डिजिटल सुरक्षा और बचाओ

Samhita CGF

कार्यक्रम परिचय

सार्वजनिक और निजी सेवाओं के डिजिटलीकरण और डिजिटल संचार के आगमन, विशेष रूप से सोशल मीडिया के उपयोगकर्ताओं की वित्तीय अखंडता और व्यक्तिगत गोपनीयता के लिए महत्वपूर्ण निहितार्थ हैं। अधिकतम लाभ प्राप्त करने के लिए डिजिटल साक्षरता का एक इष्टतम स्तर साइबर अपराध और डिजिटल धोखाधड़ी से उत्पन्न डिजिटल सुरक्षा के नुकसान की पहचान करने और उससे बचने के लिए आवश्यक हो जाता है।

इंटरनेट और स्मार्टफोन की बढ़ती पहुंच ने हमें ऑनलाइन धोखाधड़ी के प्रति संवेदनशील बना दिया है और हमारे डेटा के संभावित ऑनलाइन खतरों के कारण हमारी सुरक्षा को खतरे में डाल दिया है। हमें इन खतरों से खुद को बचाने की जरूरत है जो हमारी व्यक्तिगत जानकारी को खतरे में डालते हैं और यहां तक कि हमारे मानसिक स्वास्थ्य को भी प्रभावित करते हैं।

इस कार्यक्रम में हम निम्नलिखित के बारे में जानेंगे:

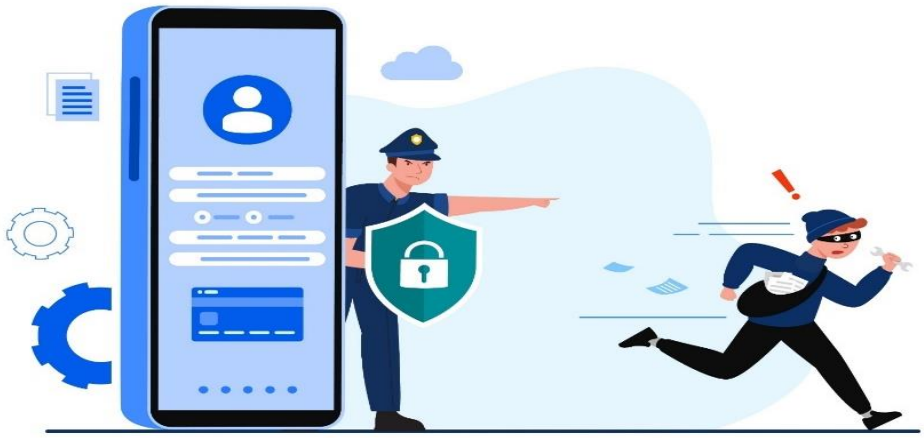
- डिजिटल सुरक्षा और बचाओ क्या है?
- वित्तीय घोटाले और उनकी रोकथाम
- सोशल मीडिया प्लेटफॉर्म, घोटाले और शिष्टाचार
- पहचान की चोरी से खुद को सुरक्षित रखना
- इंटरनेट स्मार्ट होना
- डिजिटल अधिकार, कानून और निवारण तंत्र

इस पुस्तिका में ऑनलाइन कार्यक्रम में प्रमुख अवधारणाओं की सीख को दोहराने का प्रयास किया गया है। 20 प्रायोगिक गतिविधियों की सूची अंत में दी गई है, हम आपसे आग्रह करते हैं कि 6 मॉड्यूल से सीखने को सुदृढ़ करने के लिए उन्हें अभ्यास कार्य के रूप में करें.

विषयसूची

मॉड्यूल 1

डिजिटल सुरक्षा और बचाओ का परिचय



डिजिटल सुरक्षा और बचाओ क्या है?

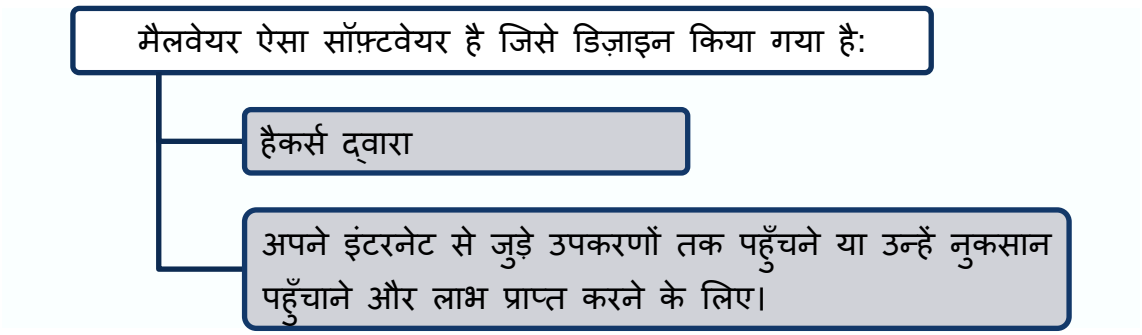
डिजिटल सेफ्टी एंड सिक्योरिटी का तात्पर्य इंटरनेट से जुड़े उपकरणों जैसे कंप्यूटर, मोबाइल डिवाइस, टैबलेट आदि को घुसपैठियों या हैकर्स से बचाना है।

फ़िशिंग

फ़िशिंग एक डिजिटल माध्यम से किया गया एक हमला है जो क्रेडिट कार्ड नंबर, बैंक जानकारी आदि जैसी व्यक्तिगत जानकारी प्रकट करने के प्रलोभन का उपयोग करके किसी व्यक्ति के पैसे या पहचान को चुराने की कोशिश करता है।

ई-मेल में वायरस हो सकते हैं जो आपके डिवाइस को नुकसान पहुंचा सकते हैं या आपके संवेदनशील डेटा जैसे कार्ड विवरण, पासवर्ड आदि को चुरा सकते हैं। इसे **फ़िशिंग** के रूप में जाना जाता है जो कई प्रकार के साइबर हमलों में से एक है।

मैलवेयर :



डिजिटल सुरक्षा और बचाओ सुनिश्चित करना

स्पैम मेल या किसी अज्ञात प्रेषक के मेल पर कभी भी क्लिक न करें

अपने व्यक्तिगत और व्यावसायिक डेटा को हमेशा सुरक्षित रखें

अपने डिवाइस को एंटी वायरस सॉफ्टवेयर्स से सुरक्षित करें

यदि आपको साइबर धोखाधड़ी का संदेह है, तो तुरंत संबंधित संगठन को कॉल करें, शिकायत दर्ज करें और उन्हें आपके खाते की सुरक्षा सुनिश्चित करने के लिए सर्वोत्तम कार्रवाई करने के लिए कहें।

सरकार में शिकायत दर्ज करें। ऑफ इंडिया ऑनलाइन साइबर क्राइम सेल

डिजिटल सुरक्षा और बचाओ के लाभ

- 24*7 सुरक्षित और सुरक्षित बैंकिंग अनुभव
- आपकी शाखा में आए बिना झंझट-मुक्त और तुरंत लेनदेन
- आर्थिक हानि से बचाता है
- फिशिंग, पासवर्ड अटैक आदि जैसे साइबर हमलों से सुरक्षा
- लेन-देन के लिए एक सुरक्षित/निजी विंडो प्रदान करता है

साइबर सुरक्षा और गोपनीयता मिथक

क्र.सं.	मिथक	असलियत
1.	सशक्त पासवर्ड हमारे उपकरणों और उनमें संग्रहीत डेटा की सुरक्षा करते हैं।	मजबूत पासवर्ड के साथ, हमें टू-फैक्टर ऑथेंटिकेशन और डेटा मॉनिटरिंग की जरूरत है।
2.	हैकर्स या साइबर अपराधी छोटे व्यवसायों और कर्मचारियों, गृहिणियों, स्वरोजगार आदि जैसे लोगों पर हमला नहीं करते हैं	उन्नत सुरक्षा समाधान और जागरूकता की कमी के कारण, ऐसे छोटे व्यवसाय और लोग हैकर्स या साइबर अपराधियों के लिए आसान लक्ष्य होते हैं।
3.	एंटी-वायरस/एंटी-मैलवेयर सॉफ्टवेयर हमारे उपकरणों या डेटा को सुरक्षित रखने के लिए पर्याप्त है।	एंटी-वायरस/एंटी-मैलवेयर सॉफ़्टवेयर केवल डिवाइस को वायरस और मैलवेयर से सुरक्षित करेगा लेकिन साइबर अपराधों के कई अन्य माध्यम हैं जैसे जानकारी प्राप्त करने के लिए फर्जी कॉल
4.	हमें केवल अपने उपकरणों को हैकर्स से सुरक्षित रखने की आवश्यकता है.	कोई भी आंतरिक व्यक्ति/कर्मचारी जानबूझकर या गलती से जानकारी लीक कर सकता है.
5.	साइबर सुरक्षा के लिए केवल इंटरनेट सेवा प्रदाता का आईटी विभाग ही जिम्मेदार है.	यह प्रत्येक व्यक्ति की सामाजिक जिम्मेदारी है कि वह अपनी व्यक्तिगत या व्यावसायिक जानकारी और डिवाइस को हैकर्स के साथ-साथ अपने आसपास के घुसपैठियों से सुरक्षित रखे।
6.	यदि डाउनलोड किया जाने वाला ऐप ऐप स्टोर से है तो यह सुरक्षित है.	ऐप स्टोर में ऐप्स को वायरस/मैलवेयर और गोपनीयता नीति के खिलाफ परीक्षण और सत्यापन से गुजरना होगा.
7.	कोई भी पासवर्ड से सुरक्षित वाई-फाई सुरक्षित है।	पासवर्ड के साथ भी कोई सार्वजनिक वाई-फाई कनेक्शन आपके डिवाइस के लिए खतरा हो सकता है। सार्वजनिक वाई-फाई कनेक्शन के माध्यम से कभी भी कोई गोपनीय जानकारी या दस्तावेज़ साझा न करें
8.	अपनी खुद की डिवाइस लाओ या BYOD काम पर इस्तेमाल के लिए सुरक्षित है	इंटरनेट से जुड़ा कोई भी उपकरण डिजिटल खतरों से ग्रस्त है.
9.	HTTPS वेबसाइट भरोसेमंद हैं और इन्हें हैक नहीं किया जा सकता है	हैकर्स HTTPS एन्क्रिप्शन को बायपास कर सकते हैं; इसलिए, केवल विश्वसनीय HTTPS वेबसाइटों का उपयोग करें उदा। बैंक द्वारा साझा की गई आपकी बैंक वेबसाइट.
10.	किसी भी उल्लंघन के खिलाफ 100% साइबर सुरक्षा प्राप्त करने योग्य है।	हर दिन एक नया खतरा विकसित होता है। 100% साइबर सुरक्षा हासिल नहीं की जा सकती.

इन सर्वोत्तम प्रथाओं का पालन करके आप साइबर अपराध के शिकार होने से बच सकते हैं:

✓ ब्राउज़र का उपयोग करते समय हमेशा गुप्त मोड का उपयोग करें।	✗ ब्राउजर पर कभी भी क्रेडेंशियल सेव न करें.	✗ कभी भी थर्ड पार्टी लिंक से ऐप डाउनलोड न करें.
✗ किसी भी असुरक्षित वेबसाइट/ऐप पर व्यक्तिगत जानकारी साझा न करें.	✓ अपने एंटीवायरस को अपडेट रखें।	✗ वायरस स्कैन किए बिना कभी भी कोई फाइल डाउनलोड न करें.
✓ अपने डेटा का बैकअप रखें।	✗ अपने डिवाइस को कभी भी उपेक्षित न छोड़ें।	✗ अपना पासवर्ड कभी साझा न करें।
	✓ हमेशा टू-फैक्टर ऑथेंटिकेशन का इस्तेमाल करें.	

