डिजिटल सुरक्षा आणि सुरक्षिततेचा

Samhita CGF

कार्यक्रमाचा परिचय

सार्वजनिक आणि खाजगी सेवांचे डिजिटायझेशन आणि डिजिटल कम्युनिकेशन्स, विशेषत: सोशल मीडियाच्या आगमनाने वापरकर्त्यांच्या आर्थिक अखंडतेवर आणि वैयक्तिक गोपनीयतेवर महत्त्वपूर्ण परिणाम झाला आहे. सायबर क्राइम आणि डिजिटल फसवणुकीमुळे डिजिटल सुरक्षेतील तोटे ओळखणे आणि ते टाळण्यासाठी डिजिटल साक्षरतेची इष्टतम पातळी आवश्यक आहे

इंटरनेट आणि स्मार्टफोन्सची वाढती पोहोच आम्हाला ऑनलाइन फसवणुकीसाठी असुरक्षित बनवत आहे आणि आमच्या डेटाच्या संभाव्य ऑनलाइन धोक्यांमुळे आमची सुरक्षा धोक्यात आली आहे. आपली वैयक्तिक माहिती धोक्यात आणणाऱ्या आणि आपल्या मानसिक आरोग्यावरही परिणाम करणाऱ्या या धोक्यांपासून आपण स्वतःचे रक्षण केले पाहिजे

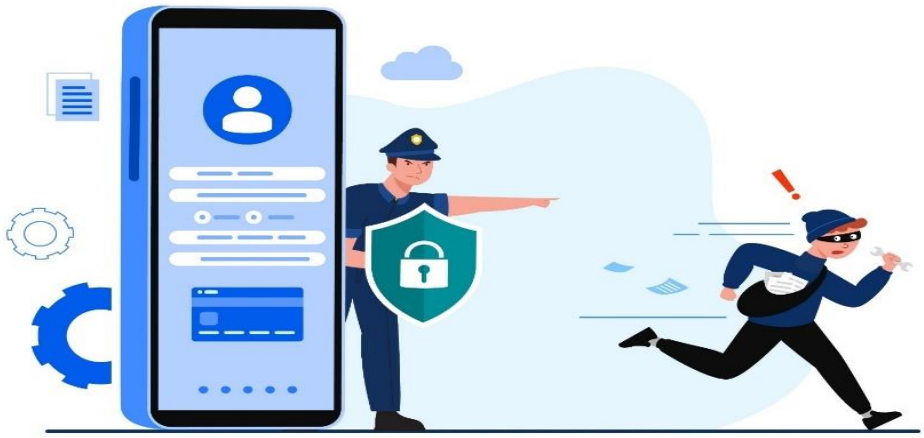
या कार्यक्रमात आपण जाणून घेणार आहोत:

- डिजिटल सुरक्षा आणि सुरक्षा म्हणजे काय?
- आर्थिक घोटाळे आणि त्यांचे प्रतिबंध
- सोशल मीडिया प्लॅटफॉर्म, घोटाळे आणि शिष्टाचार
- ओळख चोरीपासून स्वतःचे रक्षण करणे
- इंटरनेट स्मार्ट असणे
- डिजिटल अधिकार, कायदे आणि निवारण यंत्रणा

या हँडबुकने ऑनलाइन प्रोग्राममधील महत्त्वाच्या संकल्पनांच्या शिक्षणाची पुनरावृत्ती करण्याचा प्रयत्न केला आहे. 20 व्यावहारिक क्रियाकलापांची यादी शेवटी दिली आहे, आम्ही तुम्हाला 6 मॉड्युलमधून शिकण्यास बळकटी देण्यासाठी सराव कार्य म्हणून करण्यास उद्युक्त करतो

सामग्री सारणी

मॉड्यूल 1
डिजिटल सुरक्षा आणि सुरक्षिततेचा परिचय



डिजिटल सुरक्षा आणि सुरक्षा म्हणजे काय?

