৎসৰ উদ্ধৃতি দিয়াও থাকিব পাৰে।

৭) ইতিবাচক উদ্দেশ্যত ছ'চিয়েল মিডিয়া ব্যৱহাৰ কৰকঃ ইতিবাচক বাৰ্তা ভাগ-বতৰা আৰু সামাজিক পৰিৱৰ্তনক প্ৰসাৰিত কৰাৰ বাবে ছ'চিয়েল মিডিয়া এক শক্তিশালী আহিলা হ'ব পাৰে। গুৰুত্বপূৰ্ণ বিষয়সমূহৰ বিষয়ে সজাগতা সৃষ্টি কৰিবলৈ বা দয়া আৰু ইতিবাচকতা বিয়পাবলৈ আপোনাৰ মঞ্চ ব্যৱহাৰ কৰাৰ কথা চিন্তা কৰক।

এই উত্তম পদ্ধতিসমূহ অনুসৰণ কৰি আপুনি আপোনাৰ ছ'চিয়েল মিডিয়াৰ ব্যৱহাৰ যাতে দায়িত্বশীল, ফলপ্ৰসূ আৰু সন্মানজনক হোৱাটো নিশ্চিত কৰাত সহায় কৰিব পাৰে। ইয়াৰ উপৰিও ই এটা ইতিবাচক আৰু সহায়ক অনলাইন সম্প্ৰদায় গঢ়ি তোলাত সহায় কৰিব পাৰে।

৮.৮ ক্ষেত্ৰ অধ্যয়ন

সমগ্ৰ বিশ্বতে ছ'চিয়েল মিডিয়াৰ সুৰক্ষাৰ সমস্যাৰ অসংখ্য দৃষ্টান্ত দেখা গৈছে। কেইটামান উদাহৰণ তলত দিয়া হৈছে।

সমগ্ৰ বিশ্বতে ছ'চিয়েল মিডিয়াৰ সুৰক্ষাৰ সমস্যাৰ অসংখ্য দৃষ্টান্ত দেখা গৈছে। কেইটামান উদাহৰণ তলত দিয়া হৈছে।

১) কেম্ব্ৰিজ এনালিটিকা কেলেংকাৰী হৈছে ছ'চিয়েল মিডিয়া প্লেটফৰ্মৰ সৈতে জড়িত নিৰাপত্তাজনিত বিষয়সমূহৰ ওপৰত আলোকপাত কৰা এটা সুপৰিচিত গোচৰ। কেম্ব্ৰিজ এনালিটিকা আছিল এক ৰাজনৈতিক পৰামৰ্শদাতা প্ৰতিষ্ঠান যিয়ে লাখ লাখ ফেচবুক ব্যৱহাৰকাৰীৰ পৰা তেওঁলোকৰ অজ্ঞাতে বা সন্মতি অবিহনে তথ্য লাভ কৰিছিল। এই তথ্যসমূহ ব্যৱহাৰ কৰি ২০১৬ চনৰ আমেৰিকাৰ ৰাষ্ট্ৰপতি নিৰ্বাচনৰ প্ৰচাৰৰ সময়ত লক্ষ্য নিৰ্ধাৰণ কৰি ৰাজনৈতিক বিজ্ঞাপন সৃষ্টি কৰিছিল প্ৰতিষ্ঠানটোৱে। এই কেলেংকাৰী আৰম্ভ হৈছিল যেতিয়া কেম্ব্ৰিজ বিশ্ববিদ্যালয়ৰ এজন অধ্যাপক আলেকজেণ্ডাৰ কোগানে এটা ব্যক্তিত্ব কুইজ এপ তৈয়াৰ কৰিছিল যিটো প্ৰায় ২ লাখ ৭০ হাজাৰ ফেচবুক ব্যৱহাৰকাৰীয়ে ব্যৱহাৰ কৰিছিল। অৱশ্যে এপটোৱে ব্যৱহাৰকাৰীৰ ফেচবুক বন্ধুৰ পৰাও তথ্য সংগ্ৰহ কৰিছিল, যাৰ ফলত শেষত লাখ লাখ ব্যৱহাৰকাৰীৰ পৰা তেওঁলোকৰ সন্মতি অবিহনে তথ্য সংগ্ৰহ কৰা হৈছিল। ইয়াৰ পিছত

এই তথ্যসমূহ কেম্ব্রিজ এনালিটিকাক বিক্রী কৰা হয়, যিয়ে ইয়াক ব্যৱহাৰ কৰি ট্রাম্পৰ প্রচাৰ অভিযানৰ বাবে লক্ষ্য নির্ধাৰণ কৰি ৰাজনৈতিক বিজ্ঞাপন সৃষ্টি কৰে। এই কেলেংকাৰীয়ে ছ'চিয়েল মিডিয়া প্লেটফর্মত ব্যক্তিগত তথ্যৰ সুৰক্ষাৰ লগতে ৰাজনৈতিক প্রচাৰত লক্ষ্য বিজ্ঞাপনৰ ব্যৱহাৰক লৈ উদ্বেগ প্রকাশ কৰে। এই কেলেংকাৰীত ফেচবুকে লোৱা ভূমিকাৰ বাবে যথেষ্ট সমালোচনাৰ সন্মুখীন হ'বলগীয়া হৈছিল, য'ত অভিযোগ আছিল যে ফেচবুকে ব্যৱহাৰকাৰীৰ তথ্য সঠিকভাৱে সুৰক্ষিত কৰাত ব্যর্থ হোৱাৰ লগতে নিজৰ প্লেটফর্মৰ অপব্যৱহাৰ ৰোধ কৰিবলৈ পর্যাপ্ত কাম কৰা নাই। কেম্ব্রিজ এনালিটিকা কেলেংকাৰীৰ ফলত ফেচবুক আৰু অন্যান্য ছ'চিয়েল মিডিয়া প্লেটফর্মে ব্যৱহাৰকাৰীৰ তথ্য চম্ভালাৰ পদ্ধতিত কেইবাটাও পৰিৱর্তন ঘটিছিল। উদাহৰণস্বৰূপে ফেচবুকে তৃতীয় পক্ষৰ এপসমূহত নতুন গোপনীয়তা ছেটিংছ আৰু নিষেধাজ্ঞা প্রৱর্তন কৰিছিল। এই কেলেংকাৰীয়ে ছ'চিয়েল মিডিয়া প্লেটফর্মত ব্যক্তিগত তথ্য ব্যৱহাৰৰ ক্ষেত্রত স্বচ্ছতা আৰু জবাবদিহিতা বৃদ্ধিৰ প্রয়োজনীয়তাৰ ওপৰতো আলোকপাত কৰে। সামগ্রিকভাৱে কেম্ব্রিজ এনালিটিকা কেলেংকাৰীয়ে ছ'চিয়েল মিডিয়া প্লেটফর্মৰ সৈতে জড়িত নিৰাপত্তাজনিত বিষয়সমূহৰ ওপৰত এক গুৰুত্বপূর্ণ কেছ ষ্টডি হিচাপে কাম কৰে। ইয়াত ব্যৱহাৰকাৰীসকলে তেওঁলোকৰ ব্যক্তিগত তথ্য কেনেকৈ ব্যৱহাৰ কৰা হৈছে সেই বিষয়ে সচেতন হোৱাৰ প্রয়োজনীয়তাৰ ওপৰত আলোকপাত কৰা হৈছে, লগতে ছ'চিয়েল মিডিয়া কোম্পানীসমূহে ব্যৱহাৰকাৰীৰ তথ্য সুৰক্ষিত কৰা আৰু ইয়াৰ অপব্যৱহাৰ ৰোধ কৰাৰ দায়িত্ব লোৱাৰ প্রয়োজনীয়তাৰ ওপৰত আলোকপাত কৰা হৈছে।

২) শেহতীয়াকৈ ভাৰতত ছ'চিয়েল মিডিয়াত নিৰাপত্তাজনিত সমস্যাৰ সৈতে জড়িত এটা গোচৰ হৈছে ফেচবুকৰ মালিকানাধীন মেছেজিং এপ হোৱাটছএপৰ পৰা লাখ লাখ ভাৰতীয় ব্যৱহাৰকাৰীৰ ব্যক্তিগত তথ্য ফাদিল হোৱা। ২০২০ চনৰ অক্টোবৰ মাহত প্রকাশ পাইছিল যে বিশ্বজুৰি ৫৩.৩ কোটিতকৈ অধিক ফেচবুক ব্যৱহাৰকাৰীক প্রভাৱিত কৰা বৃহৎ ডাটা ভংগৰ অংশ হিচাপে ফাদিল হোৱা তথ্যৰ ভিতৰত প্রায় ১৩ লাখ ভাৰতীয় ব্যৱহাৰকাৰীৰ ব্যক্তিগত তথ্যও আছে। এই ফাদিলটোৱে ছ'চিয়েল মিডিয়া প্লেটফর্মত ব্যক্তিগত তথ্যৰ নিৰাপত্তা, লগতে ব্যৱহাৰকাৰীৰ গোপনীয়তা ৰক্ষাৰ ক্ষেত্রত এই প্লেটফর্মসমূহৰ ভূমিকাক লৈ উদ্বেগ প্রকাশ কৰে।ডাটা ভংগৰ প্রতি সঁহাৰি জনাই ভাৰত চৰকাৰে হোৱাটছএপক এই ভংগৰ প্রকৃতি বুজাবলৈ আৰু ব্যৱহাৰকাৰীৰ তথ্যৰ গোপনীয়তা আৰু সুৰক্ষা নিশ্চিত কৰাৰ বাবে উপযুক্ত পদক্ষেপ ল'বলৈ কয়। চৰকাৰে হোৱাটছএপৰ মূল কোম্পানী ফেচবুকলৈও এক জাননী জাৰি কৰি এই ভংগৰ তথ্য আৰু ভৱিষ্যতে এনেধৰণৰ ঘটনা ৰোধৰ বাবে গ্রহণ কৰা ব্যৱস্থাৰ তথ্য বিচাৰিছে। এই ঘটনাই ছ'চিয়েল মিডিয়া প্লেটফর্মসমূহে ব্যৱহাৰকাৰীৰ ব্যক্তিগত তথ্য সুৰক্ষিত কৰাৰ লগতে তেওঁলোকৰ গোপনীয়তা আৰু সুৰক্ষা নিশ্চিত কৰাৰ বাবে অধিক শক্তিশালী ব্যৱস্থা গ্রহণ কৰাৰ প্রয়োজনীয়তাক উজ্জ্বল কৰি তুলিছে। ইয়াৰ উপৰিও ই ছ'চিয়েল মিডিয়া কোম্পানীসমূহক

যিকোনো নিৰাপত্তা উলংঘা বা ব্যৱহাৰকাৰীৰ অধিকাৰ উলংঘাৰ বাবে জবাবদিহি কৰিবলৈ চৰকাৰী তদাৰকী আৰু নিয়ন্ত্রণৰ গুৰুত্বৰ ওপৰত আলোকপাত কৰে।

৩) অসমৰ ছ'চিয়েল মিডিয়াত নিৰাপত্তাজনিত সমস্যাৰ সৈতে জড়িত এটা কেছ ষ্টডি হৈছে ২০১৮ চনত ৰাজ্যত শিশু অপহৰণকাৰীক লৈ ছ'চিয়েল মিডিয়া প্লেটফর্মত উৰাবাতৰি প্রচাৰ হোৱা ঘটনা। এই উৰাবাতৰিয়ে ব্যাপক আতংকৰ সৃষ্টি কৰাৰ লগতে শিশু অপহৰণকাৰী বুলি বিশ্বাস কৰা কেইবাজনো নিৰীহ লোকক লিঞ্চিং কৰে। ২০১৮ চনৰ মে' মাহৰ শেষৰ ফালে ফেচবুক, হোৱাটছএপকে ধৰি ছ'চিয়েল মিডিয়া প্লেটফর্মত এই উৰাবাতৰি প্রচাৰ আৰম্ভ হৈছিল।ৰাজ্যত শিশু অপহৰণকাৰীৰ এটা দলে সক্রিয় হৈ থকা আৰু অংগ সংগ্রহৰ বাবে শিশু অপহৰণ কৰা বুলি দাবী কৰা হৈছিল। এই উৰাবাতৰি ৰাজ্যজুৰি দ্রুতগতিত বিয়পি পৰিল, আৰু মানুহে ইয়াক ছ'চিয়েল মিডিয়াত ব্যাপকভাৱে শ্বেয়াৰ কৰিবলৈ ধৰিলে। আতংক আৰু ভয় বাঢ়ি অহাৰ লগে লগে গোট গঠন কৰি শিশু অপহৰণকাৰী বুলি সন্দেহ কৰা যিকোনো ব্যক্তিক আক্রমণ কৰিবলৈ ধৰিলে। গাড়ীৰে গৈ থকা দুজন লোককে ধৰি কেইবাজনো নিৰীহ লোকক প্রহাৰ কৰি হত্যা কৰা হয় আৰু তেওঁলোকক শিশু অপহৰণকাৰী বুলি ভুল কৰা হয়। ৰাজ্য চৰকাৰ আৰু আৰক্ষী কর্তৃপক্ষই ক্ষিপ্রতাৰে হিংসাত্মক ঘটনা দমন কৰাৰ লগতে উৰাবাতৰি দূৰ কৰিবলৈ আগবাঢ়িল। ছ'চিয়েল মিডিয়াত সতর্কবাণী জাৰি কৰি ভুৱা উৰাবাতৰি বিশ্বাস নকৰিবলৈ বা প্রচাৰ নকৰিবলৈ আহ্বান জনায়। লগতে উৰাবাতৰি প্রচাৰ আৰু হিংসাৰ উচটনি দিয়াত জড়িত কেইবাজনো লোকক গ্রেপ্তাৰ কৰে। এই ঘটনাই ছ'চিয়েল মিডিয়াৰ সম্ভাব্য বিপদ আৰু দায়িত্বশীল ব্যৱহাৰৰ প্রয়োজনীয়তাক উজ্জ্বল কৰি তুলিছে। ছ'চিয়েল মিডিয়া প্লেটফর্মত ভুৱা তথ্য দ্রুতগতিত বিয়পিব পাৰে, যাৰ ফলত আতংক আৰু হিংসাৰ সৃষ্টি হ'ব পাৰে। ব্যক্তি আৰু কর্তৃপক্ষই ভুৱা তথ্য বিয়পি পৰাৰ সম্ভাৱনাৰ বিষয়ে সচেতন হোৱাটো গুৰুত্বপূর্ণ আৰু ইয়াক প্রতিৰোধৰ বাবে পদক্ষেপ লোৱাটো গুৰুত্বপূর্ণ। এই কাণ্ডই ছ'চিয়েল মিডিয়া কোম্পানীসমূহে নিজৰ প্লেটফর্মত শ্বেয়াৰ কৰা কন্টেনটৰ দায়িত্ব লোৱাৰ প্রয়োজনীয়তাকো উজ্জ্বল কৰি তুলিছে। কিছুমান কোম্পানীয়ে নিজৰ প্লেটফর্মত ভুৱা তথ্য আৰু ঘৃণামূলক ভাষণৰ বিৰুদ্ধে যুঁজিবলৈ পদক্ষেপ গ্রহণ কৰিছে যদিও ছ'চিয়েল মিডিয়া যাতে সকলো ব্যৱহাৰকাৰীৰ বাবে এক নিৰাপদ আৰু দায়িত্বশীল স্থান হিচাপে পৰিগণিত হয় তাৰ বাবে অধিক কাম কৰাৰ প্রয়োজন।



আপোনাৰ অগ্রগতি পৰীক্ষা কৰক

১) ছ'চিয়েল মিডিয়াত আপোনাৰ দর্শক অনুসৰি নিজৰ কন্টেনট এডজাষ্ট কৰাৰ গুৰুত্ব কি?

২) ছ'চিয়েল মিডিয়াত শ্বেয়াৰ কৰা ব্যক্তিগত তথ্যৰ প্রতি সচেতন হোৱাটো কিয় গুৰুত্বপূর্ণ?

কার্যকলাপ

৩) ছ'চিয়েল মিডিয়াৰ সুৰক্ষাৰ সৈতে জড়িত কোনো বিষয়ৰ সৈতে জড়িত গোচৰ এটা বিচাৰি উলিয়াওক আৰু তাৰ বিষয়ে কিবা এটা লিখি থওক।



৮.৯ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ

• ছ'চিয়েল মিডিয়া সুৰক্ষাৰ বিষয়সমূহৰ ভিতৰত গোপনীয়তা, চাইবাৰ বুলিং, পৰিচয় চুৰি, মেলৱেৰ, আৰু ভুৱা একাউণ্ট আদি অন্তর্ভুক্ত।

• ছ'চিয়েল মিডিয়া প্লেটফর্ম আৰু ব্যৱহাৰকাৰী উভয়েই এই সমস্যাসমূহৰ সমাধানৰ বাবে পদক্ষেপ গ্রহণ কৰিব লাগে, য'ত সুৰক্ষা ব্যৱস্থা ৰূপায়ণ আৰু ছ'চিয়েল মিডিয়াৰ দায়িত্বশীল ব্যৱহাৰৰ প্রচাৰকে ধৰি।

• প্লেটফর্মৰ নীতিসমূহ বুজি থকাৰ সময়তে আপত্তিজনক বিষয়বস্তু তৎকালীনভাৱে আৰু নির্দিষ্ট বিৱৰণৰ সৈতে প্রতিবেদন কৰাটো অনলাইন স্থানসমূহ সুৰক্ষিত আৰু অন্তর্ভুক্ত ৰখাৰ এটা ফলপ্রসূ উপায়।

• প্রতিশোধমূলক আচৰণ এৰাই চলা আৰু প্রতিবেদন আৰু ফ্লেগিং প্রক্রিয়াৰ সীমাবদ্ধতাসমূহ বুজি পোৱাটো গুৰুত্বপূর্ণ, লগতে সন্মানজনক আৰু ইতিবাচক অনলাইন পাৰস্পৰিক ক্রিয়া-কলাপক প্রসাৰিত কৰাটোও গুৰুত্বপূর্ণ।

• ছ'চিয়েল মিডিয়াত আপত্তিজনক সামগ্রী প্রকাশৰ গুৰুতৰ পৰিণতি হ'ব পাৰে আৰু এই ক্ষেত্রখন নিয়ন্ত্রণ কৰা আইনসমূহ দেশ বা বিচাৰ ক্ষমতাৰ ওপৰত নির্ভৰ কৰি ভিন্ন হ'ব পাৰে।

• অনিচ্ছাকৃত উলংঘাৰ পৰা হাত সাৰিবলৈ আপোনাৰ দেশ বা অধিকাৰক্ষেত্রত আপত্তিজনক সামগ্রীৰ আইনী কাঠামো আৰু সংজ্ঞা বুজাটো গুৰুত্বপূর্ণ।

• বিষয়বস্তু প্রকাশ কৰাৰ আগতে আনৰ ওপৰত আপত্তিজনক সামগ্রীৰ প্রভাৱ, বিশেষকৈ দুর্বল বা প্রান্তীয় সম্প্রদায়ৰ ওপৰত বিবেচনা কৰিব লাগে।

• কিছুমান বিষয়বস্তু প্রকাশৰ বৈধতাৰ বিষয়ে নিশ্চিত নহ'লে আইনী পৰামর্শ লোৱাটোৱে স্থানীয় আইনসমূহ মানি চলাটো নিশ্চিত কৰাত সহায় কৰিব পাৰে।

• ছ'চিয়েল মিডিয়া কোম্পানীসমূহেও নিজৰ প্লেটফর্মত আপত্তিজনক সামগ্রী প্রকাশ ৰোধ কৰিবলৈ নিজৰ সম্প্রদায়ৰ নির্দেশনা আৰু নীতি বলবৎ কৰাৰ দায়িত্ব লয়।

• ছ'চিয়েল মিডিয়া আমাৰ দৈনন্দিন জীৱনৰ এক অবিচ্ছেদ্য অংগ হৈ পৰিছে, আৰু ইয়াক দায়িত্বশীল আৰু ফলপ্রসূভাৱে ব্যৱহাৰ কৰাটো গুৰুত্বপূর্ণ।

• ছ'চিয়েল মিডিয়া ব্যৱহাৰৰ বাবে উত্তম পদ্ধতিসমূহৰ ভিতৰত আছে আপোনাৰ দৰ্শকৰ প্ৰতি সচেতন হোৱা, পোষ্ট কৰাৰ আগতে চিন্তা কৰা, সন্মানজনক হোৱা, আপোনাৰ গোপনীয়তা সুৰক্ষিত কৰা, অৱগত হোৱা, য'ত ক্ৰেডিট দিব লাগে তাত ক্ৰেডিট দিয়া, আৰু ইতিবাচক উদ্দেশ্যত ছ'চিয়েল মিডিয়া ব্যৱহাৰ কৰা।



৮.১০ অগ্ৰগতিৰ খতিয়ান

প্ৰশ্ন নং ১ৰ উত্তৰ: ছ'চিয়েল মিডিয়া সুৰক্ষাৰ কিছুমান মূল সমস্যা হ'ল: গোপনীয়তা ভংগ, হেকিং, ফিছিং, পৰিচয় চুৰি, চাইবাৰ বুলিং, আৰু অনলাইন হাৰাশাস্তি।

প্ৰশ্ন নং ২ৰ উত্তৰ: ছ'চিয়েল মিডিয়াত আপত্তিজনক বিষয়বস্তুৰ প্ৰতিবেদন বা ফ্লেগ কৰাৰ সময়ত বিবেচনা কৰিবলগীয়া কিছুমান মূল কথা হ'ল: প্ৰশ্ন কৰা বিষয়বস্তুৰ বিষয়ে নিৰ্দিষ্ট হোৱা, প্ৰমাণ বা স্ক্ৰীণশ্বট প্ৰদান কৰা, উপযুক্ত চেনেলত প্ৰতিবেদন দিয়া, আৰু প্লেটফৰ্মৰ সম্প্ৰদায়ৰ নিৰ্দেশনা আৰু নীতিৰ বিষয়ে সচেতন হোৱা।

৩ নং প্ৰশ্নৰ উত্তৰ: বিবেচনা কৰিবলগীয়া কিছুমান সাধাৰণ কথা হ'ল স্থানীয় আইনসমূহ বুজি পোৱা, আপোনাৰ বিষয়বস্তুৰ প্ৰভাৱৰ প্ৰতি সচেতন হোৱা, আৰু ঘৃণামূলক ভাষণ বা বৈষম্যমূলক ভাষা এৰাই চলা।

৪ নং প্ৰশ্নৰ উত্তৰ: নিৰ্দেশনা প্ৰদান কৰা আন্তঃৰাষ্ট্ৰীয় চুক্তি আৰু কাঠামোসমূহৰ ভিতৰত আছে মানৱ অধিকাৰৰ সাৰ্বজনীন ঘোষণা, নাগৰিক আৰু ৰাজনৈতিক অধিকাৰৰ আন্তঃৰাষ্ট্ৰীয় চুক্তি, আৰু জাতীয়, বৰ্ণ বা ধৰ্মীয় ঘৃণাৰ পোষকতা নিষিদ্ধ কৰাৰ ওপৰত ৰাবাট কাৰ্য্য পৰিকল্পনা।

৫ নং প্ৰশ্নৰ উত্তৰ: আপোনাৰ দৰ্শক অনুসৰি আপোনাৰ বিষয়বস্তু সামঞ্জস্য কৰাটো গুৰুত্বপূৰ্ণ কাৰণ এটা দৰ্শকৰ বাবে যিটো উপযুক্ত হ'ব পাৰে সেয়া আন এটা দৰ্শকৰ বাবে উপযুক্ত নহ'বও পাৰে।

৬ নং প্ৰশ্নৰ উত্তৰ: আপুনি ছ'চিয়েল মিডিয়াত শ্বেয়াৰ কৰা ব্যক্তিগত তথ্যৰ প্ৰতি সচেতন হোৱাটো গুৰুত্বপূৰ্ণ কাৰণ ই আপোনাৰ গোপনীয়তা সুৰক্ষিত কৰাত সহায় কৰিব পাৰে, আৰু আপোনাৰ গোপনীয়তা ছেটিংছ সালসলনি কৰিলে আপোনাৰ পোষ্ট আৰু ব্যক্তিগত তথ্য কোনে চাব পাৰে সীমিত হ'ব পাৰে।



৮.১১ অধিক জানিবলৈ

১) ধীৰ, এ, আৰু ধীৰ, এ (২০১৯)। ছ'চিয়েল মিডিয়া সুৰক্ষা: বিপদ কমোৱাৰ লগতে ছ'চিয়েল নেটৱৰ্কিঙৰ লাভ উঠা। এপ্রেছ।

২) ক্রুছলাৰ, আৰ ই, জনষ্টন, এ চি, ল'ৰী, পি বি, হু, কিউ, আৰু ৱাৰকেন্টিন, এম (২০১৪)। আচৰণগত তথ্য সুৰক্ষা গৱেষণাৰ বাবে ভৱিষ্যতৰ দিশ। বিহেভিয়াৰ চাইবাৰ ছিকিউৰিটি (পৃষ্ঠা ২৩১-২৪৪)ত। স্প্রিংগাৰ।

৩) হেমছলি, জে, আৰু টেইলৰ, জে (২০১৯)। ছ'চিয়েল মিডিয়া আৰু সংকটৰ যোগাযোগ। ৰাউটলেজ।



৮.১২ আৰ্হি প্রশ্ন

প্রশ্ন ১. ছ'চিয়েল মিডিয়াত কিছুমান সাধাৰণ নিৰাপত্তাৰ ভাবুকি কি কি?

প্রশ্ন ২। ব্যক্তিসকলে ছ'চিয়েল মিডিয়াত নিজৰ ব্যক্তিগত তথ্য কেনেকৈ সুৰক্ষিত কৰিব পাৰে?

প্রশ্ন ৩। ব্যৱসায়ীসকলে নিজৰ ছ'চিয়েল মিডিয়া একাউণ্টৰ সুৰক্ষা নিশ্চিত কৰিবলৈ কি পদক্ষেপ ল'ব পাৰে?

প্রশ্ন ৪। ছ'চিয়েল মিডিয়া প্লেটফর্মসমূহে নিজেই নিৰাপত্তা ভংগ ৰোধ কৰিবলৈ আৰু ব্যৱহাৰকাৰীৰ তথ্য সুৰক্ষিত কৰিবলৈ কেনেকৈ কাম কৰে?

প্রশ্ন ৫। ছ'চিয়েল মিডিয়াত নিৰাপত্তা ভংগৰ সম্ভাব্য পৰিণতি কি হ'ব, ব্যক্তি আৰু ব্যৱসায় দুয়োটাৰে বাবে?

প্রশ্ন ৬। ছ'চিয়েল মিডিয়া ব্যৱহাৰকাৰীয়ে কেনেকৈ ফিছিং আৰু অন্যান্য ছ'চিয়েল ইঞ্জিনিয়াৰিঙৰ আক্রমণ চিনাক্ত আৰু এৰাই চলিব পাৰে?

অধ্যায় ৯ : ই-কমার্চৰ পৰিচয়

অধ্যায় গাঁথনি

৯.১ উদ্দেশ্য
৯.২ পৰিচয়
৯.৩ ই-কমার্চৰ সংজ্ঞা
৯.৪ ই-কমার্চৰ মুখ্য উপাদানসমূহ
৯.৫ ই-কমার্চ সুৰক্ষাৰ উপাদানসমূহ
৯.৬ ই-কমার্চৰ ভয়-ভীতি বা সংকটসমূহ
৯.৭ ই-কমার্চৰ সুৰক্ষাৰ উৎকৃষ্ট অনুশীলনসমূহ
৯.৮ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ
৯.৯ অগ্রগতিৰ খতিয়ান
৯.১০ অধিক জানিবলৈ
৯.১১ আৰ্হি প্ৰশ্ন

৯.১ উদ্দেশ্য

এই অধ্যায়টো অধ্যয়ন কৰি আপুনি—

- ই-কমার্চ লেনদেনৰ বিভিন্ন ধৰণ চিনাক্ত কৰিব পাৰিব
- ই-কমার্চৰ সুফল আৰু অপ্ৰয়োজনীয়তা বিশ্লেষণ কৰিব পাৰিব
- এটা ই-কমার্চ ব্যৱসায়ৰ উপাদানসমূহ মূল্যায়ন কৰিব পাৰিব
- ই-কমার্চত সুৰক্ষাৰ ভূমিকা বুজিব
- ই-কমার্চৰ সুৰক্ষা উন্নয়ন কৰিবলৈ কৌশল বিকাশ কৰিব পাৰিব।

৯.২ পৰিচয়

বিগত কিছু দশক ধৰি তথ্যপ্ৰযুক্তিৰ অভূতপূৰ্ব বিকাশই আধুনিক ব্যৱসায়িক পৰিসৰত এক বৈপ্লৱিক পৰিৱৰ্তন আনিছে। ইণ্টাৰনেটৰ আগমনে গ্ৰাহক আৰু বিক্ৰেতাৰ মাজত এক নতুন ধৰণৰ যোগাযোগৰ পথ মুকলি কৰিছে, যাৰ ফলস্বৰূপ উদ্ভৱ হৈছে **ই-কমার্চ** বা **ইলেক্ট্ৰনিক কমার্চ**। ই-কমার্চ হৈছে ইণ্টাৰনেটৰ জৰিয়তে সামগ্ৰী আৰু সেৱাৰ ক্ৰয়-বিক্ৰয় সম্পাদন কৰাৰ এক ডিজিটেল পদ্ধতি, যিয়ে আজিৰ দ্ৰুত গতিসম্পন্ন যুগত ক্ৰেতা-বিক্ৰেতাৰ মাজত পৰস্পৰৰ পৰা বহু দূৰত থাকিও লেনদেনৰ সুবিধা প্ৰদান কৰে।

এই অধ্যায়টোত ই-কমার্চৰ প্ৰাথমিক সংজ্ঞা, ধৰণসমূহ, মুখ্য উপাদানসমূহ, ইয়াৰ সুবিধা আৰু চেলেঞ্জসমূহৰ লগতে ই-কমার্চৰ লগত জড়িত সুৰক্ষা ব্যৱস্থাৰ বিৱৰণ আলোচনা কৰা হৈছে। লগতে অধ্যায়টোত ই-কমার্চত প্ৰচলিত ভয়-ভীতি, সুৰক্ষাৰ উৎকৃষ্ট অনুশীলন আৰু ইয়াৰ ব্যৱসায়িক ক্ষেত্ৰত সজাগতা বৃদ্ধিৰ ক্ষেত্ৰত কিদৰে কাৰ্যকৰী হ'ব পাৰে, তাৰ বিষয়েও বহলাই আলোচনা কৰা হৈছে।

ই-কমার্চৰ বিষয়ে গভীৰ অধ্যয়নৰ জৰিয়তে, শিক্ষাৰ্থীসকলে আধুনিক অনলাইন ব্যৱসায় পৰিসৰৰ গঠন, কাৰ্যপদ্ধতি আৰু সুৰক্ষা বিষয়ক জ্ঞান অৰ্জন কৰিব পাৰিব, যিয়ে তেওঁলোকক ভৱিষ্যতৰ প্ৰযুক্তিনিৰ্ভৰ বিশ্বত আত্মবিশ্বাসেৰে আগবাঢ়িবলৈ সহায় কৰিব।

৯.৩ ই-কমার্চৰ সংজ্ঞা

ই-কমার্চ (ইলেকট্ৰনিক কমার্চৰ সংক্ষেপ) বুলিলে ইণ্টাৰনেটৰ জৰিয়তে সামগ্ৰী আৰু সেৱা ক্ৰয়-বিক্ৰয়ক বুজায়। সাধাৰণ ভাষাত ক'লে, ই হৈছে অনলাইন প্লেটফৰ্ম—যেনে ৰেবছাইট, ছচিয়েল মিডিয়া, মোবাইল এপ আৰু অন্যান্য ডিজিটেল মাধ্যমৰ জৰিয়তে ব্যৱসায়িক লেনদেন সম্পন্ন কৰাৰ প্ৰক্ৰিয়া।

ই-কমার্চৰ ধাৰণাটোৰ উদ্ভৱ ১৯৯০ চনত হৈছিল, যেতিয়া ইণ্টাৰনেট সাধাৰণ ৰাইজৰ বাবে উপলব্ধ হৈ পৰিছিল। তেতিয়াৰ পৰা ই-কমার্চ দ্ৰুতগতিত এক বিশ্বজনীন বৃহৎ উদ্যোগৰ ৰূপ লৈছে, য'ত লাখ লাখ ব্যৱসায়ে ইণ্টাৰনেটৰ সহায়ত গ্ৰাহকলৈ পোৱাটো সহজ কৰি তোলে, নিজৰ কাৰ্যপদ্ধতি উন্নত কৰে আৰু বজাৰ অংশীদাৰিত্ব বৃদ্ধি কৰে।

ই-কমার্চক বিভিন্ন ধৰণত বিভাজন কৰিব পাৰি—পক্ষৰ ধৰণ, লেনদেনৰ স্বভাৱ আৰু ব্যৱসায় মডেলৰ আধাৰত। কিছুমান সাধাৰণ ধৰণ হ'ল:

• **B2B (Business-to-Business) :** এই ধৰণৰ ই-কমার্চত দুটা ব্যৱসায়িক প্ৰতিষ্ঠানৰ মাজত লেনদেন হয়। ইয়াত কোম্পানীসমূহে নিজৰ সামগ্ৰী বা সেৱা অন্য কোনো কোম্পানীক বিক্ৰী কৰে, ব্যক্তি গ্ৰাহকক নহয়। **উদাহৰণ :** IndiaMART, TradeIndia

• **B2C (Business-to-Consumer) :** এই ধৰণৰ ই-কমার্চত ব্যৱসায় আৰু ব্যক্তি গ্ৰাহকৰ মাজত লেনদেন হয়। ই হৈছে আটাইতকৈ সাধাৰণ ই-কমার্চৰ ধৰণ, য'ত অনলাইন শ্বপিং, ভ্ৰমণ বুকিং আদিৰ অন্তৰ্ভুক্ত হয়। **উদাহৰণ :** Amazon India, Flipkart, Myntra আদি

• **C2C (Consumer-to-Consumer) :** এই ধৰণৰ ই-কমার্চত ব্যক্তিসকলৰ মাজত লেনদেন হয়, যেনে অনলাইন অকচন ৰেবছাইট। **উদাহৰণ:** OLX, Quikr

• **C2B (Consumer-to-Business):** এই ধৰণৰ ই-কমার্চত ব্যক্তি গ্ৰাহকে নিজ নিজ সেৱা বা সামগ্ৰী ব্যৱসায়িক প্ৰতিষ্ঠানক প্ৰদান কৰে। **উদাহৰণ:** Airbnb, Uber, Ola আদি

• **B2G (Business-to-Government):** এই ধৰণৰ ই-কমার্চত ব্যৱসায় আৰু চৰকাৰী সংস্থাৰ মাজত লেনদেন হয়।

উদাহৰণ: Government e-Marketplace (GeM), Indian Railways E-Procurement System (IREPS)

ই-কমার্চ লেনদেনত সাধাৰণতে কিছুমান ধাপ জড়িত থাকে—সামগ্ৰী বা সেৱাৰ সন্ধান, বাছনি, ভাৰ্চুৱেল কার্টত সংযোজন, পেমেণ্ট, নিশ্চিতকৰণ আৰু প্ৰাপ্তি। ই-কমার্চ প্লেটফর্মসমূহে বিভিন্ন পেমেণ্ট গেটৱে ব্যৱহাৰ কৰে, যেনে ক্ৰেডিট কার্ড, ডেবিট কার্ড, ডিজিটেল ৱালেট আৰু অনলাইন বেংকিং।

ই-কমার্চৰ বহুতো সুবিধা আছে যি পৰম্পৰাগত দোকান-ভিত্তিক ব্যৱসায়ৰ তুলনাত অধিক লাভজনক। ই ব্যৱসায়ক বৃহৎ গ্ৰাহক গোটলৈ পোৱাৰ সুবিধা দিয়ে, বজাৰ বিস্তৃত কৰে, কার্যকাৰিতা বৃদ্ধি কৰে আৰু ২৪x৭ সেৱা আগবঢ়ায়। গ্ৰাহকে যিকোনো স্থানৰ পৰা যিকোনো সময়ত ক্ৰয় কৰাৰ সুবিধা লাভ কৰে, অধিক বিকল্প চাব পাৰে আৰু ভিন্ন প্লেটফর্মৰ মূল্য তুলনা কৰিব পাৰে।

তথাপি, ই-কমার্চৰ কিছুমান সমস্যাও আছে—যেনে চাইবাৰ সুৰক্ষা সংকট, ঠগবাজি, আৰু তথ্য চুৰি। ইয়াৰ উপৰি, ব্যৱসায়সমূহে শক্তিশালী ই-কমার্চ ভঁৰাল (ইনফ্ৰাষ্ট্ৰাকচাৰ) গঢ়ি তুলিবলৈ—যেনে ৱেবছাইট, মোবাইল এপ, আৰু সুৰক্ষিত পেমেণ্ট গেটৱে—বিনিয়োগ কৰিব লাগে।

শেষত ক'ব পাৰি— ই-কমার্চ হৈছে এক বিপ্লৱী ব্যৱসায়িক পদ্ধতি যিয়ে বিশ্বৰ ব্যৱসায়িক দৃশ্যপটক পৰিৱর্তন কৰিছে। ই ব্যৱসায়ক অধিক গ্ৰাহকৰ ওচৰলৈ পঠিয়াইছে, কার্যপদ্ধতি সহজ কৰিছে আৰু বজাৰ বিস্তৃত কৰাৰ সুযোগ দিছে। লগতে, ই গ্ৰাহকক অধিক সুবিধা, বিকল্প আৰু সময় বচাইছে আৰু স্বাধীনভাৱে ক্ৰয় কৰাৰ অভিজ্ঞতা দিছে।



অগ্ৰগতি নিৰীক্ষণ

প্ৰশ্ন নং ১ : ই-কমার্চ কি?

প্ৰশ্ন নং ২ : ই-কমার্চৰ মুখ্য ধৰণসমূহ কি কি?

প্ৰশ্ন নং ৩ : ই-কমার্চৰ মুখ্য উপাদানসমূহ কি কি?

প্ৰশ্ন নং ৪ : ই-কমার্চৰ কিছুমান সুবিধা কি কি?

৯.৫ ই-কমার্চ সুৰক্ষাৰ উপাদানসমূহ

ই-কমার্চ সুৰক্ষা হৈছে যিকোনো অনলাইন ব্যৱসায়ৰ এটা গুৰুত্বপূৰ্ণ দিশ, বিশেষকৈ যিবিলাকে গ্ৰাহকৰ পৰা পেমেন্ট গ্ৰহণ কৰে। অনলাইন লেনদেনৰ সংখ্যা দিনে দিনে বৃদ্ধি হোৱাৰ সৈতে, ব্যক্তিগত আৰু वित्तीय় তথ্য যেন দুষ্ট উদ্দেশ্য থকা ব্যক্তিৰ পৰা সুৰক্ষিত থাকে সেয়া নিশ্চিত কৰাটো অত্যন্ত জৰুৰি। ই-কমার্চ সুৰক্ষাৰ মুখ্য উপাদানসমূহ হ'লঃ

• **Secure Socket Layer (SSL) প্ৰমাণপত্ৰ:** SSL হৈছে এটা সুৰক্ষা প্ৰ'টকল যি এখন ৱেব ছার্ভাৰ আৰু ব্যৱহাৰকাৰীৰ ব্ৰাউজাৰৰ মাজত প্ৰেৰণ হোৱা তথ্য এনক্ৰিপ্ট কৰে। SSL প্ৰমাণপত্ৰ

হৈছে এটা ডিজিটেল প্ৰমাণপত্ৰ যি এখন ৱেবছাইটৰ পৰিচয় নিশ্চিত কৰে আৰু তাৰ আৰু ব্যৱহাৰকাৰীৰ মাজত প্ৰেৰণ হোৱা তথ্য এনক্ৰিপ্ট কৰে। SSL অনলাইন লেনদেন সুৰক্ষিত কৰি ডাটা চুৰি ৰোধ কৰিবলৈ অত্যন্ত গুৰুত্বপূৰ্ণ।

• **দুই-স্তৰীয় প্ৰমাণীকৰণ (Two-Factor Authentication):** দুই-স্তৰীয় প্ৰমাণীকৰণ (2FA) হৈছে সুৰক্ষাৰ এটা অতিৰিক্ত স্তৰ, য'ত ব্যৱহাৰকাৰীয়ে নিজৰ একাউণ্টত প্ৰৱেশ কৰাৰ বাবে দুটা পৃথক চিনাক্তকৰণ পদ্ধতি প্ৰদান কৰিব লাগে। ইয়াত এটা পাছৱৰ্ড আৰু এটা ইউনিক ক'ড থাকিব পাৰে যি ব্যৱহাৰকাৰীৰ ফোন বা ই-মেইললৈ পঠিওৱা হয়। 2FA-এ অনাধিকৃত প্ৰৱেশ ৰোধ কৰে আৰু ঠগবাজি বা ডাটা চুৰিৰ আশংকা কমাই।

• **পেমেণ্ট গেটৱেৰ সুৰক্ষা:** পেমেণ্ট গেটৱেৰ সুৰক্ষা অনলাইন লেনদেন সুৰক্ষিত কৰাৰ ক্ষেত্ৰত অত্যন্ত গুৰুত্বপূৰ্ণ। পেমেণ্ট গেটৱেৰ উচিত **PCI DSS (Payment Card Industry Data Security Standard)** অনুকূল হ'ব, অৰ্থাৎ ই পেমেণ্ট কাৰ্ড উদ্যোগৰ দ্বাৰা নিৰ্ধাৰিত নিৰ্দিষ্ট সুৰক্ষা মানদণ্ড পূৰণ কৰে। পেমেণ্ট গেটৱেৰ উচিত এনক্ৰিপশ্যন আৰু ট'কেনাইজেশ্যন ব্যৱহাৰ কৰা যাতে ক্ৰেডিট কাৰ্ডৰ দৰে সংবেদনশীল তথ্য সুৰক্ষিত থাকে।

• **ঠগবাজি চিনাক্তকৰণ আৰু ৰোধ:** ই-কমার্চ ব্যৱসায়ে সুদৃঢ় ঠগবাজি চিনাক্তকৰণ আৰু ৰোধ ব্যৱস্থা গঢ়ি তোলা উচিত যাতে সন্দেহজনক লেনদেন চিনাক্ত আৰু ৰোধ কৰিব পৰা যায়। ইয়াৰ অন্তৰ্গত হ'ব পাৰে লেনদেনৰ পেটাৰ্ণ মনিটৰিং কৰা, যান্ত্ৰিক শিক্ষাৰ (machine learning) সহায়ত অস্বাভাৱিকতা চিনাক্ত কৰা, আৰু উচ্চ-পৰিমাণৰ লেনদেনৰ ক্ষেত্ৰত কঠোৰ নিশ্চিতকৰণ প্ৰক্ৰিয়া অনুসৰণ কৰা।

• **নিয়মিত সুৰক্ষা পৰ্যবেক্ষণ আৰু আপডেট:** ই-কমার্চ ৱেবছাইটৰ সুৰক্ষা বজাই ৰখাৰ বাবে নিয়মিত সুৰক্ষা পৰ্যবেক্ষণ আৰু আপডেট অত্যন্ত প্ৰয়োজনীয়। ইয়াৰ অন্তৰ্গত হ'ব পাৰে – ভাৰ্নাৰেবিলিটি স্কেনিং, পেনেট্ৰেচন টেষ্টিং আৰু ছফ্টৱেৰ আপডেট, যিয়ে আগেৰে চিনাক্ত হোৱা সুৰক্ষা সমস্যাসমূহ সমাধান কৰে। এই পৰ্যবেক্ষণে হেকাৰসকলৰ দ্বাৰা ব্যৱহাৰ হোৱাৰ আগতেই সম্ভাব্য সুৰক্ষা জোখ গমি ইয়াক সমাধান কৰিব পাৰে।

পৰিশেষত ক'ব পাৰি ই-কমার্চ সুৰক্ষা হৈছে গ্ৰাহকৰ তথ্য সুৰক্ষিত ৰখা আৰু ঠগবাজি বা ডাটা চুৰি ৰোধ কৰাৰ ক্ষেত্ৰত অত্যন্ত গুৰুত্বপূৰ্ণ। ই-কমার্চ সুৰক্ষাৰ মুখ্য উপাদানসমূহ হ'ল: SSL প্ৰমাণপত্ৰ, দ্বৈত-স্তৰীয় প্ৰমাণীকৰণ, পেমেণ্ট গেটৱেৰ সুৰক্ষা, ঠগবাজি চিনাক্তকৰণ আৰু ৰোধ, আৰু নিয়মিত সুৰক্ষা পৰীক্ষা আৰু আপডেট। ই-কমার্চ ব্যৱসায়বোৰে সুৰক্ষাক অগ্ৰাধিকাৰ দিয়াৰ লগতে এই উপাদানসমূহ বাস্তৱায়ন কৰিব লাগে যাতে গ্ৰাহকৰ তথ্য সুৰক্ষিত আৰু বিশ্বাসযোগ্য হয়।

৯.৬ ই-কমার্চৰ ভয়-ভীত বা সংকটসমূহ

ই-কমার্চ আমাৰ দৈনন্দিন জীৱনৰ এক অৱিচ্ছেদ্য অংশ হৈ পৰিছে, আৰু ই অনলাইনত কেনেকৈ ক্ৰয়-বিক্ৰয় আৰু লেনদেন কৰা হয়, তাৰ পথ সহজ কৰি তুলিছে। কিন্তু ই-কমার্চৰ বৃদ্ধিৰ লগে লগে ইয়াৰ সৈতে জড়িত ভয়ংকৰ আশংকাবোৰো বৃদ্ধি পাইছে। এই আশংকাবোৰে অনলাইন লেনদেনৰ সুৰক্ষাত বিঘ্ন ঘটাব পাৰে, সংবেদনশীল তথ্য চুৰি কৰিব পাৰে আৰু গুৰুতৰ আৰ্থিক ক্ষতি সাধন কৰিব পাৰে। তলত কিছুমান সাধাৰণ ই-কমার্চৰ আশংকা উল্লেখ কৰা হ'ল, যিবোৰৰ বিষয়ে ব্যৱসায় আৰু ব্যৱহাৰকাৰীসকলে সাৱধান হোৱা উচিতঃ

মেলৱেয়াৰ আৰু ফিছিং (Malware and Phishing):

মেলৱেয়াৰ আৰু ফিছিং আক্ৰমণসমূহ ই-কমার্চৰ আটাইতকৈ সাধাৰণ আশংকাসমূহৰ ভিতৰত পৰে। **মেলৱেয়াৰ** হৈছে এনে ছফ্টৱেৰ যি কম্পিউটাৰ ব্যৱস্থাত অনুপ্ৰবেশ কৰিবলৈ বা ক্ষতি সাধন কৰিবলৈ সাজু কৰা হয়, আৰু **ফিছিং** হৈছে এনেধৰণৰ প্ৰতাৰণামূলক প্ৰচেষ্টা যাৰ জৰিয়তে ব্যৱহাৰকাৰীৰ পৰা পাছৱৰ্ড, ক্ৰেডিট কার্ডৰ তথ্য আদিৰ দৰে সংবেদনশীল তথ্য সংগ্ৰহ কৰা হয়। হেকাৰসকলে মেলৱেয়াৰ আৰু ফিছিংৰ জৰিয়তে গোপন তথ্য চুৰি কৰি অনলাইন লেনদেনৰ সুৰক্ষা বিঘ্নিত কৰিব পাৰে।

SQL Injection:

SQL ইনজেকশ্যন হৈছে এটা বিশেষ আক্ৰমণ যি তেনে ৱেবছাইটৰ ওপৰত লক্ষ্য ৰক্ষা কৰে যিবোৰ SQL ডেটাবেছ ব্যৱহাৰ কৰে। হেকাৰসকলে SQL ইনজেকশ্যন ব্যৱহাৰ কৰি ডেটাবেছত দুষিত ক'ড সিঁচি দিয়ে আৰু গ্ৰাহকৰ তথ্য, ক্ৰেডিট কার্ডৰ বিৱৰণ আদি সংবেদনশীল তথ্য চুৰ কৰে।

DDoS আক্ৰমণ (Distributed Denial of Service):

DDoS আক্ৰমণ হৈছে এটা ছাইবৰ আক্ৰমণ যাৰ লক্ষ্য হৈছে এখন ৱেবছাইটত বিপুল পৰিমাণৰ ভিজিটৰ পঠিয়াই সেই ৱেবছাইট অচল কৰি তোলা যাতে প্ৰকৃত ব্যৱহাৰকাৰীসকলে ব্যৱহাৰ কৰিব নোৱাৰে। DDoS আক্ৰমণ ই-কমার্চ ৱেবছাইট বিকল কৰি লেনদেনৰ প্ৰক্ৰিয়া বন্ধ কৰিব পাৰে।

পেমেণ্ট ঠগবাজি (Payment Fraud):

পেমেণ্ট ঠগবাজি হৈছে ই-কমার্চ ব্যৱসায়ৰ বাবে এটা গুৰুত্বপূৰ্ণ আশংকা। হেকাৰসকলে চুৰি কৰা ক্ৰেডিট কার্ডৰ তথ্য ব্যৱহাৰ কৰি ভুৱা ক্ৰয়-বিক্ৰয় বা গ্ৰাহকৰ একাউণ্টৰ পৰা ধন স্থানান্তৰ কৰিব পাৰে। এইধৰণৰ ঠগবাজিয়ে গুৰুতৰ আৰ্থিক ক্ষতি আৰু ব্যৱসায়ৰ সুনামহানি কৰিব পাৰে।

একাউণ্ট টেকঅ'ভাৰ (Account Takeover):

Account takeover বা একাউণ্ট অধিকাৰ গ্ৰহণ বুলিলে বুজায়, যেতিয়া হেকাৰ এজন ব্যৱহাৰকাৰীৰ একাউণ্টত প্ৰৱেশ কৰি সম্পূৰ্ণ নিয়ন্ত্ৰণ লৈ লয়। ইয়াৰ জৰিয়তে হেকাৰসকলে গোপন তথ্য চুৰি, ভুৱা লেনদেন, আৰু অনলাইন লেনদেনৰ সুৰক্ষা লঙ্ঘন কৰিব পাৰে।

এই আশংকাবোৰৰ পৰা সুৰক্ষিত থাকিবলৈঃ

ই-কমার্চ ব্যৱসায়সকলে SSL প্ৰমাণপত্ৰ, টু-ফেক্টৰ অথেণ্টিকেশ্যন, আৰু ঠগবাজি চিনাক্তকৰণ আৰু ৰোধ ব্যৱস্থা যেনে শক্তিশালী সুৰক্ষা ব্যৱস্থা ব্যৱহাৰ কৰা উচিত। ব্যৱহাৰকাৰীসকলে শক্তিশালী পাছৱৰ্ড ব্যৱহাৰ, চফটৱেৰ আপডেট কৰি ৰখা, আৰু সন্দেহজনক ৱেবছাইট বা ই-মেইল এৰাই চলা আদি সতর্কতা অবলম্বন কৰিব লাগে। ই-কমার্চ ব্যৱসায় আৰু ব্যৱহাৰকাৰীসকলে এই আশংকাবোৰৰ বিৰুদ্ধে সদায় সজাগ আৰু সক্ৰিয় থাকিবলৈ লাগিব যাতে অনলাইন লেনদেনৰ সুৰক্ষা নিশ্চিত কৰিব পৰা যায়।

৯.৭ ই-কমার্চ সুৰক্ষাৰ উৎকৃষ্ট অনুশীলনসমূহ

ই-কমার্চ সুৰক্ষা হৈছে যিকোনো অনলাইন ব্যৱসায়ৰ এক গুৰুত্বপূৰ্ণ দিশ, বিশেষকৈ যিসকল ব্যৱসায়ে গ্ৰাহকৰ পৰা পেমেণ্ট গ্ৰহণ কৰে। ই-কমার্চ সুৰক্ষাৰ উৎকৃষ্ট অনুশীলনসমূহ কার্যকৰী কৰাৰ জৰিয়তে তথ্য চুৰি, সংবেদনশীল তথ্যৰ অপব্যৱহাৰ ৰোধ কৰা আৰু অনলাইন লেনদেনৰ সুৰক্ষা নিশ্চিত কৰা যায়। তলত কিছুমান সর্বোত্তম অনুশীলন উল্লেখ কৰা হ'ল—

১. সবল পাছৱৰ্ড নীতি (Strong Password Policies) প্ৰৱর্তন:

ই-কমার্চ ব্যৱসায়সকলে ব্যৱহাৰকাৰীসকলক এনে পাছৱৰ্ড নির্মাণ কৰিবলৈ নির্দেশ দিয়া উচিত যিবোৰ অনুমান কৰা কঠিন হয়। পাছৱৰ্ডৰ দৈর্ঘ্য কমেও ৮ টা আখৰ হ'ব লাগিব আৰু ইয়াত অক্ষৰ, সংখ্যা আৰু বিশেষ চিহ্নৰ সংমিশ্ৰণ থাকিব লাগিব। লগতে, পাছৱৰ্ডৰ মিয়াদ শেষ হোৱাৰ নীতি (password expiration policy) আৰু টু-ফেক্টৰ অথেণ্টিকেশ্যন ব্যৱহাৰ কৰি এক অতিৰিক্ত সুৰক্ষা স্তৰ যোগ কৰা উচিত।

২. সুৰক্ষিত পেমেণ্ট গেটৱে ব্যৱহাৰ:

ই-কমার্চ ব্যৱসায়সকলে এনে পেমেণ্ট গেটৱে ব্যৱহাৰ কৰা উচিত যি **PCI DSS** (Payment Card Industry Data Security Standard) মানদণ্ডৰ সৈতে সঙ্গতিপূৰ্ণ। এই গেটৱে'সমূহে ক্ৰেডিট কার্ডৰ তথ্য যেনে সংবেদনশীল তথ্য এনক্ৰিপ্ট কৰি ডাটা চুৰি আৰু ঠগবাজিৰ পৰা ৰক্ষা কৰে।

৩. ছফ্টৱেৰ সদায় আপডেট কৰি ৰখা:

ই-কমার্চ ব্যৱসায়সকলে নিজা ছফ্টৱেৰ আৰু ব্যৱস্থাসমূহ নিয়মিতভাৱে আপডেট কৰি ৰখা উচিত যাতে প্রচলিত সুৰক্ষা দুৰ্বলতাৰ পৰা সুৰক্ষিত থাকিব পৰা যায়। ইয়াত ৱেব ছার্ভাৰ, কণ্টেনট মেনেজমেণ্ট ছিষ্টেম (CMS), আৰু পেমেণ্ট গেটৱে আদিৰ আপডেটসমূহ অন্তর্ভুক্ত।

৪. নিয়মিত সুৰক্ষা পর্যবেক্ষণ (Security Audit):

ই-কমার্চ ব্যৱসায়সকলে সম্ভাব্য দুৰ্বলতা চিনাক্ত কৰিবলৈ নিয়মিত সুৰক্ষা পৰীক্ষা কৰাৰ ব্যৱস্থা ৰাখিব লাগে। ইয়াৰ ভিতৰত আছে—ভালনেৰেবিলিটি স্কেনিং, পেনেট্রেচন টেষ্টিং আৰু ক'ড ৰিভিউ।

৫. লেনদেন মনিটৰিং :

ই-কমার্চ ব্যৱসায়সকলে সন্দেহজনক লেনদেন যেনে—অস্বাভাৱিক পেমেণ্ট ৰাশি বা সন্দেহজনক ডেলিভাৰী ঠিকনা আদিৰ ওপৰত নজৰ ৰাখিব লাগে। ইয়াৰ জৰিয়তে ঠগবাজি চিনাক্ত কৰি অনাধিকৃত লেনদেন ৰোধ কৰিব পৰা যায়।

৬. কর্মচাৰীসকলক সজাগ কৰাৰ বাবে প্রশিক্ষণ প্রদান:

ই-কমার্চ ব্যৱসায়সকলে কর্মচাৰীসকলক নিয়মিতভাৱে সুৰক্ষাৰ উৎকৃষ্ট অনুশীলনসমূহৰ বিষয়ে প্রশিক্ষণ দিয়াটো এক বাধ্যতামূলক বিষয় হ'ব লাগে। ইয়াত অন্তর্ভুক্ত—ফিছিং আক্রমণ চিনাক্ত আৰু ৰোধ কৰাৰ পদ্ধতি, সবল পাছৱর্ড সৃষ্টি কৰাৰ নিয়ম, সংবেদনশীল তথ্যৰ ব্যৱহাৰ আদিৰ বিষয়ে জ্ঞান প্রদান।

ই-কমার্চ সুৰক্ষাৰ উৎকৃষ্ট অনুশীলন অনুসৰণ কৰাটো অতিগুৰুত্বপূর্ণ যাতে গ্রাহকৰ সংবেদনশীল তথ্য সুৰক্ষিত থাকে আৰু অনলাইন লেনদেন নিৰাপদ হয়। ই-কমার্চ ব্যৱসায়সকলে সবল পাছৱর্ড নীতি, সুৰক্ষিত পেমেণ্ট গেটৱে, নিয়মিত ছফ্টৱেৰ আপডেট, সুৰক্ষা পৰীক্ষা, লেনদেন মনিটৰিং আৰু কর্মচাৰীসকলৰ সজাগতা বৃদ্ধিৰ ব্যৱস্থা ল'ব লাগে। এই অনুশীলনবোৰ অনুসৰণ কৰি তথ্য চুৰি ৰোধ কৰি গ্রাহকৰ বিশ্বাস আৰু আস্থা অটুট ৰাখিব পাৰি।



অগ্রগতি নিৰীক্ষণ

প্রশ্ন নং ৫ : SSL চার্টিফিকেট বুলিলে কি বুজায়?

প্রশ্ন নং ৬ : ই-কমার্চত দেখা পোৱা এটা সাধাৰণ বিপদসমূহ কি কি?

প্রশ্ন নং ৭ : ই-কমার্চ সুৰক্ষাৰ এটা উৎকৃষ্ট অনুশীলন কি?