पासवर्डों

एक पासवर्ड वर्णों की एक स्ट्रिंग है जो कंप्यूटर सिस्टम या सेवा तक पहुंच की अनुमति देता है।

एक अद्वितीय पासवर्ड बनाने के लिए

- अनुक्रमिक अक्षरों या संख्याओं से बचें
- लंबे पासवर्ड बनाएं

अलग-अलग ऐप्स के लिए अलग-अलग पासवर्ड का इस्तेमाल करें और अपना पासवर्ड बार-बार बदलते रहें जानकारी तक अनधिकृत पहुंच के परिणामस्वरूप पहचान की चोरी, वित्तीय नुकसान, डिजिटल घोटालों की बढ़ती भेद्यता, या उत्पीड़न सहित जोखिम हो सकते हैं।

वन-टाइम पासवर्ड (OTP):

ओटीपी वन-टाइम पासवर्ड हैं, जो ऑनलाइन वित्तीय लेनदेन के लिए सुरक्षा प्रदान करते हैं

अपने ओटीपी को गोपनीय रखने के लिए

- अपना ओटीपी कभी साझा न करें।
- हमेशा आधिकारिक वेबसाइटों के माध्यम से लॉग इन करें.
- कभी भी अनजान ऐप डाउनलोड न करें।
- बैंक अधिकारी बनकर और आपसे अपना खाता विवरण सत्यापित करने के लिए कहकर।

- एसएमएस या व्हाट्सएप के माध्यम से लिंक भेजकर और जब आप उन्हें क्लिक करते हैं तो मैलवेयर फैलाते हैं।
- आपको एक स्क्रीन-शेयरिंग ऐप डाउनलोड करने के लिए कहकर जिससे आपके डेटा तक दूरस्थ पहुंच प्राप्त हो सके.

क्रेडिट/डेबिट कार्ड धोखाधड़ी:

क्रेडिट/डेबिट कार्ड धोखाधड़ी तब होती है जब कोई आपकी जानकारी के बिना वित्तीय लेन-देन के लिए अवैध रूप से आपके क्रेडिट कार्ड की जानकारी का उपयोग करता है।

डेबिट/क्रेडिट कार्ड धोखाधड़ी से सुरक्षित रहना:

- अपना कार्ड हमेशा अपने पास रखें.
- अपना पिन नियमित रूप से बदलें.
- अपना पिन किसी के साथ साझा न करें।
- अपने मासिक क्रेडिट कार्ड स्टेटमेंट को ध्यान से देखें
- अज्ञात वेबसाइटों या ऐप्स पर अपने कार्ड का उपयोग करने से बचें।
- संदिग्ध लिंक पर क्लिक न करें.
- आपका कार्ड चोरी या खो जाने की स्थिति में तुरंत अपने बैंक को सूचित करें

दस्तावेज़ धोखाधड़ी पूर्वक्रय

- जालसाज विभिन्न कारणों से आधार और पैन कार्ड जैसे जाली दस्तावेज बनाते हैं। वे नकली दस्तावेजों का उपयोग करते हैं:
- एक नया बैंक खाता खोलें
- ऋण के लिए आवेदन करें

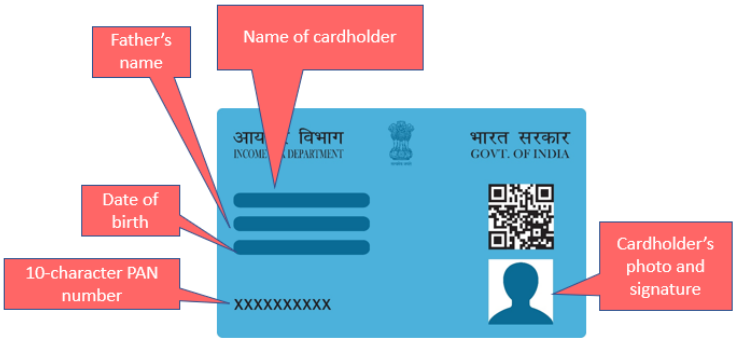
- संपत्ति खरीदें
- फ़ाइल आयकर रिटर्न/बीमा फाइलिंग

- **आधार कार्ड** इतना महत्वपूर्ण है क्योंकि यह:
- प्रत्येक निवासी भारतीय के लिए पहचान को सक्षम बनाता है.
- पते के प्रमाण के रूप में कार्य करता है.
- पहचान के प्रमाण के रूप में कार्य करता है.

- धारकों को सरकारी सब्सिडी का लाभ उठाने में सक्षम बनाता है।
- बैंक खाता खोलते समय पहचान के लिए इस्तेमाल किया जा सकता है।
- नौकरियों के लिए आवेदन करते समय पहचान के लिए इस्तेमाल किया जा सकता है।

निम्नलिखित में से कोई भी लेनदेन करने के लिए हमें पैन कार्ड की आवश्यकता होती है:

- बैंक खाता खोलना.
- टैक्स रिटर्न दाखिल करना।
- नए ऋण के लिए आवेदन करना।
- नई संपत्ति खरीदना या बेचना.
- डेबिट/क्रेडिट कार्ड प्राप्त करना।
- बीमा प्रीमियम का भुगतान करना



आधार/पैन कार्ड धोखाधड़ी से सुरक्षित रहने के लिए

- आकस्मिक लेन-देन के लिए अपने आधार या पैन कार्ड का उपयोग न करें।
- आधार या पैन कार्ड विवरण के साथ साझा न करें।
- उपयोग और उपयोग की तारीख के विशिष्ट कारण के साथ अपने आधार या पैन कार्ड की केवल हस्ताक्षरित फोटोकॉपी जमा करने का प्रयास करें.
- ऑनलाइन पोर्टल पर अपना पूरा नाम और जन्म तिथि दर्ज न करें।

महत्वपूर्ण दस्तावेजों को सुरक्षित रखना

डिजिलॉकर एक डिजिटल लॉकर है, जो भारत सरकार द्वारा प्रदान की जाने वाली एक सुविधा है, जो आपको आधार, पैन, ड्राइविंग लाइसेंस, पासपोर्ट, मार्क शीट, चुनावी मतदाता पहचान पत्र आदि जैसे आधिकारिक दस्तावेजों की स्कैन की गई प्रतियों को संग्रहीत करने में सक्षम बनाती है। आप इन तक पहुंच सकते हैं। दस्तावेज़ कहीं भी, कभी भी।

डिजिलॉकर के फायदे

संदर्भ पढ़ना:

- साइबर स्वच्छता केंद्र : https://www.csk.gov.in/
- भारत में साइबर अपराधों पर पूरी गाइड: https://indiaforensic.com/compcrime.htm
- जी 20 प्रेसीडेंसी की भारत की साइबर सुरक्षा प्राथमिकताएं: https://www.orfonline.org/expert-speak/indias-cybersecurity-priorities-for-g20-presidency/
- भारतीय साइबर अपराध समन्वय केंद्र के बारे में विवरण: https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C- योजना

मॉड्यूल 2

वित्तीय घोटाले और उनकी रोकथाम

वित्तीय नुकसान को रोकने के लिए अज्ञात नंबरों और अंतर्राष्ट्रीय कॉलों से कॉल प्रबंधित करना:

वन-रिंग स्कैम तब होता है जब कॉलर कॉल करता है और एक रिंग के बाद फोन हैंग कर देता है। लोगों को अपना पैसा देने के लिए बरगलाना एक घोटाला है।

वन-रिंग घोटाला कैसे काम करता है

- स्कैमर एक अंतरराष्ट्रीय प्रीमियम दर संख्या (आईपीआरएन) किराए पर लेता है।
- स्कैमर आपको एक रिंग देगा और फिर कॉल काट देगा।
- आप सोचेंगे कि आपसे एक महत्वपूर्ण कॉल छूट गई है और आप उसी नंबर पर वापस कॉल करेंगे।
- आपकी कॉल तो ली जाएगी लेकिन दूसरी तरफ से आपसे कोई बात नहीं करेगा.
- कोई जवाब न मिलने के बाद, आप अपनी कॉल काट देंगे।
- कॉल के बाद, आप महसूस करेंगे कि एक अंतरराष्ट्रीय कॉल करने के लिए आपने एक बड़ी राशि खो दी है।

वन-रिंग घोटाले से सुरक्षित रहने के लिए :

वन रिंग स्कैम से सुरक्षित रहने के लिए

- जिन नंबरों को आप नहीं पहचानते हैं, उनसे किसी भी कॉल का जवाब न दें या वापस न करें।
- अपरिचित नंबरों पर कॉल करने से पहले, यह देखने के लिए जांचें कि क्षेत्र कोड अंतरराष्ट्रीय है या नहीं।
- अपने फ़ोन ऑपरेटर को सभी संदिग्ध कॉलों की रिपोर्ट करें.

वित्तीय घोटालों के प्रकार

वित्तीय घोटालों के प्रकार

- फ़िशिंग
- भाला फ़िशिंग
- व्हेल के शिकार
- सीईओ धोखाधड़ी
- चोरी की पहचान
- लॉटरी शुल्क घोटाला
- ऑनलाइन शॉपिंग धोखाधड़ी
- घर के घोटालों से काम करें
- चोरी कार्ड घोटाला
- चालान धोखाधड़ी

फ़िशिंग एक डिजिटल माध्यम से किया गया एक हमला है जो व्यक्तिगत जानकारी जैसे क्रेडिट कार्ड नंबर, बैंक जानकारी आदि प्रकट करने के लिए किसी व्यक्ति के पैसे या पहचान को चुराने की कोशिश करता है।

स्पीयर-फ़िशिंग एक प्रकार की फ़िशिंग है जो बहुत विशिष्ट और वैयक्तिकृत संदेशों का उपयोग करके किसी व्यक्ति के धन या पहचान को चुराने का प्रयास करती है.

भाला-फ़िशिंग के समान, व्हेलिंग हाई-प्रोफाइल, प्रसिद्ध और धनी व्यक्तियों जैसे सीईओ और मशहूर हस्तियों को लक्षित करती है.

एक **सीईओ फ्रॉड** में, जालसाज उस कंपनी के सीईओ होने का दिखावा करते हैं जिसके लिए आप काम करते हैं या कोई अन्य प्राधिकरण व्यक्ति है और आपको पैसे भेजने या उन्हें आपकी संवेदनशील जानकारी तक पहुंच प्रदान करने के लिए कहता है।.

पहचान की चोरी में, धोखेबाज आपकी व्यक्तिगत जानकारी, जैसे नाम, पता, ईमेल पता, साथ ही क्रेडिट कार्ड या खाता जानकारी को लक्षित करते हैं। वे तब आपके नाम के तहत ऑनलाइन आइटम ऑर्डर करते हैं और आपकी क्रेडिट कार्ड जानकारी का उपयोग करके भुगतान करते हैं.

लॉटरी शुल्क घोटाले में, आपको एक सूचना मिलती है कि आपने लॉटरी जीत ली है और आपको अपने पुरस्कार का दावा करने के लिए शुल्क जमा करने के लिए कहा जाता है।

एक ऑनलाइन शॉपिंग धोखाधड़ी में, एक नकली शॉपिंग पोर्टल उत्पादों को आकर्षक कीमतों पर प्रदर्शित करता है। भुगतान हो जाने के बाद, आपको एक नकली उत्पाद या कोई उत्पाद प्राप्त नहीं होता है।

वर्क-फ्रॉम-होम घोटालों में, धोखेबाज लोगों को यह वादा करके ठगते हैं कि वे घर से काम करके अच्छा वेतन अर्जित करेंगे। वे नौकरी चाहने वालों को एक निश्चित राशि जमा करने के लिए कहते हैं। पैसा जमा होने के बाद नौकरी करने वालों का कोई पता नहीं चलता।

डेबिट/क्रेडिट कार्ड घोटाला तब होता है जब कोई आपकी जानकारी के बिना वित्तीय लेनदेन के लिए अवैध रूप से आपके डेबिट/क्रेडिट कार्ड की जानकारी का उपयोग करता है।

एक इनवॉइस धोखाधड़ी में, जालसाज़ एक आपूर्तिकर्ता के रूप में प्रस्तुत करके और उस बैंक खाते के विवरण को अपडेट करने के लिए कहकर व्यवसायों को लक्षित करते हैं जिसमें इनवॉइस का भुगतान किया जाता है.