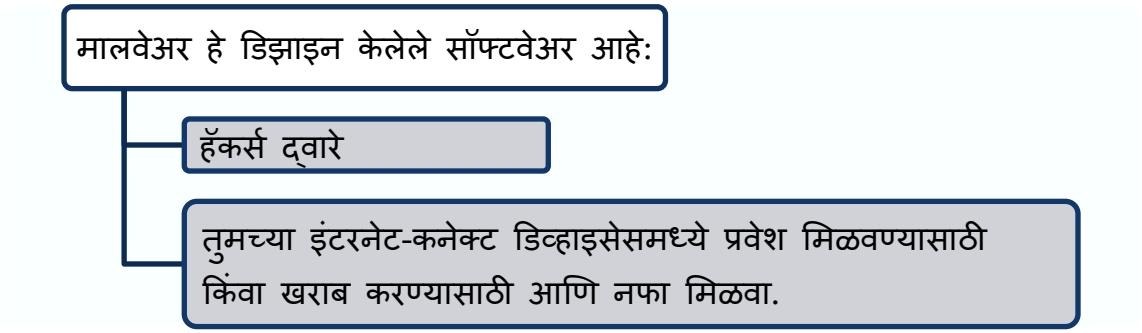
डिजिटल सेफ्टी आणि सिक्युरिटी म्हणजे इंटरनेट कनेक्टेड डिव्हाइसेस जसे की कॉम्प्युटर, मोबाईल डिव्हाईस, टॅब्लेट इ. घुसखोर किंवा हॅकर्सपासून संरक्षित करणे.

फिशिंग

फिशिंग हा डिजिटल माध्यमाद्वारे केलेला हल्ला आहे जो क्रेडिट कार्ड नंबर, बँक माहिती इत्यादीसारखी वैयक्तिक माहिती उघड करण्याचा प्रलोभन वापरून एखाद्या व्यक्तीचे पैसे किंवा ओळख चोरण्याचा प्रयत्न करतो.

ई-मेलमध्ये व्हायरस असू शकतात जे तुमच्या डिव्हाइसला हानी पोहोचवू शकतात किंवा कार्ड तपशील, पासवर्ड इ. सारखा तुमचा संवेदनशील डेटा चोरू शकतात. याला **फिशिंग** म्हणून ओळखले जाते जे अनेक प्रकारच्या सायबर हल्ल्यांपैकी एक आहे.

मालवेअर:



डिजिटल सुरक्षा आणि सुरक्षितता सुनिश्चित करणे

अनोळखी प्रेषकाच्या स्पॅम मेलवर किंवा मेलवर कधीही क्लिक करू नका

तुमचा वैयक्तिक आणि व्यावसायिक डेटा नेहमी सुरक्षित करा

तुमचे डिव्हाइस अँटी व्हायरस सॉफ्टवेअरसह सुरक्षित करा

तुम्हाला सायबर फसवणुकीचा संशय असल्यास, ताबडतोब संबंधित संस्थेला कॉल करा, तक्रार नोंदवा आणि त्यांना तुमच्या खात्याची सुरक्षितता सुनिश्चित करण्यासाठी सर्वोत्तम कारवाई करण्यास सांगा