৯.৮ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ

- ই-কমার্চ বা ইলেক্ট্রনিক কমার্চ বুলিলে ইণ্টাৰনেটৰ জৰিয়তে সামগ্রী আৰু সেৱা ক্রয়-বিক্রয় কৰাৰ প্রক্রিয়াক বুজোৱা হয়।
- ই-কমার্চ ১৯৯০ চনৰ দশকত উদ্ভৱ হৈছিল আৰু অতি সোনকালে ই এটা বৃহৎ বিশ্বব্যাপী উদ্যোগলৈ পৰিণত হৈছে।
- ই-কমার্চৰ বিভিন্ন ধৰণ আছে, যেনে B2B (Business-to-Business), B2C (Business-to-Consumer), C2C (Consumer-to-Consumer), C2B (Consumer-to-Business), আৰু B2G (Business-to-Government)।
- ই-কমার্চ লেনদেনত সামগ্রী সন্ধান কৰা, কার্টত সংযোজন কৰা, পেমেণ্ট কৰা আৰু নিশ্চিতকৰণ তথা ডেলিভাৰী লাভ কৰাৰ দৰে বিভিন্ন পর্যায় থাকে।
- ই-কমার্চত সাধাৰণতে ক্রেডিট কার্ড, ডেবিট কার্ড, ডিজিটেল ৱালেট, আৰু অনলাইন বেংকিঙৰ দৰে পেমেণ্ট গেটৱে ব্যৱহাৰ কৰা হয়।
- ই-কমার্চৰ বহুতো সুবিধা আছে, যেনে অধিক সংখ্যক গ্রাহকলৈ পোৱালৈ সক্ষম হোৱাটো, ব্যৱসায়ৰ ব্যয় হ্রাস কৰা, আৰু ২৪ ঘণ্টা সেৱা আগবঢ়োৱা।
- ই-কমার্চৰ কিছুমান চেলেঞ্জো আছে, যেনে চাইবৰ সুৰক্ষা সংকট, ঠগবাজি আৰু তথ্য চুৰিৰ আশংকা।
- ই-কমার্চৰ মুখ্য উপাদানবোৰ হৈছে—এখন ৱেবছাইট বা অনলাইন ষ্ট'ৰ, শ্বপিং কার্ট, পেমেণ্ট গেটৱে, লজিষ্টকচ আৰু পূৰণ প্রক্রিয়া (fulfillment), গ্রাহক সম্পর্ক ব্যৱস্থাপনা (CRM), আৰু সুৰক্ষা।
- এখন ৱেবছাইট বা অনলাইন ষ্ট'ৰ হৈছে ই-কমার্চ ব্যৱসায়ৰ ডিজিটেল মুকলি দোকান, য'ত গ্রাহকে সামগ্রী চাব পাৰে আৰু ক্রয় কৰিব পাৰে।
- শ্বপিং কার্ট হৈছে এক চফটৱেৰ এপ্লিকেশ্যন, যিয়ে গ্রাহকক সামগ্রী যোগ কৰাৰ আৰু প্রয়োজন মতে চেকআউট কৰাৰ সুবিধা দিয়ে।
- পেমেণ্ট গেটৱে'ই ই-কমার্চ ব্যৱসায়ক গ্রাহকৰ পৰা সুৰক্ষিতভাৱে পেমেণ্ট গ্রহণ কৰাৰ সুবিধা দিয়ে।
- লজিস্টিক্স আৰু পূৰণ প্রক্রিয়াই সামগ্রী মজুত, পেকিং আৰু গ্রাহকলৈ প্রেৰণ কৰাৰ কাম সম্বোধন কৰে।
- CRM বা গ্রাহক সম্পর্ক ব্যৱস্থাপনাই গ্রাহকৰ তথ্য ব্যৱস্থাপনা, আচৰণ অনুসৰণ আৰু ব্যক্তিগতভাৱে পৰামর্শ/প্রস্তাৱ আগবঢ়ায়।
- SSL এনক্রিপশ্যন, দুই-স্তৰীয় প্রমাণীকৰণ আৰু সুৰক্ষিত ছার্ভাৰৰ দৰে সুৰক্ষা ব্যৱস্থাসমূহ গ্রাহকৰ তথ্য ৰক্ষা কৰিবলৈ অতিপ্রয়োজনীয়।

- সামগ্রিকভাৱে, ই-কমার্চে বিশ্বৰ ব্যৱসায় পৰিৱেশক এক বৃহৎ ৰূপান্তৰ প্রদান কৰিছে, যিয়ে ব্যৱসায়ক অধিক গ্রাহকলৈ পোৱালৈ সক্ষম কৰি, কার্যপদ্ধতি অধিক ফলপ্রসূ কৰি তুলিছে, আৰু গ্রাহকক অধিক সুবিধা আৰু বিভিন্ন সামগ্রী-সেৱাৰ সহজলভ্য কৰি দিছে।

৯.৯ অগ্রগতিৰ খতিয়ান

১ নং উত্তৰ প্রশ্নৰ : ই-কমার্চ (E-commerce) বুলিলে ইণ্টাৰনেটৰ জৰিয়তে সামগ্রী আৰু সেৱা ক্রয়-বিক্রয় কৰাৰ প্রক্রিয়াক বুজোৱা হয়।

২ নং উত্তৰ প্রশ্নৰ : ই-কমার্চৰ মুখ্য ধৰণসমূহ হ'ল—B2B (Business-to-Business), B2C (Business-to-Consumer), C2C (Consumer-to-Consumer), C2B (Consumer-to-Business), আৰু B2G (Business-to-Government)।

৩ নং উত্তৰ প্রশ্নৰ : ই-কমার্চৰ মুখ্য উপাদানসমূহ হ'ল—এখন ৱেবছাইট বা অনলাইন ষ্ট'ৰ, এখন শ্বপিং কার্ট, এখন পেমেণ্ট গেটৱে, লজিচটিকচ আৰু পূৰণ প্রক্রিয়া, গ্রাহক সম্পর্ক ব্যৱস্থাপনা (CRM), আৰু সুৰক্ষা।

৪ নং উত্তৰ প্রশ্নৰ : ই-কমার্চে ব্যৱসায়ক অধিক সংখ্যক গ্রাহকলৈ পোৱালৈ, বজাৰ বিস্তাৰ কৰিবলৈ, কার্যকৰী ব্যয় হ্রাস কৰিবলৈ আৰু ২৪/৭ সেৱা আগবঢ়াবলৈ সক্ষম কৰি তুলিছে; আনহাতে, গ্রাহকে সুবিধাজনকভাৱে কেনেকৈযে সময়ত শ্বপিং কৰিব পাৰে আৰু অধিক সামগ্রী/সেৱাৰ এক্সেছ লাভ কৰে।

৫ নং উত্তৰ প্রশ্নৰ : SSL চার্টিফিকেট (ডিজিটেল চার্টিফিকেট) হৈছে যিয়ে এটা ৱেবছাইট আৰু ব্যৱহাৰকাৰীৰ ব্রাউজাৰৰ মাজত প্রেৰণ হোৱা ডাটাক এনক্রিপ্ট কৰে।

৬ নং উত্তৰ প্রশ্নৰ : ই-কমার্চত দেখা পোৱা সাধাৰণ সংকটসমূহৰ ভিতৰত মেলৱেৰ (Malware) আৰু ফিছিং (Phishing) আক্রমণ অতি জনপ্রিয়।

৭ নং উত্তৰ প্রশ্নৰ : ই-কমার্চ সুৰক্ষাৰ এটা উৎকৃষ্ট অনুশীলন হৈছে—শক্তিশালী পাছৱর্ড নীতি (Strong Password Policies) ব্যৱহাৰ কৰা।

৯.১০ অধিক জানিবলৈ

1) Field, A. P. (2018). An adventure in statistics: The reality enigma. Sage.

2) Cohen, J. (1992). A power primer. Psychological Bulletin, 112(1), 155-159.



৯.১১ আৰ্হি প্ৰশ্ন

প্ৰশ্ন ১ : ই-কমার্চৰ বিভিন্ন ধৰণ কি কি আৰু এইসকলৰ মাজত লেনদেনত জড়িত পক্ষসমূহ আৰু লেনদেনৰ স্বভাৱ অনুসৰি কেনেদৰে পাৰ্থক্য থাকে?

প্ৰশ্ন ২ : ই-কমার্চৰ মুখ্য উপাদানসমূহ কি কি, আৰু এই উপাদানসমূহ কেনেদৰে পৰস্পৰ মিলি গ্ৰাহকসকলৰ বাবে এটা সহজ আৰু সুসংগত অনলাইন ক্ৰয় অভিজ্ঞতাৰ সৃষ্টি কৰে?

প্ৰশ্ন ৩ : ই-কমার্চৰ ব্যৱসায়ৰ বাবে লাভ আৰু অসুবিধাসমূহ কি কি, আৰু অনলাইন লেনদেন সম্পন্ন কৰাৰ সময়ত উদ্ভৱ হোৱা সমস্যাসমূহ কেনেদৰে ব্যৱসায়ে পাৰ কৰিব পাৰে?

প্ৰশ্ন ৪: ই-কমার্চৰ লগত জড়িত মুখ্য সু�ৰক্ষা-সংক্ৰান্ত চিন্তাসমূহ কি কি, আৰু কেনেদৰে কোনো ব্যৱসায়ে নিশ্চিত কৰিব পাৰে যে তেওঁলোকৰ গ্ৰাহকৰ ব্যক্তিগত আৰু বিত্তীয় তথ্য সুৰক্ষিত হৈ আছে?

প্ৰশ্ন ৫: ই-কমার্চে কেনেদৰে বিশ্বৰ ব্যৱসায় পৰিৱেশক ৰূপান্তৰিত কৰিছে, আৰু ইয়াৰ প্ৰভাৱ পৰম্পৰাগত দোকানসমূহ (brick-and-mortar businesses)ৰ ওপৰত কেনেদৰে পৰিছে?

অধ্যায় ১০: ডিজিটেল পেমেণ্টৰ পৰিচয়

অধ্যায় গাঁথনি

১০.১ উদ্দেশ্য

১০.২ পৰিচয়

১০.৩ ডিজিটেল পেমেণ্ট

১০.৩.১ ডিজিটেল পেমেণ্টৰ গুৰুত্ব

১০.৩.২ ডিজিটেল পেমেণ্টৰ ইতিবৃত্ত

১০.৩.৩ ডিজিটেল পেমেণ্টৰ উপাদানসমূহ

১০.৩.৪ ডিজিটেল পেমেণ্টত জড়িত অংশীদাৰসকল

১০.৪ ডিজিটেল পেমেণ্টৰ বিভিন্ন পদ্ধতি

১০.৪.১ ডেবিট কার্ড

১০.৪.২ ক্রেডিট কার্ড

১০.৪.৩ Unified Payment Interface (UPI)

১০.৪.৪ ই-ৱালেট (e-Wallets)

১০.৪.৫ Unstructured Supplementary Service Data (USSD)

১০.৪.৬ আধাৰ-ভিত্তিক পেমেণ্ট (Aadhaar-enabled Payments)

১০.৫ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ

১১.৫ অগ্রগতিৰ খতিয়ান

১১.৯ অধিক জানিবলৈ

১১.১০ আৰ্হি প্রশ্ন

১১.১ উদ্দেশ্য

এই অধ্যায়টো অধ্যয়ন কৰি আপুনি—

- আধুনিক অর্থনীতিৰ ক্ষেত্রত ডিজিটেল পেমেণ্টৰ গুৰুত্ব আৰু বিত্তীয় লেনদেনত ইয়াৰ প্রভাৱ বুজিব পাৰিব।
- ডিজিটেল পেমেণ্টৰ ইতিহাস আৰু সময়ৰ সৈতে ইয়াৰ বিকাশ বিশ্লেষণ কৰিব পাৰিব।
- ডিজিটেল লেনদেনত ব্যৱহৃত প্রযুক্তি আৰু প্রক্রিয়াসমূহসহ ডিজিটেল পেমেণ্টৰ বিভিন্ন উপাদান চিনাক্ত কৰিব পাৰিব।
- গ্রাহক, ব্যৱসায়ী, পেমেণ্ট সেৱা প্রদানকাৰী আৰু নিয়ন্ত্রণকাৰী সংস্থাসহ ডিজিটেল পেমেণ্টত জড়িত বিভিন্ন অংশীদাৰৰ ভূমিকা বুজিব পাৰিব।

- ডেবিট কার্ড, ক্রেডিট কার্ড, UPI, ই-ৱালেট, USSD আৰু আধাৰ-ভিত্তিক পেমেণ্টসহ ডিজিটেল পেমেণ্টৰ বিভিন্ন পদ্ধতি বর্ণনা কৰিব পাৰিব।

১০.২ পৰিচয়

ডিজিটেল পেমেণ্ট বুলিলে এনে ইলেক্ট্রনিক লেনদেনক বুজোৱা হয়, যিয়ে গ্রাহকসকলক **নগদৰ প্রয়োজন নোহোৱাকৈ** সামগ্রী কিনা-বেচা, টকা স্থানান্তৰ, বা বিল পৰিশোধ কৰাৰ সুবিধা দিয়ে।

ডিজিটেল পেমেণ্ট আজি আমাৰ দৈনন্দিন জীৱনৰ **এটা অপৰিহার্য অংশ** হৈ পৰিছে, কিয়নো ইয়াত **সুবিধা, গতি আৰু সুৰক্ষা** থকা বেছি। প্রযুক্তিৰ বেছি ব্যৱহাৰৰ লগে লগে ডিজিটেল পেমেণ্টৰ ব্যৱহাৰ যথেষ্ট বৃদ্ধি পাইছে।

বিশেষকৈ **COVID-19 মহামাৰীৰ সময়ছোৱাত**, যেতিয়া **মানুহে স্পর্শৰ পৰা বাচি চলা** অত্যন্ত প্রয়োজনীয় হৈছিল, তেতিয়া **contactless পেমেণ্ট** এক আবশ্যকতাত পৰিণত হৈছিল।

এই অধ্যায়টোত ডিজিটেল পেমেণ্টৰ প্রাথমিক ধাৰণাসমূহ আলোচনা কৰা যাব—মূলতঃ ইয়াৰ ইতিহাস, গুৰুত্ব আৰু উপাদানসহ। লগতে ইয়াত ডিজিটেল পেমেণ্টৰ বিভিন্ন পদ্ধতি, যেনে **ব্যাংকিং কার্ড, Unified Payment Interface (UPI), ই-ৱালেট (e-Wallets), USSD, আৰু আধাৰ-ভিত্তিক পেমেণ্ট (Aadhaar-enabled payments)** আদিৰ বিষয়ে আলোচনা কৰা হৈছে।

এই অধ্যায়টি অধ্যয়ন কৰি আপুনি ডিজিটেল পেমেণ্টৰ বিষয়ে **এটা স্পষ্ট আৰু গভীৰ ধাৰণা লাভ কৰিব**—তাৰ অর্থনীতিৰ ওপৰত প্রভাৱ, আৰু ব্যক্তিগত আৰু ব্যৱসায়িক ক্ষেত্রত উপলব্ধ বিভিন্ন ডিজিটেল পেমেণ্ট পদ্ধতিৰ বিষয়েও জ্ঞাত হ'ব। তদুপৰি আপুনি **আপোনাৰ প্রয়োজন অনুসৰি উপযুক্ত পেমেণ্ট পদ্ধতি বাছনি** কৰিবলৈ প্রয়োজনীয় জ্ঞান লাভ কৰিব।

১০.৩ ডিজিটেল পেমেণ্ট

ডিজিটেল পেমেণ্ট বুলিলে এনে ইলেকট্রনিক লেনদেনক বুজোৱা হয়, যি **ব্যক্তি বা প্রতিষ্ঠানে নগদৰ প্রয়োজন নোহোৱাকৈ অনলাইনযোগে টকা স্থানান্তৰ, বিল পৰিশোধ, আৰু কিনা-বেচাৰ** সুবিধা দিয়ে। ডিজিটেল পেমেণ্টত, ধন **ব্যাংক একাউণ্টৰ মাজত** বা **ডিজিটেল ৱালেটৰ** জৰিয়তে ইলেকট্রনিকভাৱে স্থানান্তৰ হয়।

ডিজিটেল পেমেণ্টৰ ব্যৱহাৰ দিনে দিনে বাঢ়ি গৈছে, কিয়নো ইয়াত **সুবিধা, গতি, আৰু সুৰক্ষা** থাকে। ই লেনদেনৰ ধাৰণাটোক একেবাৰে পৰিৱৰ্তন কৰিছে, আৰু এতিয়া ব্যক্তি আৰু প্ৰতিষ্ঠানসকলে **যিকোনো সময়ত আৰু যিকোনো স্থানৰ পৰা বিত্তীয় লেনদেন** কৰিব পাৰি। প্ৰযুক্তিৰ বিকাশৰ লগে লগে ডিজিটেল পেমেণ্ট আজি আমাৰ **জীৱনৰ এটা অপৰিহাৰ্য অঙ্গ** হৈ পৰিছে।

১০.৩.১ ডিজিটেল পেমেণ্টৰ গুৰুত্ব

ডিজিটেল পেমেণ্টে আমাৰ আধুনিক অৰ্থনীতিৰ ক্ষেত্ৰত অত্যন্ত গুৰুত্বপূৰ্ণ ভূমিকা পালন কৰে। ডিজিটেল পেমেণ্ট কিয় গুৰুত্বপূৰ্ণ, তাৰ কিছুমান কাৰণ তলত উল্লেখ কৰা হ'ল—

(a) সুবিধা: ডিজিটেল পেমেণ্টে ব্যক্তি আৰু ব্যৱসায়িক ক্ষেত্ৰত নগদ বা চেকৰ প্ৰয়োজন নোহোৱাকৈ লেনদেন কৰিবলৈ এক সহজ আৰু সুবিধাজনক মাধ্যম প্ৰদান কৰে।

(b) গতি: ডিজিটেল পেমেণ্ট প্ৰায় তৎক্ষণাত প্ৰক্ৰিয়াকৰণ হয়, যাৰ ফলত দ্ৰুত লেনদেন আৰু পেমেণ্ট সম্ভৱ।

(c) সুৰক্ষা: ডিজিটেল পেমেণ্ট নগদ আৰু চেকৰ দৰে পৰম্পৰাগত পদ্ধতিতকৈ অধিক সুৰক্ষিত, কিয়নো ইয়াত **এনক্ৰিপচন আৰু প্ৰমাণীকৰণ** ব্যৱহাৰ কৰি ব্যক্তিগত আৰু বিত্তীয় তথ্য সুৰক্ষিত কৰা হয়।

(d) কম খৰচী: ডিজিটেল পেমেণ্ট কম খৰচী, কিয়নো ইয়াত **হাতে-হাতে হস্তান্তৰকৰণ প্ৰয়োজন নাথাকে**, যাৰ ফলত কাগজত আধাৰিত লেনদেনৰ ব্যয় কমে।

(e) বিত্তীয় অন্তৰ্ভুক্তি: ডিজিটেল পেমেণ্টে তেনে ব্যক্তিসকলকো ডিজিটেল অৰ্থনীতিত অংশগ্ৰহণৰ সুযোগ দিয়ে, যিসকলে পৰম্পৰাগত বেংক ব্যৱস্থাৰ পৰা বঞ্চিত।

(f) অধিক কাৰ্যক্ষমতা: ডিজিটেল পেমেণ্টে বহু প্ৰক্ৰিয়া স্বয়ং চালিত কৰি ৰিয়েল টাইমত লেনদেনৰ তথ্য প্ৰদান কৰে, যাৰ ফলত ই পৰম্পৰাগত পদ্ধতিতকৈ অধিক কাৰ্যক্ষম।

ডিজিটেল পেমেণ্টে আমাৰ লেনদেন কৰাৰ পদ্ধতিক একেবাৰে পৰিৱৰ্তন কৰিছে—তেনেদৰে ই অধিক তীব্ৰ, সুৰক্ষিত আৰু কাৰ্যকৰী। ই আমাৰ আধুনিক অৰ্থনীতিৰ এক অপৰিহাৰ্য অংশ, যিয়ে বিত্তীয় অন্তৰ্ভুক্তি আগবঢ়ায় আৰু অৰ্থনৈতিক বিকাশত সহায় কৰে।

১০.৩.২ ডিজিটেল পেমেণ্টৰ ইতিহাস (History of Digital Payments)

ডিজিটেল পেমেণ্টৰ ইতিহাস **১৯৭০ দশকৰ আৰম্ভণি**তে শুভাৰম্ভ হৈছিল; মূলতঃ প্ৰথম **ইলেকট্ৰনিক ফাণ্ড স্থানান্তৰ ব্যৱস্থা (EFT)** আৰম্ভ হোৱাৰ সময়ৰ পৰাই। এই সময়ছোৱাত ই যদিও অধিক জনপ্ৰিয় হৈছে, তথাপি ইণ্টাৰনেট আৰু ই-কমাৰ্চৰ আৰম্ভ হোৱাৰ লগে লগে **১৯৯০ দশকৰ শেষভাগত আৰু ২০০০ দশকৰ আৰম্ভণিত** ডিজিটেল পেমেণ্ট জনপ্ৰিয়তা লাভ কৰে।

১৯৯৮ চনত **PayPal** প্ৰতিষ্ঠা কৰা হয়, যিয়ে ব্যক্তি আৰু ব্যৱসায়িক ক্ষেত্ৰত অনলাইন পেমেণ্ট কৰাৰ এক নতুন মাধ্যম আগবঢ়ায়।

২০০৩ চনত কেনিয়াত **প্ৰথম মোবাইল পেমেণ্ট ব্যৱস্থা M-Pesa** আৰম্ভ হয়, যিয়ে মোবাইল ফোন ব্যৱহাৰ কৰি ধন পঠিয়াব আৰু লাভ কৰিবৰ সুবিধা দিয়ে।

ক্ৰেডিট আৰু ডেবিট কার্ডৰ প্ৰচলনে ডিজিটেল পেমেণ্টৰ বিকাশত উল্লেখযোগ্য ভূমিকা পালন কৰে। ১৯৫০ চনত **Diner's Club Card** নামেৰে প্ৰথম ক্ৰেডিট কার্ড চালু হৈছিল, আৰু তাৰ পাছত ১৯৬০ চনত **ATM কার্ড** ৰূপে প্ৰথম ডেবিট কার্ড চালু হয়।

আজিকালি, ডিজিটেল পেমেণ্ট আমাৰ দৈনন্দিন জীৱনৰ এক অপৰিহার্য অংশ হৈ পৰিছে— অনলাইন বেংকিং, ই-ৱালেট, মোবাইল পেমেণ্ট, আৰু সংস্পৰ্শবিহীন পেমেণ্টৰ দৰে বহু বিকল্প উপলব্ধ। নতুন প্ৰযুক্তি আৰু পেমেণ্ট পদ্ধতিৰ বিকাশ অব্যাহত আছে, যিয়ে ডিজিটেল পেমেণ্টৰ বিস্তাৰ আগবঢ়াই আধুনিক অর্থনীতিত ইয়াৰ গুৰুত্ব অধিক বঢ়াইছে।

১০.৩.৩ ডিজিটেল পেমেণ্টৰ উপাদানসমূহ

ডিজিটেল পেমেণ্টৰ উপাদানসমূহৰ ভিতৰত অন্তর্ভুক্ত—

(a) পেমেণ্ট গেটৱে (Payment Gateway):

এটা ছফ্টৱেৰ সেৱা, যিয়ে ব্যৱসায়ীক অনলাইন লেনদেন প্ৰক্ৰিয়া সুৰক্ষিতভাৱে কৰাৰ সুবিধা দিয়ে। ই **ব্যৱসায়ীৰ ৱেবছাইট বা মোবাইল এপ** আৰু **ব্যাংক বা পেমেণ্ট প্ৰচালকৰ** মাজত তথ্য স্থানান্তৰৰ কার্য সম্পন্ন কৰে।

(b) ডিজিটেল ৱালেট (Digital Wallet):

এইবোৰ হৈছে **ভার্চুৱেল একাউণ্ট**, য'ত পেমেণ্ট কার্ডৰ তথ্য আৰু অন্যান্য পেমেণ্ট পদ্ধতি সংৰক্ষণ কৰা হয়। এইবোৰে ব্যৱহাৰকাৰীক **স্মার্টফোন বা অন্যান্য ডিভাইচৰ জৰিয়তে সহজে আৰু সুৰক্ষিতভাৱে** পেমেণ্ট কৰিবলৈ সহায় কৰে।

(c) পইণ্ট অফ চেল (POS) টার্মিনেল:

ব্যৱসায়ীয়ে নিজৰ **দোকান বা আউটলেটত কার্ডৰ জৰিয়তে পেমেণ্ট গ্ৰহণ** কৰিবলৈ এই টার্মিনেল ব্যৱহাৰ কৰে। ই **স্বতন্ত্ৰ যন্ত্ৰ** হ'ব পাৰে বা **নগদ ৰেজিষ্টাৰত অন্তর্ভুক্ত** হৈ থাকিব পাৰে।

(d) পেমেণ্ট প্ৰচালক (Payment Processor):

এইসকল সংস্থাই **ব্যৱসায়ী আৰু গ্ৰাহকৰ মাজত পেমেণ্ট প্ৰক্ৰিয়া আৰু অনুমোদন** সম্পন্ন কৰে। তেওঁলোকে এনক্ৰিপচন আৰু প্ৰতাৰণা চিনাক্তকৰণৰ দৰে **প্ৰযুক্তিগত দিশবোৰ** হেণ্ডল কৰে আৰু **ব্যাংকৰ মাজত ধনৰ স্থানান্তৰ** নিশ্চিত কৰে।

(e) মোবাইল পেমেণ্ট:

এইবোৰ হৈছে তেনে লেনদেন, যি **মোবাইল ডিভাইচ (যেনে স্মার্টফোন বা টেবলেট)** ব্যৱহাৰ কৰি কৰা হয়। ই **NFC, QR ক'ড, বা মোবাইল এপ**ৰ সহায়ত সম্পন্ন হ'ব পাৰে।

(f) ইলেকট্রনিক ফাণ্ড স্থানান্তৰ (EFT):

এই পদ্ধতিৰ দ্বাৰা **ব্যাংক একাউণ্টৰ মাজত ধন ইলেকট্রনিকভাৱে স্থানান্তৰ** কৰা হয়। ই ব্যক্তি বা প্রতিষ্ঠানক **পেমেণ্ট আৰু ৰিছিভিং** দুয়ো সুবিধা দিয়ে।

এই উপাদানসমূহ একেলগে কাম কৰি **ডিজিটেল পেমেণ্টক এক সুৰক্ষিত আৰু সহজ অভিজ্ঞতা** হিচাপে গঢ়ি তোলে, যাৰ ফলত অনলাইন বা ব্যক্তিগতভাৱে লেনদেন অধিক সুবিধাজনক হৈ পৰিছে।

১০.৩.৪ ডিজিটেল পেমেণ্টত অংশীদাৰসকল

ডিজিটেল পেমেণ্টত বহু অংশীদাৰ জড়িত থাকে, যিবোৰ হ'ল—

(a) গ্রাহক (Consumers):

গ্রাহকসকল হৈছে ডিজিটেল পেমেণ্টৰ শেষ ব্যৱহাৰকাৰী। তেওঁলোকে অনলাইন বা সশৰীৰভাৱে লেনদেন কৰিবলৈ ডিজিটেল পেমেণ্ট ব্যৱহাৰ কৰে।

(b) ব্যৱসায়ী (Merchants):

ব্যৱসায়ী বা বেপাৰীসকল হৈছে সেইসকল ব্যক্তি বা প্রতিষ্ঠান, যিসকলে **নিজৰ পণ্য বা সেৱাৰ বিনিময়ত ডিজিটেল পেমেণ্ট গ্রহণ** কৰে। তেওঁলোকে পেমেণ্ট গেটৱে, মোবাইল পেমেণ্ট, বা POS টার্মিনেল আদিৰ সহায় লয়।

(c) বেংক (Banks):

বেংকসমূহ ডিজিটেল পেমেণ্টৰ ক্ষেত্রত **অতি গুৰুত্বপূর্ণ ভূমিকা** পালন কৰে, কিয়নো তেওঁলোকে **লেনদেন প্রক্রিয়া কৰাৰ বাবে প্রয়োজনীয় অবকাঠামো** প্রদান কৰে—যেনে পেমেণ্ট গেটৱে, মার্চেণ্ট একাউণ্ট, আদি।

(d) পেমেণ্ট প্রচালক (Payment Processors):

এই সংস্থাসমূহ **বেংক আৰু ব্যৱসায়ীৰ মাজত ধনৰ স্থানান্তৰ সুগম** কৰে। তেওঁলোকে লেনদেনৰ সুৰক্ষা নিশ্চিত কৰিবলৈ এনক্রিপচন আৰু প্রতাৰণা চিনাক্তকৰণৰ দৰে প্রযুক্তিগত দিশবোৰ সমাধান কৰে।

(e) নিয়ন্ত্রক সংস্থা (Regulators):

এইসকল সংস্থাই নিশ্চিত কৰে যে ডিজিটেল পেমেণ্ট **সদায় আইন আৰু বিধি-বিধানৰ** অধীনত চলি আছে। তেওঁলোকে গ্রাহক, ব্যৱসায়ী, আৰু আন অংশীদাৰৰ সুৰক্ষাৰ বাবে নিয়ম আৰু নির্দেশনা প্রণয়ন কৰে।

(f) প্ৰযুক্তি প্ৰদানকাৰী (Technology Providers):

এইসকল সংস্থাই ডিজিটেল পেমেণ্ট ব্যৱস্থাৰ বাবে প্ৰয়োজনীয় **ছফ্টৱেৰ আৰু হার্ডৱেৰ** বিকাশ আৰু ৰক্ষণাবেক্ষণ কৰে। তেওঁলোকে পেমেণ্ট গেটৱে, মোবাইল এপ, POS টাৰ্মিনেল বা অন্যান্য পেমেণ্ট সমাধান প্ৰদান কৰে।



অগ্ৰগতি নিৰীক্ষণ

প্ৰশ্ন নং ১ : সঠিক বিকল্প বাছনি কৰক

ক. পৰম্পৰাগত পেমেণ্ট পদ্ধতিতকৈ ডিজিটেল পেমেণ্টৰ মুখ্য সুবিধা কি?

(i) অধিক দ্ৰুত লেনদেন

(ii) বেছি কাৰ্যক্ষমতা

(ii) অধিক সুৰক্ষিত

(iv) ওপৰৰ সকলো শুদ্ধ

খ. ১৯৭০ দশকত চালু কৰা প্ৰথম ইলেকট্ৰনিক ফাণ্ড স্থানান্তৰ ব্যৱস্থাটো কি আছিল?

(i) PayPal

(ii) M-Pesa

(iii) EFT

(iv) Diner's Club Card

গ. তলৰ কোনটো উপাদান ডিজিটেল পেমেণ্টৰ অংশ নহয়?

(i) পেমেণ্ট গেটৱে

(ii) POS টাৰ্মিনেল

(iii) ডিজিটেল কুপন

(iv) মোবাইল পেমেণ্ট

ঘ. ডিজিটেল পেমেণ্টত জড়িত অংশীদাৰসকল কোনে?

(i) গ্ৰাহক, ব্যৱসায়ী, বেংক, পেমেণ্ট প্ৰচালক, নিয়ন্ত্ৰক, প্ৰযুক্তি প্ৰদানকাৰী

(ii) গ্ৰাহক, বিক্ৰেতা, ক্ৰেতা, বেংক, প্ৰযুক্তি প্ৰদানকাৰী, পেমেণ্ট প্ৰচালক

(iii) গ্ৰাহক, বিক্ৰেতা, বেংক, পেমেণ্ট প্ৰচালক, প্ৰযুক্তি প্ৰদানকাৰী, বিজ্ঞাপনদাতা

(iv) গ্ৰাহক, বেংক, পেমেণ্ট প্ৰচালক, নিয়ন্ত্ৰক, প্ৰযুক্তি প্ৰদানকাৰী, বিজ্ঞাপনদাতা

ঙ. বিত্তীয় অন্তৰ্ভুক্তি আগবঢ়োৱাৰ ক্ষেত্ৰত ডিজিটেল পেমেণ্টৰ গুৰুত্ব কি?

(i) ই তেনে ব্যক্তিসকলক ডিজিটেল অৰ্থনীতিত অংশগ্ৰহণৰ সুবিধা দিয়ে, যিসকলে পৰম্পৰাগত বেংক ব্যৱস্থালৈ প্ৰৱেশ নাপায়

(ii) ই ব্যক্তি আৰু ব্যৱসায়ৰ বাবে অধিক দ্ৰুত লেনদেনৰ সুবিধা দিয়ে

(iii) ই পৰম্পৰাগত পেমেণ্ট পদ্ধতিতকৈ অধিক ব্যয়-সাশ্রয়ী

(iv) ওপৰৰ কোনোও নহয়

১০.৪ ডিজিটেল পেমেণ্টৰ পদ্ধতিসমূহ

ডিজিটেল পেমেণ্ট হৈছে এনে এক ইলেকট্রনিক লেনদেন, যাৰ জৰিয়তে গ্রাহকে **নগদৰ প্রয়োজন নোহোৱাকৈ সামগ্রী আৰু সেৱা** ক্রয় কৰিব পাৰে। আজিৰ দিনত বহুতো ডিজিটেল পেমেণ্টৰ পদ্ধতি উপলব্ধ। এই অংশত আমি ডিজিটেল পেমেণ্টৰ বিভিন্ন পদ্ধতি সন্দর্ভত সংক্ষেপে আলোচনা কৰিম। তলত কিছুমান আটাইতকৈ সাধাৰণ ডিজিটেল পেমেণ্ট পদ্ধতি উল্লেখ কৰা হৈছে:

(a) মোবাইল পেমেণ্ট (Mobile Payments):

মোবাইল পেমেণ্টে গ্রাহকক **নিজৰ মোবাইল ফোনৰ জৰিয়তে পেমেণ্ট** কৰিবলৈ সক্ষম কৰি তোলে। এই পদ্ধতিত **Apple Pay, Google Pay, আৰু Samsung Pay** ধৰণৰ মোবাইল ৱালেট অন্তর্ভুক্ত থাকে, যিসকলে গ্রাহকৰ **ক্রেডিট কার্ডৰ তথ্য সুৰক্ষিতভাৱে সংৰক্ষণ** কৰিবলৈ সহায় কৰে।

(b) অনলাইন বেংকিং (Online Banking):

অনলাইন বেংকিঙে গ্রাহকক **বিল পৰিশোধ আৰু অনলাইন ধনৰ স্থানান্তৰৰ** সুবিধা দিয়ে। বেংকৰ দ্বাৰা প্রদান কৰা অনলাইন বেংকিং সেৱাৰ সহায়ত পেমেণ্ট সম্পন্ন কৰিব পৰা যায়।

(c) ই-ৱালেট (E-Wallets):

ই-ৱালেট হৈছে এনে ডিজিটেল ৱালেট, য'ত গ্রাহকে **ইলেকট্রনিকভাৱে ধন সংৰক্ষণ** কৰিব পাৰে। গ্রাহকে নিজৰ ই-ৱালেটত **ডেবিট/ক্রেডিট কার্ড, বেংক স্থানান্তৰ বা অন্য পেমেণ্ট পদ্ধতিৰ** জৰিয়তে ধন যোগ কৰিব পাৰে।

(d) ক্রিপ্ট'কাৰেন্সী (Cryptocurrencies):

Bitcoin, Ethereum আদিৰ দৰে ক্রিপ্ট'কাৰেন্সী ব্যৱহাৰ কৰি **আর্থিক মধ্যস্থৰ অবিহনে পেমেণ্ট** সম্পন্ন কৰিব পৰা যায়। এইবোৰ **বিকেন্দ্রীকৃত** (decentralized) আৰু **ব্লকচেইন প্রযুক্তিৰ** জৰিয়তে **সুৰক্ষিত আৰু স্বচ্ছ লেনদেন** নিশ্চিত কৰে।

(e) POS ছিষ্টেম (Point of Sale Systems):

POS ছিষ্টেম ব্যৱসায়ীৰ দ্বাৰা গ্রাহকৰ পৰা পেমেণ্ট গ্রহণৰ বাবে ব্যৱহাৰ কৰা হয়। এই ছিষ্টেমে গ্রাহকক **ক্রেডিট/ডেবিট কার্ড, মোবাইল ৱালেট বা অন্য ডিজিটেল পদ্ধতি** ব্যৱহাৰ কৰি পেমেণ্ট কৰিবলৈ সহায় কৰে।

(f) অনলাইন মার্কেটপ্লেছ (Online Marketplaces):

Amazon আৰু eBay-ৰ দৰে অনলাইন মার্কেটপ্লেছসমূহে গ্রাহকক **বহুবিধ পেমেণ্ট বিকল্প** প্রদান কৰে, যেনে ক্রেডিট/ডেবিট কার্ড, মোবাইল পেমেণ্ট, আৰু ডিজিটেল ৱালেট।

১০.৪.১ ডেবিট কার্ড

ডেবিট কার্ডৰ জৰিয়তে কৰা ডিজিটেল পেমেণ্ট হৈছে ইলেকট্রনিক লেনদেনৰ এক জনপ্রিয় পদ্ধতি। এই পদ্ধতি কেনেদৰে কাম কৰে, চাওঁ আহক:

1. প্রথমে, ডেবিট কার্ডধাৰীৰ **এটা বেংক একাউণ্ট** থাকিব লাগিব, য'ত সেই বেংকে **ডেবিট কার্ড প্রদান** কৰিব।
2. **ডেবিট কার্ডটো সেই একাউণ্টৰ সৈতে সংযুক্ত** হ'ব লাগিব আৰু **অনলাইন লেনদেনৰ বাবে সক্রিয়** হ'ব লাগিব।
3. কিনা-বেচাৰ সময়ত গ্রাহকে **ডেবিট কার্ড** পেমেণ্ট বিকল্প হিচাপে বাছনি কৰিব লাগে।
4. তৰ পাছত, গ্রাহকে **ডেবিট কার্ড নম্বৰ, মিয়াদ কালৰ তাৰিখ, আৰু CVV ক'ড (কার্ডৰ পিঠিত থকা তিনি সংখ্যাৰ সুৰক্ষা ক'ড)** প্রৱিষ্ট কৰিব লাগে।
5. তাৰপিছত, **লেনদেনৰ পৰিমাণ** উল্লেখ কৰি পেমেণ্ট প্রক্রিয়া আৰম্ভ হয়।
6. কিছুমান ক্ষেত্রত, **অতিৰিক্ত সুৰক্ষাৰ বাবে OTP (one-time password)** পাঠোৱা হয়, যি **ৰেজিষ্টাৰ কৰা মোবাইল নম্বৰত** আহে।
7. লেনদেন **অনুমোদিত হ'লে**, গ্রাহকৰ বেংক একাউণ্টৰ পৰা **উল্লেখ কৰা পৰিমাণৰ ধন ডেবিট** কৰা হয়।

ডেবিট কার্ডৰ জৰিয়তে ডিজিটেল পেমেণ্ট **সুবিধাজনক আৰু সুৰক্ষিত**, কিয়নো ইয়াত নগদ বা চেক বাহক নোহোৱাকৈ লেনদেন সম্ভৱ।

উল্লেখযোগ্য যে, **বহু বেংকে ডেবিট কার্ড লেনদেনত ৰিওৱার্ড আৰু কেশব্যাক** অফাৰ দিয়ে, যাৰ ফলত ই এক জনপ্রিয় পেমেণ্ট পদ্ধতিত পৰিণত হৈছে।

১০.৪.২ ক্রেডিট কার্ড

ক্রেডিট কার্ডৰ জৰিয়তে ডিজিটেল পেমেণ্ট সামগ্রী আৰু সেৱা অনলাইন বা পইণ্ট অফ চেলত (POS) ক্রয় কৰাৰ এক জনপ্রিয় পদ্ধতি। তলত ক্রেডিট কার্ডৰ জৰিয়তে ডিজিটেল পেমেণ্ট কৰাৰ কিছু ধাপ থাকে, সেয়া তলত উল্লেখ কৰা হ'ল—

(a) অনলাইন লেনদেনত ক্রেডিট কার্ডৰ ব্যৱহাৰ (Use of Credit Card for Online Transaction):

ধাপ ১ : ৰেবছাইট বা এপ বাছনি কৰক — য'ত আপুনি পেমেণ্ট কৰিব বিচাৰে, সেই **বিশ্বাসযোগ্য আৰু সুৰক্ষিত** ৰেবছাইট বা মোবাইল এপ বাছনি কৰক।

ধাপ ২ : সামগ্রী কার্টত যোগ কৰক — প্রয়োজনীয় সামগ্রী বা সেৱা কার্টত ভৰাওক।

ধাপ ৩ : Checkout কৰক — সকলো সামগ্রী যোগ কৰাৰ পাছত Checkout ত আগবাঢ়ক।

ধাপ ৪ : পেমেণ্ট পদ্ধতি বাছনি কৰক — পেমেণ্টৰ বাবে **"Credit Card"** বাছনি কৰক।

ধাপ ৫ : ক্রেডিট কার্ডৰ তথ্য দিয়ক — ক্রেডিট কার্ড নম্বৰ, মিয়াদ কাল, আৰু CVV (পিছফালে থকা ৩ সংখ্যাৰ সুৰক্ষা ক'ড) প্রবিষ্ট কৰক। সঠিক তথ্য দিয়াটো নিশ্চিত কৰক।

ধাপ ৬ : লেনদেন নিশ্চিত কৰক — ক্রয়ৰ সামগ্রী আৰু মুঠ পৰিমাণ নিশ্চিত কৰক।

ধাপ ৭ : পেমেণ্ট নিশ্চিত কৰক — সকলো তথ্য প্রদান কৰাৰ পাছত Confirm কৰক। OTP বা সুৰক্ষা ক'ড দিয়াৰ প্রয়োজন হ'ব পাৰে।

ধাপ ৮ : নিশ্চিতকৰণৰ বাবে অপেক্ষা কৰক — পেমেণ্ট নিশ্চিত কৰাৰ পাছত, কিছুমান ছেকেণ্ড অপেক্ষা কৰক; লেনদেন সফল হ'লে এক নির্দেশনা পাব।

ধাপ ৯ : ক্রেডিট কার্ড ষ্টেটমেণ্ট পৰীক্ষা কৰক — লেনদেন সঠিকভাৱে সম্পন্ন হৈছে নে নাই, সেইটো নিশ্চিত কৰিবলৈ আপোনাৰ ষ্টেটমেণ্ট পৰীক্ষা কৰক।

(b) POS (পইণ্ট অফ চেল) ত ক্রেডিট কার্ড ব্যৱহাৰ (Use of Credit Card at a Point of Sale):

ধাপ ১ : সামগ্রী বাছনি কৰক — দোকানৰ পৰা ক্রয় কৰিব লগা সামগ্রী বাছনি কৰক।

ধাপ ২ : Checkout কাউণ্টাৰত যাওক — সকলো সামগ্রী সংগ্রহ কৰাৰ পাছত Checkout কাউণ্টাৰত যাওক।

ধাপ ৩ : মূল্য প্রবিষ্ট কৰক — কেছিয়াৰে কোৱা মুঠ পৰিমাণ মেচিনত প্রবিষ্ট কৰক।

ধাপ ৪ : কার্ড swipe কৰক বা insert কৰক — ক্রেডিট কার্ড swipe বা chip থাকিলে insert কৰক।

ধাপ ৫ : PIN দিয়ক বা স্বাক্ষৰ কৰক — PIN নম্বৰ দিয়ক বা ৰচিদত স্বাক্ষৰ কৰক।

ধাপ ৬ : অনুমোদনৰ অপেক্ষা কৰক — মেচিনে বেংকৰ সৈতে যোগাযোগ কৰি লেনদেন অনুমোদন কৰে।

ধাপ ৭ : কার্ড আৰু ৰচিদ লওক — অনুমোদনৰ পাছত ৰচিদ লওক আৰু কার্ড উলিয়াই লওক।

এইদৰে, আপুনি সফলভাৱে ক্রেডিট কার্ডৰ জৰিয়তে POS-ত ডিজিটেল পেমেণ্ট সম্পন্ন কৰিব পাৰিব।

১০.৪.৩ ইউনিফাইড পেমেণ্ট ইণ্টাৰফেচ

Unified Payment Interface (UPI) হৈছে **National Payments Corporation of India (NPCI)**-এ বিকাশ কৰা এটা পেমেণ্ট ছিষ্টেম, যি **মোবাইল ডিভাইচৰ জৰিয়তে দুটা বেংক একাউণ্টৰ মাজত তৎক্ষণাত ধনৰ স্থানান্তৰ** সম্ভৱ কৰে। ই **ইণ্টাৰ-বেংক স্থানান্তৰ** ব্যৱস্থা, য'ত গ্রাহকে **Virtual Payment Address (VPA)** বা **ব্যাংক একাউণ্ট নম্বৰ আৰু IFSC ক'ড** ব্যৱহাৰ কৰি ধন পঠিয়াব পাৰে।

UPI ২০১৬ চনত আৰম্ভ হয় আৰু তাৰ পৰা এতিয়ালৈ ভাৰতত এটা জনপ্ৰিয় পেমেণ্ট পদ্ধতিত পৰিণত হৈছে। ইয়াৰ দ্বাৰা **২৪ ঘণ্টা, বছৰৰ ৩৬৫ দিন** পেমেণ্ট কৰিবলৈ সক্ষম, আৰু **OTP বা বেংক একাউণ্ট তথ্যৰ প্ৰয়োজন নথকে**।

UPI ৰ জৰিয়তে **বিল পৰিশোধ, মোবাইল ৰিচার্জ, টিকট বুকিং** আদিও কৰিব পাৰি, যি গ্ৰাহকসকলৰ বাবে এক সুবিধাজনক বিকল্প। UPI লেনদেন **ৰিয়েল-টাইমত সম্পন্ন হয়** আৰু **ধন তৎক্ষণাত প্ৰাপক একাউণ্টত জমা হয়**। এতিয়া এটা UPI লেনদেনত **সৰ্বাধিক ₹১ লাখ** পৰ্যন্ত পৰিমাণ অনুমোদিত।

UPI কেনেদৰে ব্যৱহাৰ কৰিব?

UPI ব্যৱহাৰৰ বাবে, গ্ৰাহকে **তেওঁৰ বেংকৰ বা অন্য third-party provider-ৰ UPI-enabled এপ** ডাউনলোড কৰিব লাগে।

তাৰপিছত **বেংক একাউণ্ট সংযোগ** কৰিব লাগে আৰু **একটা VPA (Virtual Payment Address)** সৃষ্টি কৰিব লাগে, যি UPI লেনদেনৰ বাবে তেওঁৰ unique চিনাক্তক ৰূপে কাম কৰে।

VPA সৃষ্টি কৰাৰ পিছত, গ্ৰাহকে **প্ৰাপকৰ VPA বা বেংক একাউণ্ট নম্বৰ আৰু IFSC কোড** দিয়াৰ লগতে **UPI PIN** দিয়ক, আৰু পেমেণ্ট সম্পন্ন কৰক।

UPI-এ ভাৰতত পেমেণ্ট ক্ষেত্ৰক এক বিপ্লৱী ৰূপ দিছে—ই পেমেণ্ট **দ্ৰুত, সুবিধাজনক আৰু সুৰক্ষিত** কৰি তুলিছে।

ই **ডিজিটেল পেমেণ্টৰ প্ৰসাৰ** ঘটোৱাৰ লগতে **অবেংকীয় আৰু আংশিক বেংকযুক্ত লোকসকলক** আনুষ্ঠানিক বেংকিং ব্যৱস্থালৈ আগবঢ়াই আনিছে।

UPI ৰ বিভিন্ন ধৰণৰ লেনদেন:

- **Peer-to-Peer (P2P):** ব্যক্তি-টু-ব্যক্তি ধন স্থানান্তৰ; বন্ধু-বান্ধৱীৰ মাজত ধন পঠিয়াবলৈ বা বিল ভাগ দিয়াৰ ক্ষেত্ৰত ব্যৱহাৰ হয়।
- **Peer-to-Merchant (P2M): পঞ্জীয়নভুক্ত ব্যৱসায়ীলৈ পেমেণ্ট** কৰিবলৈ ব্যৱহৃত। ইয়াৰ দ্বাৰা নগদৰ প্ৰয়োজন হ্ৰাস পায়।
- **Merchant-to-Peer (M2P):** ব্যৱসায়ীয়ে গ্ৰাহকক **ধন উভতাই দিয়াৰ ক্ষেত্ৰত** ব্যৱহৃত হয়।
- **Merchant-to-Merchant (M2M): দুটা ব্যৱসায়ীৰ মাজত পেমেণ্টৰ** বাবে ব্যৱহৃত হয়—যেনে B2B, জোগানদাৰ পেমেণ্ট আদিত।
- **Bill Payments: বিদ্যুৎ, পানী, গেছ, ফোন বিল** আদিৰ পৰিশোধত ব্যৱহৃত হয়।
- **Donations:** গ্ৰাহকে **চাৰিটেবল সংস্থা বা NGO-লৈ অনুদান** দিব পাৰে।

এইবোৰ হৈছে ভাৰতত উপলব্ধ UPI লেনদেনৰ ধৰণসমূহ। UPI-এ ভাৰতৰ পেমেণ্ট ব্যৱস্থাক সৰল, গতিশীল আৰু অধিক সুবিধাজনক কৰি তুলিছে।

১০.৪.৪ ই-ৱালেট (e-Wallets)

ই-ৱালেট, যাক **ডিজিটেল ৱালেট** বা **মোবাইল ৱালেট** বুলিও কোৱা হয়, হৈছে ইলেকট্রনিক পেমেণ্ট ছিষ্টেমৰ এটা ৰূপ, যাৰ জৰিয়তে ব্যৱহাৰকাৰীয়ে নিজৰ **পেমেণ্ট কার্ডৰ তথ্য ডিজিটেল ৰূপত সুৰক্ষিতভাৱে সংৰক্ষণ** কৰিব পাৰে। এই ৱালেটসমূহে ব্যৱহাৰকাৰীক **নগদ বা ক্রেডিট কার্ড লৈ নাফুৰাকৈ** লেনদেন কৰিবলৈ সক্ষম কৰে।

ই-ৱালেট ব্যৱহাৰ কৰি **অনলাইন কিনা-বেচা, বিল পৰিশোধ, মোবাইল ৰিচার্জ, আৰু ব্যক্তি-টু-ব্যক্তি (P2P) স্থানান্তৰ** কৰিব পৰা যায়। প্রচলিত কিছুমান ই-ৱালেটৰ ভিতৰত BHIM, **Paytm, Google Pay, PhonePe, Amazon Pay, আৰু PayPal** উল্লেখযোগ্য।

(a) BHIM

BHIM (Bharat Interface for Money) হৈছে **NPCI**-ৰ দ্বাৰা বিকাশ কৰা এটা **UPI-ভিত্তিক পেমেণ্ট এপ**। ইয়াৰ সহায়ত আপুনি নিজৰ মোবাইল ডিভাইচৰ জৰিয়তে **সৰাসৰি বেংক একাউণ্টৰ পৰা সুৰক্ষিতভাৱে তৎক্ষণাত লেনদেন** কৰিব পাৰে।

BHIM ব্যৱহাৰৰ ধাপসমূহ:

1. **Google Play Store** বা **Apple App Store**-ৰ পৰা BHIM UPI এপটো ডাউনলোড আৰু ইনষ্টল কৰক।
2. আপোনাৰ **বেংক সংযুক্ত মোবাইল নম্বৰ** দাঙি ধৰি **UPI PIN** নির্মাণ কৰি পঞ্জীয়ন কৰক।
3. আপোনাৰ বেংক একাউণ্ট সংযুক্ত কৰক।
4. একবাৰ সংযুক্ত হ'লে, আপোনি **Send Money, Request Money, Bill Payment** আদি কৰিব পাৰে।
5. 'Send Money' বাছনি কৰি **UPI ID বা বেংক তথ্য**, পৰিমাণ, আৰু UPI PIN দিয়ে পেমেণ্ট কৰক।
6. ধন গ্রহণ কৰিবলৈ আপোনাৰ **UPI ID শ্বেয়াৰ** কৰক বা 'Request Money' ব্যৱহাৰ কৰক।
7. **লেনদেনৰ ইতিহাস, একাউণ্ট ব্যৱস্থাপনা**, আৰু সীমা নির্ধাৰণো কৰিব পাৰে।

UPI PIN গোপন ৰাখিব আৰু কাকো দিব নালাগে। BHIM হৈছে এক **সুৰক্ষিত আৰু সুবিধাজনক** পেমেণ্ট পদ্ধতি।

(b) Google Pay

Google Pay হৈছে ভাৰতৰ আটাইতকৈ জনপ্ৰিয় UPI সেৱাসমূহৰ অন্যতম। এই এপটো **Android আৰু iOS** দুয়ো প্লেটফৰ্মতে উপলব্ধ।

Google Pay ব্যৱহাৰৰ ধাপসমূহ:

1. Google Play Store বা Apple App Store-ৰ পৰা **Google Pay ডাউনলোড** কৰক।
2. আপোনাৰ **Google Account** লগ ইন কৰক বা নতুন একাউণ্ট সৃষ্টি কৰক।
3. **Payment Method** হিচাপে ক্ৰেডিট/ডেবিট কার্ড, বেংক একাউণ্ট বা গেটৱে সংযুক্ত কৰক।
4. সংযুক্ত হোৱাৰ পাছত **ব্যৱসায়ীৰ ওচৰত পেমেণ্ট** কৰিবলৈ ব্যৱহাৰ কৰক।
5. এপ খুলি "Pay" বাছনি কৰক।
6. **QR ক'ড স্কেন কৰক** বা **টার্মিনেলৰ ওচৰত মোবাইল ধৰি ৰাখক**।
7. পৰিমাণ দিয়ক, তথ্য প্ৰদান কৰক।
8. **PIN বা বায়োমেট্ৰিকৰ** জৰিয়তে পেমেণ্ট নিশ্চিত কৰক।
9. পেমেণ্ট সফল হ'লে **নটিফিকেশ্যন পাব**।

Google Pay-এ পেমেণ্টক **দ্ৰুত, সহজ, আৰু সুৰক্ষিত** কৰি তোলে।

(c) Paytm

Paytm হৈছে ভাৰতৰ আন এটা জনপ্ৰিয় UPI আৰু মোবাইল ৱালেট প্লেটফৰ্ম। ই **ধন পঠিয়াব, গ্ৰহণ কৰিব, বিল দিব, টিকট বুকিং** আদিত সহায় কৰে।

Paytm ব্যৱহাৰৰ ধাপসমূহ:

1. Google Play Store বা Apple App Store-ৰ পৰা **Paytm ডাউনলোড** কৰক।
2. মোবাইল নম্বৰ, ইমেইল ID, আৰু পাছৱৰ্ড দিয়ক।
3. **Paytm Wallet-ত ধন যোগ** কৰক বা **বেংক একাউণ্ট সংযুক্ত** কৰক।
4. 'Pay' বাছনি কৰক।
5. প্ৰাপকৰ **মোবাইল নম্বৰ বা UPI ID**, পৰিমাণ, আৰু পেমেণ্ট ম'ড বাছনি কৰক।
6. তথ্য প্ৰদাৰ কৰি 'Proceed to Pay' ক্লিক কৰক।
7. OTP বা PIN প্ৰৱিষ্ট কৰি পেমেণ্ট নিশ্চিত কৰক।
8. সফল হ'লে **SMS আৰু এপত নিশ্চিতকৰণ বার্তা** পাব।

Paytm-এ **ৰিচার্জ, মুভি/ফ্লাইট টিকট, বিল পেমেণ্ট** আদিও প্ৰদান কৰে।

(d) PhonePe

PhonePe হৈছে এটা UPI-ভিত্তিক ডিজিটেল পেমেণ্ট প্লেটফর্ম, যি **ধন স্থানান্তৰ, বিল পেমেণ্ট, ৰিচার্জ** আদিৰ সুবিধা দিয়ে।

PhonePe ব্যৱহাৰৰ ধাপসমূহ:

1. PhonePe ডাউনলোড কৰি **মোবাইল নম্বৰ, ইমেইল ID**, আৰু পাছৱর্ড দিয়ক।
2. **বেংক একাউণ্ট সংযুক্ত** কৰক বা UPI ID ব্যৱহাৰ কৰক।
3. 'Send' বাছনি কৰক।
4. প্ৰাপকৰ মোবাইল নম্বৰ বা UPI ID দিয়ক।
5. পৰিমাণ, পেমেণ্ট ম'ড বাছনি কৰক।
6. তথ্য প্ৰদাৱ কৰি 'Send' টিপক।
7. PIN বা OTP দিয়ক।
8. সফল হ'লে নিশ্চিতকৰণ পাব।

PhonePe-এ **অন্যান্য সেৱা** যেনে টিকট বুকিং, বিল, ৰিচার্জ আদি প্ৰদান কৰে।

(e) Amazon Pay

Amazon Pay হৈছে **ডিজিটেল ৱালেট**, যি **অনলাইন পেমেণ্ট আৰু ট্ৰেন্সফাৰ** কৰিবলৈ ব্যৱহৃত হয়।

Amazon Pay ব্যৱহাৰৰ ধাপসমূহ:

1. Amazon একাউণ্টত লগ ইন কৰক।
2. ডেবিট/ক্ৰেডিট কার্ড বা বেংক একাউণ্ট যোগ কৰি **Amazon Pay-ত ধন যোগ** কৰক।
3. পেমেণ্ট পৃষ্ঠাত 'Amazon Pay' বাছনি কৰক।
4. লগ-ইন কৰক আৰু 'Pay Now' ক্লিক কৰক।
5. যদি যথেষ্ট ব্যালেন্স নাই, তেন্তে সংযুক্ত কার্ড বা বেংকৰ জৰিয়তে পেমেণ্ট কৰক।
6. পৰিমাণ দিয়ক, তথ্য প্ৰদাৱ কৰক।
7. 'Pay Now' ক্লিক কৰি পেমেণ্ট সম্পন্ন কৰক।
8. সফল হ'লে **Amazon, ইমেইল, আৰু ৰেবছাইটত নিশ্চিতকৰণ বার্তা** পাব।

Amazon Pay-এ বিল পেমেণ্ট, ৰিচার্জ, ধন স্থানান্তৰ আদি সুবিধা দিয়ে।

ই-ৱালেট ব্যৱহাৰৰ ক্ষেত্ৰত সাৱধানতাসমূহ (Precautions for Using e-Wallets)

1. **দৃঢ় পাছৱর্ড ব্যৱহাৰ কৰক** — সহজে অনুমান কৰিব পৰা নহয় আৰু প্ৰতিটো একাউণ্টৰ বাবে বেলেগ পাছৱর্ড দিয়ক।

2. **Two-factor authentication সক্ৰিয় কৰক** — এই ব্যৱস্থা আপোনাৰ একাউণ্ট অধিক সুৰক্ষিত কৰে।
3. **এপটো সদায় আপডেট ৰাখক** — নতুন সুৰক্ষা বৈশিষ্ট্যৰ বাবে।
4. **Public Wi-Fi এপ ব্যৱহাৰ নকৰিব** — সুৰক্ষাহীন নেটৱৰ্কত হেকাৰসকলে তথ্য চুৰি কৰিব পাৰে।
5. প্ৰেৰণকাৰীক নিশ্চিত কৰক — পেমেণ্ট কৰাৰ আগতে প্ৰেৰণকাৰীক নিশ্চিত কৰক।
6. **বিশ্বাসযোগ্য উৎসৰ পৰা এপ ডাউনলোড কৰক** — আপোনাৰ মোবাইলৰ অফিচিয়েল এপ ষ্টোৰ ব্যৱহাৰ কৰক।
7. **লেনদেনৰ ইতিহাস পৰীক্ষা কৰক** — অননুমোদিত লেনদেন পৰ্যবেক্ষণ কৰক।
8. **ডিভাইচ সুৰক্ষিত ৰাখক** — পাছৱৰ্ড/PIN, antivirus ব্যৱহাৰ কৰি সংৰক্ষণ কৰক।

এই সাৱধানতাসমূহ মানিলে, আপোনাৰ ই-ৱালেট **সুৰক্ষিত** থাকিব আৰু **ব্যক্তিগত আৰু বিত্তীয় তথ্য** ৰক্ষা পাব।

১০.৪.৫ আনষ্ট্ৰাকচাৰ্ড ছাপ্লিমেণ্টাৰী চাৰ্ভিচ ডাটা

USSD (Unstructured Supplementary Service Data) হৈছে এটি প্ৰ'টকল, যাৰ জৰিয়তে **মোবাইল ডিভাইচ আৰু সেৱা প্ৰদানকাৰীৰ কম্পিউটাৰ ছিষ্টেমৰ মাজত যোগাযোগ** স্থাপন হয়। ই হৈছে **এটা ছেছন-ভিত্তিক, ৰিয়েল-টাইম বার্তা সেৱা**, যিয়ে ব্যৱহাৰকাৰীক **মেনু-চালিত ইণ্টাৰফেচ**ৰ সহায়ত সেৱা প্ৰদানকাৰীৰ ছিষ্টেমৰ সৈতে যোগাযোগ কৰিবলৈ সক্ষম কৰি তোলে, **সৰু আৰু সহজে মনত ৰখা ক'ড** ব্যৱহাৰ কৰি।

USSD বার্তা সাধাৰণতে **ব্যৱহাৰকাৰীয়ে মোবাইলত সৰু ক'ড ডায়েল কৰাৰ** জৰিয়তে আৰম্ভ হয়, যাৰ পাছত কিছু সংখ্যা বা অক্ষৰ থাকে যিয়ে তেওঁ বিচৰা নির্দিষ্ট সেৱাটোক প্ৰতিনিধিত্ব কৰে। সেৱা প্ৰদানকাৰীৰ ছিষ্টেমে উত্তৰস্বৰূপে **এটা মেনু প্ৰদান কৰে**, যি ব্যৱহাৰকাৰীয়ে অধিক সংখ্যাৰ বা অক্ষৰৰ সহায়ত নেভিগেট কৰিব পাৰে।

USSD **মোবাইল বেংকিং, মোবাইল ধন স্থানান্তৰ, আৰু মোবাইল ৰিচার্জ সেৱাৰ** ক্ষেত্ৰত ব্যাপকভাৱে ব্যৱহৃত হয়। ই **বিশেষকৈ উন্নয়নশীল দেশসমূহত জনপ্ৰিয়**, য'ত বহু লোকৰ ওচৰত **স্মাৰ্টফোন বা মোবাইল এপ উপলব্ধ নহয়**, কাৰণ **USSD সর্বসাধাৰণ মোবাইল ফোনতেও চলিব পাৰে**। ই **দুর্বল নেটৱৰ্ক বা ধীৰ ইণ্টাৰনেট সংযোগ থকা অঞ্চলত**ও কার্যকৰী হোৱাত ই বিশ্বাসযোগ্য বুলি গণ্য।

ব্যৱহাৰকাৰীয়ে নিজৰ মোবাইল অপাৰেটৰে প্ৰদান কৰা বিভিন্ন সেৱা **মাত্ৰ এটা কোড ডায়েল কৰি** লাভ কৰিব পাৰে।

USSD ব্যৱহাৰৰ এটা উদাহৰণ (বেলেন্স চেক কৰিবলৈ):

1. আপোনাৰ মোবাইল ফোনৰ পৰা ***123# ডায়েল** কৰক।
2. কল বুটাম টিপক।
3. আপোনাৰ ফোনৰ স্ক্রিনত এটা বার্তা আহিব, য'ত এটা বিকল্প বাছনি কৰিবলৈ কোৱা হ'ব।
4. **বিকল্প ১ বাছনি কৰক** — একাউণ্ট বেলেন্স চাবলৈ।
5. স্ক্রিনত আপোনাৰ **বর্তমান একাউণ্ট বেলেন্স** প্রদর্শন হ'ব।

এইটো USSD ব্যৱহাৰৰ এটা উদাহৰণ। আন সাধাৰণ ব্যৱহাৰসমূহত আছে **ৰিচার্জ, ডাটা প্লেন চাবস্ক্রিপচন, ধন স্থানান্তৰ** আদিৰ সুবিধা। **ইণ্টাৰনেট নথকা বা এপ নব্যৱহাৰ কৰা ব্যৱহাৰকাৰীৰ বাবে** USSD হৈছে এক **দ্রুত আৰু সুবিধাজনক** পদ্ধতি।

১০.৪.৬ আধাৰ-ভিত্তিক পেমেণ্ট

আধাৰ-ভিত্তিক পেমেণ্ট হৈছে এক ডিজিটেল পেমেণ্ট ছিষ্টেম, যাৰ সহায়ত **ভোক্তাই নিজৰ আধাৰ নম্বৰ আৰু বায়োমেট্রিক প্রমাণীকৰণ ব্যৱহাৰ কৰি লেনদেন** কৰিব পাৰে। আধাৰ হৈছে ভাৰত চৰকাৰে নির্গত কৰা **১২ সংখ্যাৰ এটা অনন্য পৰিচয় নম্বৰ**, য'ত **আঙুলিৰ ছাপ আৰু চকুৰ স্কেনৰ দৰে বায়োমেট্রিক তথ্য** অন্তর্ভুক্ত থাকে।

এই পেমেণ্ট ছিষ্টেমে **ব্যৱহাৰকাৰীৰ বেংক একাউণ্ট আধাৰৰ সৈতে সংযোগ** কৰিবলৈ দিয়ে আৰু **বায়োমেট্রিক প্রমাণীকৰণৰ জৰিয়তে পেমেণ্ট** সম্পন্ন কৰিব পৰা যায়—ব্যৱসায়ী প্রতিষ্ঠানত বা অনলাইন পেমেণ্টত। ই বিশেষকৈ **তেওঁলোকৰ বাবে সুবিধাজনক**, যিসকলে **স্মার্টফোন বা ডেবিট কার্ড নাথাকে**।

ব্যৱহাৰকাৰীয়ে আধাৰ-ভিত্তিক পেমেণ্ট ব্যৱহাৰ কৰিবলৈ:

1. **বেংকত বা আধাৰ ৰেবচাইটত** গৈ **আপোনাৰ বেংক একাউণ্ট আধাৰৰ সৈতে সংযোগ** কৰিব লাগে।
2. সংযুক্ত হোৱাৰ পিছত, **POS টার্মিনেলত বা অনলাইনত আধাৰ নম্বৰ দিয়ক** আৰু **আঙুলিৰ ছাপ বা অন্য বায়োমেট্রিক প্রমাণীকৰণ** দিয়ক।
3. প্রমাণীকৰণ সফল হ'লে লেনদেন সম্পন্ন হয়।

এই ব্যৱস্থা **আর্থিক অন্তর্ভুক্তি আগবঢ়োৱা** লক্ষ্যৰে **ভাৰতজুৰি** প্রয়োগ কৰা হৈছে। ই **বিশেষকৈ গ্রাম্য অঞ্চলসমূহত**, য'ত **বেংকিং সেৱা সীমিত আৰু স্মার্টফোন বা ডেবিট কার্ড অনুপস্থিত**, তেনে ঠাইত অতি সহায়ক হৈ পৰিছে।



অগ্রগতি নিৰীক্ষণ

প্রশ্ন নং ২ : সঠিক বিকল্প বাচনি কৰকঃ

1. তলৰ কোনটো ডিজিটেল পেমেণ্টৰ এটা পদ্ধতি নহয়?