वित्तीय घोटालों के परिणाम:

ऑनलाइन वित्तीय घोटालों से सुरक्षित रहना :

- सभी व्यक्तिगत जानकारी, पहचान पत्र और बैंक कार्ड को हर समय सुरक्षित रखें।
- अपना पिन नंबर गोपनीय रखें।
- अपना पिन नंबर नीचे न लिखें या उन्हें बैंक कार्ड के साथ स्टोर न करें।
- किसी भी व्यक्ति को कभी भी बैंक खाते का विवरण या अन्य सुरक्षा जानकारी न दें।
- अपना एटीएम कार्ड किसी और को इस्तेमाल न करने दें।

- संदिग्ध लेन-देन के लिए मासिक क्रेडिट कार्ड स्टेटमेंट और अन्य बैंक स्टेटमेंट ध्यान से देखें।
- अपने कार्ड के चोरी होने या खो जाने की तुरंत रिपोर्ट करें।
- इंटरनेट पर भुगतान करने के लिए अपने कार्ड का उपयोग करते समय सावधान रहें।

- केवल सुरक्षित भुगतान वेबसाइटों पर ही अपने कार्ड सत्यापन मूल्य (सीवीवी) का खुलासा करें।
- किसी भी वित्तीय अनुबंध पर डिजिटल रूप से हस्ताक्षर करते समय सावधान रहें।
- कॉल, पत्र, ई-मेल या फैक्स से सावधान रहें, जो किसी विदेशी बैंक में बड़ी रकम जमा करने के लिए आपकी मदद मांग रहे हैं।
- स्पैम या अवांछित ई-मेल का जवाब न दें जो आपको नौकरी या किसी अन्य लाभ का वादा करता है।

यदि आपके ऑनलाइन बैंकिंग विवरण से छेड़छाड़ की गई है, तो निम्नलिखित उपाय करें...

1. अपने बैंक को तुरंत सूचित करें।
2. अपना क्रेडिट/डेबिट कार्ड या यूपीआई ऐप ब्लॉक करें।
3. नेट बैंकिंग के लिए अपना पासवर्ड बदलें।
4. अपना यूपीआई, डेबिट कार्ड और क्रेडिट कार्ड पिन बदलें।
5. मौजूदा डेबिट/क्रेडिट कार्ड रद्द करें और बदलने के लिए कहें।
6. एक नई सुरक्षा सुविधा (बहु-चरण प्रमाणीकरण) सेट करें।

Reference Reading:

- वित्तीय धोखाधड़ी के बारे में अधिक जानकारी:https://cybercrime.gov.in/pdf/Financial%20Fraud%20Brochures%20final.pdf

मॉड्यूल 3

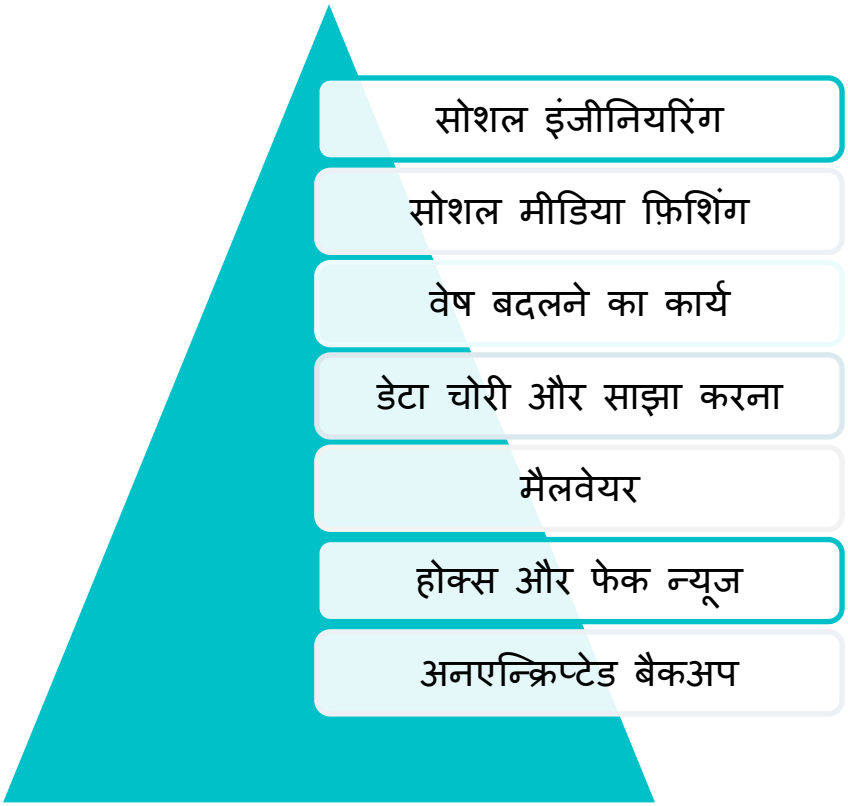
सामाजिक मीडिया

व्यापक रूप से प्रयुक्त सोशल मीडिया प्लेटफॉर्म

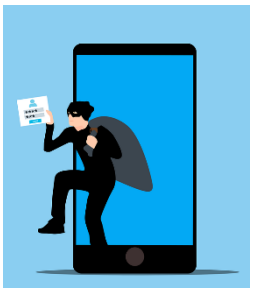
- व्हाट्सएप
- इंस्टाग्राम
- फेसबुक
- ट्विटर
- शेयरचैट
- स्नैपचैट

सोशल मीडिया प्लेटफॉर्म उपयोगकर्ताओं को तस्वीरें प्रदर्शित करने और उन्हें सार्वजनिक रूप से पोस्ट करने में सक्षम बनाता है। जालसाज उपयोगकर्ता की जानकारी के बिना गुप्त रूप से जानकारी एकत्र करते हैं। एकत्र की गई जानकारी के साथ, जालसाज फिर अलग-अलग तरीकों से उपयोगकर्ताओं से संपर्क करते हैं।

धोखेबाज विभिन्न तरीकों से सोशल मीडिया यूजर्स को स्कैम करते हैं:



सोशल इंजीनियरिंग



इस हमले में अनधिकृत पहुंच, नेटवर्क और वित्तीय लाभ हासिल करने के लिए हेरफेर शामिल है। जालसाज लेन-देन या धन हस्तांतरण करने के लिए खुद को बैंक या अन्य संगठन के प्रामाणिक प्रतिनिधि के रूप में प्रस्तुत करके उपयोगकर्ता को बरगलाते हैं।

अपने आप को सुरक्षित रखने के लिए, कभी भी लेन-देन न करें या फोन कॉल के आधार पर बैंक विवरण न दें।

सोशल मीडिया फ़िशिंग

फ़िशिंग का उद्देश्य व्यक्तिगत डेटा प्राप्त करना या उपयोगकर्ता के सोशल मीडिया खातों तक पहुँच प्राप्त करना है।

वेष बदलने का कार्य

इस घोटाले में, जालसाज किसी ऐसे व्यक्ति का दिखावा करते हैं जिस पर संवेदनशील जानकारी चुराने के लिए उपयोगकर्ता द्वारा भरोसा किया जा सकता है।

सोशल मीडिया स्क्रैपिंग

यह सोशल मीडिया फ़िशिंग और प्रतिरूपण का एक उदाहरण है। जालसाज व्यक्तिगत जानकारी प्राप्त करने के लिए ग्राहक कार्यकारी के रूप में फर्जी कॉल करते हैं। इसमें नाम, जन्म तिथि, व्यक्तिगत फोटो और स्थान शामिल हैं। जालसाज इस जानकारी का उपयोग भविष्य में डेटा/पहचान की चोरी के लिए करते हैं।

सोशल मीडिया स्क्रैपिंग से खुद को सुरक्षित रखने के लिए:

- अपना व्यक्तिगत विवरण कभी साझा न करें
- ऐसी कॉल्स के बारे में तुरंत रिपोर्ट करें
- संदिग्ध प्रोफ़ाइल की रिपोर्ट करें और ब्लॉक करें

डेटा चोरी

इस घोटाले में जालसाज अवैध रूप से गोपनीय जानकारी ट्रांसफर करते हैं। मैलवेयर आमतौर पर सोशल मीडिया पर लाइक बटन, ऑडियो क्लिप, वीडियो या लिंक में छिपे हो सकते हैं।

होक्स और फेक न्यूज

इस स्कैम में जालसाज कुछ प्रोपगंडा को बढ़ावा देकर यूजर्स को गुमराह करने के लिए गलत जानकारी फैलाते हैं।

फर्जी कॉल और संदेशों से खुद को बचाने के लिए हमें चाहिए:

- फोटो और मीडिया को हमेशा ध्यान से देखें।
- विश्वसनीय स्रोतों से जानकारी की पुष्टि करें।
- अवैध और खतरनाक संवादी समूहों को ब्लॉक और रिपोर्ट करें।
- स्वयं को अवांछित समूहों में जोड़े जाने से रोकने के लिए समूह गोपनीयता सेटिंग्स का उपयोग करें।

अनएन्क्रिप्टेड बैकअप

इस घोटाले में, डेटा एल्गोरिथम द्वारा एन्कोड नहीं किया गया है और इसे किसी के द्वारा पढ़ा जा सकता है।

नकली खातों की पहचान करने के लिए, सोशल मीडिया पर धोखेबाज़ के निम्नलिखित व्यवहारों पर गौर करें:

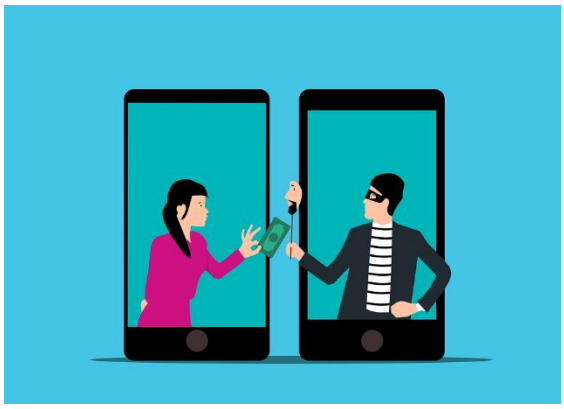
- कॉल और मीटिंग लेने से बचते हैं
- कोई ऑनलाइन उपस्थिति नहीं
- सीमित मित्र/अनुयायी
- बहुत हाल की प्रोफ़ाइल
- पेशेवर तस्वीरें
- चोरी की तस्वीरें
- पैसे मांगता है

अश्लील चित्र या वीडियो के लिए पूछता है

सोशल मीडिया फ्रॉड का सबसे आम रूप **कैटफिशिंग** है।

कैटफ़िशिंग ऑनलाइन धोखाधड़ी का एक रूप है। जालसाज नकली पहचान का उपयोग करके किसी और के होने का दिखावा करता है और रोमांटिक संबंध बनाकर आसान लक्ष्यों को धोखा देता है

- नकली पहचान का समर्थन करने के लिए, एक कैट-फ़िशर बनावटी कहानियों और नकली फ़ोटो का उपयोग करता है।
- एक कैट-फिशर आमतौर पर पैसे और व्यक्तिगत जानकारी मांगता है



सभी सोशल मीडिया प्लेटफॉर्म में "रिपोर्ट" और "ब्लॉक" की विशेषताएं होती हैं, जो एक उपयोगकर्ता को किसी अन्य परेशानी या नकली उपयोगकर्ता से बचाने के समान कार्य के साथ होती हैं।

अवरोध पैदा करना

संपर्क को अवरोधित करने से उपयोगकर्ता से संदेश प्राप्त करना अक्षम हो जाता है।

प्रतिवेदन

यदि किसी उपयोगकर्ता या समूह द्वारा नियमों और शर्तों का उल्लंघन किया जा रहा है, तो रिपोर्टिंग कंपनी को सूचित करने में मदद करती है

व्हाट्सएप के फायदे हैं:

- कोई पॉप-अप विज्ञापन नहीं
- प्रयोग करने में आसान
- कोई शुल्क नहीं संदेश सेवा
- मीडिया, स्थान और स्थिति साझा करना
- समूह जन संपर्क को सक्षम बनाता है
- वीडियो कॉल करना

व्हाट्सएप के नुकसान हैं:

- गोपनीयता संबंधी कई चिंताएँ हैं
- बहुत सारी असत्यापित जानकारी साझा की जा रही है
- व्हाट्सएप बहुत व्यसनी है

सोशल मीडिया शिष्टाचार:

सोशल मीडिया शिष्टाचार वे दिशानिर्देश हैं जिनका उपयोग सोशल मीडिया प्लेटफॉर्म और उपयोगकर्ता ऑनलाइन अपनी प्रतिष्ठा को बनाए रखने के लिए करते हैं।

सोशल मीडिया क्या करें

- ज्ञात संपर्कों के साथ संवाद करें
- अनुमति मांगें और सीमाओं का सम्मान करें
- समूह नियंत्रणों का उपयोग करें
- केवल सही फोटो और वीडियो साझा करें
- उचित फोटो और वीडियो पोस्ट करें
- सोशल मीडिया प्लेटफॉर्म के दिशा-निर्देशों का पालन करें।

सोशल मीडिया न करें

- अन्य उपयोगकर्ताओं को स्पैम करें
- दूसरों की व्यक्तिगत जानकारी का उपयोग या साझा करें
- थोक संदेश
- अभद्र भाषा का प्रयोग करें
- फेक न्यूज और भ्रामक सूचनाओं को बढ़ावा दें
- ओवर-शेयर

व्हाट्सएप क्या करें:

- ✓ अपने ज्ञात संपर्कों के लिए प्रोफ़ाइल फ़ोटो, स्थिति और जानकारी की दृश्यता सीमित करें।
- ✓ यादृच्छिक समूहों में जोड़े जाने से बचने के लिए समूह गोपनीयता सेटिंग का उपयोग करें।
- ✓ एंड-टू-एंड एन्क्रिप्शन का उपयोग करें।
- ✓ चैट में लाइव लोकेशन को बंद कर दें।
- ✓ उन अज्ञात उपयोगकर्ताओं को ब्लॉक करें जो आपसे संपर्क करने का प्रयास कर रहे हैं।

व्हाट्सएप न करें

- ✗ अजनबियों के साथ अपनी व्यक्तिगत जानकारी साझा करें।
- ✗ अपनी गोपनीयता सेटिंग को सार्वजनिक पर सेट करें।
- ✗ दूसरे उपयोगकर्ता की गोपनीयता का अनादर करें।

इंस्टाग्राम क्या करें

- जाने-पहचाने लोगों को अपने फ़ॉलोअर्स में जोड़ें।
- उपयुक्त फोटो, वीडियो, जानकारी पोस्ट करें।
- उपयुक्त फोटो, वीडियो, जानकारी पोस्ट करें।
- जालसाजों के लिए ब्लॉक/रिपोर्ट का उपयोग करें।

इंस्टाग्राम न करें

- सार्वजनिक खातों पर संवेदनशील जानकारी साझा करें।
- दूसरे की पोस्ट को बिना इजाजत यूज करें।
- अनुयायी खरीदें।
- दूसरों का अनादर करो

फेसबुक क्या करें

- सत्यापित समाचार और जानकारी साझा करें।
- अपने डेटा और जानकारी को सुरक्षित रखने के लिए गोपनीयता सेटिंग्स का उपयोग करें।
- केवल सही मीडिया साझा करें।
- ज्ञात उपयोगकर्ताओं के साथ बातचीत करें।

फेसबुक मत करो

- असत्यापित समाचार साझा करें।
- असत्यापित समाचार साझा करें।
- किसी भी विज्ञापन पर अपने क्रेडेंशियल जैसे बैंक खाते का विवरण भरें।

ट्विटर क्या करें

- अपने डेटा और ट्वीट्स को दुरुपयोग से बचाने के लिए गोपनीयता और सुरक्षा विकल्प का उपयोग करें।
- ट्वीट के माध्यम से अपने विचार व्यक्त करने के लिए उपयुक्त भाषा का प्रयोग करें।
- केवल ज्ञात उपयोगकर्ताओं के अनुरोध स्वीकार करें।

ट्विटर न करें

- अपनी राय दूसरों पर थोपें।
- अभद्र भाषा का प्रयोग करें।
- अपना लाइव स्थान सार्वजनिक रूप से साझा करें।

सोशल मीडिया संचार में बहुत सहायक है और हमें दुनिया के साथ अद्यतन रखता है। लेकिन हमें इसका इस्तेमाल जिम्मेदारी से करना चाहिए। सोशल मीडिया पर कई दिलचस्प तथ्य और खबरें उपलब्ध हैं। उन्हें प्रसारित करने से पहले हमें सतर्क रहने की जरूरत है।

संदर्भ पढ़ना:

- साइबर जागरुकता दिवस: https://www.youtube.com/watch?v=6whmq4EwIIo
- साइबरबुलिंग तथ्य:https://www.youtube.com/watch?v=0Xo8N9qlJtk

मॉड्यूल 4

चोरी की पहचान

पासवर्ड और प्रमाणीकरण

पासवर्ड प्रमाणीकरण प्रक्रिया के दौरान उपयोगकर्ता की पहचान सत्यापित करने के लिए उपयोग किए जाने वाले वर्णों की एक स्ट्रिंग है।

पासवर्ड आपके स्मार्ट उपकरणों और व्यक्तिगत जानकारी तक अनधिकृत पहुंच के विरुद्ध पहली सुरक्षा प्रदान करते हैं।

- पासवर्ड में कम से कम दस वर्ण होने चाहिए और वर्णों का संयोजन होना चाहिए जैसे:

विशेष वर्ण	अपरकेस और लोअरकेस अक्षर	नंबर

- "12345" या "क्वर्टी" जैसे अनुक्रमों का उपयोग करने से बचें
- आप अक्षरों के बजाय समान दिखने वाली संख्याओं का उपयोग कर सकते हैं–O के बजाय शून्य

ज़ूम	के रूप में लिखें	**ज़ूम**
चाल	के रूप में लिखें	**चाल**
Basket	के रूप में लिखें	**845KE7**
Ball	के रूप में लिखें	**8411**

- आप संख्याओं को उन विशेष आप संख्याओं को उन विशेष वर्णों से भी बदल सकते हैं जिनका उल्लेख आपके कीबोर्ड पर संख्याओं के साथ किया गया है। वर्णों से भी बदल सकते हैं जिनका उल्लेख आपके कीबोर्ड पर संख्याओं के साथ किया गया है।

प्रमाणीकरण में निम्नलिखित कारक शामिल हैं:

- उपयोगकर्ता कुछ जानता है जैसे पासवर्ड, पिन
- उपयोगकर्ता के पास कुछ है जैसे डेबिट कार्ड और क्रेडिट कार्ड
- उपयोगकर्ता के लिए कुछ अनूठा जैसे बायोमेट्रिक विशेषताएँ

यूपीआई पिन, बैंकिंग कार्ड पिन और बायोमेट्रिक प्रमाणीकरण

1. यूपीआई प्रमाणीकरण

UPI Stands for Unified Payments Interface

A payment system that allows you to transfer funds across banks

To use UPI you need:

- A smartphone
- An active bank account
- A mobile number linked with bank account
- Internet connection
- UPI ID
- UPI PIN

UPI ID	• Automatically Generated • Required to access UPI account
UPI PIN	• Unique, 4 or 6-digit passcode created by the user • Safeguards your UPI account

2. बैंकिंग कार्ड प्रमाणीकरण

Banking Card PIN includes PIN for:

P Personal

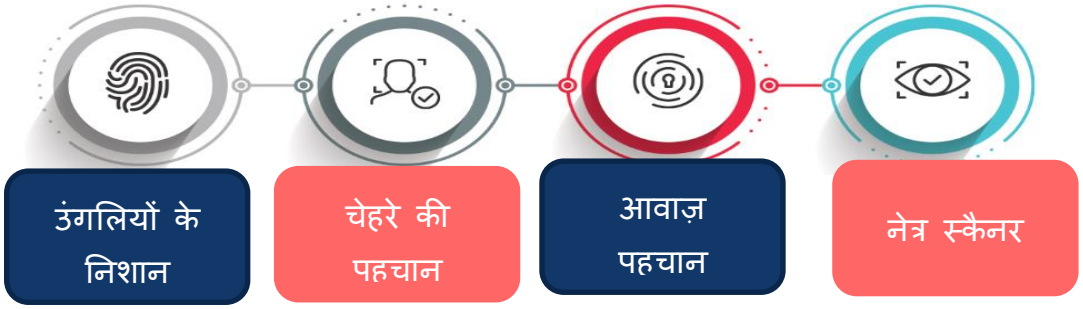
I Identification

N Number

A four-digit code that is unique to an account holder's card.

3. बायोमेट्रिक प्रमाणीकरण

बायोमेट्रिक प्रमाणीकरण निम्नलिखित बायोमेट्रिक से मेल खाता है स्मार्ट डिवाइस या अपने बैंकिंग खाते तक पहंचने की सुविधाएँ।



दो तरीकों से प्रमाणीकरण

Two-factor authentication is also referred to as 2FA

Safeguards your online accounts by verifying user details and passcode

Monitors and helps safeguard your online account credentials and data

दुर्भावनापूर्ण वेबसाइटें और ऐप्स

टू-फैक्टर ऑथेंटिकेशन एक पासवर्ड और वन-टाइम पासकोड/ऑथेंटिकेशन कोड का इस्तेमाल करता है, जिसे भेजा जाता है एसएमएस के माध्यम से मोबाइल फोन जो दर्ज करने पर उपयोगकर्ता को अंततः खाते तक पहुंचने की अनुमति देता है।

Enter Username And Password to

Authentication Code

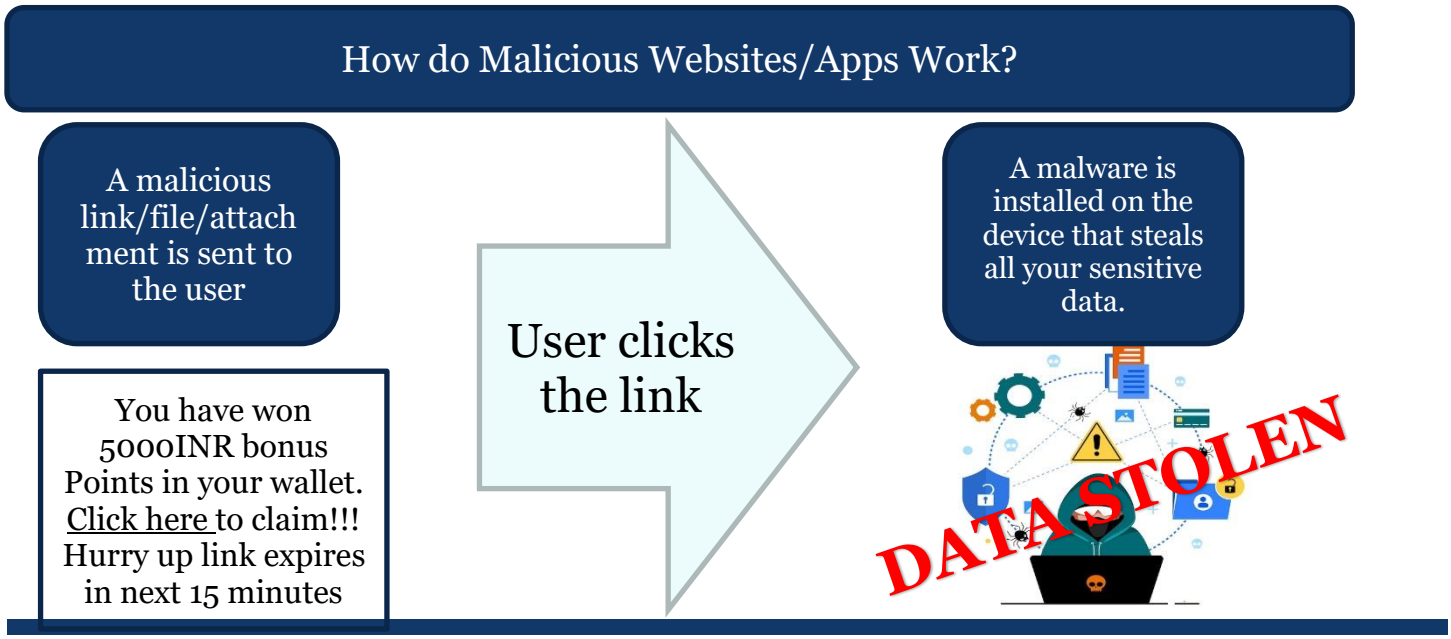
Enter Authentication Code

दुर्भावनापूर्ण वेबसाइटें और ऐप्स

दुर्भावनापूर्ण वेबसाइटें और ऐप्स उपयोग किए जा रहे साइबर-हमले के सबसे सामान्य रूपों में से एक हैं। हैकर्स आपको एसएमएस, ईमेल या आपके सोशल मीडिया खातों पर प्रदर्शित विज्ञापनों के माध्यम से लिंक भेजते हैं।