शासनाकडे तक्रार दाखल करा. भारताचा ऑनलाइन सायबर क्राईम सेल

डिजिटल सुरक्षितता आणि सुरक्षिततेचे फायदे

24*7 सुरक्षित आणि सुरक्षित बँकिंग अनुभव

तुमच्या शाखेला भेट न देता त्रासमुक्त आणि झटपट व्यवहार

आर्थिक नुकसान टाळते

फिशिंग, पासवर्ड अटॅक इत्यादी सायबर हल्ल्यांपासून संरक्षण

व्यवहारांसाठी सुरक्षित/खाजगी विंडो प्रदान करते

सायबर सुरक्षा आणि गोपनीयता मिथक

एस क्र	समज	वास्तव
1.	सशक्त संकेतशब्द आमच्या डिव्हाइसेसचे आणि त्यावर संचयित केलेल्या डेटाचे रक्षण करतात.	सशक्त पासवर्डसह, आम्हाला द्वि-घटक प्रमाणीकरण आणि डेटा मॉनिटरिंग असणे आवश्यक आहे.
2.	हॅकर्स किंवा सायबर गुन्हेगार लहान व्यवसायांवर आणि कर्मचारी, गृहिणी, स्वयंरोजगार इत्यादी लोकांवर हल्ला करत नाहीत.	प्रगत सुरक्षा उपाय आणि जागरुकतेच्या अभावामुळे, असे छोटे व्यवसाय आणि लोक हॅकर्स किंवा सायबर गुन्हेगारांसाठी सॉफ्ट टार्गेट आहेत.
3.	अँटी-व्हायरस/अँटी-मालवेअर सॉफ्टवेअर आमच्या डिव्हाइसेस किंवा डेटाचे रक्षण करण्यासाठी पुरेसे आहे.	अँटी-व्हायरस/अँटी-मालवेअर सॉफ्टवेअर केवळ व्हायरस आणि मालवेअरपासून डिव्हाइसचे संरक्षण करेल परंतु सायबर-गुन्ह्यांची इतर अनेक माध्यमे आहेत जसे की माहिती पुनर्प्राप्त करण्यासाठी बनावट कॉल
4.	आम्हाला फक्त आमची उपकरणे हॅकर्सपासून सुरक्षित ठेवण्याची गरज आहे.	कोणतीही अंतर्गत व्यक्ती/कर्मचारी जाणूनबुजून किंवा चुकून माहिती लीक करू शकतो
5.	सायबर सुरक्षेची जबाबदारी फक्त इंटरनेट सेवा प्रदात्याच्या आयटी विभागाची आहे.	हॅकर्सपासून तसेच त्यांच्या सभोवतालच्या घुसखोरांपासून त्यांची वैयक्तिक किंवा व्यावसायिक माहिती आणि उपकरणांचे रक्षण करणे ही प्रत्येक व्यक्तीची सामाजिक जबाबदारी आहे.
6.	डाउनलोड करायचे ॲप ॲप स्टोअरवरून असल्यास ते सुरक्षित आहे.	ॲप स्टोअरमधील ॲप्सना व्हायरस/मालवेअर आणि गोपनीयता धोरणाविरुद्ध चाचणी आणि पडताळणी करणे आवश्यक आहे.
7.	कोणताही पासवर्ड-संरक्षित Wi-Fi सुरक्षित आहे.	पासवर्डसह कोणतेही सार्वजनिक वाय-फाय कनेक्शन तुमच्या डिव्हाइससाठी धोकादायक असू शकते. सार्वजनिक वाय-फाय कनेक्शनद्वारे कोणतीही गोपनीय माहिती किंवा दस्तऐवज कधीही सामायिक करू नका
8.	तुमचे स्वतःचे डिव्हाइस आणा किंवा BYOD कामावर वापरण्यासाठी सुरक्षित आहे	इंटरनेटशी कनेक्ट केलेले कोणतेही उपकरण डिजिटल धोक्यांसाठी प्रवण असते.
9.	HTTPS वेबसाइट विश्वासार्ह आहेत आणि त्या हॅक केल्या जाऊ शकत नाहीत	हॅकर्स HTTPS एन्क्रिप्शन बायपास करू शकतात; म्हणून, फक्त विश्वसनीय HTTPS वेबसाइट वापरा उदा. बँकेने शेअर केल्याप्रमाणे तुमच्या बँकेची वेबसाइट.
10.	कोणत्याही उल्लंघनाविरूद्ध 100% सायबर सुरक्षा साध्य करता येते.	दररोज एक नवीन धोका विकसित होत आहे. 100% सायबर सुरक्षा साध्य करता येत नाही.

या सर्वोत्कृष्ट पद्धतींचे अनुसरण करून, तुम्ही सायबर गुन्ह्यांचे बळी होण्याचे टाळू शकता:

- ✓ ब्राउझर वापरताना नेहमी गुप्त मोड वापरा.
- ✗ ब्राउझरवर क्रेडेन्शियल्स कधीही सेव्ह करू नका.
- ✗ थर्ड पार्टी लिंकवरून कधीही ॲप्स डाउनलोड करू नका.
- ✗ कोणत्याही असुरक्षित वेबसाइट/ॲपवर वैयक्तिक माहिती कधीही शेअर करू नका
- ✓ तुमचा अँटीव्हायरस अपडेट ठेवा.
- ✗ व्हायरस स्कॅनिंगशिवाय कोणतीही फाईल कधीही डाउनलोड करू नका.
- ✓ तुमच्या डेटाचा बॅकअप ठेवा.
- ✗ तुमचे डिव्हाइस कधीही लक्ष न देता सोडू नका.
- ✗ तुमचे पासवर्ड कधीही शेअर करू नका.
- ✓ नेहमी द्वि-घटक प्रमाणीकरण वापरा.

पासवर्ड

पासवर्ड ही अक्षरांची एक स्ट्रिंग आहे जी संगणक प्रणाली किंवा सेवेमध्ये प्रवेश करण्यास अनुमती देते.

एक अद्वितीय पासवर्ड तयार करण्यासाठी

- अनुक्रमिक अक्षरे किंवा संख्या टाळा
- वैयक्तिक माहिती टाळा
- लांब पासवर्ड बनवा
- असंबंधित शब्द वापरा

वेगवेगळ्या ॲप्ससाठी वेगवेगळे पासवर्ड वापरा आणि तुमचे पासवर्ड वारंवार बदला

माहितीच्या अनधिकृत प्रवेशामुळे ओळख चोरी, आर्थिक नुकसान, डिजिटल घोटाळ्यांची वाढलेली असुरक्षा किंवा छळ यासह जोखीम होऊ शकतात

वन-टाइम पासवर्ड (OTP):

ओटीपी हे वन-टाइम पासवर्ड आहेत, जे ऑनलाइन आर्थिक व्यवहारांसाठी सुरक्षा प्रदान करतात

तुमचा OTP गोपनीय ठेवण्यासाठी

- तुमचा OTP कधीही शेअर करू नका.
- व्यवहार पूर्ण केल्यानंतर OTP हटवा.
- नेहमी अधिकृत वेबसाइटद्वारे लॉग इन करा.
- अज्ञात ॲप्स कधीही डाउनलोड करू नका.