(ক) মোবাইল পেমেণ্ট

(খ) অনলাইন বেংকিং

(গ) নগদ পেমেণ্ট

(ঘ) ই-ৱালেট

2 ডেবিট কার্ডৰ জৰিয়তে ডিজিটেল পেমেণ্ট ব্যৱহাৰৰ সুবিধাসমূহৰ ভিতৰত কোনটো সঠিক?

(ক) এই পদ্ধতিত লেনদেনৰ উচ্চ সুৰক্ষা প্রদান কৰে।

(খ) নগদ বা চেক বহন নকৰাকৈ লেনদেন কৰাৰ সুবিধা দিয়ে।

(গ) লেনদেনত ৰিৱার্ড আৰু কেছবেক লাভ কৰিব পাৰে।

(ঘ) ওপৰৰ সকলো উত্তৰ সঠিক

3 অনলাইন লেনদেনত ক্রেডিট কার্ড ব্যৱহাৰ কৰি ডিজিটেল পেমেণ্ট কৰাৰ এটা ধাপ কোনটো?

(ক) এটা ৱেবছাইট বা এপ বাছনি কৰা

(খ) আপোনাৰ কার্ড swipe বা insert কৰা

(গ) ক্রয় পৰিমাণ প্রবিষ্ট কৰা

(ঘ) ওপৰৰ কোনোটো নহয়

4 Unified Payments Interface (UPI) ব্যৱহাৰ কৰি ডিজিটেল পেমেণ্ট কৰাৰ ক্ষেত্রত তলৰ কোনটো সুবিধা নহয়?

(ক) ই নিৰবচ্ছিন্ন আৰু তৎক্ষণাত লেনদেনৰ সুবিধা দিয়ে।

(খ) ইয়াৰ সহায়ত বিল পেমেণ্ট আৰু ধন স্থানান্তৰ কৰিব পাৰি।

(গ) ইয়াত লেনদেনৰ বাবে শাৰীৰিক কার্ডৰ প্রয়োজন হয়।

(ঘ) ই ২৪x৭ লেনদেনৰ সুবিধা দিয়ে।

5 Point of Sale (POS)-ত ক্রেডিট কার্ড ব্যৱহাৰ কৰি ডিজিটেল পেমেণ্ট কৰাৰ এটা ধাপ কোনটো?

(ক) ক্রেডিট কার্ডৰ তথ্য প্রবিষ্ট কৰা

(খ) লেনদেনৰ তথ্য প্রদান কৰা

(গ) সামগ্রী কার্টত যোগ কৰা

(ঘ) ওপৰৰ কোনোটো নহয়



১০.৫ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ

• **ডিজিটেল পেমেণ্ট** হৈছে এক ইলেকট্রনিক লেনদেন পদ্ধতি, যাৰ জৰিয়তে ব্যক্তি আৰু ব্যৱসায়ীকেইজনে **নগদৰ প্রয়োজন নোহোৱাকৈ অনলাইনত ধন স্থানান্তৰ, বিল পৰিশোধ, আৰু সামগ্রী কিনিব** পাৰে।

• ডিজিটেল পেমেণ্ট গুৰুত্বপূর্ণ কাৰণ ই **সুবিধা, গতি, সুৰক্ষা, ব্যয়-দক্ষতা, আর্থিক অন্তর্ভুক্তি আৰু অধিক কার্যকৰিতা** আগবঢ়ায়।

• ডিজিটেল পেমেণ্টৰ ইতিহাস **১৯৭০ চনৰ আৰম্ভণ হৈছে, ই ইলেকট্রনিক ফাণ্ড স্থানান্তৰ (EFT) ছিষ্টেমৰ পৰা আৰম্ভ হয়**, যদিও ১৯৯০ৰ অন্তিম সময় আৰু ২০০০ৰ আৰম্ভণিতে ইণ্টাৰনেট আৰু ই-কমার্চৰ বিকাশৰ লগে লগে ইয়াৰ জনপ্রিয়তা বৃদ্ধি পায়।

• ডিজিটেল পেমেণ্টৰ উপাদানসমূহত আছে **পেমেণ্ট গেটৱে, ডিজিটেল ৱালেট, পইণ্ট অফ ছেল (POS) টার্মিনেল, পেমেণ্ট প্রচেছৰ, মোবাইল পেমেণ্ট**, আৰু **ইলেকট্রনিক ফাণ্ড স্থানান্তৰ (EFT)**।

• ডিজিটেল পেমেণ্টৰ ধৰণসমূহত আছে **অনলাইন বেংকিং, ই-ৱালেট, মোবাইল পেমেণ্ট, কণ্টাক্টলেছ পেমেণ্ট**, আৰু **পিয়াৰ-টু-পিয়াৰ (P2P) পেমেণ্ট**।

• **ডেবিট কার্ড আৰু ক্রেডিট কার্ড** হৈছে অনলাইন আৰু POS লেনদেনৰ বাবে জনপ্রিয় ডিজিটেল পেমেণ্টৰ পদ্ধতি।

• ডেবিট বা ক্রেডিট কার্ডৰ জৰিয়তে ডিজিটেল পেমেণ্ট **সুবিধাজনক আৰু সুৰক্ষিত**, আৰু বহু বেংকে এই লেনদেনত **ৰিৱার্ড আৰু কেছবেক** দিয়ে।

• **Unified Payment Interface (UPI)** হৈছে NPCI-ৰ দ্বাৰা বিকাশ কৰা এটা **ইণ্টাৰ-বেংক স্থানান্তৰ ছিষ্টেম**, যি মোবাইল ডিভাইচৰ জৰিয়তে দুটা বেংক একাউণ্টৰ মাজত তৎক্ষণাত ধন স্থানান্তৰ সহজ কৰি তোলে।

• UPI ব্যৱহাৰ কৰি **২৪ ঘণ্টা আৰু বছৰৰ ৩৬৫ দিন** Virtual Payment Address বা বেংক একাউণ্ট নম্বৰ আৰু IFSC ক'ডৰ সহায়ত ধন স্থানান্তৰ কৰিব পৰা যায়, লগতে **বিল পেমেণ্ট, মোবাইল ৰিচার্জ, টিকট বুকিং** আদি মূল্য সংযোজিত সেৱাও প্রদান কৰে।

• UPI-এ ভাৰতত **পেমেণ্ট পদ্ধতিক এক বিপ্লৱী ৰূপত পৰিৱর্তন** কৰিছে, যিয়ে **ধন স্থানান্তৰক অধিক তৎক্ষণাত, সুবিধাজনক আৰু সুৰক্ষিত** কৰি তোলে আৰু ডিজিটেল পেমেণ্টক উৎসাহিত কৰাত উল্লেখযোগ্য ভূমিকা গ্রহণ কৰিছে।

• **ই-ৱালেট** হৈছে ইলেকট্রনিক পেমেণ্ট ছিষ্টেমৰ এটা ৰূপ, যিয়ে **পেমেণ্ট কার্ডৰ তথ্য ডিজিটেল ৰূপত সুৰক্ষিতভাৱে সংৰক্ষণ** কৰে।

• ই-ৱালেট ব্যৱহাৰ কৰি **ব্যৱহাৰকাৰীয়ে নগদ বা ক্রেডিট কার্ড বহন নকৰাকৈ তৎক্ষণাত আৰু সুবিধাজনকভাৱে লেনদেন** কৰিব পাৰে।

• ই-ৱালেট ব্যৱহাৰ কৰি **অনলাইন কেনাকাটা, বিল পেমেণ্ট, মোবাইল ৰিচার্জ আৰু ব্যক্তি-টু-ব্যক্তি ধন স্থানান্তৰ** কৰা যায়।

• জনপ্রিয় কিছুমান ই-ৱালেট হৈছে **Paytm, Google Pay, PhonePe, Amazon Pay**, আৰু **PayPal**।

• ই-ৱালেটৰ সহায়ত **লেনদেন অধিক সুবিধাজনক আৰু সুৰক্ষিত** হৈ পৰিছে, বিশেষকৈ আজিৰ ডিজিটেল যুগত।

• **আধাৰ-ভিত্তিক পেমেণ্ট** হৈছে এটা ডিজিটেল পেমেণ্ট ছিষ্টেম, যাৰ সহায়ত **ভোক্তাই নিজৰ আধাৰ নম্বৰ আৰু বায়োমেট্ৰিক প্ৰমাণীকৰণ** ব্যৱহাৰ কৰি লেনদেন কৰিব পাৰে।

• আধাৰ-ভিত্তিক পেমেণ্ট ছিষ্টেম **তেওঁলোকৰ বাবে বিশেষভাবে ডিজাইন কৰা হৈছে,** যিসকলে **স্মাৰ্টফোন বা ডেবিট কাৰ্ড নাথাকে,** আৰু এই ছিষ্টেম **গ্ৰাম্য অঞ্চলত, য'ত পৰম্পৰাগত বেংকিং সেৱা সীমিত,** তাত অতি সহায়ক হিচাপে কাম কৰিছে।

১০.৬ অগ্রগতিৰ খতিয়ান

১ নং উত্তৰ প্রশ্নৰ:

(ক) (iv) (খ) (iii) (গ) (iii) (ঘ) (i) (ঙ) (i)

২ নং উত্তৰ প্রশ্নৰ:

1 (গ) 2 (ঘ) 3 (ক) 4 (গ) 5 (খ)

১০.৭ অধিক জানিবলৈ

1) Cyber Crime Impact in the New Millennium, by R. C Mishra, Auther Press. Edition 2010.
2) Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by SumitBelapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)
3) Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
4) Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
5) Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.

6) Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.
7) Fundamentals of Network Security by E. Maiwald, McGraw Hill.



১১.১০ আৰ্হি প্ৰশ্ন

প্ৰশ্ন ১ : পৰম্পৰাগত পেমেণ্ট পদ্ধতিসমূহৰ তুলনাত ডিজিটেল পেমেণ্ট ব্যৱহাৰ কৰাৰ কিছুমান সুবিধা কি ?

প্ৰশ্ন ২ : ডিজিটেল পেমেণ্টৰ ইতিহাস বৰ্ণনা কৰক আৰু সময়ৰ সৈতে ই কেনেদৰে উন্নতি লাভ কৰিছে ?

প্ৰশ্ন ৩ : ডিজিটেল পেমেণ্টত জড়িত বিভিন্ন উপাদান কি কি, আৰু এইবোৰে কেনেদৰে একে লগত কাম কৰি এক নিৰবচ্ছিন্ন অভিজ্ঞতা প্ৰদান কৰে ?

প্ৰশ্ন ৪ : ডিজিটেল পেমেণ্টত জড়িত বিভিন্ন পক্ষ কোন-কোন, আৰু তেওঁলোকে এই প্ৰক্ৰিয়াত কেনেকুৱা ভূমিকা পালন কৰে ?

প্ৰশ্ন ৫ : ডিজিটেল পেমেণ্টৰ কিছুমান উদীয়মান প্ৰৱণতা কি আৰু এইবোৰে ভৱিষ্যতৰ বিত্তীয় পৰিসৰ কেনেদৰে গঢ়ি তোলে ?

প্ৰশ্ন ৬ : ডিজিটেল পেমেণ্টে কেনেদৰে আৰ্থিক অন্তৰ্ভুক্তি আগবঢ়ায়, আৰু সকলোৰে বাবে সমান সুবিধা নিশ্চিত কৰিবলৈ কিছুমান চেলেঞ্জ কি কি সমাধান কৰিব লাগিব ?

প্ৰশ্ন ৭ : ডিজিটেল পেমেণ্ট বুলিলে কি বুজায়, আৰু ই পৰম্পৰাগত পেমেণ্টৰ পৰা কেনেদৰে ভিন্ন ?

প্ৰশ্ন ৮ : ডিজিটেল পেমেণ্টৰ আটাইতকৈ সাধাৰণ কিছুমান পদ্ধতি কি, আৰু সেইবোৰ কেনেদৰে কাম কৰে ?

প্ৰশ্ন ৯ : মোবাইল পেমেণ্ট বুলিলে কি বুজায়, আৰু কিছুমান জনপ্ৰিয় মোবাইল ৱালেটৰ নাম লিখা।

প্ৰশ্ন ১০ : অনলাইন বেংকিঙে কেনেদৰে ডিজিটেল পেমেণ্ট সহজ কৰি তোলে, আৰু বেংকে অনলাইন পেমেণ্টৰ বাবে গ্ৰাহকক কি কি সেৱা দিয়ে ?

প্ৰশ্ন ১১ : ই-ৱালেট বুলিলে কি বুজায়, আৰু ই কেনেদৰে কাম কৰে ? বৰ্তমান উপলব্ধ কিছুমান জনপ্ৰিয় ই-ৱালেটৰ নাম লিখা।

প্ৰশ্ন ১২ : ক্ৰিপ্ট'কাৰেন্সী বুলিলে কি বুজায়, আৰু এইবোৰে কেনেকৈ বিত্তীয় মধ্যস্থতাৰ প্ৰয়োজন নোহোৱাকৈ গ্ৰাহকক পেমেণ্ট কৰিবলৈ সক্ষম কৰে ?

প্ৰশ্ন ১৩ : ই-ৱালেট বুলিলে কি বুজায়, আৰু ই কেনেকৈ কাম কৰে ? ভাৰতত ব্যৱহৃত কিছুমান জনপ্ৰিয় ই-ৱালেটৰ নাম লিখা।

প্ৰশ্ন ১৪ : BHIM UPI বুলিলে কি বুজায়, আৰু এইটো ব্যৱহাৰ কৰি কেনেদৰে ডিজিটেল পেমেণ্ট আৰম্ভ কৰিব পাৰি? BHIM UPI এপ ব্যৱহাৰৰ ধাপ-ধাপ প্ৰক্ৰিয়াটো ব্যাখ্যা কৰক।

প্ৰশ্ন ১৫ : Google Pay বুলিলে কি বুজায়, আৰু এইটো ব্যৱহাৰ কৰি কেনেদৰে ব্যৱসায়িক স্থানত পেমেণ্ট কৰিব পাৰি? Google Pay ব্যৱহাৰ কৰি পেমেণ্ট কৰাৰ ধাপ-ধাপ পদ্ধতি বৰ্ণনা কৰক।

প্ৰশ্ন ১৬ : Paytm বুলিলে কি বুজায়, আৰু কেনেকৈ এইটো ব্যৱহাৰ কৰি ধন পঠিয়াব, গ্ৰহণ কৰিব, বিল দিব আৰু চিনেমাৰ টিকট বুক কৰিব পাৰি? Paytm ব্যৱহাৰ কৰি পেমেণ্ট কৰাৰ ধাপ-ধাপ পদ্ধতি বৰ্ণনা কৰক।

প্ৰশ্ন ১৭ : আধাৰ-ভিত্তিক পেমেণ্ট বুলিলে কি বুজায়, আৰু ই কেনেদৰে কাম কৰে?

প্ৰশ্ন ১৮ : গ্ৰাম্য অঞ্চলৰ লোকসকলৰ বাবে আধাৰ-ভিত্তিক পেমেণ্ট কেনেকৈ লাভজনক হয়?

প্ৰশ্ন ১৯ : বেংক একাউণ্টখন আধাৰ নম্বৰৰ সৈতে সংযোগ কৰাৰ প্ৰক্ৰিয়া কি?

প্ৰশ্ন ২০ : আধাৰ-ভিত্তিক পেমেণ্টত বায়োমেট্ৰিক প্ৰমাণীকৰণে কেনেকৈ সুৰক্ষা নিশ্চিত কৰে?

অধ্যায় ১১: ডিজিটেল পেমেণ্টত সুৰক্ষা সম্পৰ্কীয় দিশ

অধ্যায় গাঁথনি

১১.১ উদ্দেশ্য
১১.২ পৰিচয়
১১.৩ ডিজিটেল পেমেণ্টত সাধাৰণ ঠগবাজি
১১.৩.১ পৰিচয় চুৰি আৰু ফিছিং স্কেম
১১.৩.২ অনাধিকাৰ লেনদেন আৰু পেমেণ্ট গেটৱে ঠগবাজি
১১.৩.৩ নকল পেমেণ্ট এপ আৰু মেলৱেৰ আক্রমণ
১১.৩.৪ QR ক'ড ঠগবাজি আৰু SIM ছৱাপ ঠগবাজি
১১.৪ ডিজিটেল পেমেণ্টৰ ঠগবাজিৰ ৰোধ ব্যৱস্থা
১১.৪.১ নিৰাপদ ব্রাউজিং আৰু পাছৱৰ্ড ব্যৱস্থাপনা
১১.৪.২ দুই-স্তৰীয় প্রমাণীকৰণ আৰু বায়োমেট্রিক প্রমাণীকৰণ
১১.৪.৩ পাব্লিক Wi-Fi এৰাই চলা আৰু বিশ্বাসযোগ্য পেমেণ্ট গেটৱে ব্যৱহাৰ
১১.৪.৪ লেনদেন ইতিহাস নিয়মিত পৰীক্ষা আৰু লেনদেন সতর্কতা নির্ধাৰণ
১১.৫ ডিজিটেল পেমেণ্ট সম্পর্কে RBI নির্দেশনা
১১.৫.১ ডিজিটেল পেমেণ্টত RBIৰ ভূমিকা
১১.৫.২ ডিজিটেল লেনদেনত গ্রাহক সুৰক্ষাৰ ক্ষেত্রত RBI নির্দেশনা
১১.৫.৩ অভিযোগ নিষ্পত্তি আৰু বিবাদ নিষ্পত্তি প্রক্রিয়া
১১.৬ পেমেণ্ট চেটলমেণ্ট আইন, ২০০৭
১১.৬.১ পেমেণ্ট চেটলমেণ্ট আইন, ২০০৭ ৰ পৰিচয়
১১.৬.২ পেমেণ্ট ছিষ্টেম, গেটৱে আৰু চেটলমেণ্ট সম্পর্কীয় বিধান
১১.৬.৩ অনাধিকাৰ লেনদেন আৰু ঠগবাজিৰ আইনী প্রভাৱ
১১.৭ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ
১১.৮ অগ্রগতিৰ খতিয়ান
১১.৯ অধিক জানিবলৈ
১১.১০ আৰ্হি প্রশ্ন

১১.১ উদ্দেশ্য

এই অধ্যায়টো অধ্যয়ন কৰি আপুনি—

- পৰিচয় চুৰি, ফিছিং স্কেম, অনাধিকাৰ লেনদেন, নকল পেমেণ্ট এপ, আৰু QR ক'ড ঠগবাজি আদিৰ দৰে ডিজিটেল পেমেণ্টত সাধাৰণ ঠগবাজিৰ ধৰণ বুজিব পাৰিব

- ডিজিটেল পেমেণ্টৰ ঠগবাজিৰ ৰোধৰ উপায় যেনে সুৰক্ষিত ব্ৰাউজিং, দুই-স্তৰীয় প্ৰমাণীকৰণ, পাব্লিক Wi-Fi এৰাই চলা, আৰু নিয়মিত লেনদেন পৰীক্ষা আদিৰ বিষয়ে জানিবলৈ পাব
- ডিজিটেল পেমেণ্ট সম্পৰ্কে RBI দ্বাৰা প্ৰদত্ত নিৰ্দেশনা, গ্ৰাহক সুৰক্ষা, অভিযোগ নিষ্পত্তি আৰু বিবাদ নিষ্পত্তি প্ৰক্ৰিয়াৰ বিষয়ে জানিবলৈ সক্ষম হ'ব
- পেমেণ্ট চেটলমেণ্ট আইন, ২০০৭ৰ মূল বিধানসমূহ, পেমেণ্ট ছিষ্টেম আৰু গেটৱে সম্পৰ্কে বুজিবলৈ, আৰু অনাধিকাৰ লেনদেন বা ঠগবাজিৰ ক্ষেত্ৰত প্ৰণীত আইনী দিশসমূহ উপলব্ধি কৰিবলৈ সমৰ্থ হ'ব

১১.২ পৰিচয়

ডিজিটেল পেমেণ্টে সাম্প্ৰতিক বছৰবোৰত ব্যক্তি আৰু ব্যৱসায়সমূহক আৰ্থিক লেনদেন কৰাৰ এক সুবিধাজনক আৰু নিৰাপদ মাধ্যম প্ৰদান কৰিছে। কিন্তু ডিজিটেল পেমেণ্টৰ ব্যৱহাৰ বৃদ্ধিৰ লগে লগে ফ্ৰডৰ মাত্ৰাও বৃদ্ধি পাইছে। এই অধ্যায়টোত ডিজিটেল পেমেণ্টত সাধাৰণ ধৰণৰ ফ্ৰড, যেনে পৰিচয় চুৰি, ফিছিং স্কেম, অননুমোদিত লেনদেন, পেমেণ্ট গেটৱে ফ্ৰড, ভুৱা পেমেণ্ট এপ, কিউআৰ ক'ড ফ্ৰড, আৰু চিম চুইপ ফ্ৰডৰ বিষয়ে আলোচনা কৰা হৈছে। ইয়াৰ উপৰি, ডিজিটেল পেমেণ্ট ফ্ৰডৰ পৰা সুৰক্ষিত হ'বলৈ নিৰাপদ ব্ৰাউজিং অভ্যাস, দুই-ফেক্টৰ প্ৰমাণীকৰণ, আৰু বিশ্বস্ত পেমেণ্ট গেটৱে ব্যৱহাৰ কৰাৰ দৰে প্ৰতিৰোধমূলক ব্যৱস্থাবোৰৰ বিষয়েও আলোচনা কৰা হৈছে। তদুপৰি, ডিজিটেল পেমেণ্ট নিয়ন্ত্ৰণত ভাৰতীয় ৰিজাৰ্ভ বেংক (RBI)ৰ ভূমিকা, ডিজিটেল লেনদেনত গ্ৰাহক সুৰক্ষাৰ ওপৰত ইয়াৰ নিৰ্দেশনা, আৰু অভিযোগ নিষ্পত্তি পদ্ধতিৰ বিষয়েও আলোচনা কৰা হৈছে। শেষত, পেমেণ্ট ছেটেলমেণ্ট আইন, ২০০৭ৰ বিষয়ে আলোচনা কৰা হৈছে, য'ত পেমেণ্ট ব্যৱস্থা, পেমেণ্ট গেটৱে, আৰু পেমেণ্ট ছেটেলমেণ্টৰ সৈতে জড়িত ধাৰাসমূহ, আৰু আইনৰ অধীনত অননুমোদিত লেনদেন আৰু পেমেণ্ট ফ্ৰডৰ আইনী প্ৰভাৱ অন্তৰ্ভুক্ত। এই অধ্যায়টো অধ্যয়ন কৰি শিক্ষাৰ্থীসকলে ডিজিটেল পেমেণ্ট ফ্ৰডৰ বিষয়ে আৰু ইয়াৰ পৰা সুৰক্ষিত হ'বলৈ কেনেদৰে ব্যৱস্থা গ্ৰহণ কৰিব পাৰি, সেই বিষয়ে ভালদৰে বুজিব পাৰিব।

১১.৩ ডিজিটেল পেমেণ্টত সাধাৰণ ঠগবাজি

১১.৩.১ পৰিচয় চুৰি আৰু ফিছিং স্কেম

পৰিচয় চুৰি হৈছে এক ধৰণৰ ঠগবাজি, য'ত কোনোবাই আন এজন ব্যক্তিৰ ব্যক্তিগত তথ্য—যেনে নাম, জন্ম তাৰিখ, চিনাক্তকৰণ সংখ্যা (Social Security Number), বা আৰ্থিক তথ্য—চুৰি কৰে আৰু সেই তথ্য ব্যৱহাৰ কৰি অনাধিকাৰভাৱে সামগ্ৰী ক্ৰয় বা লেনদেন কৰে। পৰিচয় চুৰিয়ে ভুক্তভোগীৰ বাবে গুৰুতৰ ফলাফল বহন কৰিব পাৰে,

যেনে আৰ্থিক ক্ষতি, ঋণমানৰ (credit rating) হ্ৰাস, আৰু সম্ভাব্য আইনী বা অপৰাধজনক সমস্যা।

আনহাতে, ফিছিং স্কেম হৈছে এটা ধৰণৰ সামাজিক প্ৰৱঞ্চনামূলক আক্ৰমণ (social engineering attack), য'ত ঠগবাজসকলে নকল ৱেবছাইট বা ইমেইল ব্যৱহাৰ কৰি লোকসকলক নিজৰ ব্যক্তিগত তথ্য বা পেমেণ্টৰ তথ্য দিয়াৰ বাবে প্ৰলোভিত কৰে, যিবোৰ দেখাত আচল বা বিশ্বাসযোগ্য উৎসৰ পৰা অহা যেন লাগে। ফিছিং স্কেমসমূহে সচৰাচৰ ভুক্তভোগীক তৎকালিকভাৱে কাৰ্য কৰাৰ বাবে ভয় বা উদ্বেগৰ অনুভৱ সৃষ্টি কৰি তথ্য দিবলৈ উৎসাহিত কৰে। এই স্কেমসমূহ চিনাক্ত কৰা কঠিন হ'ব পাৰে, কাৰণ ইমেইল বা মেছেজসমূহ বিশ্বাসযোগ্য প্ৰতিষ্ঠান, যেনে বেংক বা জনপ্ৰিয় কোম্পানীৰ পৰা অহা যেন দেখা যায়।

পৰিচয় চুৰি আৰু ফিছিং স্কেম দুয়োটাই ব্যক্তি আৰু ব্যৱসায়ৰ বাবে অত্যন্ত ক্ষতিকাৰক হ'ব পাৰে, সেইবাবে সদায় সতৰ্ক থাকা আৰু নিজৰ ব্যক্তিগত আৰু আৰ্থিক তথ্য সুৰক্ষিত ৰাখিবলৈ পদক্ষেপ লোৱাটো অত্যন্ত জৰুৰী। এই উদ্দেশ্যে— সময় সময়ত আপোনাৰ ক্ৰেডিট ৰিপৰ্ট পৰীক্ষা কৰক, শক্তিশালী পাছৱৰ্ড ব্যৱহাৰ কৰক, অনলাইনত ব্যক্তিগত তথ্য শ্বেয়াৰ কৰোঁতে সাৱধান হওক, আৰু ফিছিং আৰু ঠগবাজি সম্পৰ্কীয় নতুন নতুন পদ্ধতিৰ বিষয়ে সদায় সজাগ থাকক।

১১.৩.২ অনুমতি নথকা লেনদেন আৰু পেমেণ্ট গেটৱে ফ্ৰড (Unauthorized transactions and payment gateway frauds)

অনুমতি নথকা লেনদেন (Unauthorized transactions) বুলিলে বুজায়—যেতিয়া কোনো ব্যক্তি বা গোটে আপোনাৰ অনুমতি নোহোৱাকৈ আপোনাৰ হৈ লেনদেন কৰে। এইটো সেই ক্ষেত্ৰত ঘটিব পাৰে, যেতিয়া কোনোবাই আপোনাৰ পেমেণ্ট সংক্ৰান্ত তথ্য, যেনে আপোনাৰ ক্ৰেডিট কাৰ্ড নম্বৰ বা বেংক একাউণ্টৰ বিবৰণ লাভ কৰি, আপোনাৰ জ্ঞান বা সম্মতি নোহোৱাকৈ খৰচ কৰে বা টকা স্থানান্তৰ কৰে। এনে অনুমতি নথকা লেনদেনৰ ফলত ভুক্তভোগীয়ে আৰ্থিক ক্ষতিসহ মনোবৈকল্যৰ সম্মুখীন হ'ব পাৰে, লগতে ই এক অস্বস্তিকৰ পৰিস্থিতিও সৃষ্টি কৰে।

পেমেণ্ট গেটৱে ফ্ৰড (Payment gateway frauds) অন্যফালে, লেনদেনৰ সময়ত সংঘটিত হোৱা ধোকাবাজিক বুজায়। পেমেণ্ট গেটৱে হৈছে এটা প্ৰযুক্তি ভিত্তিক প্লাটফৰ্ম, যি ব্যৱসায়ী আৰু গ্ৰাহকৰ মাজত অনলাইন লেনদেন সম্পাদন কৰিবলৈ সহায় কৰে। এই প্ৰণালীত থকা দুৰ্বলতা ব্যৱহাৰ কৰি, প্ৰতাৰকসকলে গ্ৰাহকৰ পেমেণ্ট তথ্য চুৰি কৰিব পাৰে বা লেনদেনৰ টকা নিজৰ একাউণ্টলৈ ঘূৰাই দিব পাৰে। পেমেণ্ট গেটৱে

ফ্ৰডৰ কিছুমান সাধাৰণ প্ৰকাৰ হ'ল—ফিছিং আক্ৰমণ, ভুৱা ব্যৱসায়ী ৱেবছাইট আৰু চুৰি হোৱা ক্ৰেডিট কার্ড ডাটা।

অনুমতি নথকা লেনদেন আৰু পেমেণ্ট গেটৱে ফ্ৰড—এই দুয়োটাই ভুক্তভোগীৰ বাবে গুৰুতৰ, যেনে আর্থিক ক্ষতি আৰু ক্ৰেডিট স্ক'ৰৰ ক্ষতি। এই ধৰণৰ প্ৰতাৰণাৰ পৰা ৰক্ষা পাবলৈ আপোনাৰ পেমেণ্ট তথ্য সুৰক্ষিত ৰখাটো অত্যন্ত জৰুৰী, বিশ্বস্ত পেমেণ্ট প্ৰচালক ব্যৱহাৰ কৰা, আৰু নিয়মিতভাৱে আপোনাৰ বেংক বা বিত্তীয় একাউণ্টৰ লেনদেনসমূহ মনিটৰ কৰা উচিত। যদি আপুনি সন্দেহ কৰে যে, আপুনি অনুমতি নথকা লেনদেন বা পেমেণ্ট গেটৱে ফ্ৰডৰ চিকাৰ হৈছে, তেন্তে অবিলম্বে আপোনাৰ বেংক বা বিত্তীয় প্ৰতিষ্ঠানৰ সৈতে যোগাযোগ কৰক আৰু আপোনাৰ একাউণ্টবোৰ সুৰক্ষিত কৰাৰ বাবে পদক্ষেপ লওক।

১১.৩.৩ ভুৱা পেমেণ্ট এপ আৰু মেলৱেয়াৰ আক্ৰমণ (Fake payment apps and malware attacks)

ভুৱা পেমেণ্ট এপ (Fake payment apps) হৈছে এনে জাল মোবাইল এপ্লিকেশ্যন যিবোৰ বিশ্বাসযোগ্য পেমেণ্ট এপ হিচাপে নিজৰ পৰিচয় দিয়ে, কিন্তু মূলতঃ ব্যৱহাৰকাৰীৰ ব্যক্তিগত আৰু বিত্তীয় তথ্য চুৰি কৰাৰ বাবে সাজি তোলা হয়। এইধৰণৰ ভুৱা এপ বিশ্বাসঘাতক উৎসৰ পৰা, অথবা ফিছিং আক্ৰমণৰ জৰিয়তে ডাউনলোড হ'ব পাৰে—য'ত ব্যৱহাৰকাৰীক কোনো বিপদজনক লিংক বা ইমেইল ক্লিক কৰিবলৈ প্ৰলোভন দেখুৱাই এপটো ডাউনলোড কৰাই লোৱা হয়।

এপটো ইনস্টল হোৱাৰ পাছত, ই ব্যৱহাৰকাৰীৰ ক্ৰেডিট কার্ড বা বেংক একাউণ্টৰ নম্বৰ দিয়াৰ বাবে অনুৰোধ কৰে আৰু তাৰ জৰিয়তে টকা চুৰি বা অনুমতি নথকা লেনদেন সম্পাদন কৰে। কিছুমান ভুৱা পেমেণ্ট এপ ব্যৱহাৰকাৰীৰ লগইন তথ্য, বা সমাজিক নিৰাপত্তা নম্বৰৰ দৰে ব্যক্তিগত তথ্যও বিচাৰে, যি পৰৱর্তী সময়ত পৰিচয় চুৰিৰ বাবে ব্যৱহৃত হ'ব পাৰে।

মেলৱেয়াৰ আক্ৰমণ (Malware attacks), হৈছে এনে ক্ষতিকাৰক ছফ্টৱেৰ যিসকলে কম্পিউটাৰ প্ৰণালী বা মোবাইল ডিভাইচত অনুপ্ৰবেশ কৰি ক্ষতি সাধন কৰে। মেলৱেয়াৰ ইমেইল এটাচমেণ্ট, অনিৰাপদ ৱেবছাইট, বা ফিছিং ধৰণৰ সামাজিক প্ৰলোভনেৰে তথ্য চুৰি কৰে।

মেলৱেয়াৰ ডিভাইচত প্ৰৱেশ কৰাৰ পাছত, ই নানান প্ৰকাৰৰ ক্ষতিকাৰক কার্য সম্পাদন কৰিব পাৰে—যেনেঃ গুপ্ত তথ্য চুৰি কৰা, ব্যৱহাৰকাৰীৰ একাউণ্টৰ তথ্য সংগ্ৰহ কৰা, অথবা অবাঞ্ছিত বিজ্ঞাপন দেখুওৱা। বিশেষকৈ মেলৱেয়াৰ যদি বিত্তীয় তথ্য লক্ষ্য কৰি আক্ৰমণ কৰে, তেন্তে ই গুৰুতৰ আর্থিক ক্ষতি বা পৰিচয় চুৰিৰ কাৰণ হ'ব পাৰে।

ভুৱা পেমেণ্ট এপ আৰু মেলৱেয়াৰ আক্ৰমণৰ পৰা বাঁচিবলৈ, কেতিয়াও অবিশ্বাসযোগ্য উৎসৰ পৰা এপ ডাউনলোড নকৰিব। সদায় অফিচিয়েল এপ ষ্টোৰ (যেনেঃ Google Play বা Apple App Store) ব্যৱহাৰ কৰক। অচিনাকী লিংক ক্লিক কৰোতে বা ইমেইল এটাচমেন্টণ্ট ডাউনলোড কৰোতে সচেতন হওক। ডিভাইচ আৰু ছফ্টৱেৰসমূহ সদায় নতুনতম সুৰক্ষা আপডেটৰে আপ-টু-ডেট ৰখা উচিত। লগতে, সবল পাছৱৰ্ড ব্যৱহাৰ কৰা আৰু আপোনাৰ বেংক একাউণ্ট নিয়মিতভাৱে পৰ্যবেক্ষণ কৰা উচিত, যাতে কোনো সন্দেহজনক কাৰ্য সহজে ধৰা পৰে।

১১.৩.৪ কিউ আৰ ক'ড প্ৰতাৰণা আৰু ছিম সোৱাপ প্ৰতাৰণা (QR code frauds and SIM swap frauds)

QR code প্ৰতাৰণা বুলিলে বুজায়—এনে ভুৱা কিউ আৰ ক'ডৰ ব্যৱহাৰ, যাৰ দ্বাৰা সন্দেহ নকৰা ব্যক্তিৰ পৰা ব্যক্তিগত আৰু বিত্তীয় তথ্য চুৰি কৰা হয়।
QR code হৈছে এটা ২-মাত্ৰিক বাৰ ক'ড যাক মোবাইল ডিভাইচ ব্যৱহাৰ কৰি স্কেন কৰি দ্ৰুতভাৱে কিবা তথ্য, যেনে ৱেবছাইট URL বা পেমেণ্ট তথ্য লাভ কৰিব পৰা যায়।

প্ৰতাৰকসকলে এনে ভুৱা QR code তৈয়াৰ কৰে, যিয়ে চাওঁতে সঠিক যেন লাগে, কিন্তু সেয়া ব্যৱহাৰকাৰীক এখন বিপদজনক ৱেবছাইটলৈ লৈ যায় বা তেওঁৰ ডিভাইচৰ পৰা ব্যক্তিগত তথ্য চুৰি কৰে।
QR code প্ৰতাৰণা বিভিন্ন ৰূপত সংঘটিত হ'ব পাৰে—যেনেঃ ফিছিং আক্ৰমণ, য'ত প্ৰতাৰকে ইমেইল বা ছচিয়েল মিডিয়াৰ জৰিয়তে ভুৱা QR code পঠিয়ায়; অথবা পোস্টাৰ বা যান-বাহনত থকা ভুৱা কিউ আৰ ক'ড যেনে—সাধাৰণ ঠাইত চেপি লগোৱা ভুৱা ক'ড।

SIM swap প্ৰতাৰণা আনহাতে, এজন ভুক্তভোগীৰ মোবাইল নম্বৰ প্ৰতাৰকৰ নিয়ন্ত্ৰণত থকা নতুন SIM কাৰ্ডলৈ স্থানান্তৰ কৰাৰ পৰা উদ্ভৱ হয়। এইটো তেতিয়া সম্ভৱ হয়, যেতিয়া প্ৰতাৰকে মোবাইল সেৱা প্ৰদানকাৰী সংস্থাক ভুলভুলাই victim-ৰ ফোন নম্বৰ এখন নতুন SIM কাৰ্ডলৈ স্থানান্তৰ কৰিবলৈ বাধ্য কৰে—সাধাৰণতে victim হিচাপে নিজকে চিনাক্ত কৰি বা ভুৱা চিনাক্তকৰণ নথি প্ৰদান কৰি।
যেতিয়া প্ৰতাৰকে ভুক্তভোগীৰ ফোন নম্বৰ নিয়ন্ত্ৰণ কৰে, তেতিয়া তেওঁ victim-ৰ ব্যক্তিগত আৰু বিত্তীয় একাউণ্টসমূহত প্ৰৱেশ কৰিব পাৰে, যিসমূহ দুই স্তৰীয়া প্ৰমাণীকৰণ (two-factor authentication) দ্বাৰা সুৰক্ষিত নাথাকে। এইদৰে তেওঁ

সুৰক্ষা ব্যৱস্থা উপেক্ষা কৰি অনুমতি নথকা লেনদেন কৰিবলৈ সক্ষম হয়, অথবা গুপ্ত তথ্য চুৰি কৰিব পাৰে।

QR code প্ৰতাৰণা আৰু SIM swap প্ৰতাৰণাৰ পৰা ৰক্ষা পাবলৈ, QR code স্কেন কৰোতে বিশেষকৈ অচিনাকী স্থানত বা অবাঞ্ছিত মেছেজৰ জৰিয়তে পোৱা ক'ডৰ ক্ষেত্ৰত সাৱধানতা অৱলম্বন কৰা উচিত।
ব্যৱহাৰকাৰীসকলে নিজৰ ব্যক্তিগত তথ্য আৰু পাছৱৰ্ডসমূহ সুৰক্ষিত ৰাখিবলৈ সদায় সজাগ হ'ব লাগিব আৰু নিয়মিতভাৱে নিজৰ বেংক একাউণ্ট আৰু মোবাইল ফোনৰ কাৰ্যকলাপ পৰ্যবেক্ষণ কৰি সন্দেহজনক কাৰ্যকলাপ দেখা পালে তৎক্ষণাত পদক্ষেপ ল'ব লাগিব।



অগ্ৰগতি নিৰীক্ষণ

প্ৰশ্ন নং ১: সঠিক বিকল্পটো বাছনি কৰকঃ

(ক) পৰিচয় চুৰি (Identity theft) বুলিলে কি বুজায়?

(i) লটাৰী ধৰণৰ এটা প্ৰতাৰণা

(ii) বিনিয়োগ ভিত্তিক এটা প্ৰতাৰণা

(iii) ইমেইল ভিত্তিক এটা প্ৰতাৰণা

(iv) এটা ধৰণৰ প্ৰতাৰণা, য'ত কোনোবাই আন এজন ব্যক্তিৰ ব্যক্তিগত তথ্য চুৰি কৰে ।

(খ) ফিছিং (Phishing) বুলিলে কি বুজায়?

(i) এটা সামাজিক প্ৰলোভনৰ আক্ৰমণ, য'ত প্ৰতাৰকে ব্যক্তিসকলক নিজৰ ব্যক্তিগত বা পেমেণ্ট তথ্য দিবলৈ ভুলাই কৰে

(ii) এটা নেটৱৰ্ক আক্ৰমণ

(iii) ৰেনছমৱেয়াৰ আক্ৰমণৰ এটা ধৰণ

(iv) মেলৱেয়াৰ আক্ৰমণৰ এটা ধৰণ

(গ) পৰিচয় চুৰিৰ সম্ভাব্য পৰিণাম কি হ'ব পাৰে?

(i) ছচিয়েল মিডিয়াত অনুসৰণকাৰীৰ সংখ্যা বৃদ্ধি

(ii) অধিক আৰ্থিক স্থিৰতা

(iii) ক্ৰেডিট স্ক'ৰৰ উন্নতি

(iv) আৰ্থিক ক্ষতি, ক্ৰেডিট ৰেটিঙৰ ক্ষতি, আৰু সম্ভাব্য আইনী তথা অপৰাধজনিত সমস্যা ।

(ঘ) পেমেণ্ট গেটৱে ফ্ৰড (Payment gateway fraud) বুলিলে কি বুজায়?

(i) পেমেণ্ট প্ৰক্ৰিয়াৰ সময়ত সংঘটিত হোৱা ধোকাখোৱা কাৰ্যকলাপ

(ii) ফিছিং আক্রমণৰ এটা ধৰণ

(iii) সামাজিক প্রলোভনৰ এটা ধৰণ

(iv) মেলৱেয়াৰ আক্রমণৰ এটা ধৰণ

(ঙ) ভু�ৰা পেমেণ্ট এপ (Fake payment apps) বুলিলে কি বুজায়?

(i) প্রকৃত পেমেণ্ট কৰাৰ বাবে ব্যৱহৃত বিশ্বাসযোগ্য মোবাইল এপ্লিকেশ্যন

(ii) ছচিয়েল মিডিয়াৰ বাবে ব্যৱহৃত মোবাইল এপ

(iii) এনে জাল মোবাইল এপ, যিসকলে প্রকৃত পেমেণ্ট এপৰ ৰূপ লৈ ব্যৱহাৰকাৰীৰ ব্যক্তিগত আৰু বিত্তীয় তথ্য চুৰি কৰে

(iv) অনলাইন কেনাকাটিৰ বাবে ব্যৱহৃত মোবাইল এপ

(চ) মেলৱেয়াৰ (Malware) বুলিলে কি বুজায়?

(i) ক্ষতিকাৰক ছফ্টৱেৰ, যিসকলে কম্পিউটাৰ বা মোবাইল ডিভাইচত অনুপ্রবেশ কৰি ক্ষতি কৰে

(ii) গেমিংৰ বাবে ব্যৱহৃত ছফ্টৱেৰ

(iii) কামৰ উৎপাদনশীলতাৰ বাবে ব্যৱহৃত বৈধ ছফ্টৱেৰ

(iv) ৱেব ব্রাউজিঙৰ বাবে ব্যৱহৃত ছফ্টৱেৰ

(ছ) QR কোড প্রতাৰণা (QR code frauds) বুলিলে কি বুজায়?

(i) গেমিংৰ বাবে ব্যৱহৃত QR কোড

(ii) তথ্যত দ্রুত প্রৱেশৰ বাবে ব্যৱহৃত প্রকৃত QR কোড

(iii) এনে ভুৱা QR কোড ব্যৱহাৰ, যিসকলে সন্দেহ নকৰা ব্যক্তিৰ পৰা ব্যক্তিগত আৰু বিত্তীয় তথ্য চুৰি কৰে

(iv) ছচিয়েল মিডিয়াৰ বাবে ব্যৱহৃত QR কোড

(জ) SIM সোৱাপ প্রতাৰণা (SIM swap frauds) বুলিলে কি বুজায়?

(i) ভুক্তভোগীৰ মোবাইল নম্বৰ প্রতাৰকৰ নিয়ন্ত্রণত থকা নতুন SIM কার্ডলৈ জালভাৱে স্থানান্তৰ কৰা

(ii) সামাজিক প্রলোভনৰ এটা ধৰণ

(iii) ফিছিং আক্রমণৰ এটা ধৰণ

(iv) নেটৱর্ক আক্রমণৰ এটা ধৰণ

(ঝ) ভুৱা পেমেণ্ট এপৰ পৰা কেনেকৈ ৰক্ষা পাব পাৰি?

(i) দুর্বল পাছৱর্ড ব্যৱহাৰ কৰি

(ii) যিকোনো ব্যক্তিক ব্যক্তিগত আৰু বিত্তীয় তথ্য আগবঢ়াই দি

(iii) অবিশ্বাসযোগ্য উৎসৰ পৰা এপ ডাউনলোড কৰি

(iv) কেৱল বিশ্বাসযোগ্য উৎস (যেনেঃ অফিচিয়েল এপ ষ্টোৰ)-ৰ পৰা এপ ডাউনলোড কৰি

(ঞ) SIM সোৱাপ প্ৰতাৰণাৰ পৰা কেনেকৈ ৰক্ষা পাব পাৰি?

(i) মোবাইল নম্বৰ ঘনঘনকৈ নতুন SIM কাৰ্ডলৈ স্থানান্তৰ কৰি

(ii) ব্যক্তিগত তথ্য আৰু পাছৱৰ্ড শ্বেয়াৰ কৰোতে সাৱধান হৈ

(iii) যিকোনো ব্যক্তিক ব্যক্তিগত তথ্য দিবলৈ সাজু হৈ

(iv) বেংক একাউণ্ট আৰু মোবাইল ফোনৰ কার্যকলাপ নিয়মিতভাৱে পর্যবেক্ষণ কৰি

১১.৪ ডিজিটেল পেমেণ্ট প্ৰতাৰণাৰ প্ৰতিৰোধমূলক ব্যৱস্থা (Preventive Measures for Digital Payment Frauds)

১১.৪.১ নিৰাপদ ব্ৰাউজিং অভ্যাস আৰু পাছৱৰ্ড ব্যৱস্থাপনা (Safe browsing practices and password management)

ডিজিটেল পেমেণ্ট প্ৰতাৰণাৰ পৰা ৰক্ষা পাবলৈ নিৰাপদ ইণ্টাৰনেট ব্যৱহাৰ আৰু ফলপ্ৰসূ পাছৱৰ্ড ব্যৱস্থাপনা অনুসৰণ কৰাটো অত্যন্ত প্ৰয়োজনীয়। তলত নিজকে সুৰক্ষিত ৰাখিবলৈ কিছুমান গুৰুত্বপূর্ণ পৰামর্শ দিয়া হৈছে—

(a) শক্তিশালী পাছৱৰ্ড ব্যৱহাৰ কৰক:

- এটা শক্তিশালী পাছৱৰ্ডত uppercase আৰু lowercase, সংখ্যা, আৰু বিশেষ চিহ্ন থকাটো উচিত। সাধাৰণ শব্দ বা বাক্য ব্যৱহাৰ নকৰিব, কিয়নো সেয়া সহজে অনুমান কৰিব পৰা যায়। লগতে, এটা পাছৱৰ্ড বহু একাউণ্টৰ বাবে পুনৰ ব্যৱহাৰ নকৰিব।
- শক্তিশালী পাছৱৰ্ডৰ উদাহৰণ: b7K#nL@9$pDfTm2Z
  এই পাছৱৰ্ডত uppercase আৰু lowercase আখৰ, সংখ্যা, আৰু চিহ্ন আছে। ই দীঘল আৰু জটিল হোৱাত সহজে অনুমান বা brute-force আক্রমণৰ জৰিয়তে ভংগ কৰা কঠিন।
  এইধৰণৰ পাছৱৰ্ড মনত ৰাখিব কঠিন হ'ব পাৰে, সেইবাবে পাছৱৰ্ড মেনেজাৰ ব্যৱহাৰ কৰি সুৰক্ষিতভাৱে সঞ্চয় কৰা আৰু বেলেগ-বেলেগ একাউণ্টৰ বাবে অনন্য পাছৱৰ্ড সৃষ্টি কৰা বাঞ্ছনীয়।
- Brute-force attack বুলিলে কি বুজায়?
  ই হৈছে এক হেকিং পদ্ধতি, য'ত আক্রমণকাৰীয়ে সম্ভৱপৰ সকলো আখৰৰ সমন্বয় প্রয়োগ কৰি সঠিক পাছৱৰ্ড বা এনক্রিপচন কি উলিয়াব চেষ্টা কৰে। এইটো সাধাৰণতে স্বচালিত ছফ্টৱেৰ ব্যৱহাৰ কৰি কৰা হয়, যি বহু কম সময়তে বহুবিধ সম্ভাব্য পাছৱৰ্ড সৃষ্টি আৰু পৰীক্ষা কৰিব পাৰে।

দূৰ্বল পাছৱৰ্ড (ছোট, সাধাৰণ, বা সহজে অনুমান কৰিব পৰা) এই আক্রমণৰ বাবে সহজ লক্ষ্য হয়।

কিন্তু দীঘল আৰু জটিল পাছৱৰ্ড (আখৰ, সংখ্যা, চিহ্ন মিশ্রণযুক্ত) brute-force আক্রমণৰ বিৰুদ্ধে অধিক সুৰক্ষিত।

ইয়াৰ উপৰি, বহু অনলাইন সেৱা আৰু ৱেবছাইটত brute-force আক্রমণ চিনাক্ত আৰু ৰোধ কৰিবলৈ নির্দিষ্ট সুৰক্ষা ব্যৱস্থা থাকে, যেনেঃ login চেষ্টা সীমিত কৰা বা দুই স্তৰীয় প্রমাণীকৰণ প্রয়োগ কৰা।

(b) পাছৱৰ্ড মেনেজাৰ ব্যৱহাৰ কৰক:

Password Manager হৈছে এটা ছফ্টৱেৰ, যিয়ে আপোনাৰ বিভিন্ন একাউণ্টৰ বাবে পাছৱৰ্ড সৃষ্টি, সংৰক্ষণ আৰু পৰিচালনা কৰাত সহায় কৰে।

এই ব্যৱস্থাৰে আপোনাই প্রতিটো একাউণ্টৰ বাবে শক্তিশালী আৰু অনন্য পাছৱৰ্ড ব্যৱহাৰ কৰিব পাৰিব আৰু সব মনত ৰাখিব নালাগে।

(c) Phishing প্রতাৰণাৰ পৰা সাৱধান থাকক:

Phishing হৈছে এক ধৰণৰ প্রতাৰণা, য'ত ইলেকট্রনিক মাধ্যমত বিশ্বাসযোগ্য উৎসৰ ৰূপ লৈ ব্যৱহাৰকাৰীৰ পৰা ব্যৱহাৰকাৰী নাম, পাছৱৰ্ড, ক্রেডিট কার্ডৰ তথ্য আদিৰ দৰে গুৰুত্বপূর্ণ তথ্য সংগ্রহ কৰাৰ চেষ্টা কৰা হয়।

Phishing প্রতাৰণাৰ কিছুমান উদাহৰণ হ'লঃ

ইমেইল প্রতাৰণা:

এইটো আটাইতকৈ সাধাৰণ। প্রতাৰকে নামী বেংক, অনলাইন বিক্রেতা বা ছচিয়েল মিডিয়া প্লাটফর্মৰ নামত ইমেইল পঠিয়ায় আৰু লিংকত ক্লিক কৰিবলৈ বা এটাচমেণ্ট ডাউনলোড কৰিবলৈ কয়। এই লিংক বা এটাচমেণ্টত মেলৱেয়াৰ থাকিব পাৰে, যিয়ে ব্যৱহাৰকাৰীৰ তথ্য চুৰি কৰে।

ভু�ৱা ৱেবছাইট:

প্রতাৰকে নামী অনলাইন শ্বপিং বা বেংকিং ৱেবছাইটৰ সদৃশ ভু�ৱা ৱেবছাইট সৃষ্টি কৰে। তাত লগিন কৰিলে তেওঁলোক ব্যৱহাৰকাৰীৰ তথ্য চুৰি কৰে।

SMS প্রতাৰণা:

মেছেজ যোগে বেংকৰ নামত ব্যক্তিগত তথ্য বিচৰা বা লিংকত ক্লিক কৰিবলৈ কোৱা হয়।

Spear phishing:

এইটো অধিক লক্ষ্যভিত্তিক আৰু জটিল। প্রতাৰকে আগতে victim-ৰ বিষয়ে গৱেষণা কৰি তেওঁৰ চিনাকি ব্যক্তিৰ দৰে ইমেইল পঠিয়ায়, যেনেঃ সহকর্মী বা বস। ইমেইলত টকা পঠিয়াবলৈ বা গুপ্ত তথ্য দিবলৈ কোৱা হয়।

ছচিয়েল মিডিয়া প্ৰতাৰণা:

প্ৰতাৰকে ছচিয়েল মিডিয়াত ভুৱা একাউণ্ট খুলে বা মেছেজ পঠিয়ায়, য'ত ব্যক্তিগত তথ্য বিচৰা হয় বা ভুৱা লিংক দি তাত সোমাবলৈ কোৱা হয়।

সচেতন থাকক আৰু যদি নিশ্চিত নহয়, তেন্তে কেতিয়াও ব্যক্তিগত তথ্য শ্বেয়াৰ নকৰিব।

(d) নিৰাপদ ব্ৰাউজাৰ ব্যৱহাৰ কৰক:

নিৰাপদ ব্ৰাউজাৰ ব্যৱহাৰে আপোনাৰ অনলাইন কাৰ্যকলাপ আৰু ব্যক্তিগত তথ্যক অনুমতি নথকা প্ৰৱেশৰ পৰা ৰক্ষা কৰিব পাৰে।

নিৰাপদ ব্ৰাউজাৰ ব্যৱহাৰৰ বাবে পদক্ষেপসমূহ—

- নিৰাপদ ব্ৰাউজাৰ বাছনি কৰক:
  এনে ব্ৰাউজাৰ বাচনি কৰক য'ত উন্নত সুৰক্ষা সুবিধা থাকে—এনক্ৰিপচন, anti-phishing, আৰু privacy setting।
  বিশ্বস্ত ব্ৰাউজাৰঃ Google Chrome, Mozilla Firefox, Safari, Microsoft Edge।
- ব্ৰাউজাৰ সদায় আপডেট কৰি ৰাখক:
  নতুন সংস্কৰণ ব্যৱহাৰ কৰিলে সৰ্বশেষ সুৰক্ষা প্যাচ আৰু বৈশিষ্ট্য পাব।
- সুৰক্ষা বঢ়োৱা Extensions ইনষ্টল কৰক:
  Ad blocker, password manager, VPN ইত্যাদি যেনে প্ৰাইভেছি সহায়ক extension ব্যৱহাৰ কৰক।
- Privacy settings কনফিগাৰ কৰক:
  Third-party cookies ব্লক কৰক, location tracking নিষ্ক্ৰিয় কৰক, আৰু "Do Not Track" অন কৰক।
- বিপদজনক ৱেবছাইটৰ পৰা আঁতৰি থাকক:
  যেনেঃ যিসকলে মেলৱেয়াৰ, spam বা phishing প্ৰসাৰ কৰে।
- নিৰাপদ সংযোগৰ পৰীক্ষা কৰক:
  Address bar-ত padlock চিহ্ন চাওক, আৰু URL "https://" দিয়ে আৰম্ভ হোৱা নিশ্চিত কৰক।
- Download-ত সাৱধানতা অৱলম্বন কৰক:
  ইণ্টাৰনেটৰ পৰা কোনো ফাইল বা ছফ্টৱেৰ ডাউনলোড কৰাৰ সময়ত সাৱধান থাকক, আৰু antivirus ৰ জৰিয়তে স্কেন কৰক।
- এই পদক্ষেপসমূহ অনুসৰণ কৰি আপুনি নিৰাপদ ব্ৰাউজিঙৰ জৰিয়তে নিজৰ তথ্য সুৰক্ষিত ৰাখিব পাৰে।

(e) আপোনাৰ ছফ্টৱেৰ সদায় আপডেট কৰি ৰাখক:

আপোনাৰ অপাৰেটিং চিষ্টেম আৰু ছফটৱেৰসমূহ সদায় নতুনতম সুৰক্ষা আপডেটৰে আপ-টু-ডেট ৰাখক। এইটোৱে আপোনাৰ কম্পিউটাৰ বা মোবাইল ডিভাইচক বিদ্যমান সুৰক্ষা দুৰ্বলতাৰ পৰা ৰক্ষা কৰে। এই নিৰাপদ ব্রাউজিং অভ্যাস আৰু পাছৱৰ্ড ব্যৱস্থাপনা পৰামৰ্শসমূহ অনুসৰণ কৰিলে, আপুনি ডিজিটেল পেমেণ্ট প্রতাৰণাৰ পৰা নিজকে ৰক্ষা কৰিব পাৰে আৰু নিজৰ ব্যক্তিগত আৰু বিত্তীয় তথ্য সুৰক্ষিত ৰাখিব পাৰে।

১১.৪.২ দুই-স্তৰীয় প্রমাণীকৰণ আৰু বায়োমেট্রিক প্রমাণীকৰণ (Two-factor authentication and biometric authentication)

দুই-স্তৰীয় প্রমাণীকৰণ (Two-Factor Authentication - 2FA) হৈছে এটি সুৰক্ষা প্রক্রিয়া, য'ত ব্যৱহাৰকাৰীয়ে কোনো ছিষ্টেম, ৱেবছাইট বা এপ্লিকেশ্যনত প্রৱেশ কৰিবলৈ দুটা বেলেগ ধৰণৰ পৰিচয় প্রদান কৰিব লাগে। এই প্রক্রিয়াই লগইন প্রক্রিয়াত এটা অতিৰিক্ত সুৰক্ষাৰ পর্যায় যোগ কৰে আৰু যদি পাছৱৰ্ডটো কোনোদৰে গম পোৱা হ'লেও, অনুমতি নথকা প্রৱেশ ৰোধ কৰিবলৈ সহায় কৰে।

2FA-ৰ এখন উদাহৰণ হ'ল—মোবাইল ফোন ব্যৱহাৰ কৰি ব্যৱহাৰকাৰীৰ পৰিচয় নিশ্চিত কৰা। ব্যৱহাৰকাৰীয়ে প্রথমে নিজৰ ইউজাৰনেম আৰু পাছৱৰ্ড প্রৱিষ্ট কৰাৰ পাছত, তেওঁৰ মোবাইল ফোনত টেক্সট মেছেজ বা authentication এপৰ জৰিয়তে এখন একক (unique) আৰু সময় সময়তে সলনি হোৱা কোড পঠিওৱা হয়। এই কোডটো প্রবিষ্ট নকৰিলে, কেৱল পাছৱৰ্ড জানিলেও, একাউণ্টত প্রৱেশ কৰিব নোৱাৰি।

১১.৪.৩ ৰাজহুৱা Wi-Fi ব্যৱহাৰ এৰাই চলা আৰু বিশ্বস্ত পেমেণ্ট গেটৱে ব্যৱহাৰ কৰা (Avoiding public Wi-Fi and using trusted payment gateways)

ডিজিটেল পেমেণ্ট প্রতাৰণাৰ প্রতিৰোধমূলক ব্যৱস্থা হিচাপে ব্যৱহাৰকাৰীয়ে অনলাইন লেনদেনৰ সময়ত নিজৰ ব্যক্তিগত আৰু বিত্তীয় তথ্য সুৰক্ষিত ৰাখিবলৈ কিছু পদক্ষেপ গ্রহণ কৰিব লাগে। তেনে দুটা গুৰুত্বপূর্ণ পদক্ষেপ হ'ল:

(1) ৰাজহুৱা Wi-Fi ব্যৱহাৰ নকৰিব:

ৰাজহুৱা Wi-Fi নেটৱর্ক সাধাৰণতে সুৰক্ষিত নহয়, আৰু চাইবৰ অপৰাধীসকলে এই নেটৱর্কৰ ওপৰত প্রেৰণ হোৱা তথ্য, যেনে লগইন তথ্য বা পেমেণ্ট তথ্য, চুৰি কৰিব পাৰে।

এই কাৰণেই অনলাইন পেমেণ্ট কৰাৰ সময়ত বা গুৰুত্বপূৰ্ণ তথ্য আহৰণ কৰাৰ সময়ত ৰাজহুৱা Wi-Fi ব্যৱহাৰ এৰাই চলাটো উত্তম। যদি ব্যৱহাৰ কৰিবই লাগে, তেন্তে VPN (Virtual Private Network) ব্যৱহাৰ কৰি আপোনাৰ তথ্য এনক্ৰিপ্ট কৰাৰ পৰামৰ্শ দিয়া হয়।

(2) **বিশ্বাসযোগ্য পেমেণ্ট গেটৱে ব্যৱহাৰ কৰক:**

বিশ্বস্ত পেমেণ্ট গেটৱে হৈছে সুৰক্ষিত প্লাটফৰ্ম, যিয়ে অনলাইন পেমেণ্টৰ সহায় কৰে। এইবোৰে এনক্ৰিপচন আৰু দুয়ো-স্তৰীয় প্ৰমাণীকৰণৰ দৰে অতিৰিক্ত সুৰক্ষা সুবিধা প্ৰদান কৰে, যাতে প্ৰতাৰণামূলক লেনদেন ৰোধ কৰা যায়।

অনলাইন পেমেণ্ট কৰাৰ সময়ত সদায় বিশ্বস্ত, জনপ্ৰিয় আৰু ভাল ৰিভিউ থকা পেমেণ্ট গেটৱে ব্যৱহাৰ কৰক। Visa বা Mastercard-ৰ দৰে পেমেণ্ট কার্ড নেটৱৰ্কে স্বীকৃত পেমেণ্ট গেটৱে বাচনি কৰক যাতে সেইবোৰে ঔদ্যোগিক সুৰক্ষা মানদণ্ড পূৰণ কৰা নিশ্চিত হয়।

১১.৪.৪ লেনদেনৰ ইতিহাস নিয়মিতভাৱে পৰীক্ষা কৰা আৰু লেনদেন সতৰ্কতা ছেট কৰা (Regularly checking transaction history and setting transaction alerts)

ডিজিটেল পেমেণ্ট প্ৰতাৰণাৰ প্ৰতিৰোধমূলক ব্যৱস্থাৰ অংশ হিচাপে, অনলাইন লেনদেনৰ সময়ত প্ৰতাৰণাৰ আশংকা কমাবলৈ ব্যক্তিসকলে কিছু বিশেষ পদক্ষেপ ল'ব পাৰে। তেনে দুটা পদক্ষেপ হ'ল:

(1) **লেনদেনৰ ইতিহাস পৰীক্ষা কৰা (Checking transaction history):**

ডিজিটেল পেমেণ্ট চেনেলৰ জৰিয়তে কৰা সকলো লেনদেন নিয়মিতভাৱে পৰীক্ষা কৰা উচিত, যাতে সেইবোৰ বৈধ আৰু অনুমোদিত হয়।

এই ব্যৱস্থাই সন্দেহজনক কার্যকলাপ চিনাক্ত কৰাত সহায় কৰে আৰু দ্ৰুত পদক্ষেপ ল'ব পাৰি, যাৰ ফলত অধিক প্ৰতাৰণা ৰোধ কৰিব পাৰি।

(2) **লেনদেন সতৰ্কতা ছেট কৰা (Setting transaction alerts):**

এনে ব্যৱস্থাৰ জৰিয়তে ব্যৱহাৰকাৰীয়ে নিজৰ ডিজিটেল পেমেণ্ট একাউণ্ট ব্যৱহাৰ কৰি যেতিয়া কোনো লেনদেন সংঘটিত হয়, তেতিয়া notification পায়। এইদৰে কোনো সন্দেহজনক লেনদেন বাস্তৱ সময়ত চিনাক্ত কৰি তৎক্ষণাত পদক্ষেপ ল'ব পাৰি আৰু অধিক ক্ষতি ৰোধ কৰিব পাৰি।



অগ্ৰগতি নিৰীক্ষণ

প্ৰশ্ন নং ২ : অসমীয়াত প্ৰশ্নবোৰৰ চমু উত্তৰ:

(ক) এটা শক্তিশালী পাছৱৰ্ড কি ?