आपको सतर्क रहने की आवश्यकता है क्योंकि एक क्लिक पर आपकी सभी व्यक्तिगत जानकारी हैकर्स के पास लीक हो जाएगी। दुर्भावनापूर्ण वेबसाइटें आपको निम्न कार्य करने का निर्देश दे सकती हैं:

- सॉफ्टवेयर/कोई चालान/फ़ाइल/ऐप डाउनलोड करें
- फ़ाइल सहेजें
- एक कार्यक्रम चलाएँ



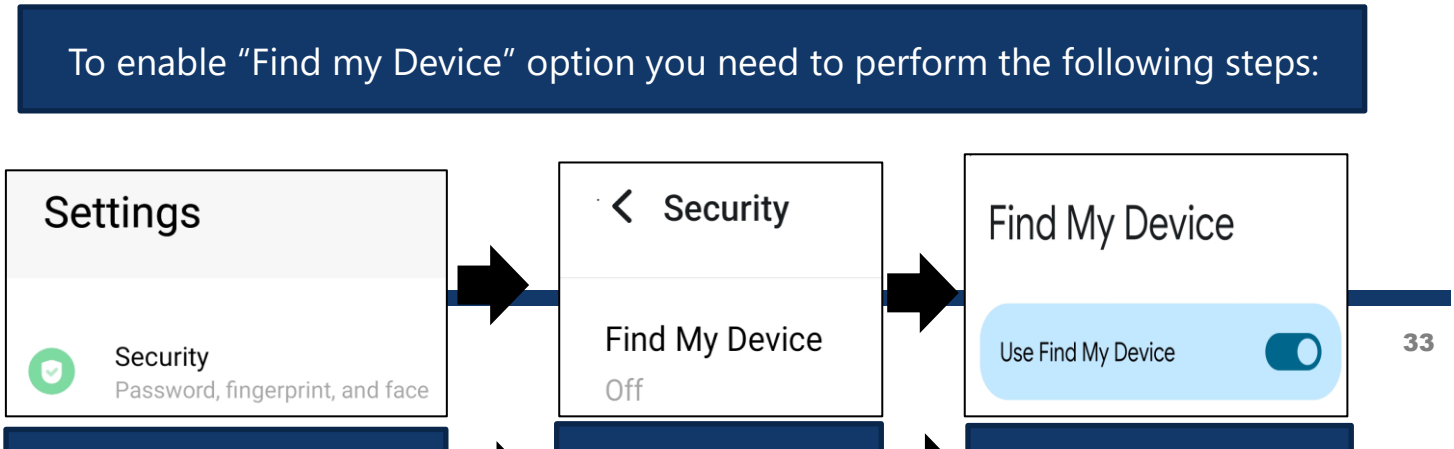
यहां कुछ बिंदु दिए गए हैं जो आपके डिवाइस को दुर्भावनापूर्ण वेबसाइटों और ऐप से सुरक्षित रखने में मदद करेंगे:

- कभी भी किसी ईमेल में एम्बेड किए गए लिंक पर क्लिक न करें।
- कभी भी किसी बाहरी तृतीय-पक्ष संदेश से प्राप्त लिंक पर क्लिक न करें।
- कभी भी ऐसा कोई ऐप इंस्टॉल न करें जो आपकी व्यक्तिगत संवेदनशील जानकारी मांगता हो।
- कोई भी ऑनलाइन भुगतान करते समय हमेशा URL में "https" की जांच करें।
- URL को ध्यान से पढ़ें। वेबसाइट की स्पेलिंग में मामूली सा मोड़ खतरे का कारण बन सकता है।
- बैंक द्वारा दिए गए लिंक से अपना बैंकिंग ऐप इंस्टॉल करें।
- किसी भी वेबसाइट तक पहुँचने से पहले हमेशा URL की जाँच करें।
- केवल विश्वसनीय वेबसाइटों पर ही खरीदारी करें और प्राप्त किसी भी यादृच्छिक लिंक के माध्यम से नहीं।
- विश्वसनीय प्ले स्टोर से सुरक्षित ऐप्स इंस्टॉल करें।
- ईमेल खोलने से पहले उनकी जांच करें। यदि आप प्रेषक को जानते हैं तो ही खोलें।
- अगर आपने किसी भी खाते में ऑनलाइन लॉग इन किया है, तो वेबसाइट छोड़ने से पहले हमेशा लॉग ऑफ करें।
- अपने एंटीवायरस को नियमित रूप से अपडेट करें।

खोए हुए फोन को दूरस्थ रूप से प्रबंधित करना

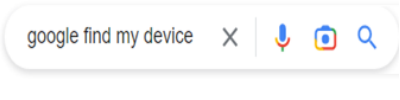
केवल निम्न स्थितियों में, खोए हुए फ़ोन को दूरस्थ रूप से एक्सेस किया जा सकता है

- फोन चालू है
- Google खाते (एंड्रॉइड के मामले में) या आईफ़ोन के मामले में iCloud में साइन इन किया हुआ
- इंटरनेट से जुड़ा हुआ
- फाइंड माई डिवाइस सक्षम है

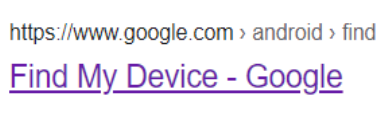


To remotely erase your lost smartphone data, you need to perform the steps shown:

Open Google Chrome and Sign-in to your account

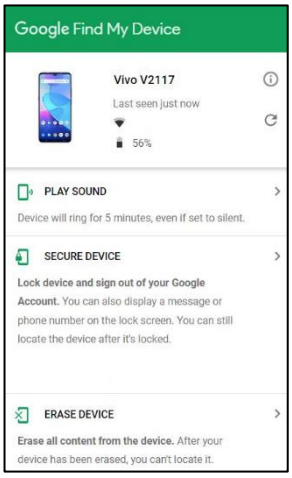


Type Google Find My Device in the search bar



Click on the link shown. The Google Find my device screen appears.

अब, आप अपने डिवाइस को सुरक्षित कर सकते हैं या स्क्रीन पर दिखाए अनुसार उपयुक्त विकल्प का चयन करके उस पर मौजूद सामग्री को मिटा सकते हैं।



फ़िशिंग और ऑनलाइन फ़ॉर्म

हम सभी जानते हैं कि ऑनलाइन फॉर्म हैं:

- एक से अधिक प्रश्नों वाले सर्वेक्षण प्रपत्र बनाने के लिए उपयोग किया जाता है।
- वास्तविक समय में सर्वेक्षण के परिणामों का विश्लेषण करने के लिए उपयोग किया जाता है।
- किसी भी उपकरण से पहुँचा जा सकता है

लेकिन हैकर्स द्वारा अक्सर इनका इस्तेमाल आपकी निजी जानकारी को हैक करने के लिए भी किया जाता है।

हैकर्स आपके बैंक कर्मचारी होने का दिखावा कर सकते हैं और आपको सूचित करेंगे कि उन्होंने आपको एक फॉर्म संलग्न के साथ एक ईमेल भेजा है, जिसमें आपको भरने और इसे जल्द से जल्द भेजने के लिए कहा गया है ताकि आपकी बचत योजना का नवीनीकरण किया जा सके।

ऐसे फिशिंग स्कैम के झांसे में न आएं। अगर आपको अपने बैंक से ऑनलाइन फॉर्म भरने की जरूरत है तो तुरंत पुष्टि करें।

यहाँ फ़िशिंग ऑनलाइन फ़ॉर्म ईमेल का एक नमूना है।

Attention: Urgent | External email Dear Account Holder This is to notify you that there is some missing information with respect to your KYC. Kindly fill in the attached form and submit it by today otherwise your account will be frozen till further notice and you won't be able to make any financial transactions from this account. Please click the link below to update your account: Update Now We respect your privacy! Thanks and Regards MSN20002 Unnamed 555555.png	Fill in the details: First Name:*_____ Last Name:* Address 1:* Address 2 Email ID:* Registered Mobile Number:* Aadhaar Number:*

Phishing Form e-mail

Dos and don'ts of online forms to remain safe:

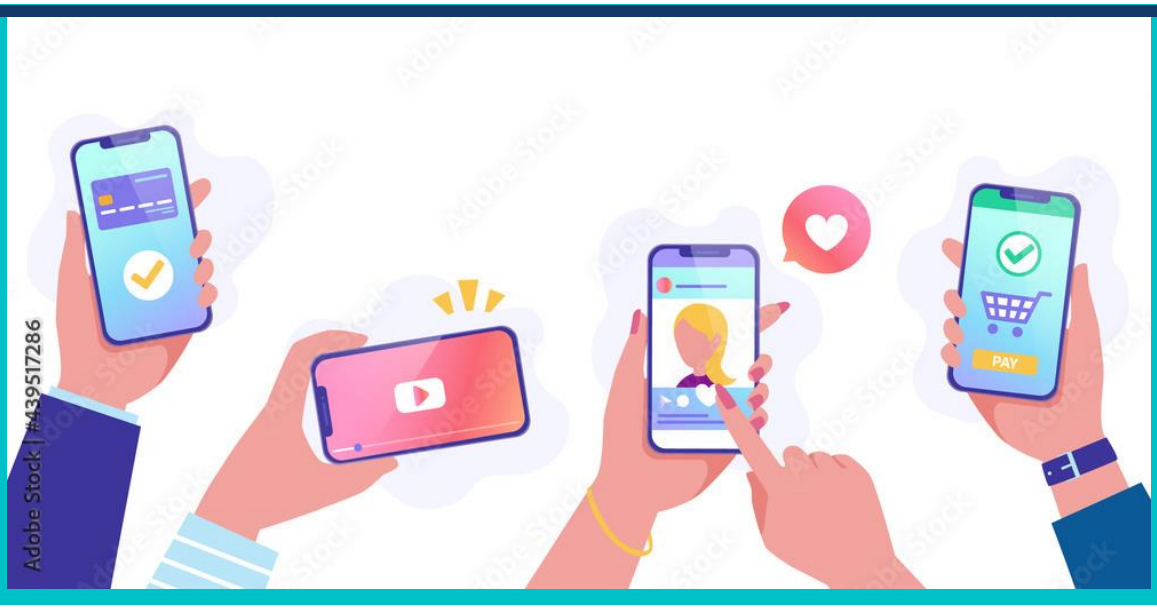
- Never provide sensitive information via online forms unless and until you are sure about the source sending the form.
- Never open an email from an external third-party vendor.
- Always cross-check with your bank or the concerned authority about you receiving the form via e-mail.
- Read the sender's email id and confirm before replying to them.