ओटीपी चोरण्याचे काही सामान्य मार्ग आहेत:

- बँक अधिकारी म्हणून दाखवून आणि तुम्हाला तुमचे खाते तपशील सत्यापित करण्यास सांगून.
- SMS किंवा WhatsApp द्वारे लिंक पाठवून आणि तुम्ही क्लिक करता तेव्हा मालवेअर पसरवून.
- तुम्हाला स्क्रीन-शेअरिंग ॲप डाउनलोड करण्यास सांगून त्याद्वारे तुमच्या डेटावर रिमोट ॲक्सेस मिळेल.

क्रेडिट/डेबिट कार्ड फसवणूक:

क्रेडिट/डेबिट कार्ड फसवणूक होते जेव्हा एखादी व्यक्ती तुमच्या माहितीशिवाय आर्थिक व्यवहारांसाठी तुमच्या क्रेडिट कार्डची माहिती बेकायदेशीरपणे वापरते.

डेबिट/क्रेडिट कार्डच्या फसवणुकीपासून सुरक्षित राहणे:

- तुमचे कार्ड नेहमी तुमच्याकडे ठेवा.
- तुमचा पिन नियमितपणे बदला.
- तुमचा पिन कोणाशीही शेअर करू नका.
- तुमचे मासिक क्रेडिट कार्ड विवरण काळजीपूर्वक तपासा
- तुमचे कार्ड अज्ञात वेबसाइट किंवा ॲप्सवर वापरणे टाळा.
- संशयास्पद लिंकवर क्लिक करू नका.
- तुमचे कार्ड चोरीला गेल्यास किंवा हरवल्यास त्वरित तुमच्या बँकेला कळवा

दस्तऐवज फसवणूक पूर्व

फसवणूक करणारे विविध कारणांसाठी आधार आणि पॅन कार्डसारखी बनावट कागदपत्रे तयार करतात. यासाठी ते बनावट कागदपत्रांचा वापर करतात:

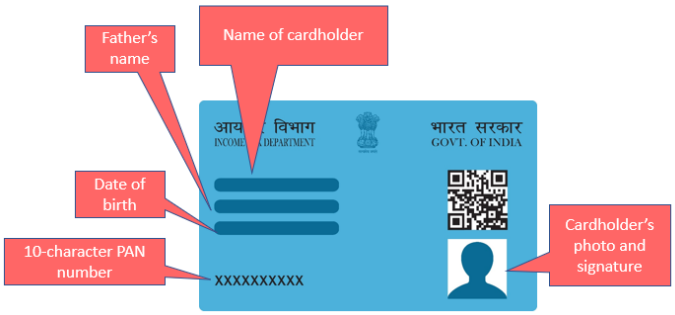
- नवीन बँक खाते उघडा
- कर्जासाठी अर्ज करा
- मालमत्ता खरेदी करा
- आयकर रिटर्न/विमा फाइलिंग फाइल करा

आधार कार्ड हे तितकेच महत्त्वाचे आहे:

- प्रत्येक रहिवासी भारतीयासाठी ओळख सक्षम करते.
- पत्त्याचा पुरावा म्हणून काम करते.
- ओळखीचा पुरावा म्हणून काम करते.
- धारकांना सरकारी अनुदानाचा लाभ घेण्यास सक्षम करते.
- बँक खाते उघडताना ओळखीसाठी वापरले जाऊ शकते.
- नोकऱ्यांसाठी अर्ज करताना ओळखीसाठी वापरले जाऊ शकते.