(খ) পাছৱৰ্ড মেনেজাৰ কি ?

(গ) ফিছিং স্কেমৰ কিছুমান উদাহৰণ কি কি ?

(ঘ) দুই-ফেক্টৰ প্ৰমাণীকৰণ কি ?

(ঙ) এটা সুৰক্ষিত ব্ৰাউজাৰ কেনেকৈ ব্যৱহাৰ কৰিব পাৰি ?

১১.৫ ডিজিটেল পেমেণ্ট সম্পৰ্কে আৰ.বি.আই.-ৰ নিৰ্দেশনা (RBI Guidelines on Digital Payments)

১১.৫.১ ডিজিটেল পেমেণ্টৰ নিয়ন্ত্ৰণত আৰ.বি.আই.-ৰ ভূমিকা: এক পৰ্যালোচনা (Overview of RBI's role in regulating digital payments)

ভাৰতীয় ৰিজাৰ্ভ বেংক (RBI)-এ ভাৰতত ডিজিটেল পেমেণ্টৰ নিয়ন্ত্ৰণত অতি গুৰুত্বপূৰ্ণ ভূমিকা পালন কৰে। ৰাষ্ট্ৰৰ কেন্দ্ৰীয় বেংক হিচাপে, RBI-ৰ দায়িত্ব হ'ল পেমেণ্ট ব্যৱস্থাৰ স্থিৰতা, দক্ষতা নিশ্চিত কৰা আৰু বিত্তীয় অন্তৰ্ভুক্তিক উৎসাহিত কৰা। ডিজিটেল পেমেণ্টৰ নিয়ন্ত্ৰণত RBI-ৰ কিছুমান মুখ্য ভূমিকা আৰু দায়িত্ব হ'ল—

নিৰ্দেশনা আৰু বিধি-নিষেধ প্ৰদান

RBI-এ ডিজিটেল পেমেণ্ট সেৱা প্ৰদানকাৰী (PSP)-সকলৰ বাবে নিৰ্দেশনা আৰু বিধিমালা জাৰী কৰে, যাতে সেইসকলে নিয়মৰ কাঠামোৰ ভিতৰত সুৰক্ষিতভাৱে কাৰ্যকৰী হয়।

পৰ্যবেক্ষণ আৰু তদাৰকিঃ

ডিজিটেল পেমেণ্ট চিষ্টেম আৰু সেৱাসমূহৰ ওপৰত পৰ্যবেক্ষণ আৰু তদাৰকি কৰি, ইয়াৰ সুৰক্ষা, নিৰ্ভৰযোগ্যতা নিশ্চিত কৰে।

লাইচেন্স প্রদান আৰু অনুমোদন:

RBI-এ পেমেণ্ট ছিষ্টেম অপাৰেটৰ (PSO) আৰু পেমেণ্ট মধ্যস্থ (PI) সকলক লাইচেন্স আৰু অনুমোদন দিয়ে, যাতে তেওঁলোকে ভাৰতত বৈধভাৱে কাম কৰিব পাৰে।

গ্রাহক সুৰক্ষা:

গ্রাহকৰ স্বার্থ ৰক্ষাৰ বাবে RBI-এ স্বচ্ছতা, সুৰক্ষা আৰু দক্ষতা বজাই ৰখাৰ মানদণ্ড নির্ধাৰণ কৰে।

উদ্ভাৱন আৰু বিকাশৰ উৎসাহ:

RBI-এ নতুন প্রযুক্তিৰ গ্রহণ আৰু PSP, PSO আৰু PI-সকলৰ মাজত সহযোগিতা আগবঢ়াই ডিজিটেল পেমেণ্ট খণ্ডত উদ্ভাৱন আৰু বিকাশ উৎসাহিত কৰে।

শেষত ক'ব পাৰি যে ডিজিটেল পেমেণ্টৰ ক্ষেত্রত RBI-ৰ ভূমিকা হৈছে পেমেণ্ট চিষ্টেমৰ সুৰক্ষা, দক্ষতা, আৰু জন-বান্ধৱ ৰূপ নিশ্চিত কৰাৰ লগতে আর্থিক সম্পত্তিৰ সুৰক্ষা আগবঢ়োৱা।

১১.৫.২ ডিজিটেল লেনদেনত গ্রাহক সুৰক্ষা সম্পর্কে আৰ.বি.আই.-ৰ নির্দেশনা (RBI guidelines on customer protection in digital transactions)

ডিজিটেল লেনদেনত সুৰক্ষা আৰু নিশ্চয়তা নিশ্চিত কৰাৰ উদ্দেশ্যে, ভাৰতীয় ৰিজার্ভ বেংকে কিছুমান গুৰুত্বপূর্ণ নির্দেশনা প্রদান কৰিছে। সেইবোৰ হ'ল—

- **গ্রাহকৰ সম্মতি (Customer Consent):**
  বেংক আৰু অন্য পেমেণ্ট সেৱা প্রদানকাৰীসকলে নিশ্চিত কৰিব লাগিব যে— প্রত্যেক ডিজিটেল লেনদেনৰ পূর্বে গ্রাহকৰ স্পষ্ট অনুমতি গ্রহণ কৰা হৈছে।
- **দুই-স্তৰীয় প্রমাণীকৰণ (Two-Factor Authentication):**
  সকলো ডিজিটেল লেনদেনত OTP বা একক পাছৱর্ডৰ মাধ্যমে 2FA থাকিব লাগিব, যি গ্রাহকৰ ৰেজিষ্টাৰ কৰা মোবাইল নম্বৰ বা ই-মেইললৈ পঠিওৱা হয়।
- **গ্রাহক শিক্ষাদান (Customer Education):**
  বেংক আৰু পেমেণ্ট সেৱা প্রদানকাৰীসকলে গ্রাহকক ডিজিটেল চেনেল ব্যৱহাৰৰ সময়ত সম্ভাব্য ভাবুকি আৰু ভাল অভ্যাসসমূহৰ বিষয়ে জনাব লাগিব।
- **অভিযোগ নিষ্পত্তি ব্যৱস্থা (Complaint Redressal):**
  ডিজিটেল লেনদেন সম্পর্কীয় অভিযোগসমূহ মোকাবিলা কৰাৰ বাবে উপযুক্ত অভিযোগ নিষ্পত্তি ব্যৱস্থা প্রত্যেক সংস্থাৰ থাকিব লাগিব।

- **সুৰক্ষা ব্যৱস্থা (Security Measures):**
  গ্ৰাহকৰ ব্যক্তিগত আৰু বিত্তীয় তথ্য চাইবাৰ আক্ৰমণৰ পৰা সুৰক্ষিত ৰাখিবলৈ দৃঢ় সুৰক্ষা ব্যৱস্থা গ্ৰহণ কৰিব লাগিব।
- **লেনদেন সীমা (Limits on Transactions):**
  ডিজিটেল চেনেলৰ জৰিয়তে লেনদেন কৰিবলৈ টকাৰ সীমা নিৰ্ধাৰণ কৰিব লাগিব, যাতে বৃহৎ পৰিসৰৰ প্ৰতাৰণা ৰোধ কৰিব পাৰি।
- **প্ৰতিৱেদন প্ৰদান (Reporting):**
  যিকোনো প্ৰতাৰণা বা অনুমতি নথকা লেনদেন হ'লে, বেংক বা PSP-এ নিৰ্ধাৰিত সময়ছোৱাৰ ভিতৰত RBI-লৈ প্ৰতিৱেদন দিব লাগিব।
- এই সকলো নিৰ্দেশনাৰ লক্ষ্য হ'ল—ডিজিটেল লেনদেনত গ্ৰাহকক সুৰক্ষা প্ৰদান কৰা, প্ৰতাৰণাৰ পৰা ৰক্ষা কৰা, আৰু ডিজিটেল ব্যৱহাৰ প্ৰচাৰ কৰা।

১১.৫.৩ অভিযোগ নিষ্পত্তি ব্যৱস্থা আৰু বিবাদ নিষ্পত্তি পদ্ধতি (Complaint redressal mechanisms and dispute resolution procedures)

ডিজিটেল পেমেণ্ট সম্পৰ্কে RBI-ৰ নিৰ্দেশনা অনুসৰি, বেংক আৰু পেমেণ্ট সেৱা প্ৰদানকাৰীসকলে গ্ৰাহকৰ যিকোনো অভিযোগ বা বিবাদ সলনি কৰিবলৈ উপযুক্ত অভিযোগ নিষ্পত্তি আৰু বিবাদ নিষ্পত্তি ব্যৱস্থা বজাই ৰাখিব লাগিব। তলত এই ব্যৱস্থাসমূহৰ কিছুমান মুখ্য দিশ উল্লেখ কৰা হ'ল—

- **অভিযোগ নিষ্পত্তি বিষয়া (Grievance Redressal Officer):**
  প্ৰত্যেক বেংক বা PSP-এ অভিযোগ নিষ্পত্তি বিষয়া নিযুক্ত কৰিব লাগিব, যিয়ে ডিজিটেল লেনদেন সম্পৰ্কীয় গ্ৰাহকৰ অভিযোগসমূহ সলনি কৰিব।
- **সমাধানৰ সময়সীমা (Timelines for Resolution):**
  RBI-এ নিৰ্ধাৰণ কৰিছে—বেংকে অভিযোগ লাভৰ ৩ কৰ্মদিনৰ ভিতৰত স্বীকৃতি দিব লাগিব আৰু ৩০ দিনৰ ভিতৰত নিষ্পত্তি কৰিব লাগিব।
- **এস্কেলেচন মেট্ৰিক্স (Escalation Matrix):**
  যদি নিৰ্ধাৰিত সময়ছোৱাৰ ভিতৰত অভিযোগ নিষ্পত্তি নহয়, তেন্তে গ্ৰাহকে উচ্চতৰ স্তৰৰ প্ৰাধিকৰণ বা RBI-লৈ অভিযোগ Eskalate কৰিব পাৰে।
- **অভিযোগ দাখিলৰ ব্যৱস্থা (Complaint Registration):**
  বেংক আৰু PSP-এ ফোন, ইমেইল, অনলাইন ফৰ্ম আদিৰ জৰিয়তে অভিযোগ দাখিলৰ একাধিক মাধ্যম প্ৰদান কৰিব লাগিব।
- **বিবাদ নিষ্পত্তি ব্যৱস্থা (Dispute Resolution Mechanism):**
  যেতিয়া গ্ৰাহক আৰু ব্যৱসায়ী বা PSP-ৰ মাজত বিবাদ হয়, তেতিয়া এই

বিষয়ে নিষ্পত্তিৰ বাবে এক সুসংগঠিত ব্যৱস্থা থকা উচিত।

RBI-এ ডিজিটেল লেনদেনৰ বাবে এক বাধ্যতামূলক dispute resolution scheme প্ৰচলন কৰিছে, যি সকলো payment system operator-ৰ বাবে প্ৰযোজ্য।

শেষত ক'ব পাৰি RBI-ৰ এই অভিযোগ নিষ্পত্তি আৰু বিবাদ নিষ্পত্তি ব্যৱস্থাৰ লক্ষ্য হ'ল—গ্ৰাহকে ডিজিটেল লেনদেন সম্পৰ্কীয় যিকোনো অসুবিধাৰ ক্ষেত্ৰত উপযুক্ত ন্যায় আৰু সুৰক্ষা নিশ্চিত কৰা।

১১.৬ পেমেণ্ট ছেটেলমেণ্ট আইন, ২০০৭ (Payment Settlement Act, 2007)

১১.৬.১ পেমেণ্ট ছেটেলমেণ্ট আইন, ২০০৭-ৰ এক পৰ্যালোচনা (Overview of the Payment Settlement Act, 2007)

পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেম আইন, ২০০৭ হৈছে ভাৰতীয় আইনৰ অন্তৰ্গত এক বিধান, যিয়ে দেশে পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেমৰ নিয়ন্ত্ৰণ আৰু তদাৰকিৰ বাবে আইনি ব্যৱস্থা প্ৰদান কৰে।

এই আইন ২০০৭ চনৰ ডিচেম্বৰ মাহত ভাৰতীয় সংসদে অনুমোদন কৰে আৰু ২০০৮ চনৰ আগষ্ট মাহৰ পৰা কাৰ্যকৰী হয়।

এই আইনৰ মুখ্য উদ্দেশ্যসমূহ হ'ল:

ভাৰতত পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেমৰ উন্নয়ন আৰু নিয়ন্ত্ৰণক উৎসাহিত কৰা।

দেশত পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেমৰ স্থিতিশীলতা আৰু দক্ষতা নিশ্চিত কৰা।

পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেমত গ্ৰাহকৰ স্বাৰ্থ ৰক্ষা কৰা।

ইলেকট্ৰনিক পেমেণ্ট আৰু ছেটেলমেণ্ট ব্যৱহাৰ উৎসাহিত কৰা।

এই আইনৰ কিছুমান মুখ্য ধাৰা হ'ল—

পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেমৰ নিয়ন্ত্ৰণ:

এই আইনে ভাৰতীয় ৰিজাৰ্ভ বেংক (RBI)-ক পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেমৰ নিয়ন্ত্ৰণ আৰু তদাৰকিৰ ক্ষমতা প্ৰদান কৰে।

পেমেণ্ট ছিষ্টেম অপাৰেটৰৰ অনুমোদন:

আইন অনুসৰি, সকলো পেমেণ্ট ছিষ্টেম অপাৰেটৰে কাৰ্য আৰম্ভ কৰাৰ পূৰ্বে RBI-ৰ অনুমোদন লাভ কৰাটো বাধ্যতামূলক।

ছেটেলমেণ্টৰ চূড়ান্ততা (Settlement Finality):

এই আইনে "ছেটেলমেণ্ট চূড়ান্ততা"ৰ ব্যৱস্থা কৰে, অৰ্থাৎ এটা লেনদেন একবাৰ সম্পন্ন হ'লে, তাক পিছত উভটাই ল'ব নোৱাৰি।

Netting ব্যৱস্থা:

আইনটোৱে Netting-ৰ অনুমতি দিয়ে, অর্থাৎ এটা পেমেণ্টক আন এটা পেমেণ্টৰ সৈতে পৰস্পৰে হ্রাস কৰি ছেটেলমেণ্ট ৰিস্ক কমাব পৰা যায়।

গ্রাহক সুৰক্ষা (Consumer Protection):

এই আইন অনুসৰি, পেমেণ্ট ছিষ্টেম অপাৰেটৰসকলে গ্রাহকৰ তথ্যৰ সুৰক্ষা আৰু গোপনীয়তা নিশ্চিত কৰিব লাগিব, লগতে অভিযোগ নিষ্পত্তি ব্যৱস্থাও বজাই ৰাখিব লাগিব।

RBI-ৰ ক্ষমতা:

এই আইনে RBI-ক নির্দেশনা জাৰী, ফিচ আৰু মাচুল নিয়ন্ত্রণ, আৰু পেমেণ্ট অপাৰেটৰৰ পৰিদর্শনৰ ক্ষমতা প্রদান কৰে।

শোষত ক'ব পাৰি যে, পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেম আইন, ২০০৭-এ ভাৰতত পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেমসমূহৰ নিয়ন্ত্রণ আৰু তদাৰকিৰ বাবে এটা আইনি কাঠামো প্রদান কৰে, যাৰ মূল লক্ষ্য হ'ল দক্ষতা, স্থিতিশীলতা, আৰু গ্রাহক সুৰক্ষা নিশ্চিত কৰা।

১১.৬.২ পেমেণ্ট ছিষ্টেম, পেমেণ্ট গেটৱে, আৰু পেমেণ্ট ছেটেলমেণ্ট সম্পৰ্কীয় ধাৰাসমূহ (Provisions related to payment systems, payment gateways, and payment settlement)

পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেম আইন, ২০০৭-এ ভাৰতত পেমেণ্ট ছিষ্টেম, পেমেণ্ট গেটৱে আৰু পেমেণ্ট ছেটেলমেণ্ট-ৰ নিয়ন্ত্রণ আৰু তদাৰকিৰ বাবে ধাৰাসমূহ প্রদান কৰিছে। তলত এই ক্ষেত্রসমূহৰ সৈতে জড়িত কিছুমান মুখ্য ধাৰা উল্লেখ কৰা হ'ল—

পেমেণ্ট ছিষ্টেম (Payment Systems):

এই আইনে পেমেণ্ট ছিষ্টেমক এনে এক ছিষ্টেম হিচাপে সংজ্ঞায়িত কৰিছে, যিয়ে পেয়াৰ (payer) আৰু বেণিফিচিয়াৰী (beneficiary)ৰ মাজত পেমেণ্ট লেনদেন সলনি কৰিবলৈ সক্ষম। ইয়াত ক্রেডিট কার্ড লেনদেন, ইলেকট্রনিক ফাণ্ড স্থানান্তৰ (EFT), আৰু মোবাইল পেমেণ্ট প্রক্রিয়াক অন্তর্ভুক্ত কৰা হৈছে। এই আইনে ভাৰতীয় ৰিজার্ভ বেংক (RBI)-ক এই পেমেণ্ট ছিষ্টেমসমূহৰ নিয়ন্ত্রণ আৰু তদাৰকিৰ দায়িত্ব প্রদান কৰিছে।

পেমেণ্ট গেটৱে (Payment Gateways):

আইনে পেমেণ্ট গেটৱে হিচাপে সেইবোৰ সংস্থাক সংজ্ঞায়িত কৰিছে, যিয়ে বেপাৰী

(merchant) আৰু গ্ৰাহক (customer)ৰ মাজত পেমেণ্ট লেনদেন ৰাউট আৰু প্ৰক্ৰিয়া কৰিবলৈ প্ৰযুক্তি-ভিত্তিক অবকাঠামো (technology infrastructure) প্ৰদান কৰে। এই গেটৱে কাৰ্য আৰম্ভ কৰাৰ পূৰ্বে RBI-ৰ অনুমোদন লাভ কৰা বাধ্যতামূলক। এই আইনে পেমেণ্ট গেটৱে সমূহক গ্ৰাহকৰ তথ্যৰ সুৰক্ষা আৰু গোপনীয়তা নিশ্চিত কৰাৰ বাবে বাধ্যবাধকতা প্ৰদান কৰিছে।

পেমেণ্ট ছেটেলমেণ্ট (Payment Settlement):

আইনটোৱে Settlement Finality-ৰ ব্যৱস্থা কৰিছে, অৰ্থাৎ—এটা পেমেণ্ট লেনদেন একবাৰ সম্পন্ন হ'লে, তাক উভটাই ল'ব নোৱাৰি।

আইনটোৱে Netting-ৰ অনুমতি দিয়ে, অৰ্থাৎ পেমেণ্টসমূহ পৰস্পৰে সমন্বয় কৰি Settlement ৰিস্ক কমাব পাৰি।

উল্লেখযোগ্যভাৱে, এই আইন অনুসৰি এখন Payment and Settlement Systems Fund স্থাপন কৰাৰ ব্যৱস্থাও আছে, যাৰ জৰিয়তে পেমেণ্ট ইক'ছিষ্টেমত Settlement Risk হ্ৰাস কৰা হয়।

পেমেণ্ট ছিষ্টেম অপাৰেটৰসকলৰ অনুমোদন (Authorization of Payment System Operators):

আইন অনুসৰি, সকলো পেমেণ্ট ছিষ্টেম অপাৰেটৰে RBI-ৰ অনুমোদন লাভ কৰাৰ পাছতে কাৰ্য আৰম্ভ কৰিব পাৰে। এই আইনে RBI-ক পেমেণ্ট ছিষ্টেম অপাৰেটৰসকলক নিৰ্দেশনা জাৰি, ফিচ-মাচুল নিয়ন্ত্ৰণ, আৰু পৰিদৰ্শনৰ ক্ষমতা প্ৰদান কৰে।

গ্ৰাহক সুৰক্ষা (Consumer Protection):

আইন অনুসৰি, পেমেণ্ট ছিষ্টেম অপাৰেটৰ আৰু পেমেণ্ট গেটৱে সকলক গ্ৰাহকৰ তথ্যৰ সুৰক্ষা আৰু গোপনীয়তা নিশ্চিত কৰাৰ লগতে অভিযোগ নিষ্পত্তি ব্যৱস্থা বজাই ৰাখিবলৈ বাধ্য কৰে। এই আইনে তেওঁৰ ধাৰাসমূহ উলংঘা কৰাৰ বাবে জৰিমনা আৰু দণ্ডৰ ব্যৱস্থাও ৰাখিছে।

পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেম আইন, ২০০৭-এ ভাৰতত পেমেণ্ট ছিষ্টেম, পেমেণ্ট গেটৱে, আৰু ছেটেলমেণ্ট সম্পৰ্কে এক দৃঢ় আইনি কাঠামো প্ৰদান কৰিছে—যাৰ মূল লক্ষ্য হ'ল দক্ষতা, স্থিতিশীলতা, আৰু গ্ৰাহক সুৰক্ষা নিশ্চিত কৰা।

১১.৬.৩ এই আইনৰ অধীনত অনুমতি নথকা লেনদেন আৰু পেমেণ্ট প্ৰতাৰণাৰ আইনি দিশ (Legal implications of

unauthorized transactions and payment frauds under the Act)

পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেম আইন, ২০০৭-এ অনুমতি নথকা লেনদেন আৰু পেমেণ্ট প্ৰতাৰণাৰ ক্ষেত্ৰত আইনি দিশসমূহ স্পষ্টকৈ উল্লেখ কৰিছে। তলত এই ক্ষেত্ৰৰ সৈতে সম্পৰ্কিত কিছুমান মুখ্য ধাৰা দিয়া হৈছে—

অনুমতি নথকা লেনদেন (Unauthorized Transactions):

আইন অনুসৰি, পেমেণ্ট ছিষ্টেম অপাৰেটৰ আৰু পেমেণ্ট গেটৱে সকলে অনুমতি নথকা লেনদেন ৰোধ কৰিবলৈ যথেষ্ট সুৰক্ষা ব্যৱস্থা বজাই ৰাখিব লাগিব। যদি অনুমতি নথকা লেনদেন সংঘটিত হয়, তেন্তে সেই লেনদেনৰ পৰিস্থিতিৰ ওপৰত নিৰ্ভৰ কৰি পেমেণ্ট ছিষ্টেম অপাৰেটৰ, পেমেণ্ট গেটৱে, আৰু গ্ৰাহকৰ উত্তৰদায়িত্ব (liability) নিৰ্ধাৰণ কৰা হয়।

যদি গ্ৰাহকে যুক্তিসঙ্গত সময়ছোৱাৰ ভিতৰত পেমেণ্ট ছিষ্টেম অপাৰেটৰক সেই লেনদেনৰ বিষয়ে অৱগত কৰে, তেন্তে গ্ৰাহকৰ দায়বদ্ধতা সীমিত থাকে, যিটো RBI-য়ে নিৰ্ধাৰণ কৰা এক নিৰ্দিষ্ট পৰিমাণত সীমাবদ্ধ।

কিন্তু যদি গ্ৰাহকে সেই লেনদেনৰ বিষয়ে যুক্তিসঙ্গত সময়ছোৱাৰ ভিতৰত জনোৱা নাছিল, তেন্তে গ্ৰাহকৰ দায়বদ্ধতা অসীম (unlimited) হ'ব পাৰে।

পেমেণ্ট প্ৰতাৰণা (Payment Frauds):

এই আইনে পেমেণ্ট প্ৰতাৰণাৰ বাবে জৰিমনা আৰু দণ্ডৰ ব্যৱস্থা কৰিছে।

যিকোনো ব্যক্তি যদি পেমেণ্ট প্ৰতাৰণাত লিপ্ত হয়, তেন্তে তেওঁক সৰ্বাধিক তিনি বছৰ পৰ্যন্ত কাৰাদণ্ড, বা সৰ্বাধিক পাঁচ লাখ টকা পৰ্যন্ত জৰিমনা, বা উভয়তে দণ্ডিত কৰা হ'ব পাৰে। পেমেণ্ট ছিষ্টেম অপাৰেটৰ বা পেমেণ্ট গেটৱে যিসকলে এই আইনৰ ধাৰাসমূহ—বিশেষকৈ পেমেণ্ট প্ৰতাৰণা ৰোধ সংক্ৰান্ত ধাৰা উলংঘা কৰে, তেওঁলোকৰ ওপৰতো জৰিমনা আৰোপ কৰিব পৰা যায়।

গ্ৰাহক সুৰক্ষা (Consumer Protection):

আইন অনুসৰি, পেমেণ্ট ছিষ্টেম অপাৰেটৰ আৰু পেমেণ্ট গেটৱে সকলে অনুমতি নথকা লেনদেন আৰু পেমেণ্ট প্ৰতাৰণাৰ ক্ষেত্ৰত গ্ৰাহকৰ অভিযোগ নিষ্পত্তিৰ বাবে উপযুক্ত ব্যৱস্থা বজাই ৰাখিব লাগিব।

এই ক্ষেত্ৰত গ্ৰাহকে RBI-য়ে নিযুক্ত কৰা Ombudsman-ৰ ওচৰত অভিযোগ দাখিল কৰি সমাধান বিচাৰিব পাৰে।

এই আইনে RBI-লৈ ইয়াৰ অধীনস্থ পেমেণ্ট ছিষ্টেম অপাৰেটৰ আৰু পেমেণ্ট

গেটৱে-ৰ ওপৰত জৰিমনা আৰু দণ্ড আৰোপ কৰাৰ ক্ষমতা দিয়ে, যদি তেওঁলোকে গ্ৰাহকৰ স্বাৰ্থৰ সুৰক্ষা নিশ্চিত কৰিব নোৱাৰে।

পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেম আইন, ২০০৭-এ অনুমতি নথকা লেনদেন আৰু পেমেণ্ট প্ৰতাৰণাৰ ক্ষেত্ৰত আইনি কাঠামো প্ৰদান কৰিছে, যাৰ মুখ্য লক্ষ্য হৈছে— গ্ৰাহকৰ সুৰক্ষা নিশ্চিত কৰা, আৰু পেমেণ্ট ছিষ্টেমৰ স্থিতিশীলতা আৰু দক্ষতা অটুট ৰাখা।



অগ্ৰগতি নিৰীক্ষণ

প্ৰশ্ন নং ৩ : সঠিক বিকল্প বাচনি কৰকঃ

(ক) পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেম আইন, ২০০৭-ৰ মুখ্য উদ্দেশ্য কি?

(i) ভাৰতত পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেমৰ উন্নয়ন আৰু নিয়ন্ত্ৰণক উৎসাহিত কৰা।

(ii) পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেমত গ্ৰাহকৰ স্বাৰ্থৰ সুৰক্ষা নিশ্চিত কৰা।

(iii) ইলেকট্ৰনিক পেমেণ্ট আৰু ছেটেলমেণ্টৰ ব্যৱহাৰ উৎসাহিত কৰা।

iv) ওপৰৰ সকলো শুদ্ধ।

(খ) ভাৰতত ডিজিটেল পেমেণ্টৰ নিয়ন্ত্ৰণত RBI-ৰ ভূমিকা কি?

(i) নিৰ্দেশনা আৰু বিধিমালা প্ৰদান কৰা।

(ii) পৰ্যবেক্ষণ আৰু তদাৰকি কৰা।

(iii) লাইচেন্সিং আৰু অনুমোদন প্ৰদান কৰা।

(iv) ওপৰৰ সকলো শুদ্ধ।

(গ) ডিজিটেল লেনদেনত গ্ৰাহক সুৰক্ষাৰ বাবে RBI-ৰ নিৰ্দেশনা অনুসৰি দুই-স্তৰীয় প্ৰমাণীকৰণ ব্যৱস্থা কি?

(i) গ্ৰাহকে নিজৰ ৰেজিষ্টাৰ কৰা মোবাইল নম্বৰ বা ই-মেইললৈ পঠিওৱা OTP বা একক পাছৱৰ্ড প্ৰবিষ্ট কৰিব লাগে।

(ii) প্ৰতিটো লেনদেনৰ বাবে গ্ৰাহকে নিজৰ নাম আৰু ঠিকনা প্ৰদান কৰিব লাগে।

(iii) প্ৰতিটো লেনদেনৰ বাবে গ্ৰাহকে নিজৰ বেংক একাউণ্ট নম্বৰ আৰু IFSC ক'ড প্ৰদান কৰিব লাগে।

(iv) প্ৰতিটো লেনদেনৰ বাবে গ্ৰাহকে নিজৰ আধাৰ নম্বৰ প্ৰদান কৰিব লাগে।

(ঘ) ডিজিটেল পেমেণ্ট সম্পৰ্কে RBI-ৰ নিৰ্দেশনা অনুসৰি অভিযোগ নিষ্পত্তি ব্যৱস্থাত অভিযোগ নিষ্পত্তি বিষয়াৰ (Grievance Redressal Officer) ভূমিকা কি?

(i) সংগঠনৰ ভিতৰত গ্ৰাহকক উচ্চপদস্থ কৰ্তৃপক্ষৰ ওচৰত নিযুক্তি দিয়াৰ ব্যৱস্থা কৰা।

(ii) গ্ৰাহকে অভিযোগ দাখিল কৰিবলৈ একাধিক মাধ্যম প্ৰদান কৰা।

(iii) ডিজিটেল লেনদেন সম্পৰ্কীয় গ্ৰাহকৰ অভিযোগ সমাধান কৰা।

(iv) গ্ৰাহক আৰু বেপাৰী বা পেমেণ্ট সেৱা প্ৰদানকাৰীৰ মাজৰ বিবাদৰ বাবে এক নিষ্পত্তি ব্যৱস্থা প্ৰদান কৰা।

(ঙ) ডিজিটেল লেনদেনৰ বাবে RBI-এ প্ৰবৰ্তন কৰা বিবাদ নিষ্পত্তি আঁচনি কি?

(i) ছেটেলমেণ্ট ৰিস্ক হ্ৰাস কৰিবলৈ Netting পদ্ধতি।

(ii) প্ৰতাৰণা বা অনুমতি নথকা লেনদেন RBI-লৈ ৰিপ'ৰ্ট কৰাৰ এক পদ্ধতি।

(iii) সকলো পেমেণ্ট ছিষ্টেম অপাৰেটৰসকলৰ বাবে বাধ্যতামূলক বিবাদ নিষ্পত্তি ব্যৱস্থা।

(iv) চাইবাৰ আক্ৰমণৰ পৰা গ্ৰাহকৰ ব্যক্তিগত আৰু বিত্তীয় তথ্য ৰক্ষাৰ বাবে এক সুৰক্ষা ব্যৱস্থা।



১১.৭ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ

- **ডিজিটেল পেমেণ্টত সাধাৰণভাৱে হোৱা প্ৰতাৰণাসমূহ**ৰ ভিতৰত পৰিচয় চুৰি, ফিছিং স্কেম, অনুমতি নথকা লেনদেন, পেমেণ্ট গেটৱে প্ৰতাৰণা, ভুৱা পেমেণ্ট এপ, মেলৱেয়াৰ আক্ৰমণ, QR ক'ড প্ৰতাৰণা আৰু SIM সোৱাপ প্ৰতাৰণাৰ কথা উল্লেখযোগ্য।
- এই প্ৰতাৰণাসমূহে আৰ্থিক ক্ষতি, ক্ৰেডিট স্ক'ৰৰ ক্ষতি আৰু পৰিচয় চুৰিৰ দৰে সমস্যা সৃষ্টি কৰিব পাৰে।
- এই প্ৰতাৰণাৰ পৰা ৰক্ষা পাবলৈ, ব্যৱহাৰকাৰীসকলে নিজৰ পেমেণ্ট তথ্য সুৰক্ষিত ৰাখিব, বিশ্বস্ত পেমেণ্ট প্ৰচালক ব্যৱহাৰ কৰিব, কেৱল বিশ্বাসযোগ্য উৎসৰ পৰা এপ ডাউনলোড কৰিব আৰু নিজৰ বিত্তীয় একাউণ্ট নিয়মিতভাৱে পৰ্যবেক্ষণ কৰিব লাগে।
- অচিনাকী উৎসৰ পৰা অহা লিংকত ক্লিক কৰাৰ সময়ত বা এটাচমেন্ট ডাউনলোড কৰাৰ সময়ত সাৱধান হ'ব লাগিব আৰু ব্যক্তিগত তথ্য আৰু পাছৱৰ্ডৰ সুৰক্ষাৰ ক্ষেত্ৰত সদায় সচেতন থাকিব লাগে।
- ডিজিটেল পেমেণ্ট প্ৰতাৰণাৰ পৰা ৰক্ষা পাবলৈ **নিৰাপদ ব্ৰাউজিং অভ্যাস** আৰু **ফলপ্ৰসূ পাছৱৰ্ড ব্যৱস্থাপনা**, যেনে শক্তিশালী পাছৱৰ্ড আৰু পাছৱৰ্ড মেনেজাৰ ব্যৱহাৰ কৰাটো জৰুৰী।
- **ফিছিং স্কেমৰ পৰা সতৰ্ক থাকিব**, যি গুপ্ত তথ্য লাভ কৰিবলৈ কৰা এক ধোকা দিয়াৰ প্ৰয়াস, লগতে **নিৰাপদ ব্ৰাউজাৰ** ব্যৱহাৰ কৰক আৰু **চফটৱেৰ সদায় আপডেট কৰি ৰাখক**।

- **দুই-স্তৰীয় প্ৰমাণীকৰণ (2FA)** আৰু **বায়োমেট্ৰিক প্ৰমাণীকৰণ** লগইন প্ৰক্ৰিয়াখনত অতিৰিক্ত সুৰক্ষা প্ৰদান কৰে আৰু অনুমতি নথকা প্ৰৱেশ ৰোধ কৰে।
- বিত্তীয় প্ৰতিষ্ঠানসকলে **প্ৰতাৰণা চিনাক্ত আৰু ৰোধ কৰাৰ বাবে সুৰক্ষা ছিষ্টেম** প্ৰয়োগ কৰিব লাগে।
- **পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেম আইন, ২০০৭** হৈছে ভাৰতীয় আইন, যিয়ে দেশে পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেমৰ নিয়ন্ত্ৰণ আৰু তদাৰকি নিশ্চিত কৰে।
- এই আইনে **পেমেণ্ট ছিষ্টেম অপাৰেটৰসকলৰ অনুমোদন, ছেটেলমেণ্টৰ চূড়ান্ততা, Netting, আৰু গ্ৰাহক সুৰক্ষাৰ** ব্যৱস্থা প্ৰদান কৰে।
- আইনটোৱে **পেমেণ্ট ছিষ্টেম, পেমেণ্ট গেটৱে, আৰু ছেটেলমেণ্ট** সংজ্ঞায়িত কৰি, **গ্ৰাহকৰ তথ্যৰ সুৰক্ষা আৰু গোপনীয়তা বজাই ৰখা** নিশ্চিত কৰিবলৈ পেমেণ্ট গেটৱে সকলক বাধ্য কৰে।
- **এই আইন অনুসৰি অনুমতি নথকা লেনদেন আৰু পেমেণ্ট প্ৰতাৰণাৰ ক্ষেত্ৰত আইনগত দণ্ড, জৰিমনা, আৰু পেমেণ্ট ছিষ্টেম অপাৰেটৰ, গেটৱে আৰু গ্ৰাহকৰ দায়বদ্ধতা** নিৰ্ধাৰণ কৰা হৈছে।

১১.৮ অগ্ৰগতিৰ খতিয়ান

১ নং উত্তৰ প্ৰশ্নৰ:

(ক) (iv) (খ) (i) (গ) (iv) (ঘ) (i) (ঙ) (iii)

(চ) (i) (ছ) (iii) (জ) (i) (ঝ) (iv) (ঞ) (iv)

২ নং উত্তৰ প্ৰশ্নৰ:

(ক): এটা শক্তিশালী পাছৱৰ্ডত আপাৰ কেচ আৰু লৱাৰ কেচৰ আখৰ, সংখ্যা আৰু চিহ্নৰ সমন্বয় থাকে।

(খ): পাছৱৰ্ড মেনেজাৰ হৈছে এনে এটা ছফ্টৱেৰ যি আপোনাৰ বিভিন্ন একাউণ্টৰ পাছৱৰ্ড সৃষ্টি, সংৰক্ষণ আৰু পৰিচালনা কৰাত সহায় কৰে।

(গ): ইমেইল স্কেম, ভুৱা ৱেবছাইট, SMS স্কেম, স্পিয়াৰ ফিছিং, আৰু ছচিয়েল মিডিয়া স্কেমসমূহ ফিছিংৰ কিছুমান উদাহৰণ।

(ঘ): দুই-স্তৰীয় প্ৰমাণীকৰণ (2FA) হৈছে এনে এক সুৰক্ষা প্ৰক্ৰিয়া, য'ত ব্যৱহাৰকাৰীয়ে লগইনৰ পূৰ্বে দুই ধৰণৰ পৰিচয় প্ৰদান কৰে।

(ঙ): এটা নিৰাপদ ব্ৰাউজাৰ ব্যৱহাৰৰ বাবে, উন্নত সুৰক্ষা থকা ব্ৰাউজাৰ বাচনি কৰক, সদায় আপডেট কৰি ৰাখক, উপযোগী extension ইনষ্টল কৰক, Privacy Settings কনফিগাৰ কৰক, বিপদজনক ৱেবছাইট এৰাই চলক, HTTPS সংযোগ চাওক, আৰু ডাউনলোডৰ ক্ষেত্ৰত সতৰ্ক থাকক।

৩ নং উত্তৰ প্ৰশ্নৰ:

(ক) (iv) (খ) (iv) (গ) (i) (ঘ) (iii) (ঙ) (iii)



১১.৯ অধিক জানিবলৈ

Cyber Crime Impact in the New Millennium, by R. C Mishra , Auther Press. Edition 2010.

Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)

Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson, 13th November, 2001)

Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.

Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.

Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.

Fundamentals of Network Security by E. Maiwald, McGraw Hill.



১১.১০ আৰ্হি প্ৰশ্নসমূহ

প্ৰশ্ন ১ : পেমেণ্ট গেটৱে প্ৰতাৰণাৰ কিছুমান সাধাৰণ প্ৰকাৰ কি? আৰু সেইবোৰ কেনেদৰে ৰোধ কৰিব পাৰি?

প্ৰশ্ন ২ : ডিজিটেল পেমেণ্টত পৰিচয় চুৰি আৰু ফিছিং স্কেমৰ পৰা সুৰক্ষা পাবলৈ কিছুমান সৰ্বোত্তম অভ্যাস কি?

প্ৰশ্ন ৩ : ভুৱা পেমেণ্ট এপ কেনেদৰে কাম কৰে? আৰু সেইবোৰৰ পৰা ৰক্ষা পাবলৈ কিহৰ সাৱধানতা ল'ব লাগে?

প্ৰশ্ন ৪: QR ক'ড প্ৰতাৰণা আৰু SIM সোৱাপ প্ৰতাৰণাৰ বিপদসমূহ কি? আৰু সেইবোৰৰ পৰা নিজকে কেনেদৰে সুৰক্ষিত ৰাখিব পাৰি?

প্ৰশ্ন ৫ : অনুমতি নথকা লেনদেন বা পেমেণ্ট গেটৱে প্ৰতাৰণাৰ চিকাৰ হোৱা ভুক্তভোগীয়ে ল'ব লগা মুখ্য পদক্ষেপসমূহ কি?

প্ৰশ্ন ৬ : শক্তিশালী পাছৱৰ্ড বুলিলে কি বুজায়? আৰু সেয়া কিয় গুৰুত্বপূৰ্ণ?

প্ৰশ্ন ৭ : পাছৱৰ্ড মেনেজাৰ বুলিলে কি বুজায়? আৰু সেয়া ডিজিটেল পেমেণ্ট প্ৰতাৰণা ৰোধত কেনেদৰে সহায় কৰে?

প্ৰশ্ন ৮ : ফিছিং স্কেমৰ কিছুমান সাধাৰণ ধৰণ কি? আৰু সেইবোৰ কেনেদৰে এৰাই চলিব পাৰি?

প্ৰশ্ন ৯ : দুই-স্তৰীয় প্ৰমাণীকৰণ (2FA) বুলিলে কি বুজায়? তেনে লগইন প্ৰক্ৰিয়াই কেনেদৰে সুৰক্ষা বৃদ্ধি কৰে?

প্ৰশ্ন ১০ : কেইটামান নিৰাপদ ব্ৰাউজিং অভ্যাস উল্লেখ কৰক? সেইবোৰে কেনেদৰে ডিজিটেল পেমেণ্ট প্ৰতাৰণাৰ পৰা ৰক্ষা কৰে?

প্ৰশ্ন ১১ : ভাৰতত ডিজিটেল পেমেণ্টৰ নিয়ন্ত্ৰণত RBI-ৰ ভূমিকা কি?

প্ৰশ্ন ১২ : ডিজিটেল লেনদেনত গ্ৰাহক সুৰক্ষাৰ বাবে RBI-এ জাৰি কৰা কিছুমান নিৰ্দেশনা কি?

প্ৰশ্ন ১৩ : RBI-ৰ নিৰ্দেশনা অনুসৰি অভিযোগ নিষ্পত্তি আৰু বিবাদ নিষ্পত্তি ব্যৱস্থাসমূহ কি কি?

প্ৰশ্ন ১৪ : **পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেম আইন, ২০০৭**-ৰ মুখ্য উদ্দেশ্যসমূহ কি?

প্ৰশ্ন ১৫ : ভাৰতত পেমেণ্ট আৰু ছেটেলমেণ্ট ছিষ্টেমৰ নিয়ন্ত্ৰণৰ সৈতে সম্পৰ্কিত এই আইনৰ কিছুমান ধাৰা কি কি?

অধ্যায় ১২: ডিজিটেল ডিভাইচৰ সুৰক্ষা—১

অধ্যায় গাঁথনি

১২.১ উদ্দেশ্য
১২.২ পৰিচয়
১২.৩ এণ্ড পইণ্ট ডিভাইচ আৰু মোবাইল ফোনৰ সুৰক্ষা
১২.৪ পাছৱৰ্ড নীতি
১২.৫ সুৰক্ষা পেটচ ব্যৱস্থাপনা
১২.৬ ডাটা বেকআপ
১২.৭ তৃতীয় পক্ষৰ চফটৱেৰ ডাউনলোড আৰু পৰিচালনা
১২.৮ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ
১২.৯ অধিক জনিবলৈ
১২.১০ অগ্রগতিৰ খতিয়ান
১২.১১ আৰ্হি প্রশ্ন

১২.১ উদ্দেশ্য

এই অধ্যায়টি অধ্যয়ন কৰি আপুনি—

- ডিজিটেল ডিভাইচ সুৰক্ষাৰ মূল ধাৰণাসমূহ বুজিবলৈ সক্ষম হ'ব
- ডিভাইচ সুৰক্ষা নীতি আৰু পাছৱৰ্ড নীতি সম্পর্কে অৱগত হ'ব
- ক'ড বাগ (Code bug) বা চিষ্টেম এপ্লিকেচনসমূহত থকা বাগসমূহ নাইকিয়া কৰিব পাৰিব
- তৃতীয় পক্ষৰ চফটৱেৰ ডাউনলোড আৰু পৰিচালনা কৰিব পাৰিব

১১.২ পৰিচয়

এই অধ্যায়ত আমি ডিজিটেল ডিভাইছ সুৰক্ষাৰ (Digital Device Security) মৌলিক ধাৰণাবোৰৰ বিষয়ে শিকিম। ডিজিটেল ডিভাইছ সুৰক্ষা হৈছে অনানুমোদিত প্ৰৱেশ, ব্যৱহাৰ, প্রকাশ, বিঘ্নিতকৰণ, পৰিৱর্তন বা ধ্বংসৰ পৰা ডিজিটেল তথ্য আৰু প্রযুক্তি সম্পদৰ সুৰক্ষা কৰা। ইয়াত তথ্য আৰু ব্যৱস্থাসমূহৰ গোপনীয়তা, অখণ্ডতা আৰু উপলব্ধতা নিশ্চিত কৰাৰ বাবে বিভিন্ন প্রকাৰৰ ব্যৱস্থা অন্তর্ভুক্ত কৰা হয়। ডিজিটেল ডিভাইছ সুৰক্ষাই নেটৱর্ক সুৰক্ষা, তথ্য সুৰক্ষা, এপ্লিকেচন সুৰক্ষা আৰু ডিভাইছ সুৰক্ষাৰ

দৰে বিভিন্ন ক্ষেত্রক সামৰি লয়। ইয়াত এনক্রিপশন, ফায়াৰৱল, এণ্টিভাইৰাছ ছফ্টৱেৰ, প্ৰৱেশ নিয়ন্ত্রণ আৰু অন্যান্য সা-সঁজুলি আৰু কৌশল ব্যৱহাৰ কৰি মেলৱেৰ, ফিছিং আক্রমণ, হেকিং আৰু পৰিচয় চুৰিৰ দৰে চাইবাৰ বিপদৰ পৰা ডিজিটেল সম্পদক সুৰক্ষিত কৰা হয়। ডিজিটেল ডিভাইছ সুৰক্ষা আজিৰ যুগত অতি প্রয়োজনীয়, য'ত প্রযুক্তি আমাৰ জীৱনৰ প্রতিটো দিশত সঘনাই সংহত হৈ আছে আৰু সংবেদনশীল তথ্য ইলেক্ট্রনিকভাৱে সংৰক্ষণ আৰু প্রেৰণ কৰা হয়। ফলপ্রসূ ডিজিটেল ডিভাইছ সুৰক্ষা অনুশীলনে ডটা ভংগ হোৱাৰ পৰা ৰক্ষা কৰিব পাৰে, ব্যক্তিগত গোপনীয়তা ৰক্ষা কৰিব পাৰে আৰু গুৰুত্বপূর্ণ কাঠামো আৰু ৰাষ্ট্রীয় সুৰক্ষা সুৰক্ষিত কৰিব পাৰে। এই অধ্যায়ত, বিভিন্ন এণ্ডপইণ্ট ডিভাইছসমূহ সুৰক্ষিত কৰি আমি এটা সংস্থাৰ নেটৱর্ক আৰু ডাটাক সম্ভাব্য সুৰক্ষা বিপদৰ পৰা কেনেকৈ ৰক্ষা কৰিব পাৰি সেই বিষয়েও আলোচনা কৰিম। আমি ডিভাইছ সুৰক্ষা নীতি, সুৰক্ষা প্যাচ ব্যৱস্থাপনা, ডাটা বেকআপৰ ধাৰণা আৰু তৃতীয় পক্ষৰ ছফ্টৱেৰ ডাউনলোড আৰু ব্যৱস্থাপনাৰ বাবে কিছুমান শ্রেষ্ঠ অনুশীলনৰ বিষয়েও আলোচনা কৰিম।

১২.৩ এণ্ড পইণ্ট ডিভাইচ আৰু মোবাইল ফোনৰ সুৰক্ষা

এণ্ডপইণ্ট ডিভাইচসমূহ, যাক ডাটাৰ শেষ ব্যৱহাৰকাৰী ডিভাইচসমূহ বুলিও কোৱা হয়। নে'টৱর্কৰ জৰিয়তে পঠোৱা ডাটা পেকেটসমূহৰ চূড়ান্ত গন্তব্যস্থানকে যি কোনো এটা নে'টৱর্কত এটা এণ্ডপইণ্ট হিচাপে বিবেচনা কৰা হয় । এণ্ডপইণ্ট ডিভাইচসমূহৰ কিছুমান সাধাৰণ উদাহৰণ হ'ল—

- ডেস্কটপ কম্পিউটাৰ
- লেপটপ
- টেবলেট
- স্মার্টফোন
- প্রিণ্টাৰসমূহ
- স্কেনাৰ
- কপিকাৰক
- ফেক্স মেচিন
- আই পি ফোন
- ভিঅ'আইপি ফোন
- পি অ' এছ (পইণ্ট অৱ চেল) ব্যৱস্থা
- চিকিৎসা সঁজুলি
- ঔদ্যোগিক নিয়ন্ত্রণ ব্যৱস্থা

- স্মার্ট হোম ডিভাইচ, যেনে স্মার্ট থার্মোষ্টেট আৰু সুৰক্ষা ব্যৱস্থা
- ইণ্টাৰনেট অৱ থিংছ (IoT) ডিভাইচ, যেনে স্মার্ট ঘড়ী আৰু ফিটনেছ ট্রেকাৰ আদি।

চাইবাৰ ভাবুকিৰ বাবে এণ্ডপইণ্ট ডিভাইচসমূহ প্রায়ে আটাইতকৈ দুর্বল প্রৱেশ বিন্দু, কাৰণ ইয়াক সাধাৰণতে কর্মচাৰীসকলে জটিল ব্যৱসায়িক তথ্য প্রৱেশ কৰিবলৈ ব্যৱহাৰ কৰে আৰু নেটৱর্কত প্রৱেশ লাভ কৰিব বিচৰা হেকাৰসকলে ইয়াক সহজে লক্ষ্য কৰি ল'ব পাৰে। ইয়াৰ ফলত এণ্ডপইণ্ট সুৰক্ষা সমাধানৰ বিকাশ ঘটিছে, যিবোৰ এই ডিভাইচসমূহক মেলৱেৰ, ভাইৰাছ আৰু অন্যান্য চাইবাৰ ভাবুকিৰ পৰা সুৰক্ষিত কৰিবলৈ ডিজাইন কৰা হৈছে। এণ্ডপইণ্ট সুৰক্ষা সমাধানসমূহে সাধাৰণতে এণ্টিভাইৰাছ চফটৱেৰ, ফায়াৰৱাল, অনুপ্রৱেশ ধৰা পেলোৱা ব্যৱস্থাপ্রণালী আৰু এণ্ডপইণ্ট ব্যৱস্থাপনা সঁজুলিসমূহ অন্তর্ভুক্ত কৰা হয়। যি এটা নে'টৱর্কত এণ্ডপইণ্ট ডিভাইচসমূহৰ সুৰক্ষা নিৰীক্ষণ আৰু ব্যৱস্থাপনা কৰিবলে ব্যৱহাৰ কৰিব পাৰি। ইয়াত ডাটা এনক্রিপচন, সুৰক্ষিত দূ�ৰৱর্তী প্রৱেশ আৰু স্পর্শকাতৰ তথ্যৰ অকর্তৃত্বশীল প্রৱেশ প্রতিৰোধ কৰিবলৈ প্রৱেশ নিয়ন্ত্রণৰ দৰে বৈশিষ্ট্যসমূহো অন্তর্ভুক্ত হ'ব পাৰে।

বহু সংস্থাই যিহেতু দূৰৱর্তী কামৰ নীতি গ্রহণ কৰিছে আৰু মোবাইল ডিভাইচসমূহ ক্রমান্বয়ে প্রচলিত হৈছে, সেইবাবে এইবোৰ এণ্ডপইণ্ট সুৰক্ষা সামগ্রিক চাইবাৰ সুৰক্ষা কৌশলৰ এক জটিল উপাদান হিচাপে পৰিণত হৈছে। ফলপ্রসূ এণ্ডপইণ্ট সুৰক্ষাৰ বাবে প্রযুক্তিগত সমাধান আৰু কর্মচাৰী প্রশিক্ষণ আৰু সজাগতা কার্যসূচী দুয়োটাকে ধৰি বহুস্তৰীয় পদ্ধতিৰ প্রয়োজন, যাতে এণ্ডপইণ্ট ডিভাইচসমূহ সুৰক্ষিত আৰু চাইবাৰ ভাবুকিৰ পৰা সুৰক্ষিত হয়।

এণ্ডপইণ্ট সুৰক্ষা হৈছে এণ্ডপইণ্টসমূহ, যেনে লেপটপ, ডেস্কটপ, মোবাইল ডিভাইচ আৰু অন্য স্মার্ট ডিভাইচসমূহ সুৰক্ষিত কৰি এটা প্রতিষ্ঠানৰ নেটৱর্ক আৰু ডাটাক সম্ভাব্য সুৰক্ষা ভাবুকিৰ পৰা সুৰক্ষা কৰা। এণ্ডপইণ্ট ডিভাইচ সুৰক্ষা স্থাপত্য হৈছে এটা বিস্তৃত সুৰক্ষা সমাধানৰ ডিজাইন যিয়ে এণ্ডপইণ্টসমূহক সম্ভাব্য সুৰক্ষা ভাবুকিৰ পৰা সুৰক্ষিত কৰিবলৈ বিভিন্ন সুৰক্ষা ব্যৱস্থা অন্তর্ভুক্ত কৰে। এণ্ডপইণ্ট সুৰক্ষা ধাৰণাটিত সুৰক্ষা ব্যৱস্থাৰ বিভিন্ন স্তৰ অন্তর্ভুক্ত কৰা হয় যিয়ে এণ্ডপইণ্টসমূহক সম্ভাব্য সুৰক্ষা ভাবুকিৰ পৰা ৰক্ষা কৰিবলৈ একেলগে কাম কৰে। এই ব্যৱস্থাসমূহৰ ভিতৰত আছে—

এণ্ডপইণ্ট সুৰক্ষা প্লেটফর্ম (EPP):

EPP হৈছে এটা সুৰক্ষা সমাধান যিয়ে এণ্ডপইণ্টসমূহক মেলৱেৰ, ভাইৰাছ আৰু অন্যান্য ক্ষতিকাৰক চফটৱেৰৰ পৰা সুৰক্ষা দিয়ে। EPP-ত এণ্টিভাইৰাছ, ফায়াৰৱাল, অনুপ্ৰৱেশ ধৰা পেলোৱা আৰু প্ৰতিৰোধ ব্যৱস্থাৰ দৰে বৈশিষ্ট্যসমূহ অন্তৰ্ভুক্ত কৰা হৈছে।

এণ্ডপইণ্ট ধৰা পেলোৱা আৰু সঁহাৰি (Endpoint detection and response-EDR): EDR হৈছে এটা সুৰক্ষা সমাধান যি বাস্তৱ-সময়ৰ ভাবুকি ধৰা পেলোৱা আৰু সম্ভাব্য সুৰক্ষা ভাবুকিৰ প্ৰতি সঁহাৰি প্ৰদান কৰে। EDR-ত এণ্ডপইণ্ট আচৰণ বিশ্লেষণ, ভাবুকি আৰু কাণ্ডৰ সঁহাৰিৰ দৰে বৈশিষ্ট্যসমূহ অন্তৰ্ভুক্ত কৰা হৈছে।

পেটচ ব্যৱস্থাপনা (Patch management): পেটচ ব্যৱস্থাপনা হৈছে শেহতীয়া সুৰক্ষা পেটচ আৰু আপডেটসমূহৰ সৈতে এণ্ডপইণ্টসমূহত চফটৱেৰ আৰু এপ্লিকেচনসমূহ আপডেট কৰাৰ প্ৰক্ৰিয়া। পেটচ ব্যৱস্থাপনাই এণ্ডপইণ্টসমূহৰ জনা দুৰ্বলতাৰ পৰা সুৰক্ষিত হোৱাটো নিশ্চিত কৰাত সহায় কৰে।