संदर्भ पढ़ना:

- **अपना यूपीआई पिन कैसे रीसेट करें:** https://www.youtube.com/watch?v=ZoEqpKF_Sjw
- **दो-कारक प्रमाणीकरण के साथ अपने Instagram खाते को सुरक्षित करना:** https://help.instagram.com/566810106808145
- **टू फैक्टर ऑथेंटिकेशन के साथ अपने फेसबुक अकाउंट को सुरक्षित करना :** https://www.facebook.com/help/148233965247823
- **खोए हुए आईफोन को दूर से प्रबंधित करना:** https://support.apple.com/en-in/guide/security/secc46f3562c/web
- **मैलवेयर संक्रमणों के लिए किसी वेबसाइट की जांच कैसे करें :** https://www.sitelock.com/blog/check-website-for-malware/
- **दुर्भावनापूर्ण संक्रमणों के लिए किसी वेबसाइट की जांच कैसे करें :** https://www.91mobiles.com/hub/malicious-apps-malware-google-play-store/

मॉड्यूल 5

इंटरनेट स्मार्ट होना



सुरक्षित ब्राउज़िंग युक्तियाँ:

ऐसे कुछ तरीके हैं जिनसे ऑनलाइन ब्राउजिंग करना सुरक्षित हो सकता है।

इंटरनेट स्मार्ट बनें

- **ध्यान से साझा करें**
  समाचार तेजी से यात्रा करता है। लोगों पर पड़ने वाले इसके परिणामों के बारे में पहले से सोचना जरूरी है।
- **जिम्मेदारी से संवाद करें**
  - आमने-सामने संचार की तरह ही ऑनलाइन संचार के माध्यम से विचारशील साझाकरण को बढ़ावा दें।
  - उपयुक्त संचार के लिए प्रपत्र दिशानिर्देश।
  - सुरक्षित परिवार और दोस्तों का विवरण।
- **इंटरनेट अलर्ट रहें**
  - फेक न्यूज के झांसे में न आएं।
  - लोगों को समझने में मदद करना महत्वपूर्ण है
  - ऑनलाइन सुरक्षा में क्या असली है और क्या नकली यह एक बहुत ही महत्वपूर्ण सबक है।
  - ऑनलाइन लोग और परिस्थितियाँ हमेशा वैसी नहीं होतीं जैसी दिखती हैं।
- **इंटरनेट मजबूत बनें**
  - अपने राज सुरक्षित करें
  - गोपनीयता और सुरक्षा ऑनलाइन उतनी ही महत्वपूर्ण हैं जितनी वे ऑफ़लाइन हैं।
  - व्यक्तिगत जानकारी की सुरक्षा करने से उपयोगकर्ता को अपने उपकरणों, प्रतिष्ठा और संबंधों को नुकसान से बचाने में मदद मिलती है।

- **इंटरनेट की तरह रहो**
  - दयालु होना अच्छा है
  - इंटरनेट सकारात्मकता के साथ-साथ नकारात्मकता फैलाने का एक शक्तिशाली साधन है। उपयोगकर्ता ऑनलाइन अपने कार्यों के लिए "दूसरों के साथ वैसा ही व्यवहार करें जैसा

आप व्यवहार करना चाहते हैं" की अवधारणा को ले सकते हैं, दूसरों पर सकारात्मक प्रभाव पैदा कर सकते हैं और अनुचित व्यवहार को समाप्त कर सकते हैं।

- **इंटरनेट बहादुर बनो**

    - उपयोगकर्ता घर पर और सार्वजनिक स्थान पर खुले संचार को बढ़ावा देकर एक-दूसरे को किसी संदिग्ध चीज़ के बारे में बात करने में सहज बना सकते हैं।

स्मार्ट ब्राउजिंग:

हैकर्स सामाजिक प्रोफ़ाइल से एकत्रित जानकारी के आधार पर फ़िशिंग स्कैम बना सकते हैं। खुद को घोटालों से बचाने के लिए यहां कुछ SMART टिप्स दिए गए हैं।

S-Safe	M-Meeting	A-Ask	R-Reliable	T-Tell
सुरक्षित रहने के लिए, कभी भी अपनी व्यक्तिगत जानकारी अजनबियों के साथ ऑनलाइन साझा न करें।	केवल उन्हीं से मिलें जिन्हें आप व्यक्तिगत रूप से जानते हों। कभी भी किसी अजनबी से उस व्यक्ति से न मिलें जिससे आप ऑनलाइन मिले हों।	जब सुरक्षा के बारे में संदेह हो, तो किसी जानकार व्यक्ति से मदद मांगें। कभी भी फ्रेंड रिक्वेस्ट स्वीकार न करें या अनजान लोगों के ईमेल न खोलें।.	किसी भी वेबसाइट को इस्तेमाल करने या किसी भी ऐप को डाउनलोड करने से पहले विश्वसनीयता जांच जरूरी है	अपने ऑनलाइन खाते के साथ देखी गई किसी भी अवैध गतिविधियों के बारे में संबंधित अधिकारियों को बताएं

- अपनी व्यक्तिगत जानकारी जैसे यात्रा योजना या परिवार का विवरण साझा न करें। हैकर्स उस पोस्ट की जानकारी का इस्तेमाल आपके खिलाफ कर सकते हैं
- अपना ई-मेल और संपर्क नंबर ऑनलाइन पोस्ट, साझा या ट्वीट न करें।
- अनजान लोगों की फ्रेंड रिक्वेस्ट एक्सेप्ट न करें।
- अपने वर्कस्टेशन से तस्वीरें साझा करते समय, सुनिश्चित करें कि आपके कंप्यूटर सिस्टम से कुछ भी प्रकट नहीं हो रहा है।
- अलग-अलग सोशल मीडिया प्लेटफॉर्म पर हमेशा अलग-अलग प्रोफाइल पिक्चर्स का इस्तेमाल करने की कोशिश करें।

सुरक्षित ब्राउज़िंग उपकरण

- **फ़ायरवॉल:** फ़ायरवॉल एक ऐसा सॉफ़्टवेयर है जो नेटवर्क पर अनधिकृत पहुँच को रोकने के लिए पहली रक्षा पंक्ति के रूप में कार्य करता है और सुरक्षा जोखिमों को कम करने के लिए कुछ नियमों का उपयोग करके ट्रैफ़िक का निरीक्षण करता है।

एंटीवायरस:

कंप्यूटर वायरस एक दुर्भावनापूर्ण कोड या प्रोग्राम है जो खुद को दोहराता है और कंप्यूटर के संचालन के तरीके को परेशान करने के लिए डिज़ाइन किया गया है। एक वायरस एक वैध कार्यक्रम में खुद को सम्मिलित या संलग्न करके संचालित होता है। एक वायरस में डेटा को दूषित या नष्ट करके सिस्टम सॉफ़्टवेयर को नुकसान पहुँचाने या नुकसान पहुँचाने की क्षमता होती है।

एंटी-वायरस एक सुरक्षा प्रोग्राम है जो आपके कंप्यूटर या मोबाइल डिवाइस पर वायरस और वर्म्स जैसे मैलवेयर से होने वाले संक्रमण को रोकने के लिए इंस्टॉल किया जाता है।

आपके डिवाइस या सिस्टम में एंटी-वायरस इंस्टॉल करने के लाभ हैं:

- वायरस का पता लगाना, ब्लॉक करना और हटाना।
- पहचान की चोरी को रोकना और फ़िशिंग को रोकना।
- दुर्भावनापूर्ण वेबसाइटों और लिंक के बारे में चेतावनी।
- ऑनलाइन खातों को सुरक्षित पासवर्ड एन्क्रिप्शन से सुरक्षित रखना।
- कंप्यूटर का सुचारू संचालन।

इंटरनेट सूचनाओं का एक जटिल मिश्रण है, विचलित करने वाले विज्ञापन, खतरनाक मैलवेयर और क्लिक-बैट लिंक को धोखा देना जो कि उपयोगकर्ताओं को साइबर दुःस्वप्न में ले जा सकता है। मैलवेयर और अन्य ब्राउज़र-आधारित हमलों के बारे में चिंता किए बिना वेब के पेचीदा इलाके मे

नेविगेट करने के लिए, ब्राउज़र विक्रेता कई सहायक सुरक्षा सुविधाएँ प्रदान करते हैं।

इंटरनेट पर सुरक्षा के लिए ब्राउज़र द्वारा प्रदान की जाने वाली सुविधाएँ

Google क्रोम द्वारा सुरक्षित ब्राउज़िंग सुविधा

- Microsoft द्वारा स्मार्टस्क्रीन फ़िल्टर
- Mozilla Firefox द्वारा फ़िशिंग फ़िल्टर
- ये सुविधाएं कंप्यूटर को फ़िशिंग हमलों और मैलवेयर से बचाने में मदद करती हैं।

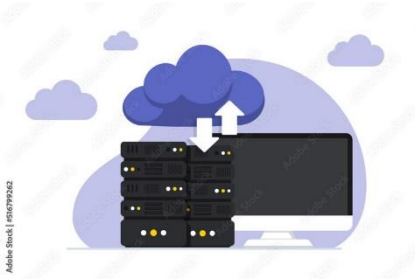
यहां कुछ चरण दिए गए हैं जो आपको ऑनलाइन सुरक्षित रख सकते हैं और ऑनलाइन सुरक्षा कवच बनाने में आपकी मदद कर सकते हैं

- **संवेदनशील ब्राउज़िंग:** हम अक्सर बैंक लेनदेन के लिए कैफे आदि में ओपन नेटवर्क का इस्तेमाल करते हैं। साइबर अपराधी पल भर में आपकी बैंक डिटेल कॉपी कर लेते हैं और आपकी गाढ़ी कमाई लूट लेते हैं।

- **स्पैम संदेश** पता लगाना और बचना आसान है। इन संदेशों में 'मैसेज फ्रॉम आरबीआई' या 'योर हेल्प इज़ रिक्वायर्ड' आदि शब्दों का इस्तेमाल किया जाता है। आपको इनसे बचना होगा और ऐसे संदेहास्पद लिंक को नहीं खोलना चाहिए।
- **मजबूत पासवर्ड** क्रैक करना मुश्किल है। प्रत्येक अलग ऑनलाइन खाते के लिए हमेशा अलग पासवर्ड का उपयोग करने का प्रयास करें। आपको अपना पासवर्ड हमेशा वेबसाइटों की पासवर्ड नीति के अनुसार सेट करना चाहिए। पासवर्ड अल्फा-न्यूमेरिक होने चाहिए और उन्हें मजबूत बनाने के लिए विशेष वर्ण होने चाहिए।

- **अपने खातों/सत्रों से साइन आउट करें:** हम आम तौर पर हमारे मेल या सोशल मीडिया खातों या हमारे उपकरणों पर बैंकिंग सत्र में लॉग इन होते हैं। लेकिन यह हमारी साइबर सुरक्षा के लिए भी खतरा हो सकता है। हमेशा अपने खातों से लॉग आउट करें और अपने उपकरणों पर अपने बैंक लॉगिन करें।

- **सोशल मीडिया पर सुरक्षा:** फेसबुक या इंस्टाग्राम और अन्य सोशल साइट्स पर तस्वीरें अपलोड करना आजकल बहुत आम है, लेकिन इन तस्वीरों का गलत इस्तेमाल किया जा सकता है। अपने ऑनलाइन डेटा को पीछा करने वालों और अन्य जोखिमों से सुरक्षित रखने के लिए, आपको अपनी खाता सेटिंग्स को सार्वजनिक से निजी में बदलना चाहिए।



- डेटा बैकअप: हमेशा अपने डेटा का बैकअप फिजिकल ड्राइव या ऑनलाइन स्टोरेज यानी क्लाउड स्टोरेज की मदद से लें। इस तरह, अगर आपके डिवाइस में कुछ भी होता है तो आपका डेटा सुरक्षित रहेगा।
- **वेबसाइटों की सुरक्षा चेतावनी :** McAfee साइट एडवाइजर जैसे कई साइट सुरक्षा एक्सटेंशन आपको वेबसाइट ब्राउज़ करने की सुरक्षा के बारे में चेतावनी देते हैं।

सार्वजनिक और मुफ्त वाई-फाई

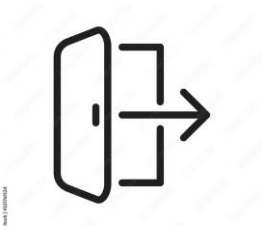
सार्वजनिक वाई-फाई असुरक्षित और जोखिम भरा है। सार्वजनिक वाई-फाई के असुरक्षित कनेक्शन से कुछ संभावित जोखिम

- मैन इन मिडिल अटैक
- अनएन्क्रिप्टेड नेटवर्क
- मैलवेयर वितरण
    - वायरस
    - कीड़े
    - ट्रोजेन हॉर्सेज
    - रैंसमवेयर
    - एडवेयर
- स्नूपिंग और स्नीफिंग
- व्यक्तिगत जानकारी की चोरी
    - लॉग इन प्रमाण - पत्र
    - वित्तीय जानकारी
    - व्यक्तिगत डेटा
    - चित्रों