মোবাইল ডিভাইচ ব্যৱস্থাপনা (MDM): MDM হৈছে এটা সুৰক্ষা সমাধান যিয়ে মোবাইল ডিভাইচ, যেনে স্মাৰ্টফোন আৰু টেবলেট পৰিচালনা আৰু সুৰক্ষিত কৰে। MDM-এ ডিভাইচ ইনক্ৰিপচন, দূৰৱৰ্তীভাৱে ডাটাখিনি মচি পেলোৱা আৰু এপ্লিকেচন হুৱাইট লিষ্টিঙৰ দৰে বৈশিষ্ট্যসমূহ অন্তৰ্ভুক্ত কৰে।

ডাটা লছ প্ৰিভেনচন (DLP): DLP হৈছে এটা সুৰক্ষা সমাধান যিয়ে স্পৰ্শকাতৰ ডাটা সংস্থাৰ নেটৱৰ্ক এৰি যোৱাত বাধা দিয়ে। DLP-এ বৈশিষ্ট্যসমূহ যেনে বিষয়বস্তু ফিল্টাৰিং, তথ্য শ্ৰেণীবিভাজন আৰু তথ্য এনক্ৰিপচন অন্তৰ্ভুক্ত।

পৰিচয় আৰু প্ৰৱেশ ব্যৱস্থাপনা (IAM): IAM হৈছে এটা সুৰক্ষা সমাধান যিয়ে ব্যৱহাৰকাৰীৰ পৰিচয় আৰু শেষ বিন্দু আৰু তথ্যলৈ প্ৰৱেশ পৰিচালনা কৰে। IAM-এ বৈশিষ্ট্যসমূহ যেনে বহু-কাৰক প্ৰমাণীকৰণ, পাছৱৰ্ড ব্যৱস্থাপনা আৰু ভূমিকা-ভিত্তিক প্ৰৱেশ নিয়ন্ত্ৰণ অন্তৰ্ভুক্ত ।

এণ্ডপইণ্ট ডিভাইচ সুৰক্ষাৰ স্থাপত্য প্ৰতিষ্ঠানৰ সুৰক্ষা নীতি আৰু বিপদ ব্যৱস্থাপনা কৌশলৰ ওপৰত ভিত্তি কৰি ডিজাইন কৰিব লাগে। প্ৰতিষ্ঠানৰ পৰিৱৰ্তিত সুৰক্ষা প্ৰয়োজনীয়তাসমূহ গ্ৰহণ কৰিবলৈ স্থাপত্য নমনীয় আৰু স্কেলেবল হ'ব লাগে। ইয়াৰ উপৰি, স্থাপত্যক নিয়মিতভাৱে আপডেট আৰু পৰীক্ষা কৰা উচিত যাতে ই সম্ভাব্য সুৰক্ষা ভাবুকিৰ বিৰুদ্ধে ফলপ্ৰসূ হয়।

এণ্ডপইণ্ট ডিভাইচ সুৰক্ষা স্থাপত্য এটা প্ৰতিষ্ঠানৰ নে'টৱৰ্ক আৰু ডাটাক সম্ভাব্য সুৰক্ষা ভাবুকিৰ পৰা সুৰক্ষিত কৰাত গুৰুত্বপূৰ্ণ। স্থাপত্যত সুৰক্ষা ব্যৱস্থাৰ বিভিন্ন স্তৰ অন্তৰ্ভুক্ত কৰা হৈছে, যেনে ইপিপি, ইডিআৰ, পেটচ ব্যৱস্থাপনা, এমডিএম, ডিএলপি, আৰু আইএএম, যিয়ে একেলগে কাম কৰি এণ্ডপইণ্টসমূহৰ বাবে এটা বিস্তৃত সুৰক্ষা সমাধান প্ৰদান কৰে। এটা সু-ডিজাইন কৰা এণ্ডপইণ্ট ডিভাইচ সুৰক্ষা আৰ্কিটেকচাৰে সুৰক্ষা বিপদসমূহ কম কৰাত সহায় কৰিব পাৰে আৰু প্ৰতিষ্ঠানৰ মূল্যৱান সম্পত্তিসমূহ সুৰক্ষিত কৰিব পাৰে।

আনহাতে, মোবাইল ছিকিউৰিটি বা মোবাইল ডিভাইচ ছিকিউৰিটি হৈছে স্মাৰ্টফোন, টেবলেট, লেপটপক বেতাঁৰ কম্পিউটিং ভাবুকিৰ পৰা সুৰক্ষা দিয়া। মোবাইল কম্পিউটিঙত ইয়াৰ গুৰুত্ব বাঢ়িছে। স্মাৰ্টফোনত সংৰক্ষিত ব্যক্তিগত আৰু ব্যৱসায়িক তথ্যৰ সুৰক্ষা আজিকালি বিশেষ চিন্তাৰ বিষয়।

বেছিভাগ ব্যৱহাৰকাৰী আৰু কোম্পানীয়ে কেৱল যোগাযোগৰ বাবেই নহয়, নিজৰ কৰ্ম আৰু ব্যক্তিগত জীৱনৰ পৰিকল্পনা আৰু সংগঠিত কৰিবলৈও স্মাৰ্টফোন ব্যৱহাৰ কৰে। কোম্পানীসমূহৰ ভিতৰত এই প্ৰযুক্তিসমূহে তথ্য ব্যৱস্থাৰ সংগঠনত গভীৰ পৰিৱৰ্তন আনে আৰু এইদৰে নতুন বিপদৰ উৎস হৈ পৰে। শুদ্ধকৈয়ে স্মাৰ্টফোনে ক্ৰমান্বয়ে স্পৰ্শকাতৰ তথ্য সংগ্ৰহ আৰু সংকলন কৰে, যাৰ প্ৰৱেশ নিয়ন্ত্ৰণ কৰি ব্যৱহাৰকাৰীৰ গোপনীয়তা আৰু কোম্পানীসমূহৰ বৌদ্ধিক সম্পত্তি সুৰক্ষিত কৰিব লাগিব। বেছিভাগ আক্ৰমণে স্মাৰ্টফোনক লক্ষ্য কৰি লয়। এই আক্ৰমণসমূহে স্মাৰ্টফোনত উপস্থিত থকা দুৰ্বলতাসমূহ আহৰণ কৰে যিবোৰ বিভিন্ন যোগাযোগ পদ্ধতিৰে সৃষ্টি কৰিব পাৰি, য'ত আছে চুটি বাৰ্তা সেৱা (এছএমএছ), মাল্টিমিডিয়া বাৰ্তা সেৱা (এমএমএছ), বেতাঁৰ, ব্লুটুথ আৰু জিএছএম সংযোগ, যিবোৰ বাস্তৱিকতে আন্তঃৰাষ্ট্ৰীয় মানদণ্ডৰ। ক'ড বিভাজন বহু প্ৰৱেশ (CDMA) অন্য যোগাযোগ পদ্ধতিতকৈ অধিক সুৰক্ষিত, কিন্তু তথাপি এটা লক্ষ্য হ'ব পাৰে। আন এটা দুৰ্বলতা হ'ল স্মাৰ্টফোনৰ অপাৰেটিং চিষ্টেম বা ব্ৰাউজাৰ। কিছুমান মেলৱেৰে সাধাৰণ ব্যৱহাৰকাৰীৰ সীমিত জ্ঞানৰ বাবেই ভাবুকিৰ সৃষ্টি কৰে। ২০০৮ চনৰ McAfee এক অধ্যয়ন অনুসৰি মাত্ৰ ২.১% ব্যৱহাৰকাৰীয়েহে কয় যে তেওঁলোকে প্ৰত্যক্ষভাৱে মোবাইল মেলৱেৰৰ সংস্পৰ্শলৈ আহিছে, য'ত প্ৰকাশ পাইছে যে ১১.৬% ব্যৱহাৰকাৰীয়ে এই সমস্যাৰ দ্বাৰা প্ৰভাৱিত হোৱা আন লোকৰ কথা শুনিছে। অৱশ্যে এই সংখ্যা বৃদ্ধি হোৱাৰ সম্ভাৱনা আছে। চফটৱেৰৰ বাবে সুৰক্ষাৰ উত্তম পদ্ধতিৰ পৰা আৰম্ভ কৰি শেষ ব্যৱহাৰকাৰীলৈ তথ্য বিতৰণলৈকে স্মাৰ্টফোনত সুৰক্ষা ব্যৱস্থা বিকশিত আৰু প্ৰয়োগ কৰা হয়। অপাৰেটিং চিষ্টেম বিকাশ, চফটৱেৰ ডিজাইন আৰু

ব্যৱহাৰকাৰীৰ আচৰণ পৰিৱৰ্তনকে ধৰি বিভিন্ন স্তৰত প্ৰতিকাৰ ব্যৱস্থা প্ৰণয়ন কৰিব পাৰি।

স্মাৰ্টফোন মোবাইল সুৰক্ষাৰ প্ৰত্যাহ্বানসমূহ:

- মেলৱেৰ আক্ৰমণ : মেলৱেৰ হৈছে ক্ষতিকাৰক চফটৱেৰ যিয়ে ডাউনলোড কৰা এপ, ফিছিং লিংক বা অসুৰক্ষিত নেটৱৰ্ক সংযোগৰ জৰিয়তে স্মাৰ্টফোনক সংক্ৰমিত কৰিব পাৰে। মেলৱেৰে ব্যক্তিগত ডাটা চুৰি কৰিব পাৰে, কাৰ্যকলাপ নিৰীক্ষণ কৰিব পাৰে, আনকি ডিভাইচৰ কাৰ্যক্ষমতাও হাইজেক কৰিব পাৰে।
- ডাটা ভংগ (Data breaches): স্মাৰ্টফোনত প্ৰায়ে স্পৰ্শকাতৰ ব্যক্তিগত তথ্য, যেনে বেংকিং তথ্য, সামাজিক সুৰক্ষা নম্বৰ আৰু পাছৱৰ্ড সংৰক্ষণ কৰা হয়। এই ডাটাত অকৰ্তৃত্বশীল ব্যৱহাৰকাৰীয়ে আহৰণ কৰিব পাৰে হেকিং বা ছ'চিয়েল ইঞ্জিনিয়াৰিঙৰ জৰিয়তে। তেনে কৰাৰে ডাটা ভংগ বোলা হয়।
- অসুৰক্ষিত বেতাঁৰ সংযোগ: ৰাজহুৱা ৰাই-ফাই নেটৱৰ্ক, যেনে কেফে, বিমানবন্দৰ, আৰু হোটেলত পোৱা নেটৱৰ্কৰ জৰিয়তে প্ৰেৰণ কৰা তথ্য হেকাৰে অতি সহজে আটক আৰু চুৰি কৰিব পাৰে।
- ডিভাইচ হেৰুৱা বা চুৰি: এটা স্মাৰ্টফোন হেৰুৱা বা ইয়াক চুৰি হোৱাটো এটা ডাঙৰ সুৰক্ষা বিপদৰ কাৰক হ'ব পাৰে। কাৰণ ই ডিভাইচৰ ডাটা আৰু কাৰ্যক্ষমতালৈ অকৰ্তৃত্বশীল প্ৰৱেশ প্ৰদান কৰিব পাৰে।
- অপা�ৰেটিং চিষ্টেমৰ দুৰ্বলতা: যিকোনো চফটৱেৰৰ দৰে মোবাইল অপাৰেটিং চিষ্টেমৰ নিজা দুৰ্বলতা থাকে যিবোৰ চাইবাৰ অপৰাধীয়ে ব্যৱহাৰ কৰি স্পৰ্শকাতৰ তথ্য বা ডিভাইচৰ নিয়ন্ত্ৰণৰ লাভ কৰিবলৈ সক্ষম হ'ব পাৰে।
- অসুৰক্ষিত এপ্লিকেচন: বেচৰকাৰী উৎসৰ পৰা ডাউনলোড কৰা বা অপৰ্যাপ্ত সুৰক্ষা ব্যৱস্থাৰ সৈতে তৃতীয় পক্ষৰ এপসমূহে হেকাৰসকলৰ বাবে স্মাৰ্টফোনত সহজ প্ৰৱেশ বিন্দু প্ৰদান কৰিব পাৰে।
- ছ'চিয়েল ইঞ্জিনিয়াৰিং আক্ৰমণ: চাইবাৰ অপৰাধীয়ে ছ'চিয়েল ইঞ্জিনিয়াৰিঙৰ কৌশল যেনে ফিছিং ইমেইল, টেক্সট মেছেজ বা ফোন কলৰ ব্যৱহাৰ কৰি স্মাৰ্টফোন ব্যৱহাৰকাৰীক স্পৰ্শকাতৰ তথ্য প্ৰকাশ বা ক্ষতিকাৰক চফটৱেৰ ইনষ্টল কৰিবলৈ ছলনা কৰিব পাৰে।

যেতিয়া কোনো স্মাৰ্টফোন চাইবাৰ আক্ৰমণকাৰীৰ দ্বাৰা সংক্ৰমিত হয়, তেতিয়া আক্ৰমণকাৰীয়ে তেওঁলোকৰ উদ্দেশ্যৰ ওপৰত নিৰ্ভৰ কৰি বিভিন্ন ধৰণৰ ক্ষতিকাৰক কাৰ্য কৰিবলৈ চেষ্টা কৰিব পাৰে। আক্ৰমণকাৰীয়ে ল'ব পৰা কিছুমান সাধাৰণ কাৰ্য্য ইয়াত উল্লেখ কৰা হ'ল:

- স্পর্শকাতৰ ডাটা চুৰি কৰা: আক্রমণকাৰীয়ে স্পর্শকাতৰ ব্যক্তিগত ডাটা চুৰি কৰিব পাৰে, যেনে লগইন কৰাৰ তথ্য, বিত্তীয় তথ্য, যোগাযোগ আৰু বার্তা।
- কার্য্যকলাপসমূহ নিৰীক্ষণ কৰা: আক্রমণকাৰীয়ে ব্যৱহাৰকাৰীৰ কার্য্যকলাপসমূহ নিৰীক্ষণ কৰিব পাৰে, যেনে কিষ্ট্রক ৰেকর্ডিং কৰা বা স্ক্রীণশ্বটসমূহ ধৰা পেলোৱা, স্পর্শকাতৰ তথ্য সংগ্রহ বা একাউণ্টসমূহত প্রৱেশ লাভ কৰিবলৈ তাৰ তথ্য।
- হাইজেক কার্যক্ষমতা: আক্রমণকাৰীয়ে স্মার্টফোনৰ কার্যক্ষমতা নিয়ন্ত্রণ কৰিব পাৰে, যেনে কল কৰা, টেক্সট মেছেজ প্রেৰণ কৰা বা কেমেৰা আৰু মাইক্র'ফোন ব্যৱহাৰ কৰা।
- প্রিমিয়াম টেক্সট মেছেজ প্রেৰণ কৰা : আক্রমণকাৰীয়ে স্মার্টফোনটো ব্যৱহাৰ কৰি প্রিমিয়াম ৰেট নম্বৰলৈ প্রিমিয়াম টেক্সট মেছেজ প্রেৰণ কৰিব পাৰে, যাৰ ফলত ব্যৱহাৰকাৰীৰ বাবে অধিক চার্জ লোৱা হয়।
- মেলৱেৰ বিয়পোৱা: আক্রমণকাৰীয়ে সংক্রমিত স্মার্টফোনটো ব্যৱহাৰ কৰি নেটৱর্কৰ অন্য ডিভাইচলৈ মেলৱেৰ বিয়পাব পাৰে। ইয়াৰ বাবে আক্রমণকাৰীয়ে সংক্রমিত ফাইল প্রেৰণ কৰিব বা স্মার্টফোনৰ ব্লুটুথ বা ৱাই-ফাই সংযোগৰ জৰিয়তে তেনে কার্য সম্পাদন কৰিব।
- ডিভাইচটোক বটনেটৰ অংশ হিচাপে ব্যৱহাৰ কৰি: আক্রমণকাৰীয়ে সংক্রমিত স্মার্টফোনটোক বটনেট, বিতৰণ কৰা সেৱা অস্বীকাৰ (DDoS) আক্রমণ বা অন্যান্য চাইবাৰ আক্রমণ কৰিবলৈ ব্যৱহাৰ কৰা আপোচ কৰা ডিভাইচৰ নেটৱর্ক হিচাপে ব্যৱহাৰ কৰিব পাৰে।
- ৰেনছমৱেৰ: আক্রমণকাৰীয়ে ব্যৱহাৰকাৰীৰ তথ্য এনক্রিপ্ট কৰিব পাৰে আৰু ডিক্রিপচন কৰি বিনিময়ত ৰেনছম পেমেণ্ট দাবী কৰিব পাৰে।

যোগাযোগ ভিত্তিক আক্রমণ

SMS আৰু MMS ভিত্তিক আক্রমণ: আক্রমণকাৰীসকলে SMS আৰু MMS ব্যৱহাৰ কৰি বিভিন্ন ধৰণৰ আক্রমণ চলাব পাৰে, যিয়ে স্মার্টফোন ব্যৱহাৰকাৰীসকলৰ তথ্য-সুৰক্ষাত বিপদ সৃষ্টি কৰিব পাৰে। এই ধৰণৰ আক্রমণৰ এক প্রকাৰভেদ হ'ল Smishing। ই phishing আক্রমণৰ এটা প্রকাৰ, য'ত আক্রমণকাৰী SMS ব্যৱহাৰ কৰি ব্যৱহাৰকাৰীসকলক ভ্রান্ত তথ্য দি গুপ্ত তথ্য প্রকাশ কৰিবলৈ বা মালৱেল (malware) ডাউনলোড কৰিবলৈ বাধ্য কৰে। আক্রমণকাৰীসকলে MMS মেছেজত অসুৰক্ষিত লিংক বা ভাইৰাছযুক্ত সংলগ্ন ফাইল প্রেৰণ কৰিব পাৰে, যি খুলিলে স্মার্টফোনত মালৱেৰ ডাউনলোড হৈ যান্ত্রিক ত্রুটি সৃষ্টি কৰিব পাৰে। আক্রমণকাৰীসকলে ব্যৱহাৰকাৰীৰ অনুমতি নোলোৱাকৈ অত্যাধিক খৰচ বিশিষ্ট (premium rate) নম্বৰৰ

উদ্দেশ্যে SMS প্রেৰণ কৰে, যাৰ ফলত ব্যৱহাৰকাৰীৰ মোবাইল বিলত বিশাল পৰিমাণৰ আর্থিক লোকচান হয়। আক্রমণকাৰীসকলে অসংখ্য SMS বা MMS প্রেৰণ কৰি স্মার্টফোনৰ প্রক্রিয়া মন্থৰ কৰি দিয়ে বা সম্পূর্ণৰূপে বিকল কৰি দিয়ে। ফলস্বৰূপে, ডিভাইচটো হেং বা অচল হৈ পৰিব পাৰে। এইধৰণৰ আক্রমণৰ পৰা বচি থাকিবলৈ অচিনাক্ত নম্বৰৰ SMS/MMS খোলাৰ আগতে সতর্কতা অৱলম্বন, সন্দেহজনক লিংকত ক্লিক নকৰা, আৰু মোবাইল ছিকিউৰিটি চফটৱেৰ ব্যৱহাৰ কৰাটো অতি প্রয়োজনীয়।

যোগাযোগ নেটৱর্ক ভিত্তিক আক্রমণ

GSM নেটৱর্কত আধাৰিত আক্রমণ: GSM (Global System for Mobile Communications) নেটৱর্কসমূহ, যাক বিশ্বৰ বেছিভাগ মোবাইল সেৱা প্রদানকাৰী সংস্থাই ব্যৱহাৰ কৰে আৰু ই বিভিন্ন আক্রমণৰ বাবে সংবেদনশীল। এটা সাধাৰণ আক্রমণ “man-in-the-middle” (MITM) আক্রমণ, য’ত আক্রমণকাৰীজন মোবাইল ডিভাইচ আৰু GSM নেটৱর্কৰ মাজৰ যোগাযোগ আটক কৰি ফোন কলৰ সকলো কথা শুনিব পাৰে বা গুপ্ত তথ্য চুৰি কৰিব পাৰে। “Fake base station” (নকল বেইছ ষ্টেচন) আক্রমণ হৈছে আন এক প্রকৃত নেটৱর্কক নকল কৰি আক্রমণ কৰাৰ পদ্ধতি, য’ত আক্রমণকাৰীজনে এটা নকল GSM বেইছ ষ্টেচন স্থাপন কৰি মোবাইল ডিভাইচৰ যোগাযোগ আটক কৰে আৰু গুপ্ত তথ্য লাভ কৰে। আন এক গুৰুত্বপূর্ণ আক্রমণ “IMSI-catcher” (International Mobile Subscriber Identity catcher) আক্রমণ, য’ত আক্রমণকাৰী এটা নকল GSM টাৱাৰ ৰূপত নিজৰ ডিভাইচ ব্যৱহাৰ কৰে আৰু মোবাইল ডিভাইচসমূহক তাৰ লগত সংযোগ কৰিবলৈ বাধ্য কৰায়। ইয়াৰ ফলত, আক্রমণকাৰীজনে কল আৰু টেক্সট মেছেজ আটক কৰি তথ্য চুৰি কৰিব পাৰে। এই আক্রমণসমূহে GSM নেটৱর্কৰ সুৰক্ষাৰ প্রতি গুৰুত্ব দিয়াৰ প্রয়োজনীয়তা স্পষ্ট কৰি তোলে।

ৱাই-ফাইৰ ওপৰত ভিত্তি কৰি আক্রমণ:

আক্রমণকাৰীয়ে তথ্যৰ বাবে ৱাই-ফাই যোগাযোগৰ আধাৰত লুকাই চুৰকৈ তথ্য চুৰ কৰিব পাৰে (যেনে ব্যৱহাৰকাৰীৰ নাম, পাছৱর্ড)। এই ধৰণৰ আক্রমণ স্মার্টফোনৰ বাবে অনন্য নহয়, কিন্তু ইয়াৰ প্রতি তেওঁলোক দুর্বল কাৰণ ৱাই-ফাই প্রায়ে যোগাযোগৰ একমাত্র মাধ্যম আৰু ইণ্টাৰনেটৰ সুবিধা থকাটো প্রয়োজন। গতিকে বেতাঁৰ নেটৱর্ক (WLAN) ৰ সুৰক্ষাৰ বিষয়ে এটা গুৰুত্বপূর্ণ বিষয়। প্রথম অৱস্থাত, বেতাঁৰ নেটৱার্কসমূহ WEP কীসমূহৰ দ্বাৰা সুৰক্ষিত কৰা হয়। WEP-ৰ দুর্বলতা হ’ল সকলো সংযুক্ত ক্লায়েণ্টে

একেটা চুটি ইনক্রিপশ্বন কী ব্যৱহাৰ কৰে। ইয়াৰ উপৰি গৱেষকসকলে মূল অনুসন্ধানৰ স্থান হ্রাস পোৱা দেখা গৈছে। আজি, বেছিভাগ বেতাঁৰ নেটৱৰ্ক WPA সুৰক্ষা প্রটোকলৰ দ্বাৰা সুৰক্ষিত। WPA টেম্প'ৰেল কী অখণ্ডতা প্রটোকল (TKIP) ৰ ওপৰত ভিত্তি কৰি কৰা হৈছে আৰু মোতায়েন কৰা ডিভাইচসমূহত WEP ৰ পৰা WPA লৈ প্রব্রজনৰ অনুমতি দিবলে ডিজাইন কৰা হৈছিল। আটাইতকৈ উল্লেখযোগ্য সুৰক্ষা বৃদ্ধি হৈছে গতিশীল ইনক্রিপশ্বন কীসমূহলৈ।

সৰু নেটৱৰ্কসমূহৰ বাবে, WPA এটা অংশীদাৰী কীৰ ওপৰত ভিত্তি কৰি তৈয়াৰ কৰা হয় যাক "পূর্ব-অংশীদাৰী কী" বুলি কোৱা হয়। যদি অংশীদাৰী কীৰ দৈর্ঘ্য চুটি হয়, চাইফাৰক আক্রমণ কৰিব পাৰি। সীমিত ইনপুট সম্ভাৱনাৰ সৈতে (অর্থাৎ কেৱল সংখ্যাগত কিপেড) মোবাইল ফোন ব্যৱহাৰকাৰীয়ে কেৱল সংখ্যা থকা চুটি এনক্রিপচন কী সংজ্ঞায়িত কৰিব পাৰে। তেওঁলোকৰ অসুৰক্ষিত ৱাই-ফাই নেটৱৰ্কৰ লগত বহুতো বিপদ জড়িত হৈ থাকে। এটা সাধাৰণ আক্রমণ হৈছে "ৰগ এক্সেছ পইণ্ট" আক্রমণ, য'ত এজন আক্রমণকাৰীয়ে এটা ভুৱা ৱাই-ফাই হটস্পট স্থাপন কৰে যিটো বৈধ যেন লাগে, কিন্তু প্রকৃততে ট্রেফিক বাধা দিয়ে আৰু স্পর্শকাতৰ তথ্য চুৰি কৰে। আন এটা আক্রমণ হ'ল "মেন-ইন-দ্য-মিডল" আক্রমণ, য'ত আক্রমণকাৰীয়ে মোবাইল ডিভাইচ আৰু ৱাই-ফাই নেটৱৰ্কৰ মাজৰ ট্রেফিকক বাধা দি যোগাযোগৰ কথা শুনি বা স্পর্শকাতৰ তথ্য চুৰি কৰে। আক্রমণকাৰীয়ে নেটৱৰ্ক ট্রেফিক ধৰি ৰাখিবলৈ আৰু বিশ্লেষণ কৰিবলৈ "পেকেট স্নিফিং" ব্যৱহাৰ কৰিব পাৰে, যাৰ ফলত তেওঁলোকে লগইন প্রমাণপত্র বা অন্য স্পর্শকাতৰ তথ্য চুৰি কৰিব পাৰে।

ব্লুটুথ ভিত্তিক আক্রমণ

সাধাৰণতে ডিভাইচসমূহৰ মাজত বেতাঁৰ যোগাযোগৰ বাবে ব্যৱহাৰ কৰা ব্লুটুথ প্রযুক্তিও বিভিন্ন ধৰণৰ আক্রমণৰ সন্মুখীন হ'বলগীয়া হয়। ব্লুটুথ-ভিত্তিক আক্রমণৰ এটা নীতি হ'ল যে এজন আক্রমণকাৰীয়ে এটা ডিভাইচ বা ইয়াৰ ডাটালৈ অকর্তৃত্বশীল প্রৱেশ লাভ কৰিবলৈ ব্লুটুথ প্রট'কল বা নির্দিষ্ট ব্লুটুথ ডিভাইচসমূহত থকা দুর্বলতাসমূহ শোষণ কৰিব পাৰে। উদাহৰণস্বৰূপ, এজন আক্রমণকাৰীয়ে ওচৰৰ ব্লুটুথ-সামর্থবান ডিভাইচসমূহলৈ অযাচিত বার্তা বা ফাইলসমূহ প্রেৰণ কৰিবলৈ "ব্লুজেকিং" ব্যৱহাৰ কৰিব পাৰে, সম্ভাৱ্যভাৱে ডিভাইচসমূহ বিকল হ'ব বা অনাকাংক্ষিত কার্যসমূহ সম্পন্ন কৰিব পাৰে। আন এটা আক্রমণ হৈছে "bluesnarfing" য'ত এজন আক্রমণকাৰীয়ে ব্লুটুথ প্রট'কলৰ দুর্বলতাসমূহ শোষণ কৰি এটা ডিভাইচৰ ডাটা, যেনে পৰিচয় তালিকা, টেক্সট বার্তা বা ইমেইললৈ অকর্তৃত্বশীল প্রৱেশ লাভ কৰিব পাৰে। আক্রমণকাৰীয়ে এটা ব্লুটুথ-সক্ষম ডিভাইচ ল'বলৈ "ব্লুবাগিং" ব্যৱহাৰ কৰিব পাৰে, যাৰ ফলত তেওঁলোকক

ব্যৱহাৰকাৰীৰ অজ্ঞাতে বা সন্মতি অবিহনে কল কৰিবলৈ, বার্তা প্রেৰণ কৰিবলৈ বা ডিভাইচত ডাটা প্ররেশ কৰিবলৈ অনুমতি দিয়া হয়।

চফটৱেৰ এপ্লিকেচনসমূহত দুর্বলতাৰ ওপৰত ভিত্তি কৰি আক্রমণ:

আক্রমণকাৰীয়ে মোবাইল ডিভাইচক লক্ষ্য কৰি লোৱাৰ এটা সাধাৰণ উপায় হ'ল চফটৱেৰ এপ্লিকেচনত থকা দুর্বলতাসমূহৰ আধাৰ লোৱা। আক্রমণকাৰীয়ে মোবাইল ডিভাইচত চফটৱেৰ এপ্লিকেচনত থকা দুর্বলতাসমূহ যেনে মেলৱেৰ ইনজেকচন, ডাটা লিকেজ আৰু বাফাৰ অভাৰফ্লঁ' আক্রমণ কৰিবলৈ বিভিন্ন কৌশল ব্যৱহাৰ কৰিব পাৰে। মেলৱেৰ ইনজেকচনে এটা এপ্লিকেচনত থকা দুর্বলতাসমূহ শোষণ কৰি ক্ষতিকাৰক ক'ড ইনজেকচন কৰাটো জড়িত কৰে যিয়ে স্পর্শকাতৰ তথ্য চুৰি কৰিব পাৰে, এপ্লিকেচনৰ আচৰণ পৰিবর্তন কৰিব পাৰে, বা ডিভাইচ নিয়ন্ত্রণ কৰিব পাৰে। উদাহৰণস্বৰূপে, আক্রমণকাৰীয়ে এই কৌশল ব্যৱহাৰ কৰি বৈধ বেংকিং এপ্লিকেচনত ভুৱা লগইন পর্দা সৃষ্টি কৰিব পাৰে আৰু ব্যৱহাৰকাৰীৰ লগইন প্রমাণপত্র চুৰি কৰিব পাৰে। ডাটা লিকেজ আক্রমণৰ লগত এটা এপ্লিকেচনৰ ভিতৰত সংৰক্ষিত স্পর্শকাতৰ ডাটালৈ অকর্তৃত্বশীল প্ররেশ লাভ কৰাটো জড়িত হৈ থাকে, যেনে লগইন প্রমাণপত্র বা বিত্তীয় তথ্য। উদাহৰণস্বৰূপে, আক্রমণকাৰীয়ে এই কৌশল ব্যৱহাৰ কৰি স্বাস্থ্য এপ্লিকেচনত সংৰক্ষিত ব্যক্তিগত তথ্য চুৰি কৰিব পাৰে।

বাফাৰ অভাৰফ্লঁ' আক্রমণত এটা এপ্লিকেচনৰ মেমৰি ব্যৱস্থাপনাত দুর্বলতাসমূহ আহৰণ কৰা আৰু ডিভাইচত ইচ্ছাকৃত ক'ড এক্সিকিউট কৰে। এই কৌশল এটা ডিভাইচৰ নিয়ন্ত্রণ ল'বলৈ, স্পর্শকাতৰ তথ্য চুৰি কৰিবলৈ, বা এটা এপ্লিকেচনৰ আচৰণ পৰিবর্তন কৰিবলৈ ব্যৱহাৰ কৰিব পাৰি। উদাহৰণস্বৰূপে, আক্রমণকাৰীয়ে এই কৌশল ব্যৱহাৰ কৰি ব্রাউজাৰ এপ্লিকেচনত ক্ষতিকাৰক ক'ড এক্সিকিউট কৰিব পাৰে আৰু স্পর্শকাতৰ তথ্য চুৰি কৰিব পাৰে।

হার্ডৱেৰ দুর্বলতাৰ ওপৰত ভিত্তি কৰি আক্রমণ:

হার্ডৱেৰ দুর্বলতাসমূহ আক্রমণকাৰীয়ে এটা ডিভাইচৰ হার্ডৱেৰ উপাদানসমূহ হেঁচা মাৰি ধৰিবলৈ, সুৰক্ষা ব্যৱস্থাসমূহ বাইপাছ কৰিবলৈ, বা ক্ষতিকাৰক চফটৱেৰ ইনষ্টল কৰিবলৈ ব্যৱহাৰ কৰিব পাৰে। মোবাইল ডিভাইচত হার্ডৱেৰ ভিত্তিক আক্রমণৰ এটা উদাহৰণ "চাইড-চেনেল আক্রমণ" বুলি জনা যায়। পার্শ্ব-চেনেল আক্রমণত আক্রমণকাৰীয়ে স্পর্শকাতৰ তথ্যৰ প্ররেশ লাভ কৰিবলৈ ডিভাইচৰ হার্ডৱেৰৰ ভৌতিক

বৈশিষ্ট্য, যেনে শক্তি খৰচ বা বিদ্যুৎচুম্বকীয় নির্গমন ব্যৱহাৰ কৰে। এই ধৰণৰ আক্রমণৰ সহায়ত ক্রিপ্টোগ্রাফিক কী, পাছৱর্ড, বা অন্য স্পর্শকাতৰ তথ্য চুৰি কৰিব পাৰি।
হার্ডৱেৰ-ভিত্তিক আক্রমণৰ আন এটা উদাহৰণক "চিপ-স্তৰৰ আক্রমণ" বুলি জনা যায়। চিপ-স্তৰৰ আক্রমণত, আক্রমণকাৰীয়ে সুৰক্ষা ব্যৱস্থাসমূহ বাইপাছ কৰিবলৈ বা ডিভাইচৰ নিয়ন্ত্রণ লাভ কৰিবলৈ এটা ডিভাইচৰ হার্ডৱেৰ উপাদানসমূহক হেঁচা মাৰি ধৰে। উদাহৰণস্বৰূপ, আক্রমণকাৰীয়ে এই কৌশল ব্যৱহাৰ কৰিব পাৰে ইনক্রিপচণ কীসমূহ এক্সট্রেক্ট কৰিবলে, মেলৱেৰ ইনষ্টল কৰিবলে, বা ডিভাইচৰ আচৰণ পৰিৱর্তন কৰিব পাৰে।

মবাইল মেলৱেৰ:

যিহেতু স্মার্টফোন ইণ্টাৰনেটৰ স্থায়ী প্রৱেশ বিন্দু (বেছিভাগেই অনলাইন), গতিকে ইয়াক মেলৱেৰ থকা কম্পিউটাৰৰ দৰেই সহজেই আপোচ কৰিব পাৰি। মেলৱেৰ হৈছে ই ইনষ্টল কৰা চিষ্টেমটোক ক্ষতিগ্রস্ত কৰিবলৈ ডিজাইন কৰা কম্পিউটাৰ প্রগ্রেম। ২০১৭ চনত মোবাইল মেলৱেৰৰ ভিন্নতা ৫৪% বৃদ্ধি পাইছে। ট্র'জান, ৱর্ম আৰু ভাইৰাছ সকলোকে মেলৱেৰ বুলি গণ্য কৰা হয়। ট্র'জান হর্চ হৈছে স্মার্টফোনৰ এনে এটা প্রগ্রেম যিয়ে বাহিৰৰ ব্যৱহাৰকাৰীক গোপনে সংযোগ স্থাপনৰ সুবিধা প্রদান কৰে। ৱর্ম হৈছে এনে এটা প্রগ্রেম যিয়ে এটা নেটৱর্কৰ জৰিয়তে একাধিক কম্পিউটাৰত প্রতিলিপি কৰে। ভাইৰাছ হৈছে কোনো বৈধ প্রগ্রেমত নিজকে সুমুৱাই দি আৰু তাৰ কাষতে প্রগ্রেমটো চলাই আন কম্পিউটাৰলৈ বিয়পিবলৈ ডিজাইন কৰা ক্ষতিকাৰক চফটৱেৰ। কিন্তু এইটো স্পষ্ট যে কম্পিউটাৰতকৈ স্মার্টফোনত মেলৱেৰৰ সংখ্যা বহু কম আৰু গুৰুত্বপূর্ণ।

মোবাইল ডিভাইচ সুৰক্ষাৰ বাবে প্রতিকাৰ ব্যৱস্থা:

মোবাইল ডিভাইচৰ সুৰক্ষা উন্নত কৰাৰ লগতে বিভিন্ন নিৰাপত্তাজনিত ভাবুকিৰ পৰা ৰক্ষা পাবলৈ কেইবাটাও প্রতিকাৰ ব্যৱস্থা গ্রহণ কৰিব পাৰি। ইয়াত কিছুমান সাধাৰণ প্রতিকাৰৰ ব্যৱস্থা উল্লেখ কৰা হ'ল:

- শক্তিশালী পাছৱর্ড আৰু/বা বায়মেট্রিক প্রমাণীকৰণ ব্যৱহাৰ কৰক: ই ডিভাইচ আৰু ইয়াত থকা তথ্যলৈ অকর্তৃত্বশীল প্রৱেশ প্রতিৰোধ কৰিব পাৰে।
- ডিভাইচ আপডেইট ৰাখক: যিকোনো জনা দুর্বলতাসমূহ পেটচ কৰা হৈছে নে নাই সেয়া নিশ্চিত কৰিবলে ডিভাইচত কার্যকৰপ্রণালী আৰু এপ্লিকেচনসমূহ নিয়মিতভাৱে আপডেইট কৰক।

- সুৰক্ষা চফটৱেৰ ইনষ্টল আৰু ব্যৱহাৰ কৰক: ডিভাইচৰ পৰা ভাবুকিসমূহ স্কেন আৰু আঁতৰাবলৈ সুনামধন্য এণ্টিভাইৰাছ আৰু এণ্টি-মেলৱেৰ চফটৱেৰ ইনষ্টল কৰক।
- এনক্রিপচন ব্যৱহাৰ কৰক: এনক্রিপচনে ডিভাইচত আৰু তথ্য সংক্রমণৰ সময়ত স্পর্শকাতৰ তথ্য সুৰক্ষিত কৰিব পাৰে, অকর্তৃত্বশীল প্ৰৱেশ ৰোধ কৰি।
- ৰাজহুৱা ৱাই-ফাই নেটৱর্ক এৰক: ৰাজহুৱা ৱাই-ফাই নেটৱর্কসমূহ অসুৰক্ষিত হ'ব পাৰে আৰু ডিভাইচটোক সুৰক্ষাৰ ভাবুকিৰ সন্মুখীন কৰিব পাৰে। ৰাজহুৱা ৱাই-ফাই ব্যৱহাৰ কৰাৰ সময়ত এটা ভার্চুৱেল ব্যক্তিগত নেটৱর্ক (VPN) ব্যৱহাৰ কৰক।
- ডাউনলোড আৰু এপ ইনষ্টলেচনৰ সৈতে সাৱধান হওক: কেৱল বিশ্বাসযোগ্য উৎসৰ পৰা এপসমূহ ডাউনলোড কৰক আৰু স্পর্শকাতৰ তথ্য বা চিষ্টেম সম্পদসমূহৰ প্ৰৱেশৰ অনুৰোধ কৰা এপসমূহৰ পৰা সাৱধান হওক।
- দূৰৱর্তীভাৱে মচি পেলোৱা আৰু বেকআপ সামর্থ্যবান কৰক : ডিভাইচ হেৰুৱা বা চুৰি হোৱাৰ ক্ষেত্ৰত, দূৰৱর্তীভাৱে মচি পেলোৱাটোৱে ডিভাইচৰ সকলো তথ্য মচি পেলাব পাৰে আৰু বেকআপে তথ্য হেৰুৱাব নোৱাৰাটো নিশ্চিত কৰিব পাৰে।
- ডিভাইচ ব্যৱস্থাপনা সমাধানসমূহ ব্যৱহাৰ কৰক: সংস্থাসমূহে সুৰক্ষা নীতিসমূহ বলবৎ কৰিবলে আৰু দূৰৱর্তীভাৱে ডিভাইচসমূহ পৰিচালনা আৰু নিৰীক্ষণ কৰিবলে মোবাইল ডিভাইচ ব্যৱস্থাপনা (MDM) সমাধানসমূহ ব্যৱহাৰ কৰিব পাৰে।

এই প্ৰতিকাৰ ব্যৱস্থাসমূহ কার্যকৰী কৰি ব্যৱহাৰকাৰীসকলে মোবাইল ডিভাইচৰ সুৰক্ষা উন্নত কৰিব পাৰে আৰু সুৰক্ষাৰ ভাবুকিৰ আশংকা হ্রাস কৰিব পাৰে। কিন্তু মন কৰিবলগীয়া যে কোনো সুৰক্ষা ব্যৱস্থাই ফুলপ্রুফ নহয় আৰু ব্যৱহাৰকাৰীসকলে সজাগ হৈ থাকিব লাগে আৰু শেহতীয়া সুৰক্ষা ভাবুকি আৰু উত্তম পদ্ধতিসমূহৰ বিষয়ে অৱগত হৈ থাকিব লাগে।

১২.৪ পাছৱর্ড নীতি

পাছৱর্ড নীতি হৈছে নিয়ম আৰু প্রয়োজনীয়তাসমূহৰ এটা গোট যি এটা প্রতিষ্ঠান বা ব্যৱস্থাপ্রণালীত পাছৱর্ডসমূহ কেনেকৈ সৃষ্টি, সংৰক্ষণ আৰু ব্যৱস্থাপনা কৰিব লাগে নির্দেশ দিয়ে। পাছৱর্ড নীতিৰ উদ্দেশ্য হৈছে পাছৱর্ডসমূহ শক্তিশালী, অনন্য আৰু অকর্তৃত্বশীল প্ৰৱেশৰ পৰা সুৰক্ষিত হোৱাটো সুনিশ্চিত কৰি চিষ্টেমৰ সুৰক্ষা বৃদ্ধি কৰা। ইয়াত কিছুমান সাধাৰণ উপাদান আছে যি এটা পাছৱর্ড নীতিত অন্তর্ভুক্ত হ'ব পাৰে:

- পাছৱর্ডৰ দৈর্ঘ্য: নীতিয়ে পাছৱর্ডৰ বাবে এটা ন্যূনতম আৰু সর্বাধিক দৈর্ঘ্য ধার্য্য কৰিব পাৰে, সাধাৰণতে ৮ৰ পৰা ১৬ আখৰৰ ভিতৰত।
- জটিলতাৰ প্রয়োজনীয়তাসমূহ: নীতিয়ে পাছৱর্ডসমূহত uppercase আৰু lowercase আখৰ, সংখ্যা আৰু বিশেষ আখৰৰ মিশ্রণ থকাটো প্রয়োজনীয় হ'ব পাৰে।

- পাছৱৰ্ডৰ সময়সীমা উকলি যোৱা: নীতি অনুসৰি ব্যৱহাৰকাৰীসকলে সময়ে সময়ে তেওঁলোকৰ পাছৱৰ্ড সলনি কৰিব লাগিব, যেনে প্রতি ৯০ দিনৰ মূৰে মূৰে। ই পাছৱৰ্ড আপোচৰ আশংকা হ্রাস কৰে।
- পাছৱৰ্ডৰ ইতিহাস: নীতিয়ে ব্যৱহাৰকাৰীসকলক তেওঁলোকৰ পূর্বৰ পাছৱৰ্ডসমূহ পুনৰ ব্যৱহাৰ কৰাত বাধা দিব পাৰে, যাতে আক্রমণকাৰীয়ে পুনৰ ব্যৱহৃত পাছৱৰ্ড অনুমান কৰিব নোৱাৰে।
- একাউণ্ট লকআউট: ব্রুট-ফর্চ আক্রমণ প্রতিৰোধ কৰিবলৈ এটা নির্দিষ্ট সংখ্যক ব্যর্থ প্ররেশ প্রচেষ্টাৰ পিছত নীতিয়ে স্বয়ংক্রিয়ভাৱে এটা একাউণ্ট লক আউট কৰিব পাৰে।
- দুটা কাৰক প্রমাণীকৰণ: নীতি অনুসৰি ব্যৱহাৰকাৰীসকলে লগ ইন কৰাৰ সময়ত তেওঁলোকৰ পৰিচয় পৰীক্ষা কৰিবলৈ এটা অতিৰিক্ত কাৰক, যেনে মোবাইল ফোন ব্যৱহাৰ কৰিব লাগিব।
- পাছৱৰ্ড সংৰক্ষণ: নীতিয়ে পাছৱৰ্ডসমূহ সুৰক্ষিতভাৱে সংৰক্ষণ কৰাৰ প্রয়োজন হ'ব পাৰে, যেনে হেচিং আৰু ছলটিং কৰি, যাতে সিহঁতক অকর্তৃত্বশীল প্ররেশৰ পৰা সুৰক্ষিত কৰিব পাৰি।

এটা শক্তিশালী পাছৱৰ্ড নীতি প্রণয়ন কৰি, প্রতিষ্ঠানসমূহে দুর্বল বা আপোচ কৰা পাছৱৰ্ডসমূহৰ ফলত হোৱা সুৰক্ষা ভংগৰ আশংকা হ্রাস কৰিব পাৰে।

১২.৫ সুৰক্ষা পেটচ ব্যৱস্থাপনা

সুৰক্ষা পেটচ ব্যৱস্থাপনাই কম্পিউটাৰ চিষ্টেমসমূহ আৰু নে'টৱর্কসমূহক জনা দুর্বলতা আৰু আক্রমণৰ পৰা সুৰক্ষিত কৰিবলে চফটৱেৰ পেটচসমূহ আৰু আপডেইটসমূহ চিনাক্ত, অগ্রাধিকাৰ, পৰীক্ষা, মোতায়েন আৰু পৰীক্ষা কৰাৰ প্রক্রিয়াক বুজায়। পেটচ ব্যৱস্থাপনা হৈছে চাইবাৰ সুৰক্ষাৰ এটা অপৰিহার্য দিশ— যিয়ে সংস্থাসমূহক তেওঁলোকৰ চিষ্টেম আৰু নেটৱর্কৰ সুৰক্ষা আৰু নির্ভৰযোগ্যতা নিশ্চিত কৰাত সহায় কৰে। চাইবাৰ সুৰক্ষাৰ ভাবুকি ক্রমান্বয়ে অত্যাধুনিক হৈ পৰিছে আৰু চাইবাৰ অপৰাধীয়ে অহৰহ নতুন দুর্বলতা আৰু আক্রমণ কৰিবলৈ বিভিন্ন ন ন ব্যৱস্থা আৱিষ্কাৰ কৰি আছে। এই ভাবুকিসমূহৰ পৰা আগবাঢ়ি থাকিবলৈ, সংস্থাসমূহৰ বাবে নিয়মিতভাৱে তেওঁলোকৰ চফটৱেৰ আৰু চিষ্টেমসমূহ শেহতীয়া সুৰক্ষা পেটচ আৰু আপডেইটসমূহৰ সৈতে আপডেইট কৰাটো অতি গুৰুত্বপূর্ণ। চফটৱেৰ আৰু চিষ্টেমসমূহ আপডেট কৰাত ব্যর্থ হ'লে সংস্থাসমূহক চাইবাৰ আক্রমণ যেনে মেলৱেৰ, ৰেনছমৱেৰ আৰু ফিছিং আক্রমণৰ সন্মুখীন হ'ব পাৰে, যিয়ে ডাটা ভংগ, আর্থিক ক্ষতি আৰু সুনামৰ ক্ষতিৰ সৃষ্টি কৰিব পাৰে। সুৰক্ষা পেটচ ব্যৱস্থাপনাই সংস্থাসমূহক এই বিপদসমূহ কম

কৰিবলৈ সহায় কৰে যাতে চফটৱেৰৰ দুৰ্বলতাসমূহ চিনাক্ত কৰা হয় আৰু তৎক্ষণাত পেটচ কৰা হয়। এনে কৰিলে সংস্থাসমূহে চাইবাৰ অপৰাধীসকলে এই দুৰ্বলতাসমূহ আক্রমণ কৰাৰ সুযোগৰ সুবিধা হ্রাস কৰিব পাৰে, যাৰ ফলত সফল চাইবাৰ আক্রমণৰ আশংকা কম হ'ব পাৰে।

সুৰক্ষা পেট্চ পৰিচালনা প্রক্রিয়া : সুৰক্ষা পেট্চ পৰিচালনা (Security Patch Management) প্রক্রিয়াত বিভিন্ন ধাপ থাকে, যিবোৰ তলত উল্লেখ কৰা হ'ল—

চিনাক্তকৰণ (Identification) - এই ধাপত ছফ্টৱেৰৰ দুৰ্বলতা (vulnerabilities) আৰু প্রয়োজনীয় পেট্চসমূহ চিনাক্ত কৰা হয়। ইয়াক ভালনেৰেবিলিটি স্কেন (vulnerability scans), সুৰক্ষা বুলেটিন, আৰু বিক্রেতাসকলৰ (vendors) পৰৱর্তী ঘোষণাৰ জৰিয়তে চিনাক্ত কৰা যায়।

প্রাধিকৰণ (Prioritization) - একেবাৰে গুৰুত্বপূর্ণ দুৰ্বলতা চিনাক্ত কৰাৰ পিছত, সেইবোৰক প্রাধিকৰণ (priority) নিদিয়া হয়। দুৰ্বলতাৰ গম্ভীৰতা (severity) আৰু সংগঠনৰ ওপৰত ইয়াৰ সম্ভাব্য প্রভাৱ বিবেচনা কৰি, সর্বাধিক বিপজ্জনক ক্ষেত্রত পেট্চ প্রয়োগ কৰিবলৈ অগ্রাধিকাৰ দিয়া হয়।

পৰীক্ষা (Testing) - পেট্চসমূহ প্রয়োগ কৰাৰ আগতে, সেইবোৰক অ-উৎপাদন পৰিৱেশ (non-production environment)ত পৰীক্ষা কৰা হয়। ইয়াৰ উদ্দেশ্য হৈছে কোনো অপ্রত্যাশিত সমস্যা নঘটাকৈ ছিষ্টেম বা এপ্লিকেচন সুস্থিৰভাৱে কাম কৰে নে, তাৰ নিশ্চিতকৰণ। এই ধাপত ভুল পোৱা গ'লে ডাউনটাইম (downtime) বা ব্যৱসায়িক কার্যক্ষমতাত ব্যাঘাত হোৱাৰ আশংকা কমে।

মুকলি (Deployment) - যেতিয়া পেট্চসমূহ পৰীক্ষা আৰু নিশ্চিত কৰা হয়, তেতিয়া উৎপাদন পৰিৱেশত (production environment) সেইবিলাক মুকলি কৰা হয়। এই প্রক্রিয়া ম্যানুৱেল বা স্বয়ংক্রিয় পেট্চ পৰিচালনা টুল (automated patch management tools)ৰ জৰিয়তে সম্পন্ন কৰিব পৰা যায়।

সত্যতা নিৰূপণ কৰা কার্য বা প্রক্রিয়া (Verification) - পেট্চসমূহ প্রয়োগ হোৱাৰ পিছত, ইয়াৰ সত্যতা নিৰূপণ (verify) কৰাটো অতি গুৰুত্বপূর্ণ। ইয়াৰ জৰিয়তে নিশ্চিত কৰা হয় যে পেট্চসমূহ সঠিকভাৱে প্রয়োগ কৰা হৈছে আৰু ছিষ্টেম বা এপ্লিকেচন স্বাভাৱিকভাৱে কাম কৰি আছে।

সঠিক পেট্চ পৰিচালনাৰ মাধ্যমে ছিষ্টেমৰ সুৰক্ষা নিশ্চিত কৰি, চাইবাৰ আক্রমণ আৰু তথ্য চুৰি হোৱাৰ আশংকা হ্রাস কৰিব পৰা যায়।

সুৰক্ষা পেটচ ব্যৱস্থাপনাৰ প্রত্যাহ্বানসমূহ : সুৰক্ষা পেটচ ব্যৱস্থাপনাৰ গুৰুত্ব সত্ত্বেও, বহু সংস্থাই ইয়াক প্রণয়ন কৰাৰ সময়ত উল্লেখযোগ্য প্রত্যাহ্বানৰ সন্মুখীন হয়। কিছুমান সাধাৰণ প্রত্যাহ্বানৰ ভিতৰত আছে:

[i] জটিলতা - একাধিক চিষ্টেম আৰু এপ্লিকেচনসমূহৰ সৈতে বৃহৎ প্রতিষ্ঠানসমূহৰ বাবে পেটচ ব্যৱস্থাপনা প্রক্রিয়া জটিল হ'ব পাৰে । এই জটিলতাই দুর্বলতাসমূহ চিনাক্ত কৰা আৰু পেটচসমূহ ফলপ্রসূভাৱে মোতায়েন কৰাটো প্রত্যাহ্বানজনক কৰি তুলিব পাৰে।

[ii]. অগ্রাধিকাৰ - পেটচসমূহক অগ্রাধিকাৰ দিয়াটো প্রত্যাহ্বানজনক হ'ব পাৰে, বিশেষকৈ যেতিয়া বৃহৎ সংখ্যক দুর্বলতাৰ সৈতে মোকাবিলা কৰা হয়। সংস্থাসমূহে দুর্বলতাৰ গুৰুত্ব আৰু সংস্থাটোৰ ওপৰত সম্ভাব্য প্রভাৱৰ মাজত ভাৰসাম্য ৰক্ষা কৰাটো প্রয়োজন।

[iii]. পৰীক্ষণ - পৰীক্ষণ পেটচসমূহ সময়-ব্যৱহাৰকাৰী আৰু সম্পদ-নিবিড় হ'ব পাৰে, বিশেষকৈ জটিল ব্যৱস্থাপ্রণালী আৰু এপ্লিকেচনসমূহৰ বাবে। ইয়াৰ ফলত পেটচ মোতায়নত পলম হ'ব পাৰে, যাৰ ফলত সংস্থাসমূহ চাইবাৰ আক্রমণৰ সন্মুখীন হ'ব পাৰে।

[iv]. অনুসৰণ - বহুতো সংস্থাই নিয়ন্ত্রণমূলক প্রয়োজনীয়তাসমূহ মানি চলিব লাগে, যিয়ে পেটচ ব্যৱস্থাপনা প্রক্রিয়াত জটিলতাৰ এটা অতিৰিক্ত স্তৰ যোগ কৰিব পাৰে। এই প্রয়োজনীয়তাসমূহ মানি চলাত ব্যর্থ হ'লে যথেষ্ট আর্থিক শাস্তি আৰু সুনামৰ ক্ষতি হ'ব পাৰে।

[v]. তৃতীয়-পক্ষ চফটৱেৰ পেটচিং - বহুতো প্রতিষ্ঠানে তৃতীয়-পক্ষ চফটৱেৰ ব্যৱহাৰ কৰে যি চফটৱেৰ বিক্রেতাৰ সমর্থিত নহ'বও পাৰে। ইয়াৰ ফলত এই এপ্লিকেচনসমূহত দুর্বলতাসমূহ চিনাক্ত আৰু পেটচ কৰাটো প্রত্যাহ্বানজনক হ'ব পাৰে, যাৰ ফলত সংস্থাসমূহ চাইবাৰ আক্রমণৰ সন্মুখীন হ'বলগীয়া হয়।

সুৰক্ষা পেটচ ব্যৱস্থাপনাৰ বাবে উত্তম পদ্ধতিসমূহ:

পেটচ ব্যৱস্থাপনা এটা জটিল প্রক্রিয়া আৰু বহুতো প্রতিষ্ঠানে এটা ফলপ্রসূ পেটচ ব্যৱস্থাপনা কৌশল প্রণয়ন কৰিবলৈ যত্ন কৰি থাকে। এই লেখাটোত আমি সুৰক্ষা পেটচ ব্যৱস্থাপনাৰ বাবে উত্তম পদ্ধতিসমূহৰ বিষয়ে আলোচনা কৰিম।

1. **এটা পেটচ ব্যৱস্থাপনা নীতি প্রতিষ্ঠা কৰক:** সংস্থাসমূহে এটা আনুষ্ঠানিক পেটচ ব্যৱস্থাপনা নীতি বিকশিত কৰিব লাগে যি পেটচ ব্যৱস্থাপনা প্রক্রিয়া, ভূমিকা আৰু দায়িত্বসমূহ আৰু পেটচ মোতায়েনৰ বাবে সময়ৰেখাসমূহৰ ৰূপৰেখা দাঙি ধৰে। এই নীতিত জটিল পেটচসমূহ কেনেকৈ নিয়ন্ত্রণ কৰিব লাগে তাৰ নির্দেশনাও অন্তর্ভুক্ত কৰিব লাগে। যেনে যিবোৰে শূন্য-দিনৰ দুর্বলতাসমূহ সম্বোধন কৰে। নীতিটো সকলো কর্মচাৰীক জনোৱা উচিত আৰু নিয়মীয়াকৈ প্রশিক্ষণ অনুষ্ঠিত কৰিব লাগে যাতে সকলোৱে নীতিটো বুজি পায়।

2. **নিয়মীয়া দুর্বলতা স্কেনসমূহ কৰক :** চিষ্টেমসমূহ আৰু এপ্লিকেচনসমূহত দুর্বলতাসমূহ চিনাক্ত কৰিবলে নিয়মিত দুর্বলতা স্কেনিং কৰা উচিত। দুর্বলতা স্কেনিং নিয়মীয়াকৈ, যেনে মাহেকীয়া বা ত্রিমাসিকভাৱে আৰু আন্তঃগাঁথনিৰ যিকোনো উল্লেখযোগ্য পৰিৱর্তনৰ পিছত কৰিব লাগে। মানুহৰ ভুলৰ আশংকা হ্রাস কৰিবলৈ আৰু সামঞ্জস্য নিশ্চিত কৰিবলৈ য'তেই সম্ভৱ দুর্বলতা স্কেনিং স্বয়ংক্রিয় কৰিব লাগে।

3. **পেটচসমূহক অগ্রাধিকাৰ দিয়ক:** পেটচসমূহক ইয়াৰ গুৰুত্ব আৰু সংস্থাটোৰ ওপৰত সম্ভাব্য প্রভাৱৰ ওপৰত ভিত্তি কৰি অগ্রাধিকাৰ দিব লাগে। জটিল পেটচসমূহ, যেনে যি শূন্য-দিনৰ দুর্বলতাসমূহ বা সক্রিয়ভাৱে শোষণ কৰা দুর্বলতাসমূহ সম্বোধন কৰে, যিমান পাৰি সোনকালে মোতায়েন কৰিব লাগে। ব্যৱসায়িক কার্য্যকলাপত ইয়াৰ প্রভাৱ আৰু শোষণৰ সম্ভাৱনাৰ ওপৰত ভিত্তি কৰি অগুৰুত্বপূর্ণ পেটচসমূহক অগ্রাধিকাৰ দিব লাগে।

4. **মোতায়েনৰ আগতে পেটচসমূহ পৰীক্ষা কৰক:** পেটচসমূহক উৎপাদন পৰিৱেশত মোতায়েন কৰাৰ আগতে এটা অ-উৎপাদন পৰিৱেশত ভালদৰে পৰীক্ষা কৰিব লাগে। পৰীক্ষণে নিশ্চিত কৰিব লাগে যে পেটচে চিষ্টেম বা এপ্লিকেচনত কোনো বিৰূপ প্রভাৱ নেপেলায়, যেনে ক্রেচ বা পৰিৱেশন সমস্যা। মানৱ ভুলৰ আশংকা হ্রাস কৰিবলৈ আৰু সামঞ্জস্য নিশ্চিত কৰিবলৈ য'তেই সম্ভৱ পৰীক্ষা স্বয়ংক্রিয় কৰিব লাগে।

5. **পেটচসমূহ দ্রুতভাৱে ব্যৱহাৰ কৰক:** পেটচসমূহ পৰীক্ষা আৰু পৰীক্ষা কৰাৰ পিছত যিমান পাৰি দ্রুতভাৱে ব্যৱহাৰ কৰিব লাগে। পেটচ ব্যৱহাৰত বিলম্ব কৰিলে হেকাৰ আৰু চাইবাৰ অপৰাধীসকলৰ বাবে দুর্বলতাসমূহ শোষণ কৰাৰ সুযোগৰ সুবিধা বৃদ্ধি পায়।

6. **পেটচ ব্যৱস্থাপনা স্বয়ংক্রিয় কৰক:** পেটচ ব্যৱস্থাপনা প্রক্রিয়াক সুশৃংখলিত কৰিবলৈ আৰু মানৱ ভুলৰ আশংকা হ্রাস কৰিবলৈ য'তেই সম্ভৱ স্বয়ংক্রিয় পেটচ ব্যৱস্থাপনা সঁজুলিসমূহ ব্যৱহাৰ কৰিব লাগে। স্বয়ংক্রিয় সঁজুলিসমূহে পেটচ চিনাক্তকৰণ, অগ্রাধিকাৰ, পৰীক্ষণ আৰু মোতায়েনৰ সৈতে সহায় কৰিব পাৰে।

7. **পেটচ মোতায়েন পর্যবেক্ষণ আৰু পৰীক্ষা কৰক:** পেটচসমূহ মোতায়েন কৰাৰ পিছত, সিহঁতক নিৰীক্ষণ আৰু পৰীক্ষা কৰিব লাগে যাতে সিহঁত সঠিকভাৱে প্রয়োগ কৰা হৈছে আৰু চিষ্টেম বা এপ্লিকেচন সঠিকভাৱে কার্য্যকৰী হৈছে নে নাই। পর্যবেক্ষণ দুর্বলতা স্কেনিং, লগ বিশ্লেষণ, বা অন্য সুৰক্ষা পর্যবেক্ষণ সঁজুলিসমূহৰ যোগেদি কৰিব পাৰি।