- सत्र अपहरण

सार्वजनिक वाई-फाई का उपयोग करते समय सुरक्षित रहना

Avoid	Use	Open	Enable	Use
				
Opening sensitive documents/files	VPN secure connections using encryption over a public Wi-Fi	Only https websites	Secure browser settings	A privacy screen

Switch-off	Use	Ensure	Remember
			
File sharing	Two-factor authentication	Your operating system & browser are up-to-date	To log out of public Wi-Fi

साइबर अपराध के प्रकार:

- **उल्लंघनकारी कॉपीराइट:** किसी की अनुमति के बिना कॉपीराइट किए गए कार्य का उपयोग करना। उदाहरण के लिए, किसी कंपनी की वेबसाइट से छवि का उपयोग करना और इसे अपने व्यक्तिगत खाते पर पोस्ट करना।

- **रैनसमवेयर हमले:** रैंसमवेयर मैलवेयर है जो हमलावर को फिरौती शुल्क का भुगतान किए जाने तक, इसे एन्क्रिप्ट करके प्रकाशित करने या डेटा या डिवाइस तक पहुंच को अवरुद्ध करने की धमकी देता है।
- **गैरकानुनी जुआ:** ऑनलाइन गैंबलिंग में इंटरनेट पर कैसिनो या खेलों पर दांव लगाना शामिल है।
- **साइबर जासूसी:** साइबर जासूसी प्रतिस्पर्धा में लाभ प्राप्त करने के लिए कंप्यूटर उपकरणों से या उसके माध्यम से डेटा, संवेदनशील जानकारी या बौद्धिक संपदा की जानबूझकर चोरी है। उदाहरण के लिए, राजनीतिक दल चुनावों के दौरान प्रतिस्पर्धियों का डेटा चुराते हैं।

- **ईमेल और इंटरनेट धोखाधड़ी**
- **पहचान का धोखा**
- **वित्तीय या कार्ड भुगतान डेटा की चोरी**

- **क्रिप्टोजैकिंग:** क्रिप्टोजैकिंग एक प्रकार का साइबर अपराध है जिसमें साइबर अपराधियों द्वारा लोगों के उपकरणों (कंप्यूटर, स्मार्टफोन, टैबलेट या यहां तक कि सर्वर) का अनाधिकृत उपयोग क्रिप्टोकरंसी के लिए किया जाता है। साइबर अपराध के कई रूपों की तरह, मकसद लाभ है, लेकिन अन्य खतरों के विपरीत, इसे पीड़ित से पूरी तरह छिपाकर रखने के लिए बनाया गया है।

- **साइबर एक्सटॉर्शन:** साइबर एक्सटॉर्शन एक ऐसा अपराध है जिसमें हमला या हमले की धमकी के साथ-साथ पैसे की मांग या हमले को रोकने के बदले में कुछ अन्य प्रतिक्रिया शामिल है।

अपने डिवाइस को हैकर्स से बचाने के तरीके:

- फ़ायरवॉल का प्रयोग करें
- एंटी-वायरस इंस्टॉल करें
- मजबूत पासवर्ड का प्रयोग करें
- अप-टू-डेट ब्राउज़रों का उपयोग करें
- अपने नेटवर्क को सुरक्षित करें
- दो-कारक प्रमाणीकरण का प्रयोग करें
- ऐप्स और व्यक्तिगत जानकारी के लिए सुरक्षा पिन का उपयोग करें

संदर्भ पढ़ना:

- **व्यक्तिगत गोपनीयता: इंटरनेट पर सुरक्षित ब्राउज़िंग के लिए शीर्ष 12 सुझाव :** https://cybersecurityventures.com/12-tips-for-safer-browsing/
- **महिलाओं और लड़कियों को ऑनलाइन सुरक्षित रहने में मदद करने के लिए 5 सुझाव :** https://www.globalcitizen.org/en/content/tips-to-help-women-girls-stay-safe-online/
- **सार्वजनिक वाईफाई सुरक्षा जोखिमों से कैसे बचें:** https://www.kaspersky.co.in/resource-center/preemptive-safety/public-wifi-risks

मॉड्यूल 6

डिजिटल अधिकार, कानून और निवारण तंत्र

डिजिटल नागरिक: एक डिजिटल नागरिक वह व्यक्ति होता है जो जिम्मेदारी से इंटरनेट और अन्य डिजिटल तकनीकों का उपयोग करता है

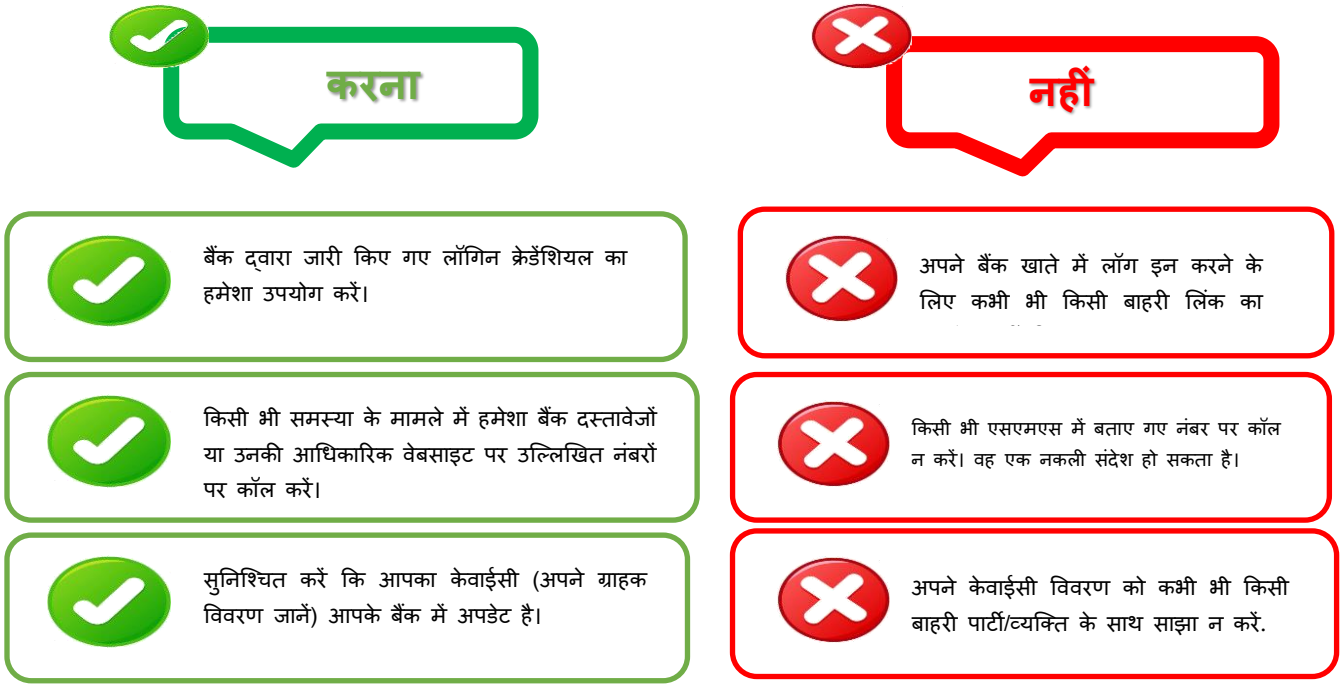
एक डिजिटल नागरिक की भूमिकाएँ:

- अपनी व्यक्तिगत जानकारी को सुरक्षित रखें
- अपने डिजिटल फ़ुटप्रिंट (किसी विशेष व्यक्ति के बारे में जानकारी जो उनकी ऑनलाइन गतिविधि के परिणामस्वरूप इंटरनेट पर मौजूद है) को सावधानीपूर्वक प्रबंधित करें
- ऑनलाइन लेनदेन कानूनों का पालन करें
- अवैध गतिविधियों के लिए खड़े हों
- डिजिटल नागरिक के रूप में अपने अधिकारों को जानें

व्यक्तिगत जानकारी साझा करते हुए एक जिम्मेदार स्मार्ट डिजिटल नागरिक बनें:

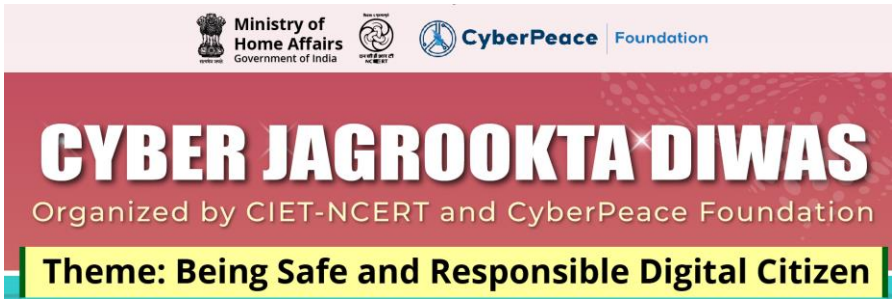
एस-सुरक्षित	एम-बैठक	ए-पूछो	आर-विश्वसनीय	टी Tell
ऑनलाइन सुरक्षित रहने के लिए, कभी भी अपनी व्यक्तिगत जानकारी अजनबियों के साथ ऑनलाइन साझा न करें.	केवल उन्हीं से मिलें जिन्हें आप व्यक्तिगत रूप से जानते हों। कभी भी किसी अजनबी से उस व्यक्ति से न मिलें जिससे आप ऑनलाइन मिले हों.	जब सुरक्षा के बारे में संदेह हो, तो किसी जानकार व्यक्ति से मदद मांगें। कभी भी फ्रेंड रिक्वेस्ट स्वीकार न करें या अनजान लोगों के ईमेल न खोलें.	किसी भी वेबसाइट को इस्तेमाल करने या किसी भी ऐप को डाउनलोड करने से पहले विश्वसनीयता जांच जरूरी है	अपने ऑनलाइन खाते के साथ देखी गई किसी भी अवैध गतिविधियों के बारे में संबंधित अधिकारियों को बताएं

बैंक खाते का ऑनलाइन उपयोग करते समय जिम्मेदारियां



डिजिटल नागरिकों की जिम्मेदारियों के प्रति सरकार की पहल

- स्कूलों और कॉलेजों के छात्रों, शिक्षकों और अभिभावकों के बीच जागरूकता पैदा करने के लिए हर महीने के पहले बुधवार को "साइबर जागरूता दिवस" मनाने का प्रस्ताव है।
- डिजिटल नागरिकों के अधिकारों और जिम्मेदारियों के बारे में जागरूकता पैदा करने के लिए पहल की गई



डिजिटल नागरिकों के अधिकार

• **पहुँच का अधिकार**: प्रत्येक नागरिक को इंटरनेट का उपयोग करने का अधिकार है। इसे राय की स्वतंत्रता के लिए एक आवश्यक अधिकार माना जाता है। भारत के सर्वोच्च न्यायालय के अनुसार, इंटरनेट का उपयोग मूलभूत मौलिक अधिकार है

- **अभिव्यक्ति, सूचना और संचार की स्वतंत्रता का अधिकार:** प्रत्येक नागरिक को किसी भी जानकारी को व्यक्त करने या संचार करने के लिए सोशल मीडिया नेटवर्क का उपयोग करने का अधिकार है।.

- **गोपनीयता का अधिकार और डेटा संरक्षण:** उपयोगकर्ता को सोशल मीडिया पर प्रस्तुत अपनी व्यक्तिगत जानकारी को सुरक्षित रखने का अधिकार है। सभी सोशल मीडिया प्लेटफॉर्म के लिए गोपनीयता और डेटा सुरक्षा सेटिंग प्रदान करना अनिवार्य है जैसे कि उपयोगकर्ता चुन सकता है कि आपकी प्रोफ़ाइल कौन देखे या उनकी प्रोफ़ाइल को निजी रखे.

- **सुरक्षा का अधिकार:** सरकार को यह सुनिश्चित करना चाहिए कि सोशल मीडिया प्लेटफॉर्म के माध्यम से इंटरनेट उपयोगकर्ताओं की सुरक्षा सुनिश्चित की जाए। इसके अलावा, उपयोगकर्ता **1930** पर कॉल करके इंटरनेट पर किसी भी अवैध गतिविधि की रिपोर्ट करने के लिए साइबर सेल तक आसानी से पहुंच सकते हैं.