8. **নিয়মীয়া পেটচ অডিটসমূহ পৰিচালনা কৰক:** নিয়মিত পেটচ অডিটসমূহ কৰিব লাগে যাতে সকলো চিষ্টেম আৰু এপ্লিকেচনসমূহ শেহতীয়া পেটচসমূহৰ সৈতে আপডেইট কৰা হয়। পেটচ অডিটসমূহে চিষ্টেমসমূহ বা এপ্লিকেচনসমূহ চিনাক্ত কৰাত সহায় কৰিব পাৰে যি পেটচ কৰা হোৱা নাই বা সময়মতে পেটচ কৰা হোৱা নাই।

9. **এটা পেটচ ৰোলবেক পৰিকল্পনা প্রতিষ্ঠা কৰক:** যদি এটা পেচে চিষ্টেম বা এপ্লিকেচনত বিৰূপ প্রভাৱ পেলায়, এটা পেটচ ৰোলবেক পৰিকল্পনা প্রতিষ্ঠা কৰিব লাগে। পৰিকল্পনাই পেটচ মোতায়েন কৰাৰ আগতে চিষ্টেম বা এপ্লিকেচনক ইয়াৰ পূর্বৰ অৱস্থালৈ ঘূৰাই অনাৰ পদক্ষেপসমূহৰ ৰূপৰেখা দাঙি ধৰিব লাগে।

10. **নিয়ম আৰু প্রামাণিকসমূহৰ সৈতে সন্মতি:** সংস্থাসমূহে নিশ্চিত কৰিব লাগে যে তেওঁলোকৰ পেটচ ব্যৱস্থাপনা প্রক্রিয়া নিয়ন্ত্রণৰ প্রয়োজনীয়তা আৰু উদ্যোগৰ মানদণ্ডসমূহৰ সৈতে মিল আছে। নিয়ম আৰু মানদণ্ড মানি চলিলে সংস্থাটোক আর্থিক শাস্তি আৰু সুনামৰ ক্ষতিৰ পৰা সুৰক্ষিত হোৱাটো নিশ্চিত কৰাত সহায় কৰে।

এটা প্রতিষ্ঠানৰ চিষ্টেম আৰু এপ্লিকেচনসমূহক চাইবাৰ আক্রমণৰ পৰা সুৰক্ষিত কৰিবলৈ ফলপ্রসূ সুৰক্ষা পেটচ ব্যৱস্থাপনা অতি গুৰুত্বপূর্ণ। এটা পেটচ ব্যৱস্থাপনা নীতি প্রতিষ্ঠা কৰা, নিয়মীয়া দুর্বলতা স্কেনসমূহ সম্পাদন কৰা, পেটচসমূহক অগ্রাধিকাৰ দিয়া, মোতায়েনৰ পূর্বে পেটচসমূহ পৰীক্ষা কৰা, পেটচসমূহ দ্রুতভাৱে মোতায়েন কৰা, পেটচ ব্যৱস্থাপনা স্বয়ংক্রিয় কৰা, পেটচ মোতায়েন নিৰীক্ষণ আৰু পৰীক্ষা কৰা, নিয়মীয়া পেটচ অডিটসমূহ চলোৱা, এটা পেটচ ৰোলবেক পৰিকল্পনা স্থাপন কৰা আৰু নিয়ম আৰু প্রামাণিকসমূহ মানি চলাই সংস্থাসমূহক এটা ফলপ্রসূ পেটচ ব্যৱস্থাপনা কৌশল বিকশিত কৰাত সহায় কৰিব পাৰে।

১২.৬ ডাটা বেকআপ

ডাটা বেকআপ ডাটা ব্যৱস্থাপনাৰ এটা অপৰিহার্য দিশ, গুৰুত্বপূর্ণ ডাটা হেৰুৱা, দুর্নীতি, বা অকর্তৃত্বশীল প্রৱেশৰ পৰা সুৰক্ষিত হোৱাটো নিশ্চিত কৰা। তথ্য বেকআপ লোৱাৰ অন্তর্গত তথ্যৰ এটা কপি সৃষ্টি কৰা হয় হস্তচালিতভাৱে বা স্বয়ংক্রিয় প্রক্রিয়াৰ যোগেদি আৰু ইয়াক এটা সুৰক্ষিত অৱস্থানত সংৰক্ষণ কৰা। এতিয়া আমি ডাটা বেকআপৰ

বিষয়ে বিতংভাৱে আলোচনা কৰিম। তাত অন্তর্ভুক্ত থাকিব ইয়াৰ গুৰুত্ব, বেকআপৰ ধৰণ, বেকআপ কৌশল আৰু উত্তম পদ্ধতিসমূহ। ডাটা বেকআপ বিভিন্ন কাৰণত গুৰুত্বপূর্ণ, তাৰে কেইটামান উল্লেখযোগ্য দিশ হ'ল—

দুর্যোগ পুনৰুদ্ধাৰ: ডাটা বেকআপ দুর্যোগ পুনৰুদ্ধাৰ পৰিকল্পনাৰ এটা অপৰিহার্য অংশ। দুর্যোগৰ ক্ষেত্রত, যেনে প্রাকৃতিক দুর্যোগ বা চাইবাৰ আক্রমণ, ডাটা বেকআপে নিশ্চিত কৰে যে ডাটা উদ্ধাৰ কৰিব পৰা যায়, যাৰ ফলত সংস্থাটোৰ ওপৰত প্রভাৱ কম হয়।

তথ্য হেৰুৱাত প্রতিৰোধ: বিভিন্ন কাৰণত তথ্য হেৰুৱাব পাৰে, য'ত হার্ডৱেৰ বিফলতা, চফটৱেৰ ভুল আৰু আকস্মিকভাৱে মচি পেলোৱা আদি অন্তর্ভুক্ত। ডাটা বেকআপে নিশ্চিত কৰে যে জটিল ডাটা পুনৰুদ্ধাৰ কৰিব পৰা যায়, ডাটা হেৰুৱাৰ আশংকা কম কৰি।

অনুসৰণ: বহু উদ্যোগৰ নিয়ন্ত্রণমূলক প্রয়োজনীয়তা আছে যিয়ে এটা নির্দিষ্ট সময়ৰ বাবে ডাটা বেকআপ বাধ্যতামূলক কৰে। আইনী আৰু আর্থিক শাস্তিৰ পৰা হাত সাৰিবলৈ এই নিয়মসমূহ মানি চলাটো অতি গুৰুত্বপূর্ণ।

খৰচ সঞ্চয়: তথ্যৰ ক্ষতিৰ ফলত যথেষ্ট আর্থিক লোকচান হ'ব পাৰে, য'ত হেৰুৱা উৎপাদনশীলতা, ডাউনটাইম আৰু পুনৰুদ্ধাৰৰ খৰচো অন্তর্ভুক্ত। ডাটা বেকআপে এই খৰচসমূহ কম কৰাত সহায় কৰে যাতে ডাটা দ্রুত আৰু কার্যক্ষমভাৱে পুনৰুদ্ধাৰ কৰিব পৰা যায়।

বেকআপসমূহৰ ধৰণসমূহ

বিভিন্ন ধৰণৰ বেকআপ আছে, য'ত আছে:

- সম্পূর্ণ বেকআপ: এটা সম্পূর্ণ বেকআপত এটা চিষ্টেম বা ডিভাইচত সকলো তথ্য কপি কৰে। সম্পূর্ণ বেকআপসমূহে পৰিৱেশন কৰিবলৈ বেছি সময় লয় আৰু অধিক সংৰক্ষণ স্থানৰ প্রয়োজন হয় কিন্তু বিস্তৃত তথ্য সুৰক্ষা প্রদান কৰে।
- বৃদ্ধিমূলক বেকআপ: বৃদ্ধিমূলক বেকআপসমূহে কৰল শেষ বেকআপৰ পিছত সলনি হোৱা তথ্য কপি কৰে, সিহঁতক দ্রুত কৰি আৰু সম্পূর্ণ বেকআপতকৈ কম সংৰক্ষণ স্থানৰ প্রয়োজন হয়।
- ভিন্নতামূলক বেকআপ: ভিন্নতামূলক বেকআপসমূহে শেষ সম্পূর্ণ বেকআপৰ পিছত সলনি হোৱা সকলো তথ্য কপি কৰে, সিহঁতক সম্পূর্ণ বেকআপসমূহতকৈ দ্রুত কিন্তু বৃদ্ধিশীল বেকআপসমূহতকৈ লেহেমীয়া কৰি তোলে।
- মিৰ'ৰ বেকআপ: এটা মিৰ'ৰ বেকআপত এটা চিষ্টেম বা ডিভাইচত তথ্যৰ এটা সঠিক কপি সৃষ্টি কৰে, ইয়াক দুর্যোগ পুনৰুদ্ধাৰৰ বাবে উপযোগী কৰি।

বেকআপ কৌশলসমূহ: সংস্থাসমূহে বিভিন্ন বেকআপ কৌশল ব্যৱহাৰ কৰিব পাৰে, তেওঁলোকৰ প্ৰয়োজন আৰু সম্পদৰ ওপৰত নিৰ্ভৰ কৰি। কিছুমান সাধাৰণ বেকআপ কৌশলৰ ভিতৰত আছে:

1. **সম্পূৰ্ণ বেকআপ কৌশল:** এটা সম্পূৰ্ণ বেকআপ কৌশলে এটা চিষ্টেম বা ডিভাইচত সকলো তথ্যৰ এটা সম্পূৰ্ণ কপি সৃষ্টি কৰি লয়। এই ধৰণৰ বেকআপে পৰিৱেশন কৰিবলৈ বেছি সময় লয় আৰু অন্য বেকআপ কৌশলতকৈ অধিক সংৰক্ষণ স্থানৰ প্ৰয়োজন হয়, কিন্তু ই বিস্তৃত তথ্য সুৰক্ষা প্ৰদান কৰে। সম্পূৰ্ণ বেকআপসমূহ সাধাৰণতে সময়ে সময়ে কৰা হয়, যেনে সাপ্তাহিক বা মাহেকীয়া।

2. **বৃদ্ধিমূলক বেকআপ কৌশল:** এটা বৃদ্ধিমূলক বেকআপ কৌশলে কেৱল শেষ বেকআপৰ পিছত সলনি হোৱা তথ্যৰ বেকআপ লয়। এই ধৰণৰ বেকআপ দ্ৰুত আৰু সম্পূৰ্ণ বেকআপতকৈ কম সংৰক্ষণ স্থানৰ প্ৰয়োজন। বৃদ্ধিমূলক বেকআপসমূহ দৈনিক ভিত্তিত বা অধিক সঘনাই কৰিব পাৰি, সৃষ্টি কৰা তথ্যৰ পৰিমাণৰ ওপৰত নিৰ্ভৰ কৰি।

3. **ভিন্নতামূলক বেকআপ কৌশল:** এটা ভিন্নতামূলক বেকআপ কৌশলে শেষ সম্পূৰ্ণ বেকআপৰ পিছত সলনি হোৱা সকলো তথ্য কপি কৰে। এই ধৰণৰ বেকআপ সম্পূৰ্ণ বেকআপতকৈ দ্ৰুত কিন্তু বৃদ্ধিশীল বেকআপতকৈ লেহেমীয়া। ভিন্নতামূলক বেকআপসমূহ সাধাৰণতে সময়ে সময়ে কৰা হয়, যেনে সাপ্তাহিক।

4. **মিৰ'ৰ বেকআপ কৌশল:** এটা মিৰ'ৰ বেকআপ কৌশলে এটা চিষ্টেম বা ডিভাইচত তথ্যৰ এটা সঠিক কপি সৃষ্টি কৰে। এই ধৰণৰ বেকআপ দুৰ্যোগ পুনৰুদ্ধাৰৰ বাবে উপযোগী, কাৰণ ই তথ্যৰ এটা সঠিক প্ৰতিলিপি প্ৰদান কৰে যি দুৰ্যোগৰ ক্ষেত্ৰত এটা চিষ্টেম পুনৰুদ্ধাৰ কৰিবলে ব্যৱহাৰ কৰিব পাৰি।

5. **হাইব্ৰিড বেকআপ কৌশল:** এটা হাইব্ৰিড বেকআপ কৌশলে এটা বিস্তৃত বেকআপ আৰু পুনৰুদ্ধাৰ পৰিকল্পনা সৃষ্টি কৰিবলে দুটা বা অধিক বেকআপ কৌশল একত্ৰিত কৰে। উদাহৰণস্বৰূপ, এটা প্ৰতিষ্ঠানে মাহত এবাৰ এটা সম্পূৰ্ণ বেকআপ কৌশল, এটা বৃদ্ধিমূলক বেকআপ কৌশল দৈনিক, আৰু এটা জটিল চিষ্টেমসমূহৰ বাবে এটা মিৰ'ৰ বেকআপ কৌশল ব্যৱহাৰ কৰিব পাৰে।

6. **অফছাইট বেকআপ কৌশল:** এটা অফছাইট বেকআপ কৌশলে বেকআপসমূহক এটা অৱস্থানত সংৰক্ষণ কৰে যি প্ৰাথমিক ডাটা কেন্দ্ৰৰ পৰা দৈহিকভাৱে পৃথক। এই ধৰণৰ বেকআপ কৌশলে প্ৰাথমিক ডাটা কেন্দ্ৰক প্ৰভাৱিত কৰিব পৰা দুৰ্যোগৰ বিৰুদ্ধে অতিৰিক্ত সুৰক্ষা প্ৰদান কৰে।

7. **ক্লাউড বেকআপ কৌশল:** এটা ক্লাউড বেকআপ কৌশলত বেকআপসমূহ ক্লাউডত সংৰক্ষণ কৰে। এই ধৰণৰ বেকআপ কৌশলে অতিৰিক্ত নমনীয়তা আৰু স্কেলেবিলিটি, লগতে অফছাইট সংৰক্ষণ প্ৰদান কৰে।

৪. **টেপ বেকআপ কৌশল:** এটা টেপ বেকআপ কৌশলে টেপত বেকআপসমূহ সংৰক্ষণ কৰে। এই ধৰণৰ বেকআপ কৌশল নির্ভৰযোগ্য আৰু খৰচ-বহনক্ষম কিন্তু অন্য বেকআপ কৌশলতকৈ অধিক হস্তক্ষেপৰ প্রয়োজন।

এটা বেকআপ কৌশল নির্বাচন কৰাৰ সময়ত, প্রতিষ্ঠানসমূহে সৃষ্টি কৰা তথ্যৰ পৰিমাণ, তথ্যৰ জটিলতা, বাজেট, আৰু বেকআপ আৰু পুনৰুদ্ধাৰৰ বাবে উপলব্ধ সম্পদসমূহৰ দৰে কাৰকসমূহ বিবেচনা কৰিব লাগে। এটা বিস্তৃত বেকআপ কৌশলে সম্পূর্ণ আৰু বৃদ্ধিমূলক বেকআপ দুয়োটা অন্তর্ভুক্ত কৰিব লাগে, লগতে অফছাইট সংৰক্ষণ বা ক্লাউড বেকআপ দুর্যোগৰ বিৰুদ্ধে অতিৰিক্ত সুৰক্ষা প্রদান কৰে। বেকআপসমূহৰ নিয়মীয়া পৰীক্ষা কৰাটোও প্রয়োজনীয় যাতে এটা দুর্যোগ বা চিষ্টেম বিফলতাৰ ক্ষেত্রত তথ্য পুনৰুদ্ধাৰ কৰিব পাৰি।

১২.৭ তৃতীয় পক্ষৰ চফটৱেৰ ডাউনলোড আৰু পৰিচালনা

তৃতীয় পক্ষৰ চফটৱেৰ বুলিলে কোনো কোম্পানী বা ব্যক্তিয়ে বিকশিত কৰা চফটৱেৰক বুজায় যি কোনো বিশেষ চফটৱেৰ বা হার্ডৱেৰ উৎপাদনৰ মূল নির্মাতা বা বিকাশক নহয়। বর্তমানৰ চফটৱেৰত নতুন বৈশিষ্ট্য বা কার্যকৰীতা যোগ কৰিবলে বা হার্ডৱেৰ ডিভাইচসমূহৰ ক্ষমতাসমূহ সম্প্রসাৰণ কৰিবলৈ তৃতীয়-পক্ষ চফটৱেৰ ব্যৱহাৰ কৰিব পাৰি ।

তৃতীয়-পক্ষ চফটৱেৰৰ উদাহৰণসমূহৰ ভিতৰত ৱেব ব্রাউজাৰসমূহৰ বাবে প্লাগইনসমূহ, এড-অনসমূহ আৰু সম্প্রসাৰণসমূহ, লগতে চফটৱেৰ এপ্লিকেচনসমূহ যেনে উৎপাদনশীলতা সঁজুলিসমূহ, সুৰক্ষা চফটৱেৰসমূহ, আৰু মিডিয়া প্লেয়াৰসমূহ অন্তর্ভুক্ত। তৃতীয় পক্ষৰ চফটৱেৰ বিভিন্ন উৎসৰ পৰা বিনামূলীয়াকৈ ক্রয় বা ডাউনলোড কৰিব পাৰি, চফটৱেৰ ডেভেলপাৰৰ ৱেবছাইট, এপ ষ্ট'ৰ, আৰু অন্যান্য অনলাইন বজাৰকে ধৰি।

তৃতীয় পক্ষৰ চফটৱেৰে বৃদ্ধি কৰা কার্যক্ষমতা আৰু উন্নত উৎপাদনশীলতাকে ধৰি বহুতো সুবিধা প্রদান কৰিব পাৰে যদিও সঠিকভাৱে পৰিচালিত নহ'লে ই সুৰক্ষাৰ ক্ষেত্রত বিপদো সৃষ্টি কৰিব পাৰে। কিছুমান তৃতীয় পক্ষৰ চফটৱেৰত দুর্বলতা থাকিব পাৰে বা ইচ্ছাকৃতভাৱে ব্যৱহাৰকাৰীৰ কম্পিউটাৰলৈ মেলৱেৰ বা অন্য ক্ষতিকাৰক চফটৱেৰ প্রেৰণ কৰিবলৈ ডিজাইন কৰা হ'ব পাৰে। ডাউনলোড বা ইনষ্টল কৰাৰ আগতে তৃতীয় পক্ষৰ চফটৱেৰ সযতনে মূল্যায়ন কৰাটো গুৰুত্বপূর্ণ, আৰু চফটৱেৰ পৰিচালনা আৰু আপডেইট কৰাৰ বাবে উত্তম পদ্ধতিসমূহ অনুসৰণ কৰাটো গুৰুত্বপূর্ণ যাতে ই সুৰক্ষিত হৈ থাকে।

তৃতীয় পক্ষৰ চফটৱেৰ ডাউনলোড আৰু পৰিচালনা কৰিলে কেইবাটাও সুৰক্ষা বিপদৰ সৃষ্টি হ'ব পাৰে, য'ত মেলৱেৰ বা অন্য ক্ষতিকাৰক চফটৱেৰ ডাউনলোড কৰাৰ আশংকাও অন্তর্ভুক্ত। তৃতীয়-পক্ষ চফটৱেৰ ডাউনলোড আৰু পৰিচালনাৰ বাবে কিছুমান উত্তম পদ্ধতি ইয়াত দিয়া হ'ল:

ডাউনলোডসমূহৰ বাবে সুনামধন্য উৎসসমূহ বাছক: তৃতীয়-পক্ষ চফটৱেৰ ডাউনলোড আৰু পৰিচালনাৰ প্ৰথম পদক্ষেপটো হ'ল ডাউনলোডসমূহৰ বাবে সুনামধন্য উৎসসমূহ বাছনি কৰা। সুনামধন্য উৎসসমূহৰ ভিতৰত আছে চফটৱেৰ বিক্ৰেতাৰ অফিচিয়েল ৱেবছাইট, চিনেট বা চষ্টনিকৰ দৰে জনপ্ৰিয় ডাউনলোড পৰ্টেল, আৰু গুগল প্লে বা এপল এপ ষ্ট'ৰৰ দৰে এপ ষ্ট'ৰ। অজ্ঞাত বা অবিশ্বাস্য উৎসৰ পৰা চফটৱেৰ ডাউনলোড কৰাটো এৰক, কাৰণ ইয়াত মেলৱেৰ বা অন্য ক্ষতিকাৰক ক'ড থাকিব পাৰে যিয়ে আপোনাৰ চিষ্টেমৰ সুৰক্ষাৰ সৈতে আপোচ কৰিব পাৰে।

চফটৱেৰৰ প্ৰামাণ্যতা পৰীক্ষা কৰক: তৃতীয় পক্ষৰ চফটৱেৰ ডাউনলোড কৰাৰ আগতে ইয়াৰ প্ৰামাণ্যতা পৰীক্ষা কৰাটো গুৰুত্বপূৰ্ণ। ইয়াৰ লগত চফটৱেৰটো বৈধ নেকি আৰু মেলৱেৰ থাকিব পৰা ভুৱা বা নকল সংস্কৰণ নহয় নেকি পৰীক্ষা কৰাটো জড়িত হৈ থাকে। চফটৱেৰৰ প্ৰামাণ্যতা পৰীক্ষা কৰিবলৈ, চফটৱেৰ বিক্ৰেতাই প্ৰদান কৰা ডিজিটেল স্বাক্ষৰ বা হেচ মান বিচাৰক। ডিজিটেল স্বাক্ষৰ হৈছে ক্ৰিপ্টোগ্ৰাফিক সঁজুলি যিয়ে চফটৱেৰ বিক্ৰেতাৰ পৰিচয় পৰীক্ষা কৰে আৰু চফটৱেৰ পেকেজৰ অখণ্ডতা নিশ্চিত কৰে। হেচ মানসমূহ হৈছে একক চিনাক্তকৰ্তা যি ডাউনল'ড প্ৰক্ৰিয়াৰ সময়ত চফটৱেৰ পেকেইজৰ সৈতে কিবা সাল-সলনি যে হোৱা নাই সেয়া নিৰ্ধাৰণ কৰে।

সুসংগততা আৰু চিষ্টেমৰ প্ৰয়োজনীয়তাসমূহ পৰীক্ষা কৰক: তৃতীয়-পক্ষ চফটৱেৰ ডাউনলোড আৰু ইনষ্টল কৰাৰ আগতে, ইয়াৰ সুসংগততা আৰু চিষ্টেমৰ প্ৰয়োজনীয়তাসমূহ পৰীক্ষা কৰাটো গুৰুত্বপূৰ্ণ। সুনিশ্চিত কৰক যে চফটৱেৰ আপোনাৰ কাৰ্যকৰপ্ৰণালীৰ সৈতে সুসংগত আৰু ন্যূনতম ব্যৱস্থাপ্ৰণালীৰ প্ৰয়োজনীয়তাসমূহ পূৰণ কৰে, যেনে প্ৰচেছৰৰ গতি, RAM, আৰু ডিস্ক স্থান। আপোনাৰ ব্যৱস্থাপ্ৰণালীৰ সৈতে সুসংগত নোহোৱা চফটৱেৰ সংস্থাপন কৰিলে সুসংগততা সমস্যাৰ সৃষ্টি হ'ব পাৰে আৰু ব্যৱস্থাপ্ৰণালীৰ পৰিৱেশন বা স্থিৰতাক আপোচ কৰিব পাৰে।

এণ্টিভাইৰাছ আৰু এণ্টি-মেলৱেৰ চফটৱেৰ ব্যৱহাৰ কৰক: আপোনাৰ চিষ্টেমক মেলৱেৰ আৰু অন্য সুৰক্ষা ভাবুকিৰ পৰা সুৰক্ষিত কৰিবলৈ এণ্টিভাইৰাছ আৰু

এণ্টি-মেলৱেৰ চফটৱেৰ ব্যৱহাৰ কৰাটো অতি প্ৰয়োজনীয়। নিশ্চিত কৰক যে আপোনাৰ এণ্টিভাইৰাছ চফটৱেৰ আপডেইট আৰু আপোনাৰ ব্যৱস্থাপ্ৰণালীৰ নিয়মীয়া স্কেনসমূহ কৰিবলে সংহতি কৰা হৈছে। এণ্টিভাইৰাছ আৰু এণ্টি-মেলৱেৰ চফ্টৱেৰে তৃতীয় পক্ষৰ চফটৱেৰত উপস্থিত হ'ব পৰা ক্ষতিকাৰক ক'ড ধৰা পেলাব পাৰে আৰু আঁতৰাব পাৰে, যাৰ ফলত আপোচ বা তথ্য হেৰুৱাৰ আশংকা হ্ৰাস পায়।

তৃতীয়-পক্ষ চফটৱেৰ নিয়মিতভাৱে আপডেইট কৰা: তৃতীয়-পক্ষ চফটৱেৰ নিয়মিতভাৱে আপডেইট কৰাটো গুৰুত্বপূৰ্ণ যাতে ই সুৰক্ষিত আৰু দুৰ্বলতাৰ পৰা মুক্ত হৈ থাকে। চফটৱেৰ বিক্ৰেতাসকলে সুৰক্ষা সমস্যাসমূহ সমাধান কৰিবলে আৰু কাৰ্যকৰীতা উন্নত কৰিবলে আপডেইটসমূহ আৰু পেটচসমূহ মুকলি কৰে, আৰু সিহঁত উপলব্ধ হোৱাৰ লগে লগে সিহঁতক সংস্থাপন কৰাটো গুৰুত্বপূৰ্ণ। তৃতীয়-পক্ষ চফটৱেৰৰ বাবে স্বয়ংক্ৰিয় আপডেইটসমূহ সংস্থাপন কৰক যাতে আপডেইটসমূহ তৎক্ষণাত সংস্থাপন কৰা হয়। নিয়মিতভাৱে আপডেইটসমূহৰ বাবে হস্তচালিতভাৱে পৰীক্ষা কৰক যদি স্বয়ংক্ৰিয় আপডেইটসমূহ উপলব্ধ নহয়।

অব্যৱহৃত আৰু অপ্ৰয়োজনীয় চফটৱেৰ আঁতৰাওক: অব্যৱহৃত আৰু অপ্ৰয়োজনীয় তৃতীয়-পক্ষ চফটৱেৰ আঁতৰোৱাটো আপোনাৰ চিষ্টেমৰ আক্ৰমণৰ পৃষ্ঠভাগ হ্ৰাস কৰিবলে আৰু সুৰক্ষা ভংগৰ আশংকা কম কৰিবলে গুৰুত্বপূৰ্ণ। অব্যৱহৃত চফ্টৱেৰে আক্ৰমণকাৰীয়ে শোষণ কৰিব পৰা দুৰ্বলতা সৃষ্টি কৰিব পাৰে, আৰু ই ব্যৱস্থাপ্ৰণালীৰ সম্পদসমূহো ব্যৱহাৰ কৰিব পাৰে আৰু ব্যৱস্থাপ্ৰণালীৰ পৰিৱেশনত প্ৰভাৱ পেলাব পাৰে। আপোনাৰ চিষ্টেমত সংস্থাপন কৰা চফটৱেৰসমূহ নিয়মিতভাৱে পৰ্যালোচনা কৰক আৰু যিকোনো চফটৱেৰ আঁতৰাওক যি প্ৰয়োজনীয় নহয় বা আৰু ব্যৱহাৰ কৰা হোৱা নাই। এইটো নিয়ন্ত্ৰণ পেনেল বা তৃতীয় পক্ষৰ চফটৱেৰ আনইনষ্টলাৰ সঁজুলি ব্যৱহাৰ কৰি কৰিব পাৰি।

ভাৰ্চুৱেলাইজেচন বা ছেণ্ডবক্সিং ব্যৱহাৰ কৰক: ভাৰ্চুৱেলাইজেচন বা ছেণ্ডবক্সিং হৈছে এটা কৌশল যি হষ্ট চিষ্টেমৰ পৰা তৃতীয়-পক্ষ চফটৱেৰ পৃথক কৰে, আপোচ বা তথ্য হেৰুৱাৰ আশংকা হ্ৰাস কৰে। ভাৰ্চুৱেলাইজেচনে এটা ভাৰ্চুৱেল পৰিৱেশ সৃষ্টি কৰাটো জড়িত কৰে য'ত চফটৱেৰ চলিব পাৰে, আনহাতে ছেণ্ডবক্সিঙে চিষ্টেম সম্পদসমূহলে চফটৱেৰৰ প্ৰৱেশ সীমিত কৰাটো জড়িত কৰে। ভাৰ্চুৱেলাইজেচন বা ছেণ্ডবক্সিং নতুন চফটৱেৰ পৰীক্ষা কৰিবলৈ বা সম্ভাব্য বিপদজনক চফটৱেৰ, যেনে মেলৱেৰ বিশ্লেষণ সঁজুলি, এটা নিয়ন্ত্ৰিত পৰিৱেশত চলাবলৈ ব্যৱহাৰ কৰিব পাৰি, হষ্ট চিষ্টেমক প্ৰভাৱিত নকৰাকৈ।

প্ৰৱেশ নিয়ন্ত্ৰণসমূহ প্ৰণয়ন কৰক: প্ৰৱেশ নিয়ন্ত্ৰণসমূহ প্ৰণয়ন কৰাটো গুৰুত্বপূৰ্ণ যাতে কেৱল অনুমোদিত ব্যৱহাৰকাৰীসকলেহে তৃতীয়-পক্ষ চফটৱেৰৰ

ডাউনলোড আৰু ইনষ্টল কৰিব পাৰে। প্ৰৱেশ নিয়ন্ত্ৰণসমূহে পাছৱৰ্ড সুৰক্ষা, দুটা-কাৰক প্ৰমাণীকৰণ, আৰু ভূমিকা-ভিত্তিক প্ৰৱেশ নিয়ন্ত্ৰণ অন্তৰ্ভুক্ত কৰিব পাৰে।



অগ্ৰগতি নিৰীক্ষণ

প্ৰশ্ন ১: শুদ্ধ নে অশুদ্ধ নিৰ্ণয় কৰক—

ক) ৰাউটাৰ এটা এণ্ডপইণ্ট ডিভাইচ।

খ) এটা ডিভাইচত ডেটা এনক্ৰিপ্ট কৰিলে হেকাৰসকলে সেই ডেটাত প্ৰৱেশ কৰাৰ সম্ভাৱনা নাথাকে।

গ) চিকিউৰিটি পেচবোৰ হৈছে চফটৱেৰ ভেণ্ডৰসকলে মুক্তি দিয়া আপডেট, যাৰ দ্বাৰা জনা চিকিউৰিটি দুৰ্বলতা সমাধান কৰা হয়।

ঘ) আধুনিক হাৰ্ড ড্ৰাইভবোৰ অতিশয় বিশ্বাসযোগ্য হোৱা বাবে নিয়মিতভাৱে ডেটা বেকআপ কৰা প্ৰয়োজন নাই।

ঙ) ইনক্ৰিমেণ্টেল বেকআপে কেৱল সেই ফাইলবোৰ কপি কৰে, যিবোৰ শেষ বেকআপৰ পিছত পৰিৱৰ্তিত বা সৃষ্টি কৰা হৈছে।

চ) তৃতীয় পক্ষৰ চফটৱেৰ সদায় ডাউনলোড আৰু ব্যৱহাৰৰ বাবে বিনামূলীয়া।

ছ) সকলো তৃতীয় পক্ষৰ চফটৱেৰ সকলো ডিভাইচ আৰু চফটৱেৰ প্লেটফৰ্মৰ সৈতে সঙ্গতিপূৰ্ণ।



১২.৮ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ

- এণ্ডপইণ্ট ডিভাইচ সুৰক্ষাই ব্যক্তিগত ডিভাইচসমূহ যেনে ডেস্কটপ, লেপটপ, স্মাৰ্টফোন, আৰু টেবলেটসমূহক সম্ভাব্য চাইবাৰ ভাবুকিৰ পৰা সুৰক্ষাক বুজায়।
- এণ্ডপইণ্ট ডিভাইচ সুৰক্ষা ব্যৱস্থাসমূহৰ ভিতৰত আছে শক্তিশালী পাছৱৰ্ডসমূহ প্ৰণয়ন কৰা, নিয়মিতভাৱে চফটৱেৰ আপডেইট কৰা, এণ্টিভাইৰাছ চফটৱেৰ ব্যৱহাৰ কৰা, আৰু স্পৰ্শকাতৰ তথ্যলৈ প্ৰৱেশ নিষিদ্ধ কৰা।
- মোবাইল সুৰক্ষাৰ প্ৰত্যাহ্বানসমূহৰ ভিতৰত আছে মোবাইল ডিভাইচ আৰু অপাৰেটিং চিষ্টেমৰ বিভিন্নতা, মোবাইল এপৰ ক্ৰমাৎ জটিলতা, আৰু আক্ৰমণৰ প্ৰতি মোবাইল নেটৱৰ্কৰ দুৰ্বলতা।
- মোবাইল ডিভাইচ সুৰক্ষাৰ বাবে প্ৰতিকাৰৰ ব্যৱস্থাসমূহৰ ভিতৰত আছে ডিভাইচ এনক্ৰিপচন প্ৰণয়ন কৰা, শক্তিশালী পাছৱৰ্ড ব্যৱহাৰ কৰা, চফটৱেৰ আপডেট ৰখা,

মোবাইল ডিভাইচ ব্যৱস্থাপনা (MDM) সমাধান ব্যৱহাৰ কৰা, আৰু ব্যৱহাৰকাৰীসকলক সুৰক্ষিত মোবাইল ডিভাইচ ব্যৱহাৰৰ প্ৰশিক্ষণ দিয়া।

• পাছৱৰ্ড নীতি হৈছে ব্যক্তিসকলে ব্যৱহাৰ কৰা পাছৱৰ্ডসমূহ শক্তিশালী, সুৰক্ষিত, আৰু চাইবাৰ আক্ৰমণৰ প্ৰতি কম দুৰ্বল হোৱাটো নিশ্চিত কৰিবলৈ ডিজাইন কৰা নিয়ম আৰু নিৰ্দেশিকাসমূহৰ এটা গোট।

• সুৰক্ষা পেটচ ব্যৱস্থাপনাত চফটৱেৰ পেটচসমূহ চিনাক্ত কৰা, অধিগ্ৰহণ কৰা, পৰীক্ষা কৰা আৰু সংস্থাপন কৰা প্ৰক্ৰিয়া জড়িত হৈ থাকে যাতে দুৰ্বলতাসমূহ সমাধান কৰিব পাৰি আৰু এটা প্ৰতিষ্ঠানৰ আই টি চিষ্টেমসমূহৰ সুৰক্ষা উন্নত কৰিব পাৰি।

• সুৰক্ষা পেটচ ব্যৱস্থাপনাৰ বাবে উত্তম পদ্ধতিসমূহে বিপদ স্তৰৰ ওপৰত ভিত্তি কৰি পেটচসমূহক অগ্ৰাধিকাৰ দিয়া, মোতায়েনৰ পূৰ্বে পেটচসমূহ পৰীক্ষা কৰা, সম্পত্তিসমূহৰ এটা বিৱৰিত তথ্য ৰখা, আৰু নতুন দুৰ্বলতাৰ বাবে নিয়মিতভাৱে নিৰীক্ষণ কৰা অন্তৰ্ভুক্ত কৰে।

• ডাটা বেকআপ হৈছে গুৰুত্বপূৰ্ণ ডাটাৰ ডুপ্লিকেট কপি সৃষ্টি কৰা আৰু ইয়াক সুৰক্ষিতভাৱে সংৰক্ষণ কৰা প্ৰক্ৰিয়া যাতে মানৱ ভুল, চিষ্টেম বিফলতা, বা চাইবাৰ আক্ৰমণৰ ফলত ডাটা হেৰুৱাৰ পৰা সুৰক্ষিত হয়।

• তৃতীয় পক্ষৰ চফটৱেৰ ইনষ্টল কৰাৰ সজাগতাত চফট্ ৱেৰটোৰ ওপৰত আগতীয়াকৈ গৱেষণা কৰা, উৎস পৰীক্ষা কৰা, চর্ত আৰু নিয়মসমূহ পঢ়া, আৰু সম্ভাব্য মেলৱেৰ বা ভাইৰাছৰ পৰা সুৰক্ষা দিবলৈ এণ্টিভাইৰাছ চফটৱেৰ ব্যৱহাৰ কৰাটো জড়িত হৈ থাকে।



১২.৯ অধিক জানিবলৈ

"Computer Security Fundamentals" by Chuck Easttom

"Network Security Essentials: Applications and Standards" by William Stallings

"Introduction to Computer Security" by Michael T. Goodrich and Roberto Tamassia

"Principles of Computer Security: CompTIA Security+ and Beyond" by Wm. Arthur Conklin, Greg White, and Chuck Cothren

"Computer Security Handbook" by Seymour Bosworth, Michel E. Kabay, and Eric Whyne

"Foundations of Computer Security" by David Salomon and Giovanni Motta

”Cybersecurity Essentials” by Charles J. Brooks and Christopher Grow



১২.১০ অগ্রগতি নিৰীক্ষণ

a) শুদ্ধ

b) অশুদ্ধ

c) শুদ্ধ

d) অশুদ্ধ

e) শুদ্ধ

f) অশুদ্ধ

g) অশুদ্ধ



১২.১১ আৰ্হি প্ৰশ্ন

প্ৰশ্ন ১ : এণ্টিভাইৰাছ আৰু এণ্টি-মেলৱেৰ চফটৱেৰৰ মাজত পাৰ্থক্য কি?

প্ৰশ্ন ২ : শক্তিশালী পাছৱৰ্ড ব্যৱহাৰ কৰিলে কি কি লাভ হয়?

প্ৰশ্ন ৩ : দুটা কাৰকৰ প্ৰমাণীকৰণ কি?

প্ৰশ্ন ৪ : মোবাইল ডিভাইচত এনক্ৰিপচনৰ উদ্দেশ্য কি?

প্ৰশ্ন ৫ : মোবাইল ডিভাইচত বিভিন্ন ধৰণৰ আক্ৰমণ কি কি?

প্ৰশ্ন ৬ : এটা সুৰক্ষা পেটচ আৰু এটা চফটৱেৰ আপডেটৰ মাজত পাৰ্থক্য কি?

প্ৰশ্ন ৭ : পেটচ ব্যৱস্থাপনা ব্যৱস্থা কি আৰু ই কেনেকৈ কাম কৰে?

প্ৰশ্ন ৮ : কিছুমান সাধাৰণ বেকআপ কৌশলৰ বিষয়ে আলোচনা কৰক।

*****

অধ্যায় ১৩: ডিজিটেল ডিভাইচৰ সুৰক্ষা—২

অধ্যায় গাঁথনি

১৩.১ উদ্দেশ্য
১৩.২ পৰিচয়
১৩.৩ ডিভাইচ সুৰক্ষা নীতি
১৩.৪ চাইবাৰ সুৰক্ষাৰ উত্তম পদ্ধতি
১৩.৫ হ'ষ্ট ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছৰ তাৎপর্য্য
১৩.৬ হ'ষ্ট ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছৰ ব্যৱস্থাপনা
১৩.৭ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ
১৩.৮ অধিক জনিবলৈ
১৩.৯ অগ্রগতিৰ খতিয়ান
১৩.১০ আৰ্হি প্রশ্ন

১৩.১ উদ্দেশ্য

এই অধ্যায়টি অধ্যয়ন কৰি আপুনি—

- ডিজিটেল ডিভাইচ সুৰক্ষা নীতিৰ মূল ধাৰণাসমূহ বুজিব
- চাইবাৰ সুৰক্ষাৰ বাবে উত্তম পদ্ধতিসমূহ ব্যৱহাৰ কৰা
- ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছ চফটৱেৰৰ ধাৰণা বুজিব পাৰিব

১৩.২ পৰিচয়

এই অধ্যায়টিত আমি ডিভাইচ সুৰক্ষা নীতিৰ মৌলিক ধাৰণা, চাইবাৰ সুৰক্ষাৰ বাবে উত্তম পদ্ধতি আৰু ফায়াৰৱেল আৰু এণ্টি-ভাইৰাছ চফটৱেৰৰ ধাৰণাসমূহৰ বিষয়ে শিকিবলৈ ওলাইছো। ডিভাইচ সুৰক্ষা নীতি হৈছে নিয়ম আৰু নির্দেশিকাসমূহৰ এটা গোট যি এটা প্রতিষ্ঠানৰ ভিতৰৰ ডিভাইচসমূহ কেনেকৈ সুৰক্ষিত হ'ব লাগে সেই বিষয়ে নির্দেশ দিয়ে। ই ডিভাইচসমূহক অকর্তৃত্বশীল প্রৱেশ, ডাটা চুৰি, মেলৱেৰ আৰু অন্যান্য চাইবাৰ ভাবুকিৰ পৰা ৰক্ষা কৰিবলৈ ব্যৱহাৰ কৰা প্রক্রিয়াসমূহ, পদ্ধতিসমূহ আৰু প্রযুক্তিসমূহ সামৰি লয়। আকৌ, এটা ফায়াৰৱাল হৈছে এটা নে'টৱর্ক সুৰক্ষা ডিভাইচ যি অহা আৰু যোৱা নে'টৱর্ক ট্রাফিক নিৰীক্ষণ আৰু নিয়ন্ত্রণ কৰে। ই এটা বিশ্বাসযোগ্য নেটৱর্ক আৰু এটা অবিশ্বাস্য নেটৱর্ক (যেনে

ইণ্টাৰনেট)ৰ মাজত বাধা হিচাপে কাম কৰে আৰু হার্ডৱেৰ বা চফটৱেৰ-ভিত্তিক হ'ব পাৰে। ফায়াৰৱালসমূহ এটা নেটৱর্কলৈ অকর্তৃত্বশীল প্ৰৱেশ প্ৰতিৰোধ কৰিবলৈ, ক্ষতিকাৰক ট্ৰেফিক বন্ধ কৰিবলৈ আৰু চাইবাৰ ভাবুকি যেনে মেলৱেৰ, ভাইৰাছ আৰু হেকিঙৰ প্ৰচেষ্টাৰ পৰা সুৰক্ষিত কৰিবলৈ ব্যৱহাৰ কৰা হয়। এণ্টি-ভাইৰাছ চফটৱেৰ হৈছে কম্পিউটাৰ বা নেটৱর্কৰ পৰা ক্ষতিকাৰক চফটৱেৰ (মেলৱেৰ) ধৰা পেলাবলৈ, প্ৰতিৰোধ কৰিবলৈ আৰু আঁতৰাবলৈ ডিজাইন কৰা এটা প্ৰগ্ৰেম। ই ফাইলসমূহ আৰু অহা/বাহিৰ হোৱা নে'টৱর্ক ট্ৰেফিকসমূহ জনা মেলৱেৰ স্বাক্ষৰৰ বাবে স্কেন কৰে আৰু অজ্ঞাত মেলৱেৰ ধৰা পেলাবলৈ হিউৰিষ্টিক আৰু আচৰণ বিশ্লেষণ ব্যৱহাৰ কৰে। এণ্টি-ভাইৰাছ চফটৱেৰ হৈছে এক বিস্তৃত চাইবাৰ সুৰক্ষা কৌশলৰ এক অপৰিহার্য উপাদান আৰু ইয়াক নিয়মিতভাৱে আপডেট কৰা উচিত যাতে ই শেহতীয়া ভাবুকি ধৰা পেলাব পাৰে। ইয়াৰ বিষয়ে অধিক বিশদভাৱে আলোচনা কৰা যাওক:

১৩.৩ ডিভাইচ সুৰক্ষা নীতি

ডিভাইচ সুৰক্ষা নীতি হৈছে এটা প্ৰতিষ্ঠানে কম্পিউটাৰ, মোবাইল ফোন, টেবলেট, আৰু অন্য ডিজিটেল ডিভাইচৰ দৰে ডিভাইচসমূহৰ সুৰক্ষা নিশ্চিত কৰিবলৈ প্ৰণয়ন কৰা নির্দেশনা আৰু পদ্ধতিসমূহৰ গোট। ডিভাইচ সুৰক্ষা নীতি এটা সংস্থাৰ ডিজিটেল সম্পত্তি সুৰক্ষিত কৰাত অতি গুৰুত্বপূর্ণ, যিবোৰ অকর্তৃত্বশীল প্ৰৱেশ, মেলৱেৰ, আৰু অন্যান্য চাইবাৰ ভাবুকিৰ দ্বাৰা আপোচ কৰিব পাৰি। এই অধ্যায়ত আমি ডিভাইচ সুৰক্ষা নীতিৰ গুৰুত্ব, এটা শক্তিশালী ডিভাইচ সুৰক্ষা নীতি গঠন কৰা উপাদানসমূহ, আৰু এটা ডিভাইচ সুৰক্ষা নীতি প্ৰণয়ন আৰু ৰক্ষণাবেক্ষণৰ বাবে উত্তম পদ্ধতিসমূহ আলোচনা কৰিম। ডিজিটেল ডিভাইচৰ প্ৰসাৰ আৰু চাইবাৰ ভাবুকিৰ বৃদ্ধিয়ে ডিভাইচ সুৰক্ষা নীতিক সকলো আকাৰৰ সংস্থাৰ বাবে এক গভীৰ চিন্তাৰ বিষয় কৰি তুলিছে। এটা শক্তিশালী ডিভাইচ সুৰক্ষা নীতিয়ে এটা প্ৰতিষ্ঠানক ইয়াৰ ডিজিটেল সম্পত্তিসমূহ সুৰক্ষিত কৰাত সহায় কৰে। গ্ৰাহকৰ তথ্য, বৌদ্ধিক সম্পত্তি আৰু বিত্তীয় তথ্যৰ দৰে ডিজিটেল সম্পত্তি এটা সংস্থাৰ সফলতাৰ বাবে অপৰিহার্য। এটা ডিভাইচ সুৰক্ষা নীতিয়ে অকর্তৃত্বশীল প্ৰৱেশাধিকাৰ, ডাটা চুৰি আৰু অন্য চাইবাৰ ভাবুকি প্ৰতিৰোধ কৰি এই সম্পত্তিসমূহ সুৰক্ষিত কৰাত সহায় কৰে। আকৌ, বহু উদ্যোগ নিয়ন্ত্ৰণমূলক প্ৰয়োজনীয়তাৰ অধীনত থাকে যিয়ে স্পর্শকাতৰ তথ্যৰ সুৰক্ষাৰ নির্দেশ দিয়ে। এটা ডিভাইচ সুৰক্ষা নীতিয়ে সংস্থাসমূহক এই প্ৰয়োজনীয়তাসমূহ মানি চলিবলৈ আৰু ব্যয়বহুল শাস্তি এৰাই চলিবলৈ সহায় কৰে। ডিভাইচ সুৰক্ষা নীতিৰ আন এটা সুবিধা হ'ল ই গ্ৰাহকৰ বিশ্বাস বর্তাই ৰাখে - গ্ৰাহকে তেওঁলোকৰ তথ্য সুৰক্ষিত হ'ব বুলি আশা কৰে যেতিয়া তেওঁলোকে এটা প্ৰতিষ্ঠানৰ সৈতে যোগাযোগ কৰে। এটা ডিভাইচ সুৰক্ষা নীতিয়ে স্পর্শকাতৰ তথ্য সুৰক্ষিত হোৱাটো নিশ্চিত কৰি গ্ৰাহকৰ বিশ্বাস বর্তাই ৰখাত সহায় কৰে।

ডিভাইচ সুৰক্ষা নীতিৰ উপাদানসমূহ

এটা বিস্তৃত ডিভাইচ সুৰক্ষা নীতিয়ে নিম্নলিখিত উপাদানসমূহ সুৰক্ষিত কৰিব লাগে:

- **প্ৰৱেশাধিকাৰ নিয়ন্ত্ৰণ** - প্ৰৱেশাধিকাৰ নিয়ন্ত্ৰণ নীতিয়ে ডিভাইচসমূহলে কাৰ প্ৰৱেশাধিকাৰ আছে আৰু তেওঁলোকৰ প্ৰৱেশাধিকাৰৰ কি স্তৰ আছে সেয়া সংজ্ঞায়িত কৰিব লাগে। প্ৰৱেশাধিকাৰ অনুমোদিত ব্যক্তিসকলৰ বাবে সীমিত হ'ব লাগে আৰু প্ৰমাণীকৰণ ব্যৱস্থা যেনে পাছৱৰ্ড বা বায়'মেট্ৰিক্স ব্যৱহাৰ কৰিব লাগে যাতে কেৱল অনুমোদিত ব্যৱহাৰকাৰীয়ে ডিভাইচসমূহ প্ৰৱেশাধিকাৰ কৰিব পাৰে।

- **ডিভাইচ বিন্যাস** - ডিভাইচ বিন্যাস নীতিয়ে সুৰক্ষা সুনিশ্চিত কৰিবলে ডিভাইচসমূহ কেনেকৈ বিন্যাস কৰা হয় সংজ্ঞায়িত কৰিব লাগে। ইয়াৰ ভিতৰত মেলৱেৰ, ডাটা চুৰি, আৰু অন্যান্য চাইবাৰ ভাবুকিৰ পৰা সুৰক্ষা দিবলৈ এনক্ৰিপচন, ফায়াৰৱাল, আৰু অন্যান্য সুৰক্ষা ব্যৱস্থাৰ ব্যৱহাৰ অন্তৰ্ভুক্ত।

- **পৰ্যবেক্ষণ আৰু লগিং** –ডিভাইচসমূহ কেনেকৈ নিৰীক্ষণ কৰা হয় আৰু সুৰক্ষাৰ পৰিঘটনাসমূহ ধৰা পেলাবলৈ আৰু সঁহাৰি দিবলৈ কি কৰা হয় সেয়া এই নীতিয়ে সংজ্ঞায়িত কৰে। ইয়াৰ ভিতৰত সন্দেহজনক কাৰ্যকলাপৰ বাবে নিৰীক্ষণ, লগিং ইভেণ্ট আৰু সম্ভাব্য ভাবুকি চিনাক্ত কৰিবলে লগ বিশ্লেষণ কৰা কামো অন্তৰ্ভুক্ত হৈ থাকে।

- **ঘটনাৰ সঁহাৰি** - নীতিয়ে নিৰাপত্তাজনিত ঘটনাৰ ৰিপৰ্ট, তদন্ত আৰু সঁহাৰি কেনেকৈ দিয়া হয় তাৰ সংজ্ঞা দিব লাগে। ইয়াৰ ভিতৰত ঘটনাৰসমূহ নিয়ন্ত্ৰণ কৰাৰ পদ্ধতি, ইয়াৰ কাৰণৰ তদন্ত, আৰু ভৱিষ্যতে একেধৰণৰ ঘটনাৰ সংঘটিত নহ'বলৈ সংশোধনীমূলক ব্যৱস্থা গ্ৰহণ কৰা আদি অন্তৰ্ভুক্ত হৈ থাকে।

- **তথ্য সুৰক্ষা** - এই নীতিয়ে ডিভাইচসমূহত তথ্য কেনেকৈ সুৰক্ষিত কৰা হয় সংজ্ঞায়িত কৰিব লাগে। ইয়াত তথ্য হেৰুৱা বা চুৰি প্ৰতিৰোধ কৰিবলে ইনক্ৰিপশ্চণ, বেকআপ, আৰু সুৰক্ষিত মচি পেলোৱাৰ ব্যৱহাৰ অন্তৰ্ভুক্ত কৰা হৈছে।

ডিভাইচ সুৰক্ষা নীতি প্ৰণয়ন আৰু ৰক্ষণাবেক্ষণৰ বাবে উত্তম পদ্ধতিসমূহ

- এটা ডিভাইচ সুৰক্ষা নীতি প্ৰণয়ন আৰু ৰক্ষণাবেক্ষণ কৰাটো এটা কঠিন কাম হ'ব পাৰে, কিন্তু নিম্নলিখিত উত্তম পদ্ধতিসমূহে সহায় কৰিব পাৰে:

- এটা বিপদ মূল্যায়ন কৰা - এটা ডিভাইচ সুৰক্ষা নীতি প্ৰণয়ন কৰাৰ আগতে, সংস্থাসমূহে তেওঁলোকৰ পৰিৱেশত থকা ভাবুকি আৰু দুৰ্বলতাসমূহ চিনাক্ত কৰিবলৈ এটা

বিপদ মূল্যায়ন কৰিব লাগে। ইয়াৰ দ্বাৰা তেওঁলোকৰ নির্দিষ্ট বিপদসমূহৰ সৈতে মোকাবিলা কৰা নীতি প্রস্তুত কৰাত সহায়ক হ'ব।

- সকলো অংশীদাৰক জড়িত কৰক - এটা ডিভাইচ সুৰক্ষা নীতিয়ে আই টি কর্মচাৰী, পৰিচালনা আৰু কর্মচাৰীকে ধৰি সকলো অংশীদাৰক জড়িত কৰিব লাগে। ইয়াৰ ফলত সকলোৱে নীতি আৰু ইয়াক কার্যকৰী কৰাৰ ক্ষেত্রত নিজৰ দায়িত্বৰ বিষয়ে সচেতন হোৱাটো নিশ্চিত হয়।

- নীতি নিয়মিতভাৱে আপডেইট কৰক - নতুন ভাবুকি আৰু দুর্বলতাসমূহ উত্থাপন হোৱাৰ লগে লগে সম্বোধন কৰিবলে এটা ডিভাইচ সুৰক্ষা নীতি নিয়মিতভাৱে আপডেইট কৰিব লাগে। ইয়াৰ ফলত সংস্থাটোৰ ডিজিটেল সম্পত্তি সুৰক্ষিত কৰাৰ ক্ষেত্রত নীতিটো প্রাসংগিক আৰু ফলপ্রসূ হৈ থকাটো নিশ্চিত হয়।

- প্রশিক্ষণ প্রদান কৰক - সকলো কর্মচাৰীয়ে ডিভাইচ সুৰক্ষা নীতিৰ ওপৰত প্রশিক্ষণ লাভ কৰিব লাগে যাতে তেওঁলোকে নীতি আৰু ইয়াক কার্যকৰী কৰাৰ ক্ষেত্রত তেওঁলোকৰ দায়িত্ব বুজি পায়। কর্মচাৰীসকলক নতুন ভাবুকি আৰু নীতিৰ পৰিৱর্তনৰ বিষয়ে অৱগত ৰাখিবলৈ নিয়মিতভাৱে প্রশিক্ষণ প্রদান কৰিব লাগে।

- স্বয়ংক্রিয়কৰণ ব্যৱহাৰ কৰক - স্বয়ংক্রিয়কৰণে সংস্থাসমূহক তেওঁলোকৰ ডিভাইচ সুৰক্ষা নীতি অধিক কার্যক্ষমভাৱে প্রণয়ন আৰু ৰক্ষণাবেক্ষণ কৰাত সহায় কৰিব পাৰে। উদাহৰণস্বৰূপ, স্বয়ংক্রিয় পেচ ব্যৱস্থাপনাই নিশ্চিত কৰিব পাৰে যে ডিভাইচসমূহক শেহতীয়া সুৰক্ষা পেচসমূহৰ সৈতে আপডেইট কৰা হৈছে।

১৩.৪ চাইবাৰ সুৰক্ষাৰ উত্তম পদ্ধতি

চাইবাৰ সুৰক্ষাৰ উত্তম পদ্ধতি বুলিলে সেই প্রক্রিয়াসমূহক সূচাই যিবোৰে সংস্থাসমূহৰ ডিজিটেল সম্পত্তিসমূহক চাইবাৰ ভাবুকিৰ পৰা সুৰক্ষিত কৰে। চাইবাৰ সুৰক্ষাৰ উত্তম পদ্ধতিসমূহত কাৰিকৰী, সাংগঠনিক আৰু মানৱীয় কাৰকৰ সংমিশ্রণ হৈ থাকে। কাৰিকৰী উত্তম পদ্ধতিসমূহে নেটৱার্ক, ডিভাইচ, আৰু তথ্য সুৰক্ষিত কৰিবলে ফায়াৰৱাল, এণ্টি-ভাইৰাছ চফটৱেৰ, এনক্রিপচন আৰু অন্য সুৰক্ষা ব্যৱস্থাসমূহৰ ব্যৱহাৰ অন্তর্ভুক্ত কৰে। সাংগঠনিক উত্তম পদ্ধতিসমূহৰ ভিতৰত চাইবাৰ সুৰক্ষা বিপদসমূহ পৰিচালনা কৰিবলৈ সুৰক্ষা নীতি, পদ্ধতি আৰু নিয়ন্ত্রণসমূহৰ বিকাশ আৰু ৰূপায়ণ অন্তর্ভুক্ত। মানৱীয় কাৰকসমূহৰ ভিতৰত আছে কর্মচাৰীসকলক চাইবাৰ সুৰক্ষাৰ বিপদৰ বিষয়ে জ্ঞান দিয়া, প্রৱেশ নিয়ন্ত্রণ কার্যকৰী কৰা আৰু সুৰক্ষা সজাগতাক প্রসাৰ কৰা। সামগ্রিকভাৱে, চাইবাৰ সুৰক্ষাৰ উত্তম পদ্ধতিসমূহ এটা সংস্থাৰ

ডিজিটেল সম্পত্তিসমূহক চাইবাৰ ভাবুকিৰ পৰা, যেনে ফিছিং আক্রমণ, মেলৱেৰ আৰু ডাটা ভংগৰ পৰা সুৰক্ষিত কৰে।

চাইবাৰ সুৰক্ষাৰ উত্তম পদ্ধতিসমূহ ৰূপায়ণৰ বাবে ফ্রেমৱার্কটো চাৰিটা মূল উপাদানত বিভক্ত কৰা হৈছে:

১) **চিনাক্তকৰণ:** এই উপাদানটোৱে এটা প্রতিষ্ঠানৰ ডিজিটেল পৰিৱেশৰ সৈতে জড়িত সম্পত্তি, দুৰ্বলতা আৰু বিপদসমূহ চিনাক্ত কৰে। এক সম্যক বিপদ মূল্যায়ন কৰি সংস্থাসমূহে তেওঁলোকৰ চাইবাৰ সুৰক্ষাৰ বিপদসমূহৰ বিষয়ে এক বিস্তৃত ধাৰণা গঢ়ি তুলিব পাৰে আৰু সেইবোৰৰ সৈতে মোকাবিলা কৰাৰ পৰিকল্পনা প্রস্তুত কৰিব পাৰে।

২) **সুৰক্ষা :** এই উপাদানটোত এটা সংস্থাৰ ডিজিটেল সম্পত্তি সুৰক্ষিত কৰিবলৈ সুৰক্ষা ব্যৱস্থা ৰূপায়ণ কৰাটো অন্তর্ভুক্ত হৈ থাকে। ইয়াৰ ভিতৰত ফায়াৰৱাল, এনক্রিপচন, আৰু এণ্টি-ভাইৰাছ চফটৱেৰৰ দৰে কাৰিকৰী ব্যৱস্থা, লগতে সুৰক্ষা নীতি আৰু পদ্ধতিৰ দৰে সাংগঠনিক ব্যৱস্থাও অন্তর্ভুক্ত।

৩) **ধৰা পেলোৱা :** এই উপাদানটোৰ লগত এটা সংস্থাৰ ডিজিটেল পৰিৱেশত চাইবাৰ ভাবুকিৰ চিন নিৰীক্ষণ কৰাটো অন্তর্ভুক্ত হৈ থাকে। ইয়াৰ ভিতৰত বিজুতি আৰু সম্ভাব্য সুৰক্ষাজনিত পৰিঘটনা ধৰা পেলাবলৈ নিৰীক্ষণ সঁজুলি আৰু কৌশল ৰূপায়ণ কৰাটোও অন্তর্ভুক্ত।

৪) **সঁহাৰি দিয়া:** এই উপাদানটোত নিৰাপত্তাজনিত কাণ্ডৰ প্রতি সঁহাৰি জনোৱা আৰু ইয়াৰ প্রভাৱ কম কৰাৰ লগত জড়িত। ইয়াৰ ভিতৰত নিৰাপত্তাজনিত কাণ্ড নিয়ন্ত্রণ আৰু লাঘৱ কৰাৰ পৰিকল্পনা ৰখাৰ লগতে ভৱিষ্যতেও অনুৰূপ কাণ্ড সংঘটিত নহ'বলৈ কাণ্ডৰ পিছৰ বিশ্লেষণ কৰাও অন্তর্ভুক্ত হৈ থাকে।

এতিয়া, প্রতিটো উপাদান আৰু ইয়াৰ সৈতে জড়িত উত্তম পদ্ধতিসমূহ বহলাই আলোচনা কৰা যাওক।

১) চিনাক্ত কৰা

কাঠামোৰ প্রথম উপাদানটো হৈছে এটা সংস্থাৰ ডিজিটেল পৰিৱেশৰ সৈতে জড়িত সম্পত্তি, দুৰ্বলতা আৰু বিপদসমূহ চিনাক্ত কৰা। ইয়াৰ ভিতৰত আছে:

১.১) বিপদ মূল্যায়ন : এটা সংস্থাৰ চাইবাৰ সুৰক্ষাৰ বিপদ চিনাক্ত কৰাৰ ক্ষেত্রত বিপদ মূল্যায়ন এক অপৰিহার্য পদক্ষেপ। ইয়াৰ ভিতৰত সম্পত্তি চিনাক্ত কৰা, দুৰ্বলতাসমূহৰ মূল্যায়ন কৰা আৰু সম্ভাব্য ভাবুকিৰ সম্ভাৱনা আৰু প্রভাৱৰ মূল্যায়ন কৰা আদি অন্তর্ভুক্ত। বিপদৰ মূল্যায়ন

কৰি সংস্থাসমূহে তেওঁলোকৰ চাইবাৰ সুৰক্ষাৰ বিপদসমূহৰ বিষয়ে এক বিস্তৃত ধাৰণা গঢ়ি তুলিব পাৰে আৰু সেইবোৰৰ সৈতে মোকাবিলা কৰাৰ পৰিকল্পনা প্ৰস্তুত কৰিব পাৰে।

১.২) সুৰক্ষা নীতি আৰু পদ্ধতিসমূহ বিকশিত কৰা : সুৰক্ষা নীতি আৰু পদ্ধতিসমূহে চাইবাৰ সুৰক্ষাৰ উত্তম পদ্ধতিসমূহ ৰূপায়ণৰ বাবে এটা কাঠামো প্ৰদান কৰে। এই নীতি আৰু পদ্ধতিসমূহে প্ৰৱেশাধিকাৰ নিয়ন্ত্ৰণ, পাছৱৰ্ড ব্যৱস্থাপনা, পৰিঘটনাৰ সঁহাৰি, আৰু অন্যান্য চাইবাৰ সুৰক্ষা সমস্যাসমূহৰ সমাধান কৰিব লাগে।

১.৩) প্ৰৱেশাধিকাৰ নিয়ন্ত্ৰণসমূহ প্ৰণয়ন কৰা : এটা সংস্থাৰ ডিজিটেল সম্পত্তিসমূহৰ অকৰ্তৃত্বশীল প্ৰৱেশাধিকাৰ প্ৰতিৰোধ কৰিবলৈ প্ৰৱেশাধিকাৰ নিয়ন্ত্ৰণ কৰাটো অতি প্ৰয়োজনীয়। ইয়াৰ ভিতৰত ব্যৱহাৰকাৰী প্ৰমাণীকৰণ, অনুমোদন, আৰু জবাবদিহিতাৰ ব্যৱস্থাসমূহ প্ৰণয়ন কৰা অন্তৰ্ভুক্ত, যাতে কেৱল অনুমোদিত ব্যক্তিসকলেহে স্পৰ্শকাতৰ তথ্যৰ প্ৰৱেশাধিকাৰ পায়।

১.৪) তৃতীয় পক্ষৰ বিপদ মূল্যায়ন কৰা: তৃতীয় পক্ষৰ বিক্ৰেতা আৰু অংশীদাৰসকলে এটা সংস্থাৰ ডিজিটেল সম্পত্তিৰ প্ৰৱেশাধিকাৰ পাব পাৰে। গতিকে তেওঁলোকে চাইবাৰ সুৰক্ষাৰ উত্তম পদ্ধতিসমূহ মানি চলিছে নে নাই সেয়া নিশ্চিত কৰিবলৈ তৃতীয় পক্ষৰ বিপদ মূল্যায়ন কৰাটো অতি প্ৰয়োজনীয়।

২) সুৰক্ষা দিয়া

কাঠামোৰ দ্বিতীয় উপাদানটো হৈছে এটা সংস্থাৰ ডিজিটেল সম্পত্তি সুৰক্ষিত কৰাৰ বাবে সুৰক্ষা ব্যৱস্থা ৰূপায়ণ কৰা। ইয়াৰ ভিতৰত আছে:

২.১) কাৰিকৰী ব্যৱস্থাসমূহ প্ৰণয়ন কৰা: ফায়াৰৱাল, এণ্টি-ভাইৰাছ চফটৱেৰ, এনক্ৰিপচন, আৰু অনুপ্ৰৱেশ ধৰা পেলোৱা আৰু প্ৰতিৰোধ ব্যৱস্থা (IDPS)ৰ দৰে কাৰিকৰী ব্যৱস্থাসমূহ এটা সংস্থাৰ ডিজিটেল সম্পত্তিসমূহক চাইবাৰ ভাবুকিৰ পৰা সুৰক্ষিত কৰিবলৈ অপৰিহাৰ্য।

২.২) সাংগঠনিক ব্যৱস্থাসমূহ প্ৰণয়ন কৰা: এটা সংস্থাৰ ডিজিটেল সম্পত্তিসমূহ সুৰক্ষিত কৰাত সাংগঠনিক ব্যৱস্থা যেনে সুৰক্ষা নীতি, পদ্ধতি, আৰু নিয়ন্ত্ৰণসমূহ অপৰিহাৰ্য। ইয়াৰ ভিতৰত ডাটা বেকআপ আৰু পুনৰুদ্ধাৰ পদ্ধতি প্ৰণয়ন কৰা, নিয়মীয়া সুৰক্ষা অডিট চলোৱা, আৰু কৰ্মচাৰী প্ৰশিক্ষণ কাৰ্য্যক্ৰম প্ৰণয়ন কৰা অন্তৰ্ভুক্ত।

২.৩) শাৰীৰিক সুৰক্ষা ব্যৱস্থাসমূহ প্ৰণয়ন কৰা: এটা সংস্থাৰ ডিজিটেল সম্পত্তিসমূহলৈ অকৰ্তৃত্বশীল ভৌতিক প্ৰৱেশ ৰোধ কৰিবলৈ ভৌতিক সুৰক্ষা ব্যৱস্থা যেনে প্ৰৱেশাধিকাৰ নিয়ন্ত্ৰণ ব্যৱস্থা, চিচিটিভি, আৰু সুৰক্ষা গাৰ্ড অতি প্ৰয়োজনীয়।

২.৪) তথ্য সুৰক্ষা ব্যৱস্থাসমূহ প্রণয়ন কৰা: তথ্য সুৰক্ষা ব্যৱস্থা যেনে তথ্য এনক্রিপচন, তথ্য মাস্কিং, আৰু তথ্য হেৰুৱা প্রতিৰোধ (DLP) এটা প্রতিষ্ঠানৰ স্পর্শকাতৰ তথ্য সুৰক্ষিত কৰাত অপৰিহার্য।

৩) ধৰা পেলোৱা

চাইবাৰ সুৰক্ষাৰ উত্তম পদ্ধতিৰ কাঠামোৰ তৃতীয় উপাদানটো হৈছে "ডিটেক্ট"। এই উপাদানটোত চাইবাৰ ভাবুকিৰ চিনসমূহৰ বাবে এটা সংস্থাৰ ডিজিটেল পৰিৱেশ নিৰীক্ষণ কৰাটো জড়িত হৈ থাকে। ইয়াৰ ভিতৰত বিজুতি আৰু সম্ভাব্য সুৰক্ষাজনিত পৰিঘটনা ধৰা পেলাবলৈ নিৰীক্ষণ সঁজুলি আৰু কৌশল ৰূপায়ণ কৰাটোও অন্তর্ভুক্ত।

কাঠামোৰ "ডিটেক্ট" উপাদানত সংস্থাসমূহে প্রণয়ন কৰিব পৰা কেইবাটাও উত্তম পদ্ধতি আছে:

৩.১) নিৰন্তৰ নিৰীক্ষণ প্রণয়ন কৰা: নিৰন্তৰ নিৰীক্ষণ হৈছে সুৰক্ষাৰ পৰিঘটনা ধৰা পেলাবলৈ এটা সংস্থাৰ ডিজিটেল পৰিৱেশ বাস্তৱ সময়ত নিৰীক্ষণ কৰাৰ প্রক্রিয়া। ইয়াত নে'টৱর্ক ট্রাফিক, লগ ফাইলসমূহ আৰু ব্যৱহাৰকাৰী কার্য্যকলাপ নিৰীক্ষণ কৰা অন্তর্ভুক্ত হৈ থাকে। নিৰন্তৰ নিৰীক্ষণ ৰূপায়ণ কৰি সংস্থাসমূহে নিৰাপত্তাজনিত কাণ্ড সংঘটিত হোৱাৰ লগে লগে ধৰা পেলাব পাৰে, যাৰ ফলত কাণ্ডৰ প্রভাৱ কম হয়।

৩.২) সুৰক্ষা তথ্য আৰু ইভেণ্ট ব্যৱস্থাপনা (SIEM) প্রণয়ন কৰক: SIEM হৈছে এটা চফটৱেৰ সমাধান, যি এটা প্রতিষ্ঠানৰ ডিজিটেল পৰিৱেশৰ ভিতৰত বিভিন্ন উৎসৰ পৰা সুৰক্ষা ইভেণ্টসমূহ সংগ্রহ, সংগ্রহ আৰু বিশ্লেষণ কৰে। SIEM এ বাস্তৱ-সময়ৰ ভাবুকি ধৰা পেলোৱা, পৰিঘটনাৰ সঁহাৰি, আৰু অনুসৰণ প্রতিবেদন প্রদান কৰে। SIEM ৰূপায়ণ কৰি সংস্থাসমূহে বাস্তৱ সময়ত সুৰক্ষাৰ কাণ্ড ধৰা পেলাব পাৰে আৰু ইয়াৰ প্রভাৱ কম কৰিবলৈ দ্রুতভাৱে সঁহাৰি জনাব পাৰে।

৩.৩) অনুপ্রৱেশ চিনাক্তকৰণ আৰু প্রতিৰোধ ব্যৱস্থাপ্রণালী (IDPS) প্রণয়ন কৰক: IDPS হৈছে এটা সুৰক্ষা সমাধান যি সুৰক্ষাৰ পৰিঘটনাসমূহ ধৰা পেলোৱা আৰু প্রতিৰোধ কৰে। আইডিপিএছে নেটৱর্ক আক্রমণ, মেলৱেৰ আৰু ভিতৰৰ ভাবুকিকে ধৰি বহুতো সুৰক্ষাৰ পৰিসৰ ধৰা পেলাব আৰু প্রতিৰোধ কৰিব পাৰে। আইডিপিএছ ৰূপায়ণ কৰি সংস্থাসমূহে ক্ষতি কৰাৰ আগতেই নিৰাপত্তাজনিত কাণ্ড ধৰা পেলাব পাৰে আৰু প্রতিৰোধ কৰিব পাৰে।

৩.৪) দুর্বলতা স্কেনিং পৰিচালনা কৰক: দুর্বলতা স্কেনিং হৈছে এটা প্রতিষ্ঠানৰ ডিজিটেল পৰিৱেশত দুর্বলতা চিনাক্ত কৰাৰ প্রক্রিয়া। ইয়াত চফটৱেৰ, হার্ডৱেৰ, আৰু নে'টৱর্ক ডিভাইচসমূহত দুর্বলতাৰ বাবে স্কেনিং অন্তর্ভুক্ত কৰা হৈছে। দুর্বলতা স্কেনিং কৰি, সংস্থাসমূহে

দুৰ্বলতাসমূহ চিনাক্ত কৰিব পাৰে আৰু আক্ৰমণকাৰীয়ে শোষণ কৰাৰ আগতে সেইবোৰ সমাধানৰ বাবে সক্ৰিয় ব্যৱস্থা গ্ৰহণ কৰিব পাৰে।

৩.৫) এণ্ডপইণ্ট চিনাক্তকৰণ আৰু প্ৰতিক্ৰিয়া (EDR) প্ৰণয়ন কৰক: EDR হৈছে এটা সুৰক্ষা সমাধান যি সুৰক্ষাৰ চিনসমূহৰ বাবে ডেস্কটপ, লেপটপ, আৰু মোবাইল ডিভাইচসমূহৰ দৰে এণ্ডপইণ্টসমূহ নিৰীক্ষণ কৰে। ইডিআৰে মেলৱেৰ, ৰেনছমৱেৰ, আৰু ফিছিং আক্ৰমণকে ধৰি বহুতো সুৰক্ষাৰ পৰিসৰ ধৰা পেলাব আৰু প্ৰতিৰোধ কৰিব পাৰে। ইডিআৰ ৰূপায়ণ কৰি সংস্থাসমূহে শেষ বিন্দুত সুৰক্ষাৰ কাণ্ড ধৰা পেলাব পাৰে, যাৰ ফলত ইয়াৰ প্ৰভাৱ কম হয়।

৩.৬) ভাবুকি চোৰাংচোৱা কাৰ্যকৰী কৰা: ভাবুকি চোৰাংচোৱা হৈছে সম্ভাৱ্য চাইবাৰ ভাবুকিৰ বিষয়ে তথ্য। ভাবুকিৰ চোৰাংচোৱা তথ্য কাৰ্যকৰী কৰি সংস্থাসমূহে শেহতীয়া চাইবাৰ ভাবুকিৰ বিষয়ে অৱগত হৈ থাকিব পাৰে আৰু তেওঁলোকৰ ডিজিটেল সম্পত্তিসমূহ সুৰক্ষিত কৰাৰ বাবে সক্ৰিয় ব্যৱস্থা গ্ৰহণ কৰিব পাৰে।

৩.৭) নিয়মীয়া সুৰক্ষা অডিট কৰা: নিয়মীয়া সুৰক্ষা অডিটে সংস্থাসমূহক তেওঁলোকৰ সুৰক্ষা নিয়ন্ত্ৰণৰ সুৰক্ষা দুৰ্বলতা আৰু ব্যৱধান চিনাক্ত কৰাত সহায় কৰিব পাৰে। নিয়মীয়াকৈ নিৰাপত্তা অডিট চলাই সংস্থাসমূহে নিৰাপত্তা নিয়ন্ত্ৰণ শক্তিশালী কৰাৰ প্ৰয়োজনীয়তা থকা ক্ষেত্ৰসমূহ চিনাক্ত কৰিব পাৰে।

৪) সঁহাৰি দিয়া

চাইবাৰ সুৰক্ষাৰ উত্তম পদ্ধতিৰ কাঠামোৰ চতুৰ্থ উপাদানটো হৈছে সঁহাৰি দিয়া। এই উপাদানটোৰ লগত জড়িত হৈ আছে নিৰাপত্তাজনিত কাণ্ডৰ প্ৰতি সময়মতে আৰু ফলপ্ৰসূভাৱে সঁহাৰি জনোৱা যাতে কাণ্ডৰ প্ৰভাৱ কম হয়।

কাঠামোৰ সঁহাৰি দিয়া উপাদানত সংস্থাসমূহে প্ৰণয়ন কৰিব পৰা কেইবাটাও উত্তম পদ্ধতি আছে:

৪.১) এটা পৰিঘটনা সঁহাৰি পৰিকল্পনা প্ৰস্তুত কৰা: এটা পৰিঘটনা সঁহাৰি পৰিকল্পনাই কোনো নিৰাপত্তাজনিত কাণ্ডৰ ক্ষেত্ৰত এটা সংস্থাই গ্ৰহণ কৰিবলগীয়া পদক্ষেপসমূহৰ ৰূপৰেখা দাঙি ধৰে। পৰিকল্পনাত নিৰাপত্তাজনিত কাণ্ড ধৰা পেলোৱা, প্ৰতিবেদন কৰা, বিশ্লেষণ কৰা, নিয়ন্ত্ৰণ কৰা আৰু উদ্ধাৰৰ পদ্ধতি অন্তৰ্ভুক্ত হ'ব লাগে। এটা পৰিঘটনা সঁহাৰি পৰিকল্পনা প্ৰস্তুত কৰি সংস্থাসমূহে নিৰাপত্তাজনিত কাণ্ডৰ প্ৰতি দ্ৰুত আৰু ফলপ্ৰসূভাৱে সঁহাৰি জনাব পাৰে।

৪.২) টেবলেটপ অনুশীলনসমূহ পৰিচালনা কৰক: টেবলটপ অনুশীলনসমূহ হৈছে সুৰক্ষাৰ কাণ্ডৰ অনুকৰণ যিয়ে সংস্থাসমূহক তেওঁলোকৰ পৰিঘটনাৰ সঁহাৰি পৰিকল্পনাসমূহ অনুশীলন কৰিবলৈ অনুমতি দিয়ে। টেবুলটপ অনুশীলন চলাই সংস্থাসমূহে তেওঁলোকৰ কাণ্ডৰ সঁহাৰি পৰিকল্পনা উন্নত কৰাৰ প্রয়োজনীয়তা থকা ক্ষেত্রসমূহ চিনাক্ত কৰিব পাৰে আৰু নিৰাপত্তাজনিত কাণ্ডৰ সময়ত সকলো অংশীদাৰে নিজৰ ভূমিকা আৰু দায়িত্ব বুজি পোৱাটো নিশ্চিত কৰিব পাৰে।

৪.৩) এটা নিৰাপত্তা কার্য্যকলাপ কেন্দ্র (SOC): এটা SOC হৈছে এটা কেন্দ্রীভূত দল যিয়ে নিৰাপত্তাজনিত পৰিঘটনাসমূহ নিৰীক্ষণ আৰু প্রতিক্রিয়া প্রকাশৰ বাবে দায়বদ্ধ। এছ অ' চিত প্রশিক্ষিত নিৰাপত্তা পেছাদাৰী লোক থাকিব লাগে যিয়ে নিৰাপত্তাৰ কাণ্ড ধৰা পেলাব পাৰে, তদন্ত কৰিব পাৰে আৰু ইয়াৰ প্রতি সঁহাৰি জনাব পাৰে। এছ অ' চি স্থাপন কৰি সংস্থাসমূহে নিৰাপত্তাজনিত কাণ্ডৰ প্রতি দ্রুত আৰু ফলপ্রসূভাৱে সঁহাৰি জনাব পাৰে।

৪.৪) অঘটন সঁহাৰি সঁজুলিসমূহ প্রণয়ন কৰক: অঘটন সঁহাৰি সঁজুলিসমূহত ফৰেনছিক বিশ্লেষণ সঁজুলিসমূহ, মেলৱেৰ বিশ্লেষণ সঁজুলিসমূহ, আৰু অঘটন সঁহাৰি প্লেটফর্মসমূহ অন্তর্ভুক্ত হৈ থাকে। এই সঁজুলিসমূহে সংস্থাসমূহক নিৰাপত্তাজনিত কাণ্ডৰ তদন্ত কৰাত সহায় কৰিব পাৰে আৰু ইয়াৰ প্রভাৱ কম কৰিবলৈ দ্রুতভাৱে সঁহাৰি জনাব পাৰে।

৪.৫) যোগাযোগ পদ্ধতি বিকশিত কৰা: গ্রাহক, কর্মচাৰী, আৰু নিয়ন্ত্রণকাৰী সংস্থাকে ধৰি অংশীদাৰসকলক সুৰক্ষাৰ কাণ্ডৰ বিষয়ে অৱগত কৰাৰ বাবে যোগাযোগ পদ্ধতি স্থাপন কৰিব লাগে। যোগাযোগ পদ্ধতিত স্পষ্ট আৰু সংক্ষিপ্ত বার্তা প্রেৰণ কৰা উচিত যিয়ে কাণ্ডৰ প্রভাৱ আৰু সংস্থাটোৱে প্রভাৱ কমোৱাৰ বাবে গ্রহণ কৰা পদক্ষেপসমূহৰ ৰূপৰেখা দাঙি ধৰে।

৪.৬) আইন প্রয়োগকাৰী সংস্থাৰ সৈতে সমন্বয় স্থাপন কৰা: কিছুমান ক্ষেত্রত নিৰাপত্তাজনিত কাণ্ডত অপৰাধমূলক কার্যকলাপ জড়িত হ'ব পাৰে। সংগঠনসমূহে আইন প্রয়োগকাৰী সংস্থাসমূহৰ সৈতে সমন্বয় স্থাপন কৰি কাণ্ডটোৰ সঠিক তদন্ত আৰু গোচৰ চলোৱাটো নিশ্চিত কৰিব লাগে।

৪.৭) সম্ভ্যাব্য ঘটনাৰ বিশ্লেষণ কৰা: কোনো নিৰাপত্তাজনিত কাণ্ডৰ পিছত সংস্থাসমূহে তেওঁলোকৰ কাণ্ডৰ সঁহাৰি পৰিকল্পনাত উন্নতিৰ প্রয়োজন হোৱা ক্ষেত্রসমূহ চিনাক্ত কৰিবলৈ সম্ভ্যাব্য ঘটনাৰ বিশ্লেষণ কৰিব লাগে। সম্ভ্যাব্য ঘটনাৰ বিশ্লেষণত ঘটনাৰ সঁহাৰি পৰিকল্পনা, ঘটনাৰ সঁহাৰিৰ সঁজুলি, যোগাযোগ পদ্ধতি, আৰু আইন প্রয়োগকাৰী সংস্থাৰ সৈতে সমন্বয়ৰ পর্যালোচনা অন্তর্ভুক্ত।

১৩.৫ হ'ষ্ট ফায়াৰৱাল আৰু এণ্ট-ভাইৰাছৰ তাৎপর্য্য

শেহতীয়া জগতসমূহত আমাৰ স্পর্শকাতৰ তথ্যসমূহ অবাঞ্ছিত আৰু অকর্তৃত্বশীল উৎসৰ পৰা সুৰক্ষিত কৰাটো এটা ডাঙৰ প্রত্যাহ্বান। বিভিন্ন সঁজুলি আৰু ডিভাইচ আছে যিয়ে বিভিন্ন স্তৰৰ সুৰক্ষা প্রদান কৰে আৰু আমাৰ ব্যক্তিগত তথ্য সুৰক্ষিত কৰাত সহায় কৰে। তেনে এটা সঁজুলি হ'ল ফায়াৰৱাল, যিয়ে অকর্তৃত্বশীল প্রৱেশ ৰোধ কৰে আৰু আমাৰ কম্পিউটাৰ আৰু ডাটা সুৰক্ষিত কৰে। এটা ফায়াৰৱালক এটা বিশেষ ধৰণৰ নে'টৱর্ক সুৰক্ষা ডিভাইচ বা চফটৱেৰ হিচাপে সংজ্ঞায়িত কৰিব পাৰি যি সুৰক্ষা নিয়মৰ এটা সংজ্ঞায়িত গোটৰ ওপৰত ভিত্তি কৰি অহা আৰু যোৱা নে'টৱর্ক ট্রাফিক নিৰীক্ষণ আৰু ফিল্টাৰ কৰে। ই আভ্যন্তৰীণ ব্যক্তিগত নেটৱর্ক আৰু ৰাজহুৱা ইণ্টাৰনেটৰ দৰে বাহ্যিক সম্পদৰ মাজত বাধা হিচাপে কাম কৰে। ফায়াৰৱালৰ মূল উদ্দেশ্য হৈছে আপোনাৰ কম্পিউটাৰক ভাইৰাছ আৰু আক্রমণৰ পৰা সুৰক্ষিত কৰা, ভাবুকিহীন ট্রেফিক অনুমতি দি আৰু ক্ষতিকাৰক বা অবাঞ্ছিত ডাটা ট্রেফিক ব্লক কৰে। ফায়াৰৱাল হৈছে নেটৱর্ক সুৰক্ষা সঁজুলি যিয়ে নেটৱর্ক ট্রেফিক ফিল্টাৰ কৰে আৰু ব্যৱহাৰকাৰীসকলক সংক্রমিত কম্পিউটাৰত ইণ্টাৰনেটত প্রৱেশ কৰাত মেলৱেৰ প্রতিৰোধ কৰাত সহায় কৰে।

কিন্তু প্রশ্ন হ'ল ফায়াৰৱাল হার্ডৱেৰ নে চফটৱেৰ। ওপৰত উল্লেখ কৰা অনুসৰি ফায়াৰৱাল এটা নেটৱর্ক সুৰক্ষা ডিভাইচ বা কম্পিউটাৰৰ এটা চফটৱেৰ প্রগ্রেম হ'ব পাৰে। ইয়াৰ অর্থ হ'ল ফায়াৰৱালৰ দুটা স্তৰ আছে, হার্ডৱেৰ আৰু চফটৱেৰ, যদিও দুয়োটা থকাটো ভাল। প্রতিটো বিন্যাস (হার্ডৱেৰ বা চফটৱেৰ হিচাপে প্রণয়ন কৰা ফায়াৰৱাল)ৰ বিভিন্ন কার্য আছে কিন্তু একে উদ্দেশ্য। হার্ডৱেৰ ফায়াৰৱাল হৈছে এটা ভৌতিক ডিভাইচ যি এটা কম্পিউটাৰ নেটৱার্কক এটা গেটৱেৰ সৈতে সংযোগ কৰে। উদাহৰণস্বৰূপে, এটা ব্রডবেণ্ড ৰাউটাৰ। আনহাতে, চফট্ ৱেৰ ফায়াৰৱাল হৈছে কম্পিউটাৰত ইনষ্টল কৰা এটা সহজ প্রগ্রেম যিয়ে পর্ট নম্বৰ আৰু অন্যান্য ইনষ্টল কৰা চফটৱেৰৰ জৰিয়তে কাম কৰে।

ইয়াৰ উপৰি ক্লাউড ভিত্তিক ফায়াৰৱাল আছে। ইহঁতক প্রায়ে FAAS (FIREWALL AS A SERVICE) বুলি কোৱা হয়। ক্লাউড-ভিত্তিক ফায়াৰৱাল ব্যৱহাৰ কৰাৰ এটা মূল সুবিধা হ'ল ইয়াক কেন্দ্রীয়ভাৱে পৰিচালনা কৰিব পাৰি। হার্ডৱেৰ ফায়াৰৱালৰ দৰে, ক্লাউড-ভিত্তিক ফায়াৰৱালে পেৰিমিটাৰ সুৰক্ষা প্রদান কৰা বুলি জনা যায়।

ফায়াৰৱাল নথকাৰ কিছুমান গুৰুত্বপূর্ণ বিপদ হ'ল:

১) অকর্তৃত্বশীল প্রৱেশ: হেকাৰে নেটৱর্কৰ দুর্বলতাসমূহ শোষণ কৰি গোপনীয় তথ্য যেনে গ্রাহকৰ তথ্য, বিত্তীয় তথ্য, আৰু বৌদ্ধিক সম্পত্তিৰ প্রৱেশাধিকাৰ লাভ কৰিব পাৰে।

২) মেলৱেৰ আক্রমণ: ভাইৰাছ, ৱর্ম, আৰু ট্র'জানৰ দৰে মেলৱেৰে নেটৱর্ক সংক্রমিত কৰি চিষ্টেমৰ ক্ষতি কৰিব পাৰে, ডাটা নষ্ট কৰিব পাৰে বা স্পর্শকাতৰ তথ্য চুৰি কৰিব পাৰে।

৩) ডিনিয়েল-অফ-চার্ভিচ (DOS) আক্রমণ: DOS আক্রমণে এটা নেটৱর্কক ট্রেফিকেৰে ভাৰাক্রান্ত কৰি পেলাব পাৰে, যাৰ ফলত ই ক্রেচ হয় আৰু বৈধ ব্যৱহাৰকাৰীয়ে নেটৱর্কত প্ৰৱেশ কৰাত বাধা প্রাপ্ত হয়।

৪) মেন-ইন-দ্য-মিডল (MITM) আক্রমণ: MITM আক্রমণত স্পর্শকাতৰ তথ্য চুৰি বা তথ্য পৰিৱর্তন কৰিবলৈ নেটৱর্ক ট্রেফিকক বাধা দিয়াৰ লগত জড়িত।

৫) ফিছিং আক্রমণ: ফিছিং আক্রমণত ব্যৱহাৰকাৰীক প্রতাৰিত কৰি পাছৱর্ড বা লগইন প্রমাণপত্রৰ দৰে স্পর্শকাতৰ তথ্য প্রকাশ কৰা হয়, প্রায়ে ভুৱা ইমেইল বা ৱেবছাইটৰ জৰিয়তে।

৬) ডাটা লিকেজ: ফায়াৰৱাল অবিহনে ডাটা লিকেজৰ পৰা কোনো সুৰক্ষা নাথাকে, যিটো হ'ব পাৰে যেতিয়া কর্মচাৰীয়ে ভুলবশতঃ বা ইচ্ছাকৃতভাৱে নেটৱর্কৰ বাহিৰত স্পর্শকাতৰ ডাটা শ্বেয়াৰ কৰে।

৭) অনুসৰণ উলংঘা: বহুতো নিয়ন্ত্রণমূলক প্রয়োজনীয়তা, যেনে পেমেণ্ট কার্ড উদ্যোগ তথ্য সুৰক্ষা মানদণ্ড (PCI DSS), স্পর্শকাতৰ তথ্য সুৰক্ষিত কৰিবলৈ ফায়াৰৱালৰ ব্যৱহাৰ বাধ্যতামূলক কৰে। এই নিয়মসমূহ মানি চলাত ব্যর্থ হ'লে জৰিমনা, আইনী ব্যৱস্থা, আৰু সংস্থাটোৰ সুনামৰ ক্ষতি হ'ব পাৰে।

ফায়াৰৱালে কেনেকৈ কাম কৰে?

ফায়াৰৱাল চিষ্টেমসমূহে পূর্বনির্ধাৰিত নিয়ম অনুসৰি নে'টৱর্ক ট্রাফিক বিশ্লেষণ কৰে। তাৰ পিছত ই ট্রেফিক ফিল্টাৰ কৰে আৰু অবিশ্বাস্য বা সন্দেহজনক উৎসৰ পৰা অহা ট্রেফিকক বাধা দিয়ে। ই কেৱল ইয়াক গ্রহণ কৰিবলে বিন্যাস কৰি অহা ট্রাফিকক হে প্রৱেশৰ অনুমতি দিয়ে।

সাধাৰণতে, এটা ফায়াৰৱালে এটা কম্পিউটাৰৰ এটা প্রৱেশ বিন্দুত নে'টৱর্ক ট্রাফিক ব্লক কৰে, যাক গেটৱে বোলা হয়। ফায়াৰৱালসমূহে পূর্বনির্ধাৰিত সুৰক্ষা নিয়মসমূহৰ ওপৰত ভিত্তি কৰি নির্দিষ্ট পেকেটসমূহ (এটা ডিজিটেল নে'টৱর্কৰ মাজেৰে পাৰ হোৱা যোগাযোগ এককসমূহ) অনুমতি বা বাধা দি এই কাম সম্পন্ন কৰে।

ফায়াৰৱালৰ কার্য্যসমূহ

ওপৰত উল্লেখ কৰা অনুসৰি ফায়াৰৱালে গেটকিপাৰৰ কাম কৰে। ই আমাৰ অপাৰেটিং চিষ্টেম প্ৰৱেশাধিকাৰ কৰাৰ প্ৰতিটো প্ৰচেষ্টা স্কেন কৰে আৰু অবাঞ্ছিত বা অচিনাক্ত উৎসৰ পৰা অহা ট্ৰেফিক ব্লক কৰে। যিহেতু ফায়াৰৱালে কম্পিউটাৰ চিষ্টেম আৰু অন্যান্য নেটৱৰ্ক (অৰ্থাৎ ৰাজহুৱা ইণ্টাৰনেট)ৰ মাজত বাধা বা ফিল্টাৰ হিচাপে কাম কৰে, গতিকে আমি ইয়াক ট্ৰেফিক নিয়ন্ত্ৰক হিচাপে ভাবিব পাৰো। গতিকে ফায়াৰৱালৰ মূল কাম হ'ল নেটৱৰ্ক ট্ৰেফিক নিয়ন্ত্ৰণ কৰি আমাৰ নেটৱৰ্ক আৰু তথ্য সুৰক্ষিত কৰা, অবাঞ্ছিতভাৱে অহা নেটৱৰ্ক ট্ৰেফিক প্ৰতিৰোধ কৰা আৰু হেকাৰ আৰু মেলৱেৰৰ দৰে ক্ষতিকাৰক বিষয়বস্তু ধৰা পেলাবলৈ নেটৱৰ্ক ট্ৰেফিক মূল্যায়ন কৰি প্ৰৱেশ পৰীক্ষা কৰা। সাধাৰণতে, বেছিভাগ অপাৰেটিং চিষ্টেম (উদাহৰণস্বৰূপে, উইণ্ড'জ অপাৰেটিং চিষ্টেম) আৰু সুৰক্ষা চফটৱেৰ বিল্ট-ইন ফায়াৰৱাল সমৰ্থনৰ সৈতে আহে। সেয়েহে এই বিকল্পসমূহ সক্ৰিয় কৰাটো নিশ্চিত কৰাটো এটা ভাল ধাৰণা। অতিৰিক্তভাৱে, আমি উপলব্ধ হ'লে স্বয়ংক্ৰিয়ভাৱে আপডেইট কৰিবলে চিষ্টেম সুৰক্ষা সংহতিসমূহ বিন্যাস কৰিব পাৰো। ফায়াৰৱাল ইমান শক্তিশালী হৈ পৰিছে আৰু ইয়াত বিভিন্ন বিল্ট-ইন বৈশিষ্ট্য যেনে:

- নেটৱৰ্ক ভাবুকি প্ৰতিৰোধ
- প্ৰয়োগ আৰু পৰিচয়-ভিত্তিক নিয়ন্ত্ৰণ
- হাইব্ৰিড ক্লাউড সমৰ্থন
- স্কেলেবল পৰিৱেশন
- নেটৱৰ্ক ট্ৰেফিক ব্যৱস্থাপনা আৰু নিয়ন্ত্ৰণ
- প্ৰৱেশাধিকাৰ বৈধকৰণ
- পৰিঘটনাৰ ৰেকৰ্ড আৰু প্ৰতিবেদন

নেটৱৰ্ক সুৰক্ষাৰ কথা আহিলে ফায়াৰৱালক প্ৰথম প্ৰতিৰক্ষা শাৰী বুলি গণ্য কৰা হয়। কিন্তু প্ৰশ্ন হয় এই ফায়াৰৱালবোৰ চাইবাৰ আক্ৰমণৰ পৰা আমাৰ ডিভাইচবোৰক সুৰক্ষিত কৰিব পৰাকৈ শক্তিশালী নেকি? উত্তৰটো হয়তো নহয়। ইণ্টাৰনেট ব্যৱহাৰ কৰাৰ সময়ত ফায়াৰৱাল ব্যৱস্থাপ্ৰণালী ব্যৱহাৰ কৰাটো বাঞ্ছনীয়। কিন্তু, নে'টৱৰ্ক আৰু আপোনাৰ কম্পিউটাৰত সংৰক্ষণ কৰা তথ্য সুৰক্ষিত কৰাত সহায় কৰিবলে অন্য প্ৰতিৰক্ষা ব্যৱস্থাপ্ৰণালী ব্যৱহাৰ কৰাটো গুৰুত্বপূৰ্ণ। সদায় বিকশিত হৈ থকা চাইবাৰ ভাবুকিৰ সৈতে, আপোনাৰ ঘৰুৱা নেটৱৰ্ক সুৰক্ষিত কৰাৰ বাবে এটা ফায়াৰৱাল একমাত্ৰ বিবেচনা হ'ব নালাগে।

ফায়াৰৱালক সুৰক্ষা ব্যৱস্থাপ্ৰণালী হিচাপে ব্যৱহাৰ কৰাৰ গুৰুত্ব স্পষ্ট; কিন্তু, ফায়াৰৱালৰ কিছুমান সীমাবদ্ধতা আছে:

১. **অসম্পূৰ্ণ সুৰক্ষা:** ফায়াৰৱালসমূহক কিছুমান বিশেষ ধৰণৰ চাইবাৰ ভাবুকিৰ পৰা সুৰক্ষা দিবলৈ ডিজাইন কৰা হৈছে, যেনে এটা নেটৱৰ্ক বা ক্ষতিকাৰক ডাটা পেকেটলৈ

অকৰ্তৃত্বশীল প্ৰৱেশাধিকাৰ। কিন্তু তেওঁলোকে সকলো ধৰণৰ চাইবাৰ ভাবুকি, যেনে ছ'চিয়েল ইঞ্জিনিয়াৰিং আক্ৰমণ বা ফিছিংৰ পৰা সুৰক্ষা দিব নোৱাৰে।

২. অতিৰিক্ত নিৰ্ভৰশীলতা: বহু সংস্থাই চাইবাৰ সুৰক্ষাৰ প্ৰাথমিক উপায় হিচাপে ফায়াৰৱালৰ ওপৰত অতিৰিক্তভাৱে নিৰ্ভৰ কৰিব পাৰে, অতিৰিক্ত ব্যৱস্থা যেনে এণ্টি-ভাইৰাছ চফটৱেৰ বা অনুপ্ৰৱেশ ধৰা পেলোৱা ব্যৱস্থা প্ৰণয়ন নকৰাকৈ। ইয়াৰ ফলত ভুৱা নিৰাপত্তাবোধৰ সৃষ্টি হ'ব পাৰে আৰু সংস্থাটো অন্য ধৰণৰ আক্ৰমণৰ সন্মুখীন হ'বলগীয়া হ'ব পাৰে।

৩. ভুল বিন্যাস: ফায়াৰৱালসমূহ ফলপ্ৰসূ হ'বলৈ সঠিকভাৱে বিন্যাস কৰিব লাগিব, আৰু আনকি এটা সৰু ভুল বিন্যাসেও ফায়াৰৱালক অকাৰ্যকৰী কৰিব পাৰে। এইটো এনে সংস্থাসমূহৰ বাবে এটা সমস্যা হ'ব পাৰে যাৰ নিৰ্দিষ্ট IT কৰ্মচাৰী নাই বা এটা ফায়াৰৱাল সঠিকভাৱে বিন্যাস কৰিবলে বিশেষজ্ঞ নাই।

৪. দুৰ্বলতাসমূহ: যিকোনো চফটৱেৰৰ দৰে, ফায়াৰৱালসমূহ দুৰ্বলতাৰ পৰা মুক্ত নহয় আৰু ইয়াত শোষণযোগ্য ত্ৰুটি থাকিব পাৰে যিবোৰ আক্ৰমণকাৰীয়ে ফায়াৰৱাল বাইপাছ কৰিবলৈ ব্যৱহাৰ কৰিব পাৰে। দুৰ্বলতাৰ আশংকা কম কৰিবলৈ ফায়াৰৱালসমূহক শেহতীয়া সুৰক্ষা পেচসমূহৰ সৈতে আপডেট কৰি ৰখাটো গুৰুত্বপূৰ্ণ।

৫. ভিতৰৰ ভাবুকি: ফায়াৰৱালসমূহ বাহ্যিক ভাবুকিৰ পৰা সুৰক্ষা দিবলৈ ডিজাইন কৰা হৈছে, কিন্তু ই অন্তৰ্দৃষ্টিৰ ভাবুকিৰ বিৰুদ্ধে ফলপ্ৰসূ নহ'বও পাৰে যেনে কৰ্মচাৰী বা ঠিকাদাৰ যিসকলৰ নেটৱৰ্কলৈ বৈধ প্ৰৱেশাধিকাৰ আছে। ভিতৰৰ ভাবুকিসমূহে বৈধ প্ৰমাণপত্ৰসমূহ ব্যৱহাৰ কৰি বা নে'টৱৰ্কত দুৰ্বলতাসমূহ শোষণ কৰি ফায়াৰৱালসমূহ বাইপাছ কৰিব পাৰে।

৬. খৰচ: ফায়াৰৱালসমূহ প্ৰণয়ন আৰু ৰক্ষণাবেক্ষণ কৰাটো ব্যয়বহুল হ'ব পাৰে, বিশেষকৈ ক্ষুদ্ৰ আৰু মজলীয়া ব্যৱসায়ৰ বাবে। যিবোৰ সংস্থাৰ হাতত বাজেট বা সম্পদ নাই সেইবোৰৰ বাবে ই এক বাধা হ'ব পাৰে, যিবোৰৰ হাতত এটা বিস্তৃত চাইবাৰ সুৰক্ষা কৌশল ৰূপায়ণ কৰিব পৰা নাযায়।

সংস্থাসমূহে এই সীমাবদ্ধতাসমূহৰ বিষয়ে সচেতন হ'ব লাগিব আৰু অন্য ধৰণৰ চাইবাৰ ভাবুকিসমূহৰ সৈতে মোকাবিলা কৰিবলৈ অতিৰিক্ত ব্যৱস্থাসমূহ ৰূপায়ণ কৰিব লাগিব, যেনে এণ্টি-ভাইৰাছ চফটৱেৰ, অনুপ্ৰৱেশ ধৰা পেলোৱা ব্যৱস্থা, আৰু কৰ্মচাৰী প্ৰশিক্ষণ।

ফায়াৰৱালৰ প্ৰকাৰসমূহ

কেইবাবিধো ফায়াৰৱাল উপলব্ধ, প্ৰত্যেকৰে নিজস্ব বৈশিষ্ট্য আৰু ক্ষমতা আছে। ইয়াত কিছুমান সাধাৰণ ধৰণৰ ফায়াৰৱাল দিয়া হৈছে:

১. পেকেট ফিল্টাৰিং ফায়াৰৱাল: এইটো আটাইতকৈ মৌলিক ধৰণৰ ফায়াৰৱাল যি তথ্যৰ অহা আৰু যোৱা পেকেটসমূহ পৰীক্ষা কৰে আৰু পূৰ্বনিৰ্ধাৰিত নিয়মৰ ভিত্তিত সিহতক অনুমতি বা ব্লক কৰে। পেকেট ফিল্টাৰিং ফায়াৰৱালসমূহে OSI আৰ্হিৰ নে'টৱৰ্ক স্তৰত কাম কৰে আৰু কেৱল IP ঠিকনা, পৰ্ট নম্বৰ, আৰু প্ৰটোকলৰ ধৰণৰ ওপৰত ভিত্তি কৰি ট্ৰাফিক ফিল্টাৰ কৰিব পাৰে।

২. ষ্টেটফুল পৰিদৰ্শন ফায়াৰৱালসমূহ: ষ্টেটফুল পৰিদৰ্শন ফায়াৰৱালসমূহ পেকেট ফিল্টাৰিং ফায়াৰৱালসমূহতকৈ অধিক উন্নত কাৰণ ই কেৱল অহা আৰু যোৱা পেকেটসমূহ পৰিদৰ্শন কৰাই নহয় কিন্তু ই বৈধ হোৱাটো নিশ্চিত কৰিবলে প্ৰতিটো সংযোগৰ অৱস্থাও অনুসৰণ কৰে। এই ফায়াৰৱালসমূহে নেটৱৰ্ক স্তৰত কাম কৰে আৰু OSI মডেলৰ পৰিবহণ স্তৰত ট্ৰেফিক পৰিদৰ্শন কৰিব পাৰে।

৩. এপ্লিকেচন ফায়াৰৱালসমূহ: এপ্লিকেচন ফায়াৰৱালসমূহে OSI আৰ্হিৰ এপ্লিকেচন স্তৰত কাম কৰে আৰু এপ্লিকেচন স্তৰত ট্ৰাফিক পৰিদৰ্শন কৰিব পাৰে, যেনে HTTP বা FTP। এই ধৰণৰ ফায়াৰৱালে নিৰ্দিষ্ট ধৰণৰ ট্ৰাফিক ধৰা পেলাব আৰু ব্লক কৰিব পাৰে, যেনে SQL ইনজেকচন আক্ৰমণ।

৪. পৰৱৰ্তী-প্ৰজন্মৰ ফায়াৰৱালসমূহ (NGFW): NGFWS হৈছে উন্নত ফায়াৰৱালসমূহ যি পেকেট ফিল্টাৰিং, অৱস্থাপূৰ্ণ পৰিদৰ্শন, আৰু এপ্লিকেচন ফায়াৰৱালসমূহৰ ক্ষমতাসমূহ উন্নত ভাবুকি ধৰা পেলোৱা আৰু প্ৰতিৰোধ কৌশলসমূহৰ সৈতে সংযুক্ত কৰে। NGFW সমূহে গভীৰ পেকেট পৰিদৰ্শন কৰিব পাৰে আৰু মেলৱেৰ, ভাই�ৰাছ, আৰু অন্যান্য উন্নত ভাবুকিসমূহ ধৰা পেলাব আৰু ব্লক কৰিব পাৰে।

৫. প্ৰক্সি ফায়াৰৱালসমূহ: প্ৰক্সি ফায়াৰৱালসমূহে ক্লায়েণ্ট আৰু চাৰ্ভাৰসমূহৰ মাজত এটা মধ্যস্থতাকাৰী হিচাপে কাম কৰে, এপ্লিকেচন-নিৰ্দিষ্ট নিয়মসমূহৰ ওপৰত ভিত্তি কৰি ট্ৰাফিক ফিল্টাৰ কৰে। প্ৰক্সি ফায়াৰৱালসমূহে অতিৰিক্ত সুৰক্ষা বৈশিষ্ট্যসমূহ যেনে বিষয়বস্তু ফিল্টাৰিং আৰু তথ্য হেৰুৱা প্ৰতিৰোধো প্ৰদান কৰিব পাৰে।

৬. ক্লাউড ফায়াৰৱালসমূহ: ক্লাউড ফায়াৰৱালে ক্লাউড-ভিত্তিক এপ্লিকেচন আৰু সেৱাসমূহৰ বাবে নেটৱৰ্ক সুৰক্ষা প্ৰদান কৰে। এই ফায়াৰৱালসমূহ ক্লাউডত হ'ষ্ট কৰা হয় আৰু কেন্দ্ৰীয়ভাৱে পৰিচালনা কৰিব পাৰি, যাৰ ফলত ইহঁতক বিতৰিত পৰিৱেশৰ বাবে আদৰ্শ কৰি তোলা হয়।

এণ্টি-ভাইৰাছ চফটৱেৰ:

আমি মানুহ যেনেকৈ সংক্রমিত হ'ব পাৰো আৰু অসুস্থ হ'ব পাৰো, তেনেদৰে আমাৰ কম্পিউটাৰো ইণ্টাৰনেটৰ সৈতে সংযোগ কৰিলে সংক্রমিত হ'ব পাৰে। আমি ইণ্টাৰনেটৰ পৰা ডাউনলোড কৰা বস্তু যেনে ইমেইল বা অনলাইন কপি কৰা ফাইলৰ জৰিয়তে ভাইৰাছে আমাৰ কম্পিউটাৰত অনুপ্রৱেশ কৰিব পাৰে। ভাইৰাছে আমাৰ ডাটা মচি পেলাব পাৰে বা ব্যৱহাৰ কৰিব নোৱাৰা কৰি ধ্বংস কৰিব পাৰে আৰু আমাৰ কম্পিউটাৰৰ কার্য্যক্ষমতাও যথেষ্ট লেহেমীয়া কৰি প্রভাৱিত কৰিব পাৰে। ভাইৰাছে আমাৰ গোপনীয় তথ্য আন মানুহলৈও পুনৰ প্রেৰণ কৰিব পাৰে বা কোনোবাই আমাৰ কম্পিউটাৰক দূৰৈৰ পৰা নিয়ন্ত্রণ কৰি নিজৰ উদ্দেশ্যত ব্যৱহাৰ কৰিবলৈ অনুমতি দিব পাৰে।

এণ্টি-ভাইৰাছ চফটৱেৰ, যাক এণ্টিমেলৱেৰ চফটৱেৰ বুলিও কোৱা হয়, ই হৈছে মেলৱেৰ প্রতিৰোধ, ধৰা পেলোৱা আৰু আঁতৰাবলৈ ব্যৱহাৰ কৰা কম্পিউটাৰ প্রগ্রেম। এণ্টি-ভাইৰাছ চফটৱেৰটো প্রথমে কম্পিউটাৰ ভাইৰাছ ধৰা পেলাবলৈ আৰু আঁতৰাবলৈ নির্মাণ কৰা হৈছিল, সেয়েহে ইয়াৰ নাম তেনেদৰে ৰখা হৈছিল। কিন্তু অধিক মেলৱেৰ বিয়পি পৰাৰ লগে লগে এণ্টি-ভাইৰাছ চফটৱেৰে কম্পিউটাৰৰ অন্যান্য ভাবুকিৰ পৰা সুৰক্ষা দিবলৈ আৰম্ভ কৰিলে। কিছুমান প্রডাক্টত ক্ষতিকাৰক URL, স্পেম, আৰু ফিছিঙৰ বিৰুদ্ধে সুৰক্ষাও অন্তর্ভুক্ত কৰা হৈছে। এণ্টি-ভাইৰাছ চফ্টৱেৰে কম্পিউটাৰ চিষ্টেমৰ পৰা মেলৱেৰ ধৰা পেলাবলৈ আৰু আঁতৰাবলৈ বিভিন্ন কৌশল ব্যৱহাৰ কৰে। আধুনিক এণ্টি-ভাইৰাছ প্রগ্রেমসমূহে ব্যৱহাৰ কৰা কিছুমান মূল প্রযুক্তিৰ ভিতৰত আছে:

- স্বাক্ষৰ-ভিত্তিক ধৰা পেলোৱা: এই কৌশলত কম্পিউটাৰ চিষ্টেমৰ ফাইলসমূহক জনা মেলৱেৰ স্বাক্ষৰৰ ডাটাবেছৰ সৈতে তুলনা কৰা হয়। যেতিয়া এটা ফাইল এটা জনা স্বাক্ষৰৰ সৈতে মিলে, এণ্টি-ভাইৰাছ প্রগ্রেমে ফাইলটোক চিষ্টেমৰ পৰা কোৱাৰেণ্টাইন কৰিব বা আঁতৰাব।

- হিউৰিষ্টিক-ভিত্তিক ধৰা পেলোৱা: এই কৌশলত কম্পিউটাৰ চিষ্টেমত থকা ফাইলসমূহৰ আচৰণ বিশ্লেষণ কৰি সম্ভাব্য ক্ষতিকাৰক আচৰণ ধৰা পেলায়। এণ্টি-ভাইৰাছ চফ্টৱেৰে তেওঁলোকৰ আচৰণৰ ওপৰত ভিত্তি কৰি নতুন বা অজ্ঞাত ভাবুকি ধৰা পেলাবলৈ কৃত্রিম বুদ্ধিমত্তা বা মেচিন লার্নিং এলগৰিথম ব্যৱহাৰ কৰিব পাৰে।

- আচৰণভিত্তিক ধৰা পেলোৱা: এই কৌশলত কম্পিউটাৰ ব্যৱস্থাপ্রণালীৰ প্রক্রিয়াসমূহৰ আচৰণ বিশ্লেষণ কৰি সম্ভাব্য ক্ষতিকাৰক কার্য্যকলাপ ধৰা পেলায়। এণ্টি-ভাইৰাছ চফটৱেৰে সন্দেহজনক কার্যকলাপৰ চিনসমূহৰ বাবে প্রক্রিয়াসমূহ নিৰীক্ষণ কৰিব পাৰে, যেনে চিষ্টেম

ফাইলসমূহ পৰিৱৰ্তন কৰাৰ চেষ্টা কৰা বা জনা বিপজ্জনক চাৰ্ভাৰসমূহৰ সৈতে যোগাযোগ কৰা।

- ছেণ্ডবক্সিং: এই কৌশলত ভাৰ্চুৱেল পৰিৱেশত সম্ভাব্য ক্ষতিকাৰক ক'ড চলাই ইয়াৰ আচৰণ পৰ্যবেক্ষণ কৰা হয়। ই এণ্টি-ভাইৰাছ চফটৱেৰক নতুন বা অজ্ঞাত ভাবুকি ধৰা পেলাবলৈ অনুমতি দিয়ে যিবোৰ স্বাক্ষৰ-ভিত্তিক বা হিউৰিষ্টিক-ভিত্তিক ধৰা পেলোৱাৰ দ্বাৰা ধৰা নপৰা হ'ব পাৰে।

- মেচিন লার্নিং: এই কৌশলত জনাজাত মেলৱেৰৰ আৰ্হি আৰু বৈশিষ্ট্যৰ ওপৰত ভিত্তি কৰি মেলৱেৰ চিনাক্ত কৰিবলৈ এলগৰিথম প্ৰশিক্ষণ দিয়া হয়। মেচিন লার্নিং এলগৰিথমে নতুন আৰু অজ্ঞাত ভাবুকি ধৰা পেলোৱা আৰু প্ৰতিৰোধ কৰাত ফলপ্ৰসূ কৰি তুলিছে।

- ক্লাউড-ভিত্তিক ধৰা পেলোৱা: এই কৌশলত বিশ্লেষণৰ বাবে সন্দেহজনক ফাইলসমূহ ক্লাউড-ভিত্তিক চাৰ্ভাৰলৈ আপলোড কৰে। চাৰ্ভাৰে সম্ভাব্য ভাবুকি ধৰা পেলাবলৈ আৰু চিনাক্ত কৰিবলৈ অধিক শক্তিশালী হাৰ্ডৱেৰ আৰু মেচিন লার্নিং এলগৰিথম ব্যৱহাৰ কৰিব পাৰে।

এণ্টি-ভাইৰাছ চফটৱেৰ সাধাৰণতে কেইবাটাও উপাদান থাকে, য'ত ৰিয়েল-টাইম স্ক্যানাৰ, কোৱাৰেণ্টাইন মেনেজাৰ আৰু আপডেট মেনেজাৰ অন্তৰ্ভুক্ত। বাস্তৱ-সময় স্ক্যানাৰসমূহ পটভূমিত চলি থাকে আৰু আপোনাৰ কম্পিউটাৰ ব্যৱস্থাপ্ৰণালীত নথিপত্ৰ আৰু প্ৰক্ৰিয়াসমূহ অহৰহ নিৰীক্ষণ কৰে ক্ষতিকাৰক কার্যকলাপৰ চিনসমূহৰ বাবে। যদি স্ক্যানাৰে কোনো সম্ভাব্য ভাবুকি ধৰা পেলায়, তেন্তে ই ব্যৱহাৰকাৰীক সতর্ক কৰি দিয়ে আৰু ফাইলটো কোৱাৰেণ্টাইন বা মচি পেলোৱাৰ ব্যৱস্থা গ্ৰহণ কৰে। সম্ভাব্য ক্ষতিকাৰক বুলি ধৰা পৰা ফাইলসমূহ পৰিচালনা আৰু কোৱাৰেণ্টাইন কৰাৰ দায়িত্ব কোৱাৰেণ্টাইন প্ৰশাসকৰ। কোৱাৰেণ্টাইন কৰা ফাইলসমূহ সাধাৰণতে এটা সুৰক্ষিত স্থানত সংৰক্ষণ কৰা হয় যাতে সিহঁতে চিষ্টেমক ক্ষতি কৰিব নোৱাৰে বা অন্য ফাইলসমূহলৈ বিয়পিব নোৱাৰে। আপডেট মেনেজাৰে এণ্টি-ভাইৰাছ চফটৱেৰক শেহতীয়া মেলৱেৰ সংজ্ঞা আৰু ধৰা পেলোৱা প্ৰযুক্তিৰ সৈতে আপডেট কৰি ৰখাৰ বাবে দায়বদ্ধ। উদীয়মান ভাবুকিৰ বিৰুদ্ধে ফলপ্ৰসূ হ'বলৈ এণ্টি-ভাইৰাছ চফটৱেৰ নিয়মিতভাৱে আপডেট কৰিব লাগিব। এই মূল উপাদানসমূহৰ উপৰি, বহুতো এণ্টি-ভাইৰাছ প্ৰগ্ৰেমত অন্য বৈশিষ্ট্যসমূহ অন্তৰ্ভুক্ত কৰে, যেনে ফায়াৰৱাল, ৱেব ফিল্টাৰিং আৰু ইমেইল স্কেনিং। এই বৈশিষ্ট্যসমূহে চাইবাৰ ভাবুকিৰ বিৰুদ্ধে অতিৰিক্ত সুৰক্ষাৰ স্তৰ প্ৰদান কৰে।

ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছ চফটৱেৰ দুয়োটা এক বিস্তৃত চাইবাৰ সুৰক্ষা কৌশলৰ গুৰুত্বপূৰ্ণ উপাদান, কিন্তু ই বিভিন্ন উদ্দেশ্য সাধন কৰে আৰু ইয়াৰ কাম বেলেগ বেলেগ। ফায়াৰৱালসমূহ হৈছে নে'টৱর্ক সুৰক্ষা ডিভাইচসমূহ যি অহা আৰু যোৱা নে'টৱর্ক ট্ৰাফিক নিৰীক্ষণ আৰু ফিল্টাৰ কৰিবলে ডিজাইন কৰা হৈছে। সিহতক হাৰ্ডৱেৰ আৰু চফটৱেৰ দুয়োটা

ৰূপতে প্ৰণয়ন কৰিব পাৰি, আৰু সিহঁতে ডাটা পেকেটসমূহ পৰীক্ষা কৰি আৰু পূৰ্বনিৰ্ধাৰিত নিয়মৰ এটা গোটৰ ভিত্তিত সিহতক অনুমতি দিব নে ব্লক কৰিব সেইটো নিৰ্ধাৰণ কৰি কাম কৰে। ফায়াৰৱালে জনা ক্ষতিকাৰক উৎসৰ পৰা অহা সংযোগসমূহ বন্ধ কৰিব পাৰে, স্পৰ্শকাতৰ তথ্যলৈ অকৰ্তৃত্বশীল প্ৰৱেশাধিকাৰ প্ৰতিৰোধ কৰিব পাৰে, আৰু দূৰৱৰ্তী চাৰ্ভাৰসমূহৰ সৈতে যোগাযোগ কৰাত মেলৱেৰ প্ৰতিৰোধ কৰিব পাৰে।

আনহাতে এণ্টি-ভাইৰাছ চফটৱেৰ কম্পিউটাৰ চিষ্টেমৰ পৰা ক্ষতিকাৰক চফটৱেৰ বা মেলৱেৰ ধৰা পেলাবলৈ আৰু আঁতৰাবলৈ ডিজাইন কৰা হৈছে। এণ্টি-ভাইৰাছ চফটৱেৰে ফাইল আৰু ডাইৰেকটৰিসমূহ জনা মেলৱেৰ স্বাক্ষৰ বা আচৰণৰ বাবে স্কেন কৰে, আৰু অজ্ঞাত বা শূন্য-দিনৰ মেলৱেৰ ধৰা পেলাবলৈ হিউৰিষ্টিক ব্যৱহাৰ কৰিব পাৰে। এণ্টি-ভাইৰাছ চফটৱেৰে কম্পিউটাৰ চিষ্টেমৰ পৰা ভাইৰাছ, ৱৰ্ম, ট্ৰ'জান, আৰু অন্যান্য ধৰণৰ মেলৱেৰ ধৰা পেলাব পাৰে আৰু আঁতৰাব পাৰে। ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছ চফটৱেৰ দুয়োটা এটা বিস্তৃত চাইবাৰ সুৰক্ষা কৌশলৰ অপৰিহাৰ্য উপাদান যদিও ই বিভিন্ন উদ্দেশ্য সাধন কৰে আৰু ইয়াৰ বিভিন্ন কাৰ্য আছে। ফায়াৰৱালে এটা নেটৱৰ্কলৈ অকৰ্তৃত্বশীল প্ৰৱেশ প্ৰতিৰোধ কৰাত গুৰুত্ব দিয়ে, আনহাতে এণ্টি-ভাইৰাছ চফটৱেৰে এটা কম্পিউটাৰ চিষ্টেমৰ পৰা মেলৱেৰ ধৰা পেলোৱা আৰু আঁতৰোৱাত গুৰুত্ব দিয়ে। চাইবাৰ ভাবুকিৰ বিৰুদ্ধে ব্যাপক সুৰক্ষা নিশ্চিত কৰিবলৈ সংস্থাসমূহে ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছ চফটৱেৰ দুয়োটা প্ৰণয়ন কৰিব লাগে।



অগ্ৰগতি নিৰীক্ষণ

১. শুদ্ধ নে অশুদ্ধ বিচাৰ কৰক—

ক) এক্সেছ নিয়ন্ত্ৰণ (ACCESS CONTROLS) ডিভাইচ সুৰক্ষা নীতিত এটা জৰুৰী উপাদান নহয়।

খ) বেকআপ আৰু পুনৰুদ্ধাৰ (BACKUP AND RECOVERY) পৰিকল্পনা প্ৰয়োগ কৰা ডিভাইচ সুৰক্ষা নীতি ৰক্ষা কৰিবলৈ জৰুৰী নহয়।

গ) ছিকিউৰিটি ইনফৰ্মেছন এণ্ড ইভেণ্ট মেনেজমেন্ট (SIEM) এ ৰিয়েল-টাইম থ্ৰেট চিনাক্তকৰণ, ঘটনা প্ৰতিক্ৰিয়া, আৰু কমপ্লায়েন্স ৰিপোৰ্টিং দিয়ে।

ঘ) হ'ষ্ট ফায়াৰৱাল সঠিকভাৱে সংৰূপণ কৰিলে এণ্টি-ভাইৰাছ চফটৱেৰ দৰকাৰ নহয়।

ঙ) এণ্টি-ভাইৰাছ চফটৱেৰে জিৰো-ডে আক্ৰমণৰ পৰা ৰক্ষা কৰিব পাৰে।

চ) পেকেট-ফিল্টাৰিং ফায়াৰৱালে প্ৰতি পেকেটৰ ভিতৰ পৰ্যন্ত পৰীক্ষা কৰে।
ছ) হ'ষ্ট ফায়াৰৱালৰ লগ মনিটৰ কৰা প্ৰয়োজনীয় নহয়।
জ) ক্লাউড ফায়াৰৱালে ক্লাউড-ভিত্তিক এপ্লিকেশ্বন আৰু সেৱাৰ বাবে নেটৱৰ্ক সুৰক্ষা প্ৰদান কৰে।

১৩.৬ হ'ষ্ট ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছৰ ব্যৱস্থাপনা

এটা সংস্থাৰ আই টি আন্তঃগাঁথনিৰ সুৰক্ষা আৰু অখণ্ডতা বজাই ৰখাৰ বাবে হ'ষ্ট ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছ চফটৱেৰৰ ব্যৱস্থাপনা অতি প্ৰয়োজনীয়। হ'ষ্ট ফায়াৰৱালে ক্ষতিকাৰক ট্ৰাফিক আৰু অকৰ্তৃত্বশীল প্ৰৱেশাধিকাৰৰ বিৰুদ্ধে সুৰক্ষাৰ এটা অতিৰিক্ত স্তৰ প্ৰদান কৰে, আনহাতে এণ্টি-ভাইৰাছ চষ্টৱেৰে চিষ্টেম আৰু তথ্যৰ সৈতে আপোচ কৰিব পৰা মেলৱেৰ ধৰা পেলোৱা আৰু আঁতৰাবলৈ সহায় কৰে। এই সুৰক্ষা ব্যৱস্থাসমূহৰ ফলপ্ৰসূ ব্যৱস্থাপনাই নিশ্চিত কৰে যে ডিভাইচ আৰু নেটৱৰ্কসমূহ চাইবাৰ ভাবুকি, যেনে ভাইৰাছ, ৰেনছমৱেৰ আৰু ফিছিং আক্ৰমণৰ পৰা সুৰক্ষিত। শেহতীয়া ভাবুকিসমূহৰ সৈতে খাপ খুৱাবলৈ নিয়মিত আপডেইটসমূহ আৰু পেচসমূহ অতি গুৰুত্বপূৰ্ণ, আৰু ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছ চষ্টৱেৰে উদ্দেশ্য অনুসৰি কাম কৰাটো নিশ্চিত কৰিবলৈ অবিৰত পৰ্যবেক্ষণ আৰু ৰক্ষণাবেক্ষণৰ প্ৰয়োজন। সঠিক ব্যৱস্থাপনা অবিহনে সংস্থাটোৰ আই টি সম্পত্তিসমূহ আপোচৰ বাবে দুৰ্বল হয়, যাৰ ফলত সম্ভাব্য তথ্য হেৰুৱা, চিষ্টেম বন্ধ, সময় আৰু আৰ্থিক লোকচান হয়।

হ'ষ্ট ফায়াৰৱালসমূহৰ ফলপ্ৰসূ ব্যৱস্থাপনা

নে'টৱৰ্ক সুৰক্ষা বজাই ৰাখিবলৈ হ'ষ্ট ফায়াৰৱালসমূহৰ ফলপ্ৰসূ ব্যৱস্থাপনা অপৰিহাৰ্য। হ'ষ্ট ফায়াৰৱাল ব্যৱস্থাপনা কৰাৰ বাবে কিছুমান উত্তম পদ্ধতি আছে:

- ফায়াৰৱাল নিয়মসমূহ নিয়মিতভাৱে আপডেইট কৰক: ফায়াৰৱাল নিয়মসমূহ নিয়মিতভাৱে আপডেইট কৰিব লাগে যাতে ই প্ৰতিষ্ঠানৰ বৰ্তমানৰ প্ৰয়োজনীয়তাসমূহ প্ৰতিফলিত কৰে আৰু শেহতীয়া সুৰক্ষা ভাবুকিসমূহৰ বিৰুদ্ধে পৰ্যাপ্ত সুৰক্ষা প্ৰদান কৰে। ইয়াৰ ভিতৰত পুৰণি নিয়ম আঁতৰোৱা আৰু উদীয়মান ভাবুকিসমূহৰ সৈতে মোকাবিলা কৰিবলৈ নতুন নিয়ম যোগ কৰা আদি অন্তৰ্ভুক্ত।

- কম বিশেষাধিকাৰ বলবৎ কৰক: হ'ষ্ট ফায়াৰৱালসমূহক কম বিশেষাধিকাৰৰ নীতি বলবৎ কৰিবলে বিন্যাস কৰিব লাগে, যাৰ অৰ্থ হৈছে যে কেৱল প্ৰয়োজনীয় পৰ্টসমূহ, প্ৰটোকলসমূহ, আৰু সেৱাসমূহ ফায়াৰৱালৰ যোগেদি অনুমতি দিয়া হৈছে। ইয়াৰ ফলত আক্ৰমণৰ পৃষ্ঠভাগ হ্ৰাস পায় আৰু অকৰ্তৃত্বশীল প্ৰৱেশৰ আশংকা কম হয়।

• ফায়াৰৱাল লগসমূহ নিৰীক্ষণ কৰক: সন্দেহজনক কার্যকলাপ আৰু সম্ভাব্য সুৰক্ষা ভংগ চিনাক্ত কৰিবলে ফায়াৰৱাল লগসমূহ নিয়মিতভাৱে পর্যবেক্ষণ কৰিব লাগে। ইয়াৰ ভিতৰত অস্বীকাৰ কৰা সংযোগসমূহ, বিফল প্ৰৱেশ প্ৰচেষ্টাসমূহ, আৰু ক্ষতিকাৰক কার্যকলাপৰ অন্য সূচকসমূহৰ বাবে লগসমূহ পর্যালোচনা কৰা অন্তর্ভুক্ত।

• সুৰক্ষা ভংগৰ প্ৰভাৱ সীমিত কৰিবলৈ এটা নে'টৱর্ক সৰু উপনেটৱর্কসমূহত বিভক্ত কৰাৰ অভ্যাস । হ'ষ্ট ফায়াৰৱালসমূহক নে'টৱর্কৰ বিভিন্ন খণ্ডসমূহৰ মাজত ট্ৰাফিক নিষিদ্ধ কৰি বিভাজন বলবৎ কৰিবলে ব্যৱহাৰ কৰিব পাৰি।

• ফায়াৰৱাল বিন্যাস কঠিন কৰক: ফায়াৰৱাল বিন্যাসসমূহ কঠিন কৰিব লাগে অকর্তৃত্বশীল পৰিৱর্তনসমূহ প্ৰতিৰোধ কৰিবলে আৰু ভুল বিন্যাসৰ আশংকা হ্ৰাস কৰিবলে। ইয়াৰ ভিতৰত অপ্ৰয়োজনীয় সেৱাসমূহ নিষ্ক্ৰিয় কৰা, শক্তিশালী প্ৰমাণীকৰণ ব্যৱহাৰ কৰা, আৰু দূৰৱর্তী প্ৰৱেশাধিকাৰৰ বাবে ইনক্ৰিপষণ সামর্থবান কৰা অন্তর্ভুক্ত।

• নিয়মিতভাৱে ফায়াৰৱাল সুৰক্ষা পৰীক্ষা কৰক: ফায়াৰৱাল সুৰক্ষা নিয়মিতভাৱে পৰীক্ষা কৰিব লাগে যাতে ই আক্ৰমণ ধৰা পেলোৱা আৰু প্ৰতিৰোধ কৰাত ফলপ্ৰসূ হয়। ইয়াৰ ভিতৰত ফায়াৰৱাল বিন্যাসত দুর্বলতাসমূহ চিনাক্ত কৰিবলে দুর্বলতা স্কেনসমূহ আৰু অনুপ্ৰৱেশ পৰীক্ষণ কৰা অন্তর্ভুক্ত।

হ'ষ্ট ফায়াৰৱালসমূহৰ ফলপ্ৰসূ ব্যৱস্থাপনাৰ বাবে নিয়মীয়া ৰক্ষণাবেক্ষণ, পর্যবেক্ষণ আৰু পৰীক্ষণৰ প্ৰয়োজন হয় যাতে সিহঁতে শেহতীয়া সুৰক্ষা ভাবুকিৰ বিৰুদ্ধে পর্যাপ্ত সুৰক্ষা প্ৰদান কৰে। এই উত্তম পদ্ধতিসমূহ অনুসৰণ কৰি, সংস্থাসমূহে তেওঁলোকৰ নেটৱর্ক আৰু তথ্যৰ অখণ্ডতা আৰু গোপনীয়তা নিশ্চিত কৰাত সহায় কৰিব পাৰে।

কম্পিউটাৰ চিষ্টেম আৰু নেটৱর্কৰ সুৰক্ষা বজাই ৰখাৰ বাবে এণ্টি-ভাইৰাছ চফটৱেৰৰ ব্যৱস্থাপনা অতি প্ৰয়োজনীয়। এণ্টি-ভাইৰাছ চফটৱেৰ পৰিচালনাৰ বাবে কিছুমান উত্তম পদ্ধতি ইয়াত দিয়া হ'ল:

• এণ্টি-ভাইৰাছ চফটৱেৰ নিয়মিতভাৱে আপডেট কৰক: এণ্টি-ভাইৰাছ চফটৱেৰ নিয়মিতভাৱে আপডেট কৰিব লাগে যাতে ই শেহতীয়া মেলৱেৰ ভাবুকি ধৰা পেলাব পাৰে আৰু সুৰক্ষা দিব পাৰে। ইয়াত ভাইৰাছৰ সংজ্ঞা, চফটৱেৰ পেচ, আৰু অন্য সুৰক্ষা আপডেইট আপডেইট কৰা আদি কাম অন্তর্ভুক্ত হৈ থাকে।

• এণ্টি-ভাইৰাছ চফটৱেৰ সংহতিসমূহ বিন্যাস কৰক: এণ্টি-ভাইৰাছ চফটৱেৰ সংহতিসমূহ সংস্থাৰ নির্দিষ্ট প্ৰয়োজনীয়তাসমূহ পূৰণ কৰিবলে বিন্যাস কৰিব লাগে। ইয়াত

নির্ধাৰিত স্কেনসমূহ সংহতি কৰা, বাস্তৱ-সময়ৰ সুৰক্ষা বিন্যাস কৰা, আৰু ইমেইল আৰু ৰেব ফিল্টাৰিং সংহতি কৰা আদি অন্তর্ভুক্ত কৰা হৈছে।

- এণ্টি-ভাইৰাছ চফটৱেৰ সতর্কবাণীসমূহ নিৰীক্ষণ কৰক: সম্ভাব্য সুৰক্ষা ভংগ চিনাক্ত কৰিবলৈ এণ্টি-ভাইৰাছ চফটৱেৰ সতর্কবাণীসমূহ নিয়মিতভাৱে নিৰীক্ষণ কৰিব লাগে। ইয়াৰ ভিতৰত মেলৱেৰ ধৰা পেলোৱা, বিফল স্কেন, আৰু ক্ষতিকাৰক কার্যকলাপৰ অন্য সূচকৰ বাবে সতর্কবাণীসমূহ পর্যালোচনা কৰা অন্তর্ভুক্ত।

- নিয়মীয়া স্কেনসমূহ কৰক: মেলৱেৰ ধৰা পেলাবলৈ আৰু আঁতৰাবলৈ সকলো চিষ্টেমত নিয়মীয়া স্কেনসমূহ কৰিব লাগে। ইয়াত সকলো ব্যৱস্থাপ্রণালীৰ নির্ধাৰিত স্কেনসমূহ আৰু নির্দিষ্ট নথিপত্র বা পঞ্জিকাসমূহৰ অন-ডিমাণ্ড স্কেনসমূহ অন্তর্ভুক্ত কৰা হৈছে।

- ব্যৱহাৰকাৰী প্রশিক্ষণ পৰিচালনা কৰক: মেলৱেৰ সংক্রমণৰ আশংকা হ্রাস কৰিবলৈ কর্মচাৰীসকলক নিৰাপদ ব্রাউজিং আৰু ইমেইল পদ্ধতিৰ বিষয়ে জ্ঞান দিবলৈ ব্যৱহাৰকাৰী প্রশিক্ষণ গুৰুত্বপূর্ণ। ইয়াৰ ভিতৰত ফিছিং ইমেইলসমূহ কেনেকৈ চিনাক্ত কৰিব লাগে, মেলৱেৰ ডাউনলোড আৰু ইনষ্টল কৰাটো কেনেকৈ এৰাই চলিব লাগে, আৰু সন্দেহযুক্ত সুৰক্ষাৰ কাণ্ডসমূহ কেনেকৈ ৰিপর্ট কৰিব লাগে তাৰ প্রশিক্ষণ অন্তর্ভুক্ত কৰা হৈছে।

- এণ্টি-ভাইৰাছ চফটৱেৰ সুৰক্ষা পৰীক্ষা কৰক: এণ্টি-ভাইৰাছ চফটৱেৰ সুৰক্ষা নিয়মিতভাৱে পৰীক্ষা কৰিব লাগে যাতে ই মেলৱেৰ ধৰা পেলোৱা আৰু প্রতিৰোধ কৰাত ফলপ্রসূ হয়। ইয়াৰ ভিতৰত এণ্টি-ভাইৰাছ কনফিগাৰেচনৰ দুর্বলতা চিনাক্ত কৰিবলৈ পেনেট্রেচন টেষ্টিং আৰু অন্যান্য সুৰক্ষা পৰীক্ষাসমূহ কৰা অন্তর্ভুক্ত।

সামগ্রিকভাৱে, এণ্টি-ভাইৰাছ চফটৱেৰৰ ফলপ্রসূ ব্যৱস্থাপনাৰ বাবে নিয়মীয়া ৰক্ষণাবেক্ষণ, নিৰীক্ষণ আৰু পৰীক্ষণৰ প্রয়োজন যাতে ই শেহতীয়া মেলৱেৰ ভাবুকিৰ বিৰুদ্ধে পর্যাপ্ত সুৰক্ষা প্রদান কৰে। এই উত্তম পদ্ধতিসমূহ অনুসৰণ কৰি সংস্থাসমূহে তেওঁলোকৰ কম্পিউটাৰ ব্যৱস্থাপ্রণালী আৰু তথ্যৰ অখণ্ডতা আৰু গোপনীয়তা নিশ্চিত কৰাত সহায় কৰিব পাৰে।

এণ্টি-ভাইৰাছ চফটৱেৰৰ ফলপ্রসূ ব্যৱস্থাপনা

এটা সংস্থাৰ আই টি আন্তঃগাঁথনিৰ সুৰক্ষা আৰু অখণ্ডতা বজাই ৰখাৰ বাবে এণ্টি-ভাইৰাছ চফটৱেৰৰ ফলপ্রসূ ব্যৱস্থাপনা অতি গুৰুত্বপূর্ণ। এণ্টি-ভাইৰাছ চফটৱেৰ পৰিচালনাৰ বাবে কিছুমান উত্তম পদ্ধতি ইয়াত উল্লেখ হ'ল:

এণ্টি-ভাইৰাছ চফটৱেৰটো নিয়মিতভাৱে আপডেট কৰক যাতে ই শেহতীয়া ভাবুকিসমূহ ধৰা পেলাব পাৰে।

• যিকোনো মেলৱেৰ ধৰা পেলাবলৈ সকলো ডিভাইচ আৰু চিষ্টেমৰ নিয়মীয়া স্কেন সময়সূচী কৰক।

• এণ্টি-ভাইৰাছ চফটৱেৰক স্বয়ংক্রিয়ভাৱে ডিভাইচসমূহ বাস্তৱ সময়ত আপডেট আৰু স্কেন কৰিবলে বিন্যাস কৰক।

• সকলো ডিভাইচ আৰু চিষ্টেমত এণ্টি-ভাইৰাছ কার্য্যকলাপ নিৰীক্ষণ কৰিবলে এটা কেন্দ্রীভূত ব্যৱস্থাপনা ক'ন্সোল ব্যৱহাৰ কৰক।

• সকলো ডিভাইচ আৰু চিষ্টেমত এণ্টি-ভাইৰাছ চফটৱেৰ ইনষ্টল আৰু সক্রিয় কৰাটো নিশ্চিত কৰক।

• সম্ভাব্য মেলৱেৰ ভাবুকি, যেনে ফিছিং ইমেইল বা সন্দেহজনক সংলগ্নসমূহ কেনেকৈ চিনাক্ত আৰু এৰাই চলিব পাৰি সেই বিষয়ে কর্মচাৰীসকলক শিক্ষিত কৰক।

• মেলৱেৰ আক্রমণৰ ক্ষেত্রত তথ্য হেৰুৱা ৰোধ কৰিবলৈ জটিল তথ্যৰ নিয়মীয়া বেকআপ কৰক।

• পেনেট্রেচন টেষ্টিং বা ৰেড টিমিং পৰীক্ষা কৰি এণ্টি-ভাইৰাছ চফটৱেৰৰ ফলপ্রসূতা পৰীক্ষা কৰক।

• সামগ্রিক সুৰক্ষা ভংগীমা বৃদ্ধি কৰিবলৈ অতিৰিক্ত সুৰক্ষা ব্যৱস্থা, যেনে এণ্ডপইণ্ট ধৰা পেলোৱা আৰু সঁহাৰি (EDR) বা ভাবুকি চোৱাংচোৱা ব্যৱহাৰ কৰাৰ কথা চিন্তা কৰক।

• ভাবুকিৰ পৰিৱেশ আৰু ব্যৱসায়িক প্রয়োজনীয়তাৰ পৰিৱর্তন প্রতিফলিত কৰিবলৈ সংস্থাটোৰ এণ্টি-ভাইৰাছ নীতি আৰু পদ্ধতিসমূহ নিয়মিতভাৱে পর্যালোচনা আৰু আপডেট কৰা।



১৩.৮ অধ্যায়টিৰ পৰা আমি কি শিকিলো

• ডিভাইচ সুৰক্ষা নীতি হৈছে এটা প্রতিষ্ঠানৰ ভিতৰত ডিভাইচসমূহৰ সুৰক্ষা নিয়ন্ত্রণ কৰা নির্দেশনা আৰু নিয়মসমূহৰ এটা গোট।

• এটা ডিভাইচ সুৰক্ষা নীতিৰ উপাদানসমূহে পাছৱর্ড ব্যৱস্থাপনা, ডিভাইচ ইনক্রিপষণ, নিয়মীয়া চফটৱেৰ আপডেইটসমূহ, আৰু ডিভাইচ ব্যৱহাৰৰ ওপৰত নিষেধাজ্ঞাসমূহ অন্তর্ভুক্ত কৰা হৈছে।

- বৰ্তমানৰ উত্তম পদ্ধতিসমূহ অন্তর্ভুক্ত কৰিবলে আৰু সম্ভাব্য সুৰক্ষা বিপদসমূহ কম কৰিবলৈ ডিভাইচ সুৰক্ষা নীতি নিয়মিতভাৱে পর্যালোচনা আৰু আপডেইট কৰক।

- মানুহ, প্রক্রিয়া আৰু প্রযুক্তিকে ধৰি সুৰক্ষাৰ সকলো দিশকে সম্বোধন কৰা এটা বিস্তৃত চাইবাৰ সুৰক্ষা কাঠামো বিকশিত আৰু প্রণয়ন কৰা।

- হ'ষ্ট ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছ এটা স্তৰযুক্ত প্রতিৰক্ষা কৌশলৰ জটিল উপাদানসমূহ মেলৱেৰ আৰু অকর্তৃত্বশীল প্রৱেশাধিকাৰৰ পৰা সুৰক্ষিত কৰিবলে, আৰু হ'ষ্ট চিষ্টেমত সুৰক্ষা পৰিঘটনাৰ প্রভাৱ প্রতিৰোধ বা সীমিত কৰিবলে ব্যৱহাৰ কৰা হয়।

- হ'ষ্ট ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছ ৰ ফলপ্রসূ ব্যৱস্থাপনাৰ বাবে নিয়মীয়া আপডেইটসমূহ, পেচসমূহ, পর্যবেক্ষণ, আৰু বিন্যাস টিউনিঙৰ প্রয়োজন হয় অনুকূল পৰিৱেশন আৰু উদীয়মান ভাবুকিসমূহৰ বিৰুদ্ধে সুৰক্ষা সুনিশ্চিত কৰিবলে।



১৩.৭ অধিক জানিবলৈ

1) "COMPUTER SECURITY FUNDAMENTALS" BY CHUCK EASTTOM

2) "NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS" BY WILLIAM STALLINGS

3) "INTRODUCTION TO COMPUTER SECURITY" BY MICHAEL T. GOODRICH AND ROBERTO TAMASSIA

4) "FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER" BY WILLIAM R. CHESWICK AND STEVEN M. BELLOVIN



১৩.৮ অগ্রগতিৰ খতিয়ান

১ নং প্রশ্নৰ উত্তৰ:

A) মিছা

B) মিছা

C) সঁচা

D) মিছা

E) মিছা

F) মিছা

G) মিছা

H) সঁচা



১৩.৯ আৰ্হি প্ৰশ্ন

প্ৰশ্ন ১. বিস্তৃত ডিভাইচ সুৰক্ষা নীতিৰ উপাদানসমূহ আলোচনা কৰক।

প্ৰশ্ন ২. ফায়াৰৱাল কি, আৰু ই এটা নে'টৱৰ্ক বা চিষ্টেম কেনেকৈ সুৰক্ষিত কৰে?

প্ৰশ্ন ৩. বিভিন্ন ধৰণৰ ফায়াৰৱালৰ বিষয়ে আলোচনা কৰা।

প্ৰশ্ন ৪. এণ্টি-ভাইৰাছ চফটৱেৰ কি, আৰু ই এটা চিষ্টেম বা নেটৱৰ্কক সুৰক্ষিত কৰিবলৈ কেনেকৈ কাম কৰে?

প্ৰশ্ন ৫. ফায়াৰৱাল আৰু এণ্টি-ভাইৰাছ চফটৱেৰৰ পাৰ্থক্য কি কি।

*****

অধ্যায় ১৪: ৰাই-ফাই সুৰক্ষা

অধ্যায় গাঁথনি

১৪.১ উদ্দেশ্য
১৪.২ পৰিচয়
১৪.৩ ৰাই-ফাই ব্যৱহাৰৰ সুবিধা
১৪.৪ ৰাই-ফাই ব্যৱহাৰৰ ভাবুকি
১৪.৫ ৰাই-ফাই নেটৱৰ্কৰ প্ৰকাৰ
১৪.৬ ৰাই-ফাইৰ ধৰণ
১৪.৭ ৰাই-ফাই-এ কেনেকৈ কাম কৰে?
১৪.৮ ৰাই-ফাই সুৰক্ষাৰ বাবে গ্ৰহণ কৰিব পৰা পদক্ষেপ
১৪.৯ এণ্ড্ৰইড মোবাইলত ৰাই-ফাই সুৰক্ষাৰ বাবে গ্ৰহণ কৰিব লগা পদক্ষেপ
১৪.১০ IOS মোবাইলত ৰাই-ফাই সুৰক্ষাৰ বাবে গ্ৰহণ কৰিব লগা পদক্ষেপ
১৪.১১ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ
১৪.১২ অগ্ৰগতিৰ খতিয়ান
১৪.১৩ অধিক জানিবলৈ
১৪.১৪ আৰ্হি প্ৰশ্ন

১৪.১ উদ্দেশ্য

এই অধ্যায়টি অধ্যয়ন কৰি আপুনি—

- ৰাই-ফাই ব্যৱহাৰ কৰাৰ সুবিধা আৰু ভাবুকিসমূহৰ বিষয়ে জ্ঞাত হ'ব
- বিভিন্ন ধৰণৰ ৰাই-ফাই নেটৱৰ্ক আৰু ইয়াৰ বৈশিষ্ট্যসমূহ চিনাক্ত কৰিব পাৰিব
- 802.11a/b/g/n/ac/ax কে ধৰি বিভিন্ন ধৰণৰ ৰাই-ফাইৰ মাজত পাৰ্থক্য নিৰ্ণয় কৰিব পাৰিব
- ৰাই-ফাই কেনেকৈ কাম কৰে আৰু ইয়াৰ আঁৰৰ প্ৰযুক্তিৰ বিষয়ে অৱগত হ'ব
- এটা নেটৱৰ্কৰ বাবে ৰাই-ফাই সুৰক্ষা সংহতি কৰাৰ প্ৰক্ৰিয়া জানিব
- এণ্ড্ৰইড মোবাইল ডিভাইচত ৰাই-ফাই সুৰক্ষা কেনেকৈ সংহতি কৰিব লাগে সেই বিষয়ে ব্যাখ্যা কৰিব পাৰিব
- iOS মোবাইল ডিভাইচসমূহত ৰাই-ফাই সুৰক্ষা কেনেকৈ সংহতি কৰিব লাগে সেয়া জ্ঞাত হ'ব।

১৪.২ পৰিচয়

ভৌতিক সংযোগ বা তাঁৰৰ প্ৰয়োজন নোহোৱাকৈ, ৰাই-ফাই ("wireless fidelity"-ৰ সংক্ষিপ্ত ৰূপ) হৈছে এক প্ৰকাৰৰ বেতাঁৰ নেটৱৰ্কিং প্ৰযুক্তি যিয়ে ডিভাইচসমূহক ইণ্টাৰনেট বা অন্য ডিভাইচৰ সৈতে সংযোগ কৰিবলৈ সক্ষম কৰে। ৰাই-ফায়ে ৰেডিঅ' তৰংগ ব্যৱহাৰ কৰি গেজেট আৰু এটা বেতাঁৰ প্ৰৰেশ পইণ্ট (যেনে ৰাউটাৰ)ৰ মাজত তথ্য প্ৰেৰণ কৰে, যিয়ে গেজেটসমূহক ইণ্টাৰনেটৰ সৈতে সংযোগ কৰাৰ বাবে এটা নলীকা হিচাপে কাম কৰে। ৰাই-ফাই সঘনাই ব্যৱহাৰ কৰা হয় কম্পিউটাৰ, স্মাৰ্টফোন, টেবলেট আৰু স্মাৰ্ট ঘৰুৱা সঁজুলিকে ধৰি বিভিন্ন ডিভাইচক ঘৰ, কৰ্মক্ষেত্ৰ, ৰাজহুৱা স্থান আৰু অন্যান্য অঞ্চলত উপলব্ধ ইণ্টাৰনেটৰ সৈতে সংযোগ কৰিবলৈ। ৰাই-ফাই নেটৱৰ্কক অবৈধ প্ৰৰেশ বা ডাটা চুৰিৰ পৰা সুৰক্ষিত কৰিবলৈ বিভিন্ন ধৰণৰ এনক্ৰিপচন কৌশল (encryption techniques) ব্যৱহাৰ কৰিব পাৰি।

১৪.৩ ৰাই-ফাই ব্যৱহাৰ কৰাৰ সুবিধা

ৰাই-ফাই সেৱা ব্যৱহাৰ কৰাৰ কিছুমান সুবিধা তলত উল্লেখ কৰা হ'ল—

- উপযোগিতা: ৰাই-ফাই নেটৱৰ্কৰ কভা�ৰেজ এলেকাৰ ভিতৰত থকা যিকোনো ঠাইৰ পৰা বেতাঁৰ ইণ্টাৰনেটৰ সুবিধা প্ৰদান কৰে।
- নমনীয়তা: ৰাই-ফাই আপোনাক কেবল বা তাঁৰৰ ব্যৱহাৰ নকৰাকৈ অনলাইন সংযোগ বৰ্তাই ৰাখি ঘূৰি ফুৰিবলৈ সক্ষম কৰে।
- বহুতো ডিভাইচৰ বাবে সমৰ্থন: ৰাই-ফাই নেটৱৰ্কে টেবলেট, লেপটপ আৰু স্মাৰ্টফোনকে ধৰি কেইবাটাও ডিভাইচক একেলগে ইণ্টাৰনেটৰ সৈতে সংযোগ কৰিবলৈ সুবিধা প্ৰদান কৰে।
- অৰ্থনৈতিক: ইণ্টাৰনেটৰ সৈতে সংযোগ স্থাপনৰ পৰম্পৰাগত পদ্ধতিতকৈ ৰাই-ফাই প্ৰযুক্তি কম খৰচী।
- সুৰক্ষা: ৰাই-ফাই নেটৱৰ্কে মুক্ত ইণ্টাৰনেটৰ ব্যৱহাৰতকৈ উচ্চ পৰ্যায়ৰ সুৰক্ষা প্ৰদান কৰে কাৰণ ইয়াক পাছৱৰ্ড আৰু এনক্ৰিপচনৰ দ্বাৰা সুৰক্ষিত কৰিব পাৰি।
- দ্ৰুত ইণ্টাৰনেট প্ৰৰেশ: ৰাই-ফাই নেটৱৰ্কে দ্ৰুত ইণ্টাৰনেট প্ৰৰেশ কৰাৰ সুযোগ প্ৰদান কৰিব পাৰে, যাৰ ফলত হাই-ডেফিনিশ্যন ভিডিঅ' ডাউনলোড, গেম খেলা আৰু ষ্ট্ৰীম কৰা সম্ভৱ।
- সৰল ইনষ্টলেচন: বিশেষজ্ঞৰ সহায় অবিহনেও এটা ৰাই-ফাই নেটৱৰ্ক স্থাপন কৰিব পৰা যায়।

- সুগমতা: ব্যৱহাৰকাৰীয়ে সহজেই বিভিন্ন ডিভাইচৰ পৰা ৱাই-ফাই নেটৱৰ্কত প্ৰৱেশ কৰিব পাৰে, যাৰ ফলত তেওঁলোকৰ বাবে ইণ্টাৰনেট প্ৰৱেশ কৰিবলৈ নিজৰ পছন্দৰ ডিভাইচ ব্যৱহাৰ কৰাটো সহজ হৈ পৰে।
- দূ�ৰৱৰ্তী নিয়ন্ত্ৰণ: এটা ৱাই-ফাই সংযোগৰ সৈতে প্ৰিণ্টাৰ, সুৰক্ষা কেমে�ৰা আৰু স্মাৰ্ট ঘৰুৱা সঁজুলিসমূহকে ধৰি বহুতো ডিভাইচ দূৰৱৰ্তীভাৱে চলাব পাৰি।
- সহযোগিতা: ৱাই-ফাই নেটৱৰ্কৰ জৰিয়তে সহযোগিতাৰেও কাম কৰা সম্ভৱপৰ। এক নিৰ্দিষ্ট ৱাই-ফাই ব্যৱহাৰকাৰীসকলে ফাইলসমূহ অংশীদাৰী কৰাটো, প্ৰকল্পসমূহত কাম কৰা আৰু ইজনে সিজনৰ সৈতে যোগাযোগ কৰাটো সহজ কৰি তোলে।

১৪.৪ ৱাই-ফাই ব্যৱহাৰ কৰাৰ ভাবুকি

- সুৰক্ষাৰ বিপদ: ৱাই-ফাই নেটৱৰ্কসমূহ সুৰক্ষা ক্ষেত্ৰত কিছু অসুবিধাৰ সন্মুখীন হ'বলগীয়া হয়; কাৰণ হেকাৰে ইয়াত দ্ৰুতভাৱে প্ৰৱেশ কৰিব পাৰে আৰু পাছৱৰ্ড আৰু ক্ৰেডিট কার্ড নম্বৰৰ দৰে স্পৰ্শকাতৰ তথ্য চুৰি কৰিব পাৰে।
- মেলৱেৰৰ সংক্ৰমণ: অসুৰক্ষিত ৱাই-ফাই নেটৱৰ্কসমূহত অতি সহজে ভাই�ৰাছ, ট্ৰ'জান হৰ্চ আৰু স্পাইৱেৰকে ধৰি মেলৱেৰে সংক্ৰমণ কৰিব পাৰে। ফলস্বৰূপে তেনে ৱাই-ফাই ব্যৱহাৰকাৰীৰ ডিভাইচসমূহক সংক্ৰমণ কৰিব পাৰে আৰু তেওঁলোকৰ সুৰক্ষা বিপন্ন কৰিব পাৰে।
- পৰিচয় চুৰি: চাইবাৰ অপৰাধীয়ে ৱাই-ফাই নেটৱৰ্কত সোমাই ব্যৱহাৰকাৰীৰ ব্যক্তিগত তথ্য, যেনে তেওঁলোকৰ নাম, ঠিকনা আৰু সামাজিক সুৰক্ষা নম্বৰ লাভ কৰিব বা চুৰি কৰিব পাৰে।
- নেটৱৰ্ক কনজেচন: যেতিয়া এটা ৱাই-ফাই নেটৱৰ্ক অভাৰলোড হয়, তেতিয়া তাৰ গতি লেহেমীয়া, ড্ৰপ সংযোগ আৰু অন্য সংযোগ সমস্যাৰ সৃষ্টি কৰিব পাৰে।
- অনুচিত বিষয়বস্তু: ৰাজহুৱা ৱাই-ফাই নেটৱৰ্ক ব্যৱহাৰ কৰি অনুপযুক্ত বিষয়বস্তুত প্ৰৱেশ কৰিলে অন্য ব্যৱহাৰকাৰীক অপমান কৰা হ'ব পাৰে বা হয়তো আইনৰ বিৰুদ্ধে হ'ব পাৰে।
- ৱাই-ফাই জামিং: ইণ্টাৰনেট আক্ৰমণকাৰীয়ে জামিং ডিভাইচ ব্যৱহাৰ কৰি ৱাই- ফাই সংকেতসমূহত হস্তক্ষেপ কৰিব পাৰে। আৰু অই ইণ্টৰানেট ব্যৱহাৰত ব্যাঘাত জন্মাব পাৰে বা ব্যৱহাৰকাৰীসকলক নেটৱৰ্কৰ সৈতে সংযোগ কৰাত বাধা দিব পাৰে।
- ৱাই-ফাই নেটৱৰ্কৰ সহায়ত ব্যৱহাৰকাৰীৰ অৱস্থান আৰু গতিবিধি অনুসৰণ কৰিব পাৰি, যাৰ ফলত তেওঁলোকৰ সুৰক্ষা আৰু গোপনীয়তা বিপন্ন হয়।

১৪.৫ ৰাই-ফাই নেটৱর্কৰ প্রকাৰ

ৰাই-ফাই নেটৱর্কৰ কেইবাটাও প্রকাৰ আছে, সেইবোৰক এনেদৰে তথ্যভুক্ত কৰিব পাৰি—

- ব্যক্তিগত এৰিয়া নেটৱর্ক (PAN): আটাইতকৈ সৰু ধৰণৰ ৰাই-ফাই নেটৱর্ক হৈছে ব্যক্তিগত এৰিয়া নেটৱর্ক (PAN), যিটো সাধাৰণতে কম্পিউটাৰ, টেবলেট আৰু স্মার্টফোনৰ মাজত যোগাযোগৰ বাবে ব্যৱহাৰ কৰা হয়।
- স্থানীয় এলেকা নে'টৱর্ক (LAN): এই ধৰণৰ নেটৱর্কে ডিভাইচসমূহক এটা কেন্দ্রীয় হাবৰ সৈতে সংযোগ কৰে, যেনে এটা ৰাউটাৰ বা অভিগম পইণ্ট, সৰুৰ পৰা মজলীয়া আকাৰৰ উদ্যোগ আৰু ঘৰসমূহত এনে ৰাই-ফাই ব্যৱহাৰ কৰা হয়।
- বহল এৰিয়া নেটৱর্ক (WAN): এটা LAN ৰ এটা বৃহৎ সংস্কৰণ হ'ল WAN। এটা WAN সাধাৰণতে বিভিন্ন ভৌগোলিক অৱস্থানত একাধিক LAN সংযোগ কৰিবলৈ ব্যৱহাৰ কৰা হয়।
- মেছ নেটৱর্ক (Mesh Natwork): এটা ডাঙৰ অঞ্চলত ৰাই-ফাই কভাৰেজ দিবলৈ ইয়াৰ ব্যৱহাৰ কৰা হয়। এই ধৰণৰ নেটৱর্কত বহুতো এক্সেছ পইণ্ট থাকে যিয়ে ইটোৱে সিটোৰ সৈতে সংযোগ স্থাপন কৰা হয়।
- হটস্পট: ৰাই-ফাই হটস্পট হৈছে সাধাৰণতে বিমানবন্দৰ, কফি দোকান আৰু অন্যান্য ৰাজহুৱা স্থানত পোৱা এটা ৰাজহুৱা ৰাই-ফাই নেটৱর্ক।
- ভার্চুৱেল ব্যক্তিগত নে'টৱর্ক (VPN): এটা VPN হৈছে দূৰৈৰ ঠাইৰ পৰা এটা নেটৱার্কলৈ এটা ইনক্রিপ্ট কৰা সংযোগ স্থাপন কৰাৰ এটা নিৰাপদ উপায়।
- এড হক নেটৱর্ক (Ad Hoc Network): এড হক নেটৱর্ক হৈছে এটা কেন্দ্রীয় হাব নথকা পিয়ৰ-টু-পিয়ৰ নেটৱর্ক য'ত ডিভাইচসমূহে ইটোৱে সিটোৰ সৈতে প্রত্যক্ষভাৱে সংযোগ কৰা হয়।

১৪.৬ ৰাই-ফাইৰ ধৰণ

- 802.11a: এই ৰাই-ফাই ষ্টেণ্ডার্ডটোৱে 5GHz ফ্রিকুৱেন্সিত কাম কৰে আৰু সর্বোচ্চ 54Mbps গতিৰে ডাটা ট্রেন্সফাৰ কৰিব পাৰে। সীমিত পৰিসৰ আৰু অধিক খৰচৰ বাবে ইয়াক অন্যান্য ৰাই-ফাই প্রট'কলৰ দৰে সাধাৰণতে ব্যৱহাৰ কৰা নহয়।
- 802.11b: আটাইতকৈ প্রাচীন ৰাই-ফাই ষ্টেণ্ডার্ড হৈছে 802.11b, যিয়ে 2.4GHz ফ্রিকুৱেন্সি ব্যৱহাৰ কৰে। সর্বোচ্চ ডাটা ট্রেন্সফাৰ হাৰ ১১এমবিপিএছৰ সৈতে ইয়াৰ ব্যাপক ব্যৱহাৰ এতিয়া নাই।
- 802.11g: 54Mbps ৰ শীর্ষ ডাটা ট্রেন্সফাৰ ৰেটৰ সৈতে, এই ৰাই-ফাই ষ্টেণ্ডার্ডেও 2.4GHz ত কাম কৰে। ইয়াৰ ব্যৱহাৰকাৰী ভিত্তি বৃহৎ আৰু ই পুৰণি গেজেটৰ সৈতে কাম কৰে।

- 802.11n: এই ৰাই-ফাই ষ্টেণ্ডার্ডটোৱে 2.4GHz আৰু 5GHz দুয়োটা ফ্ৰিকুৱেন্সিত কাম কৰে আৰু ইয়াৰ সৰ্বোচ্চ ডাটা ট্ৰেন্সফাৰ হাৰ 600Mbps। ই আটাইতকৈ বেছি ব্যৱহৃত ৰাই-ফাই ষ্টেণ্ডার্ড আৰু ই উন্নত কভাৰেজ আৰু দ্ৰুত গতি প্ৰদান কৰে।
- 802.11ac: শেহতীয়া ৰাই-ফাই ষ্টেণ্ডার্ড, 802.11ac, 5GHz কম্পাঙ্কত কাম কৰে। 802.11n ৰ তুলনাত ই অধিক কভাৰেজ আৰু অধিক গতি প্ৰদান কৰে, সৰ্বোচ্চ ডাটা ট্ৰেন্সমিছন হাৰ 1Gbps।
- 802.11ax: প্ৰায়ে ৰাই-ফাই 6 বুলি কোৱা হয়, এই ৰাই-ফাই মানদণ্ডৰ সৰ্বোচ্চ ডাটা ট্ৰেন্সফাৰ হাৰ 10Gbps লৈকে আৰু ই 2.4GHz আৰু 5GHz দুয়োটা ফ্ৰিকুৱেন্সিত কাম কৰে। ষ্টেডিয়াম আৰু বিমানবন্দৰৰ দৰে উচ্চ ঘনত্বৰ পৰিৱেশত ই অধিক নেটৱৰ্ক কাৰ্যক্ষমতা প্ৰদান কৰে।



অগ্ৰগতি নিৰীক্ষণ

1. তলৰ পৰা সঠিক উত্তৰ নিৰ্বাচন কৰক:

(a) Wi-Fi ৰ পূৰ্ণ ৰূপ কি?

(i) Wired Fidelity

(ii) Wireless Fidelity

(iii) Wide Fidelity

(iv) ওপৰত উল্লেখ কৰা এটাও নহয়

2. Wi-Fi ডিভাইচসমূহৰ মাজত তথ্য প্ৰেৰণ কৰিবলৈ কিমান ধৰণৰ তৰংগ ব্যৱহাৰ কৰে?

(i) শব্দ তৰংগ (Sound Waves)

(ii) ৰেডিঅ' তৰংগ (Radio Waves)

(iii) পোহৰ তৰংগ (Light Waves)

(iv) ওপৰত উল্লেখ কৰা এটাও নহয়

3. Wi-Fi 802.11n ৰ উচ্চতম ডাটা প্ৰেৰণ গতি কিমান?

(i) 11Mbps

(ii) 54Mbps

(iii) 600Mbps

(iv) 1Gbps

4. একাধিক LAN (Local Area Network) ভিন্ন ভৌগোলিক স্থানত সংযোগ কৰিবলৈ কোন ধৰণৰ Wi-Fi নেটৱৰ্ক ব্যৱহাৰ কৰা হয়?

(i) PAN

(ii) LAN

(iii) WAN

(iv) Mesh Network

5. কম্পিউটাৰ, টেবলেট আৰু স্মাৰ্টফোনৰ মাজত সংযোগ কৰিবলৈ ব্যৱহৃত সৰু Wi-Fi নেটৱৰ্কৰ ধৰণ কি?

(i) PAN

(ii) LAN

(iii) WAN

(iv) Mesh Network

6. কোন Wi-Fi মানদণ্ড (standard) 5GHz ফ্ৰিকুৱেন্সিত কার্য্য কৰে আৰু 1Gbps ডাটা প্ৰেৰণৰ উচ্চতম গতি থাকে?

(i) 802.11a

(ii) 802.11b

(iii) 802.11ac

(iv) 802.11ax

7. কোন ধৰণৰ Wi-Fi নেটৱৰ্কত বহুকেইটা এক্সেছ পইণ্ট (Access Points) থাকে, যিয়ে একে অন্যৰ লগত সংযোগ স্থাপন কৰি বৃহৎ অঞ্চলটোত Wi-Fi কভা�ৰেজ প্ৰদান কৰে?

(i) PAN

(ii) LAN

(iii) WAN

(iv) Mesh Network

8. Wi-Fi ব্যৱহাৰৰ সুবিধা কি?

(i) দ্ৰুত ইণ্টাৰনেট এক্সেছ (Quick internet access)

(ii) ৰিম'ট কণ্ট্ৰ'ল (Remote control)

(iii) সুৰক্ষা (Security)

(iv) ওপৰৰ সকলো (All of the above)

১৪.৭ ৰাই-ফাই কেনেকৈ কাম কৰে

ৰাই-ফাইৰ সহায়ত ডিভাইচসমূহে ইটোৱে সিটোৰ সৈতে বেতাঁৰভাৱে আৰু ভৌতিক কার্ডৰ ব্যৱহাৰ নকৰাকৈ সংযোগ কৰিব পাৰে। ৰাই-ফাই এই মৌলিক নীতিৰ ওপৰত কাম কৰে যে ৰেডিঅ' তৰংগৰ সহায়ত তথ্য প্ৰেৰণ কৰা হয়।

আপোনাৰ ডিভাইচে ৰাউটাৰলৈ এটা সংকেত প্ৰেৰণ কৰে, যি নেটৱৰ্কৰ স্নায়ু কেন্দ্ৰ হিচাপে কাম কৰে, যেতিয়া আপুনি এটা ৰাই-ফাই নেটৱৰ্কত যোগদান কৰে। অন্য ডিভাইচসমূহে ল'ব পৰা এটা ৰেডিঅ' সংকেত নিৰ্গত হয় যেতিয়া ৰাউটাৰে এই সংকেত পায়। এই ৰেডিঅ' সংকেত গঠন কৰা বিদ্যুৎচুম্বকীয় তৰংগবোৰ এটা নিৰ্দিষ্ট কম্পাঙ্কত প্ৰেৰণ কৰা হয়।

আপুনি ইণ্টাৰনেট বা অন্য নে'টৱৰ্ক সম্পদসমূহ ব্যৱহাৰ কৰিব পাৰিব কাৰণ আপোনাৰ ডিভাইচে এই ৰেডিঅ' সংকেত গ্ৰহণ কৰিবলৈ সক্ষম আৰু ইয়াক ডিকোড কৰে। ৰাই-ফাই সংকেত দেৱাল আৰু অন্যান্য বাধাৰ মাজেৰে পাৰ হ'ব পাৰে, কিন্তু আপোনাৰ ডিভাইচ আৰু ৰাউটাৰৰ মাজৰ দূৰত্বৰ লগতে বাটত থকা যিকোনো ভৌতিক বাধাই ইয়াৰ শক্তি আৰু গুণগত মানৰ ওপৰত প্ৰভাৱ পেলাব পাৰে।

ৰাই-ফাই নেটৱৰ্কসমূহে ব্যৱহাৰ কৰা কম্পাঙ্ক ব্যৱহাৰ কৰা বিশেষ প্ৰটোকলৰ ওপৰত ভিত্তি কৰি ভিন্ন হয়। ৰাই-ফাই কম্পাঙ্ক দুটা হৈছে ২.৪ GHz আৰু ৫ GHz। ২.৪ GHz পুৰণি ডিভাইচসমূহত আৰু ৫ GHz নতুন, উচ্চমানৰ ডিভাইচসমূহত ব্যৱহাৰ কৰা হয়।

১৪.৮ ৰাই-ফাই সুৰক্ষাৰ বাবে গ্ৰহণ কৰিব পৰা পদক্ষেপ

ৰাই-ফাই সুৰক্ষাৰ বাবে গ্ৰহণ কৰিবলগীয়া মূল পদক্ষেপসমূহ এনেধৰণৰ—

a) অবিকল্পিত SSID আৰু পাচৱৰ্ড পৰিৱৰ্তন কৰক: ৰাউটাৰৰ অবিকল্পিত নে'টৱৰ্ক নাম (SSID) আৰু পাচৱৰ্ড পৰিবৰ্তন কৰাটো নিশ্চিত কৰক। ই আপোনাৰ নে'টৱৰ্কলৈ অবৈধ অভিগম প্ৰতিৰোধ কৰাত সহায় কৰিব।

b) WPA2 এনক্ৰিপচন ব্যৱহাৰ কৰক: নিশ্চিত কৰক যে WPA2 আপোনাৰ Wi-Fi ত সামৰ্থ্যবান কৰা হৈছে (Wi-Fi সুৰক্ষিত অভিগম 2)। ই শক্তিশালী এনক্ৰিপচন প্ৰদান কৰে আৰু অকৰ্তৃত্বশীল ব্যক্তিসকলক আপোনাৰ তথ্য সংগ্ৰহ কৰাত বাধা দিয়াত সহায় কৰে।

c) এটা শক্তিশালী পাচৱৰ্ড ব্যৱহাৰ কৰক: নিশ্চিত কৰক যে আপুনি আপোনাৰ Wi-Fi নে'টৱৰ্কৰ বাবে সংহতি কৰা পাচৱৰ্ড সুৰক্ষিত। চিহ্ন, সংখ্যা, আৰু ডাঙৰ আৰু সৰু আখৰৰ মিশ্ৰণ ব্যৱহাৰ কৰক।

d) আপোনাৰ ৰাউটাৰ ফাৰ্মৱেৰ আপডেইট কৰক: নিশ্চিত কৰক যে আপোনাৰ ৰাউটাৰত ফাৰ্মৱেৰ আপডেইট। এইটো কৰি, আপুনি নিশ্চিত হ'ব পাৰে যে আপোনাৰ ৰাউটাৰ জনা দুৰ্বলতাৰ বিৰুদ্ধে সুৰক্ষিত।

e) WPS বন্ধ কৰক: আপোনাৰ ৰাউটাৰত, ৰাই-ফাই সুৰক্ষিত প্ৰতিষ্ঠা (WPS) নিষ্ক্ৰিয় কৰক। এই কাৰ্য্যকৰীতাৰ জনা ত্ৰুটিসমূহৰ সুবিধা হেকাৰে ল'ব পাৰে।

f) দূৰৱৰ্তী প্ৰশাসন নিষ্ক্ৰিয় কৰক: আপোনাৰ ৰাউটাৰত, দূৰৱৰ্তী প্ৰশাসন নিষ্ক্ৰিয় কৰক। ই অকৰ্তৃত্বশীল ব্যক্তিসকলক আপোনাৰ ৰাউটাৰত দূৰৱৰ্তীভাৱে অভিগম কৰা বন্ধ কৰিব।

g) এটা ফায়াৰৱাল ব্যৱহাৰ কৰক: নিশ্চিত কৰক যে আপোনাৰ ৰাউটাৰত এটা অন্তর্নির্মিত ফায়াৰৱাল আছে। ই আপোনাৰ নে'টৱর্ক অকর্তৃত্বশীল অভিগমৰ পৰা সুৰক্ষিত কৰাত সহায় কৰিব।

h) আপোনাৰ নে'টৱর্ক নিৰীক্ষণ কৰক: আপোনাৰ নে'টৱর্কত যিকোনো অদ্ভুত আচৰণৰ বাবে চকু ৰাখক। ইয়াৰ দ্বাৰা আপুনি যিকোনো সম্ভাব্য সুৰক্ষা ভাবুকি চিনাক্ত কৰিব পাৰিব আৰু প্রয়োজনীয় সাৱধানতা অৱলম্বন কৰিব পাৰিব।

এই মূল পদক্ষেপসমূহ অনুসৰণ কৰি, আপুনি এটা সুৰক্ষিত ৰাই-ফাই নেটৱর্ক সৃষ্টি কৰিব পাৰে যিয়ে আপোনাৰ ডাটা আৰু ডিভাইচসমূহক চাইবাৰ ভাবুকিৰ পৰা সুৰক্ষিত কৰে।

১৪.৯ এণ্ড্রইড মোবাইলত ৰাই-ফাই সুৰক্ষাৰ বাবে গ্রহণ কৰিব লগা পদক্ষেপ

এণ্ড্রইড মোবাইলত ৰাই-ফাই ছিকিউৰিটি কেনেকৈ ছেট আপ কৰিব পাৰি তাৰ পদক্ষেপ তলত দিয়া হ'ল:

- আপোনাৰ Android ডিভাইচৰ ছেটিংছ মেনু খোলক।
- "Wi-Fi" বিকল্পত টেপ কৰক।
- আপুনি সুৰক্ষিত কৰিব বিচৰা ৰাই-ফাই নেটৱর্ক বিচাৰি উলিয়াওক আৰু ইয়াত টেপ কৰক।
- "উন্নত" বা "নেটৱর্ক" ছেটিংছত টেপ কৰক।
- আপুনি ব্যৱহাৰ কৰিব বিচৰা সুৰক্ষা ধৰণ নির্বাচন কৰক। উপলব্ধ বিকল্পসমূহ আপুনি সংযোগ কৰা নে'টৱর্কৰ ওপৰত নির্ভৰ কৰিব পাৰে।
- নে'টৱর্কৰ বাবে পাচৱর্ড বা অন্য সুৰক্ষা প্রমাণপত্রসমূহ সুমুৱাওক।
- আপোনাৰ ছেটিংছ সংৰক্ষণ কৰক।
- আপোনাৰ ব্যক্তিগত তথ্যৰ অকর্তৃত্বশীল প্রৱেশ ৰোধ কৰিবলৈ আপোনাৰ ৰাই-ফাই সংযোগসমূহ সুৰক্ষিত কৰাটো গুৰুত্বপূর্ণ।

১৪.১০ IOS মোবাইলত ৰাই-ফাই সুৰক্ষাৰ বাবে গ্রহণ কৰিব লগা পদক্ষেপ

আপোনাৰ iOS মোবাইল ডিভাইচত Wi-Fi সুৰক্ষা সংহত কৰিবলৈ, এই পদক্ষেপসমূহ অনুসৰণ কৰক:

1. আপোনাৰ ডিভাইচত "ছেটিংছ" এপটো খোলক।
2. "ৰাই-ফাই"ত টেপ কৰক।

3. আপুনি সুৰক্ষিত কৰিব বিচৰা Wi-Fi নে'টৱৰ্ক বিচাৰি উলিয়াওক আৰু তথ্য আইকন (i) ত টেপ কৰক।

4. "DNS বিন্যাস কৰক" ত টেপ কৰক।

5. "স্বয়ংক্রিয়" বাছক।

6. ৰাই-ফাই ছেটিংছ পৰ্দালৈ উভতি যাওক আৰু একেটা নেটৱৰ্কতে টেপ কৰক।

7. Wi-Fi নে'টৱৰ্ক পাছৱৰ্ড সুমুৱাওক, যদি প্রয়োজন হয়।

8. "সুৰক্ষা"ত টেপ কৰক আৰু উপযুক্ত সুৰক্ষা ধৰণ নির্বাচন কৰক (WPA2 উপদেশিত)।

9. সুৰক্ষা কি/পাছফ্রেজ সুমুৱাওক আৰু "যোগদান কৰক" টেপ কৰক।

10. আপোনাৰ iOS ডিভাইচ এতিয়া নির্বাচিত সুৰক্ষা ধৰণৰ সৈতে Wi-Fi নেটৱৰ্কৰ সৈতে সংযুক্ত হ'ব।

টোকা: সর্বাধিক সুৰক্ষা নিশ্চিত কৰিবলৈ আপোনাৰ ৰাই-ফাই নেটৱৰ্কৰ বাবে এটা শক্তিশালী আৰু অনন্য পাছৱৰ্ড ব্যৱহাৰ কৰাটো গুৰুত্বপূর্ণ।



১৪.১১ অধ্যায়টিৰ পৰা আমি কি শিকিলোঁ

- ৰাই-ফাই হৈছে এটা বেতাঁৰ নেটৱর্কিং প্রযুক্তি যিয়ে ডিভাইচসমূহক ভৌতিক সংযোগ বা তাঁৰ অবিহনে ইণ্টাৰনেট বা অন্য ডিভাইচৰ সৈতে সংযোগ কৰিবলৈ অনুমতি দিয়ে।
- ৰাই-ফায়ে ডিভাইচ আৰু বেতাঁৰ অভিগম পইণ্ট, যেনে ৰাউটাৰৰ মাজত তথ্য প্রেৰণ কৰিবলৈ ৰেডিঅ' তৰংগ ব্যৱহাৰ কৰে।
- ৰাই-ফাই কেইবাটাও সুবিধা প্রদান কৰে, য'ত আছে উপযোগিতা, নমনীয়তা, একাধিক ডিভাইচৰ বাবে সমর্থন আৰু দ্রুত ইণ্টাৰনেট অভিগম।
- ৰাই-ফাই নেটৱৰ্কসমূহ পাছৱৰ্ড আৰু এনক্রিপচনৰ দ্বাৰা সুৰক্ষিত কৰিব পাৰি, যিয়ে মুক্ত ইণ্টাৰনেট প্রৱেশতকৈ উচ্চ পর্যায়ৰ সুৰক্ষা প্রদান কৰে।
- কিন্তু ৰাই-ফাই নেটৱৰ্কসমূহ সুৰক্ষাৰ বিপদ, মেলৱেৰৰ সংক্রমণ, পৰিচয় চুৰি, নেটৱৰ্কৰ ভিৰ, আৰু ৰাই-ফাই জামিং আদিৰ বাবেও সহজলভ্য।
- ব্যক্তিগত এৰিয়া নেটৱৰ্ক (PAN), স্থানীয় এলেকা নেটৱৰ্ক (LAN), বহল এৰিয়া নেটৱৰ্ক (WAN), মেছ নেটৱৰ্ক, হটস্পট, ভার্চুৱেল প্রাইভেট নেটৱৰ্ক (VPN), আৰু এড হক নেটৱৰ্ক আদি বিভিন্ন ধৰণৰ ৰাই-ফাই নেটৱৰ্ক আছে।
- ৰাই-ফাইৰ বিভিন্ন ধৰণৰ, যেনে 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax (Wi-Fi 6)।

- ৱাই-ফাই আমাৰ দৈনন্দিন জীৱনৰ এক অপৰিহার্য অংগ হৈ পৰিছে আৰু ঘৰ, কর্মস্থলী, ৰাজহুৱা স্থান, আৰু অন্যান্য অঞ্চলত ব্যৱহাৰ কৰা হয়।
- ৱাই-ফাই ব্যৱহাৰকাৰীসকলক কম্পিউটাৰ, স্মার্টফোন, টেবলেট আৰু স্মার্ট ঘৰুৱা সঁজুলিকে ধৰি বিভিন্ন ডিভাইচৰ পৰা ইণ্টাৰনেট ব্যৱহাৰ কৰিবলৈ সক্ষম কৰে।
- বিশেষজ্ঞৰ সহায় অবিহনে ৱাই-ফাই নেটৱর্ক স্থাপন কৰিব পাৰি, যাৰ ফলত ব্যৱহাৰকাৰীয়ে ইয়াক ইনষ্টল আৰু ব্যৱহাৰ কৰাটো সহজ হৈ পৰে।

১৪.১২ অগ্রগতিৰ খতিয়ান

প্রশ্ন নং ১ৰ উত্তৰ: ১. (ii) ২. (ii) ৩. (iii) ৪. (iii) ৫.(i) ৬. (iii) ৭.(iv) ৮. (iv)

১৪.১৩ অধিক জানিবলৈ

1) Cyber Crime Impact in the New Millennium, by R. C Mishra, Auther Press. Edition 2010.

2) Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)

3) Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson, 13th November, 2001)

4) Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.

5) Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.

6) Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.

7) Fundamentals of Network Security by E. Maiwald, McGraw Hill.

১৪.১৪ আৰ্হি প্রশ্ন

প্রশ্ন ১: ৱাই-ফাই কি আৰু ই কেনেকৈ কাম কৰে ?

প্রশ্ন ২: ৱাই-ফাই ব্যৱহাৰ কৰাৰ সুবিধা কি কি ?

প্ৰশ্ন ৩: অবৈধ প্ৰৱেশ বা ডাটা চুৰিৰ বিৰুদ্ধে ৰাই-ফাই নেটৱৰ্ক কেনেকৈ সুৰক্ষিত কৰিব পাৰি?

প্ৰশ্ন ৪: ৰাই-ফাই নেটৱৰ্কে একে সময়তে একাধিক ডিভাইচ সমৰ্থন কৰিব পাৰেনে? যদি হয় তেন্তে কিমান?

প্ৰশ্ন ৫: ৰাই-ফাই প্ৰযুক্তি ব্যৱহাৰৰ অৰ্থনৈতিক লাভ কি?

প্ৰশ্ন ৬: ৰাই-ফাই নেটৱৰ্কে মুক্ত ইণ্টাৰনেটৰ ব্যৱহাৰতকৈ উচ্চ পৰ্যায়ৰ সুৰক্ষা কেনেকৈ প্ৰদান কৰিব পাৰে?

প্ৰশ্ন ৭: স্মাৰ্ট ঘৰুৱা সঁজুলিত ৰাই-ফাই নেটৱৰ্কৰ প্ৰয়োগ কি কি?

প্ৰশ্ন ৮: ৰাই-ফাই ব্যৱহাৰৰ ভাবুকি কি কি, আৰু ইয়াক কেনেকৈ প্ৰতিৰোধ কৰিব পাৰি?

প্ৰশ্ন ৯: ৰাই-ফাই নেটৱৰ্ক কেনেকৈ জাম হ'ব পাৰে, আৰু ইয়াৰ পৰিণতি কি?

প্ৰশ্ন ১০: ৰাই-ফাই নেটৱৰ্কৰ বিভিন্ন প্ৰকাৰ কি, আৰু ইটোৱে সিটোৰ পৰা কেনেকৈ পৃথক?

প্ৰশ্ন ১১: ভিপিএন কি, আৰু ই কেনেকৈ সুৰক্ষিত স্থাপন কৰাত সহায় কৰিব পাৰে ৰাই-ফাই সংযোগ?

প্ৰশ্ন ১২: এড হক নেটৱৰ্ক কি, আৰু ই অন্য ৰাই-ফাই নেটৱৰ্কৰ পৰা কেনেকৈ পৃথক?

প্ৰশ্ন ১৩: ৮০২.১১a ৰাই-ফাই মানদণ্ড কি, আৰু ই অন্য মানদণ্ডৰ পৰা কেনেকৈ পৃথক?

প্ৰশ্ন ১৪: ৮০২.১১ac ৰাই-ফাই ষ্টেণ্ডার্ড ব্যৱহাৰ কৰাৰ সুবিধা কি?

প্ৰশ্ন ১৫: ৰাই-ফাই ৬ কি, আৰু ই অন্যান্য ৰাই-ফাই মানদণ্ডৰ পৰা কেনেকৈ পৃথক?

****