नागरिकों की ऑनलाइन सुरक्षा के लिए डिजिटल उपकरण - ऑनलाइन लेनदेन

- नागरिकों की ऑनलाइन सुरक्षा के लिए डिजिटल उपकरण - ऑनलाइन लेनदेन)
  - तत्काल भुगतान सेवा (आईएमपीएस)
  - प्री-पेड पेमेंट इंस्ट्रूमेंट्स (पीपीआई)
  - राष्ट्रीय इलेक्ट्रॉनिक टोल संग्रह (एनईटीसी)
  - रीयल-टाइम ग्रॉस सेटलमेंट (आरटीजीएस)

ऐप्स डाउनलोड करने के लिए, निम्नलिखित सुरक्षित ऑनलाइन स्टोर का उपयोग करें:

GET IT ON Google Play

Download on the App Store

अवैध साइबर गतिविधियां:

सबसे आम अवैध साइबर गतिविधियां हैं:

- **साइबर स्टॉकिंग** - साइबरस्टॉकिंग का मतलब इलेक्ट्रॉनिक मीडिया का उपयोग करने वाले किसी भी व्यक्ति का पीछा करना है। इसमें शामिल है:
  - **पहचान की चोरी के इरादे से जानकारी हासिल करना.**
  - **ओ अवांछित, भयावह, या अश्लील ईमेल, या संदेश भेजना.**
  - **सोशल मीडिया पर परेशान करना या धमकी देना.**

गोपनीयता/गोपनीयता का उल्लंघन और उल्लंघन

  - इसमें व्यक्ति की सहमति के बिना सोशल मीडिया/किसी भी मंच पर किसी भी निजी जानकारी या छवि को प्रकाशित या प्रसारित करना शामिल है.

- कानून द्वारा आवश्यक होने पर ही बैंक और सोशल मीडिया प्लेटफॉर्म किसी की व्यक्तिगत जानकारी साझा कर सकते हैं.

छिप कर देखना

- यह किसी निजी कार्य में लगे किसी व्यक्ति की सहमति के बिना उनकी छवियों या वीडियो को देखने, कैप्चर करने या साझा करने को संदर्भित करता है।
- यह **IPC** की धारा **354 (C)** के तहत दंडनीय कृत्य है।
- इसकी सूचना तुरंत साइबर सेल/महिला सेल/निकटवर्ती पुलिस स्टेशन को दी जानी चाहिए.

- **साइबर स्टॉकर्स से खुद को बचाने के लिए कदम हैं:**
  - साइबर प्रकोष्ठ/महिला प्रकोष्ठ को सूचना दें
  - उन्हें ब्लॉक करें
  - परिवार के सदस्यों को बताएं कि क्या चल रहा है
  - अपने खाते पर गोपनीयता फिल्टर सेट करें
  - सभी सबूत बचाओ
  - उन्हें रोकने के लिए कहो

अवैध डिजिटल गतिविधियों के लिए कानूनी प्रावधान

भारतीय दंड संहिता, 1860 के अनुसार निम्नलिखित कुछ कानूनी प्रावधान हैं

अनुभाग	अवैध गतिविधि	सज़ा
धारा 354ए	• महिलाओं की सहमति के बिना यौन सामग्री दिखाना या साझा करना • यौन अनुग्रह के लिए पूछना • यौन टिप्पणियां/संदेश पोस्ट करना/भेजना	• कठोर कारावास, जिसकी अवधि तीन वर्ष तक बढ़ाई जा सकती है, या जुर्माना, या दोनों.
धारा 354ग	• छिप कर देखना	• जुर्माने के साथ-साथ पहली बार दोषी पाए जाने पर तीन साल तक की कैद • बाद के दोषसिद्धि पर सात साल.
धारा 354डी	• साइबर स्टॉकिंग	• पहले अपराध के लिए तीन साल तक की कैद • जुर्माने के लिए उत्तरदायी और बाद में दोषी पाए जाने पर पांच साल की कैद

सूचना प्रौद्योगिकी अधिनियम, 2008 के अनुसार निम्नलिखित कुछ कानूनी प्रावधान हैं

आईटी अधिनियम की धारा	अवैध गतिविधि	सज़ा
धारा 66ई	• गोपनीयता का उल्लंघन • किसी भी व्यक्ति की सहमति के बिना उसके निजी क्षेत्र की तस्वीर लेना, प्रकाशित करना या प्रसारित करना	• कारावास, जिसे तीन वर्ष तक बढ़ाया जा सकता है, और/या जुर्माना।
धारा 66सी	• चोरी की पहचान • साइबर हैकिंग • इलेक्ट्रॉनिक हस्ताक्षर का दुरुपयोग	• कारावास जो तीन साल तक बढ़ाया जा सकता है • जुर्माना जो एक लाख रुपये तक हो सकता है

धारा 67	• **अश्लील सामग्री का प्रकाशन या प्रसारण।**	• **पहली बार दोष सिद्ध होने पर तीन साल तक का कारावास और जुर्माना** • **पांच से सात साल और दूसरी सजा पर जुर्माना**

कॉपीराइट अधिनियम के अनुसार, जब आप अपने रचनात्मक कार्य को सोशल मीडिया पर पोस्ट करते हैं, तो आप उसके कॉपीराइट के स्वामी होते हैं। आपकी अनुमति के बिना कोई भी कार्य का उपयोग नहीं कर सकता है और न ही प्लेटफ़ॉर्म स्वामित्व लेता है।

अवैध डिजिटल गतिविधियों के लिए निवारण तंत्र

आप किसी भी साइबर अवैध गतिविधि के खिलाफ निम्नलिखित पर अपनी शिकायत दर्ज करा सकते हैं:

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल

- https://cybercrime.gov.in/Default.aspx

राष्ट्रीय साइबर अपराध रिपोर्टिंग हेल्पलाइन नंबर -1930 (सुबह 9.00 बजे से शाम 6 बजे तक)

- https://ncrb.gov.in/en/node/2318

उमंग (न्यू-एज गवर्नेंस के लिए एकीकृत मोबाइल एप्लिकेशन)

- https://web.umang.gov.in/landing/department/cybercrime-reporting-portal.html

साइबर पुलिस पोर्टल

- https://cyberpolice.nic.in/

साइबर अपराध पोर्टल पर शिकायत दर्ज करने के लिए कदम

1. **लिंक पर जाएं:** https://cybercrime.gov.in/
2. वेबसाइट के निम्नलिखित अनुभाग तक नीचे स्क्रॉल करें और फिर शिकायत दर्ज करें बटन पर क्लिक करें
3. **गुमनाम रूप से रिपोर्ट करें बटन पर क्लिक करें**Fill in all the sections of the form and submit it for आगे की प्रक्रिया।सुनिश्चित करें कि आपके पास स्क्रीनशॉट जैसे साक्ष्य दस्तावेज तैयार हैं।
4. **आपकी शिकायत दर्ज हो जाएगी। आप किसी भी सहायता के लिए** 1930 **पर कॉल भी कर सकते हैं या शिकायत दर्ज करा सकते हैं**

संदर्भ पढ़ना:

- साइबर जागरुकता दिवस के बारे में अधिक जानने के लिए निम्नलिखित लिंक देखें
  Cyber Jaagrookta (Awareness) Diwas (Day 1 - Day 5)
- सोशल मीडिया प्लेटफॉर्म के अधिक सुरक्षित उपयोग के बारे में जानने के लिए निम्नलिखित लिंक देखें:
  Be Careful While Using Social Media Platforms

  ऑनलाइन साइबर अपराध की रिपोर्ट करने का तरीका जानने के लिए निम्नलिखित लिंक देखें:
  Cyber Crime Helpline Number

- भारत में ई-कॉमर्स कानून और विनियम कैसे हैं, यह जानने के लिए निम्नलिखित लिंक देखें
  E-Commerce Laws and Regulations in India

- मैं कैसे बता सकता हूं कि मेरा ऑनलाइन लेन-देन सुरक्षित है या नहीं, यह जानने के लिए निम्नलिखित लिंक देखें?
  Is My Online Transaction Secure

सुझाई गई व्यावहारिक गतिविधियाँ

अब जब आपने डिजिटल सुरक्षा और सुरक्षा कार्यक्रम के ऑनलाइन शिक्षण मॉड्यूल को पूरा कर लिया है, तो कृपया इन गतिविधियों को अपने वास्तविक जीवन में सीखने और लागू करने के लिए आज़माएं। हमें उम्मीद है कि ये गतिविधियां आपके सीखने को सुदृढ़ करेंगी.

1. अपने सभी सोशल मीडिया, बैंकिंग, ई-कॉमर्स और ईमेल खातों के लिए अद्वितीय और मजबूत 10-वर्णों का ASCII पासवर्ड बनाएं
2. प्रतिदिन अपने डेटा का बैकअप लें या स्वचालित बैक-अप सुविधा सेट करें
3. अपने ऑपरेटिंग सिस्टम सॉफ़्टवेयर की नियमित रूप से जाँच करें और उसे अपडेट करें (Windows/IoS/Android)
4. इंटरनेट ब्राउज़ करते समय गुप्त मोड का उपयोग करें और पता करें कि इसमें क्या अलग है
5. अपने बैंक वेबसाइटों पर सुरक्षित वित्तीय लेनदेन की सुविधा के लिए बैंकिंग और भुगतान सुरक्षा को सक्षम करने के लिए अपना एंटी-वायरस सॉफ़्टवेयर सेट करें
6. जब छोटे बच्चे आपके उपकरणों का उपयोग करते हैं तो खतरनाक और आपत्तिजनक वेबसाइटों को ब्लॉक करने के लिए माता-पिता के नियंत्रण को सक्षम करने के लिए अपना एंटीवायरस सॉफ़्टवेयर सेट करें
7. अपने फोन पर अनजान नंबरों से आने वाली कॉल्स को ध्यान से देखें और अगर वे अंतरराष्ट्रीय अज्ञात नंबरों से हैं तो जवाब न दें
8. आधार / पैन की केवल हस्ताक्षरित फोटोकॉपी जमा करें और उस तारीख का भी उल्लेख करें, जिसे आप फोटोकॉपी जमा कर रहे हैं और उन्हें जमा करने का उद्देश्य
9. एक डिजिलॉकर अकाउंट बनाएं और अपना आधार, पैन, ड्राइविंग लाइसेंस और एजुकेशन सर्टिफिकेट अपलोड करें
10. खुद को ग्रुप्स में जोड़े जाने से बचाने के लिए व्हाट्सएप पर सेटिंग्स बदलें
11. किसी अनजान व्यक्ति (या नंबर) द्वारा आपको बार-बार संदेश भेजने के लिए व्हाट्सएप पर "ब्लॉक" सुविधा का प्रयास करें
12. फेसबुक/इंस्टाग्राम/अन्य सोशल मीडिया सेटिंग्स को प्राइवेट में बदलें
13. अपनी मेल आईडी के लिए 2-फैक्टर ऑथेंटिकेशन बनाएं
14. अपने Google खाते/IoS खाते पर मेरा फ़ोन ढूंढें सक्षम करें
15. अपने वेब ब्राउज़र (Google Chrome/Microsoft Edge/Mozilla Firefox/Opera/IoS) पर सुरक्षा सुविधाओं को सक्षम करें
16. हफ्ते में एक बार अपने डिवाइस से ब्राउजिंग हिस्ट्री डिलीट करें
17. साइबरस्टॉकिंग या किसी भी अवैध साइबर गतिविधियों का अनुभव करने वाले किसी भी व्यक्ति / छोटे बच्चों को देखें, उनका समर्थन करें और उनकी सहायता करें

18. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल पर साझा की जाने वाली विभिन्न सेवाओं और सावधानियों का अन्वेषण करें (https://cybercrime.gov.in/Default.aspx)

19. अन्वेषण करें उमंग वेबसाइट (https://web.umang.gov.in/landing/department/cybercrime-reporting-portal.html)

20. राष्ट्रीय महिला आयोग के पोर्टल पर निवारण के लिए विभिन्न प्रकोष्ठों का अन्वेषण करें (http://ncw.nic.in/ncw-cells)

टिप्पणियाँ