खालीलपैकी कोणतेही व्यवहार करण्यासाठी आम्हाला **पॅन कार्ड** आवश्यक आहे:

- बँक खाते उघडणे.
- टॅक्स रिटर्न भरणे.
- नवीन कर्जासाठी अर्ज करणे.
- नवीन मालमत्ता खरेदी करणे किंवा विकणे.
- डेबिट/क्रेडिट कार्ड खरेदी करणे.
- विमा प्रीमियम भरणे



आधार/पॅन कार्डच्या फसवणुकीपासून सुरक्षित राहण्यासाठी

- अनौपचारिक व्यवहारांसाठी तुमचे आधार किंवा पॅन कार्ड वापरू नका.
- आधार किंवा पॅन कार्डचे तपशील इतरांसोबत शेअर करू नका.
- तुमच्या आधार किंवा पॅन कार्ड्सच्या फक्त स्वाक्षरी केलेल्या फोटोकॉपी वापरण्याचे विशिष्ट कारण आणि वापराच्या तारखेसह सबमिट करण्याचा प्रयत्न करा.
- ऑनलाइन पोर्टलवर तुमचे पूर्ण नाव आणि जन्मतारीख टाकू नका.

महत्त्वाची कागदपत्रे सुरक्षित ठेवणे

डिजीलॉकर हे एक डिजिटल लॉकर आहे, भारत सरकारने प्रदान केलेली एक सुविधा आहे, जी तुम्हाला आधार, पॅन, ड्रायव्हिंग लायसन्स, पासपोर्ट, मार्कशीट्स, निवडणूक मतदार ओळखपत्र इत्यादीसारख्या अधिकृत दस्तऐवजांच्या स्कॅन केलेल्या प्रती संग्रहित करण्यास सक्षम करते. तुम्ही यामध्ये प्रवेश करू शकता. कागदपत्रे कुठेही, कधीही

डिजीलॉकरचे फायदे

संदर्भ वाचन:

- सायबर स्वच्छता केंद्र : https://www.csk.gov.in/
- भारतातील सायबर गुन्ह्यांवर संपूर्ण मार्गदर्शक: https://indiaforensic.com/compcrime.htm
- G 20 प्रेसिडेन्सीची भारताची सायबरसुरक्षा प्राधान्ये: https://www.orfonline.org/expert-speak/indias-cybersecurity-priorities-for-g20-presidency/
- भारतीय सायबर क्राईम समन्वय केंद्राबद्दल तपशील: https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme

मॉड्यूल 2
आर्थिक घोटाळे आणि त्यांचे प्रतिबंध

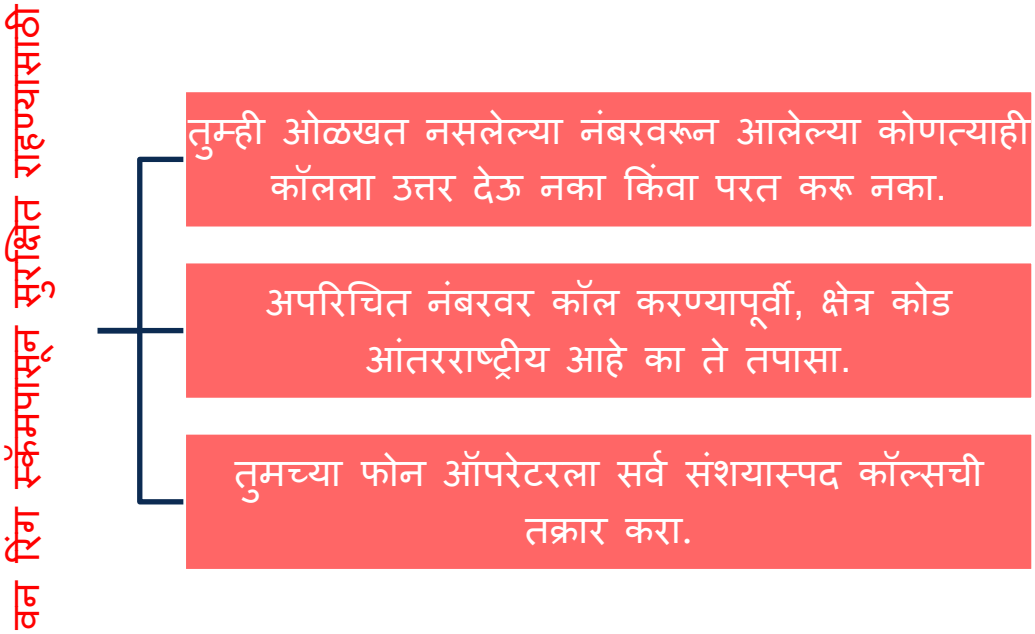
आर्थिक नुकसान टाळण्यासाठी अनोळखी नंबरवरून कॉल्स आणि आंतरराष्ट्रीय कॉल्स व्यवस्थापित करणे:

जेव्हा **कॉलर कॉल** करतो आणि एका रिंगनंतर फोन हँग करतो तेव्हा वन-रिंग घोटाळा होतो. लोकांना त्यांचे पैसे देण्यासाठी फसवणे हा एक घोटाळा आहे.

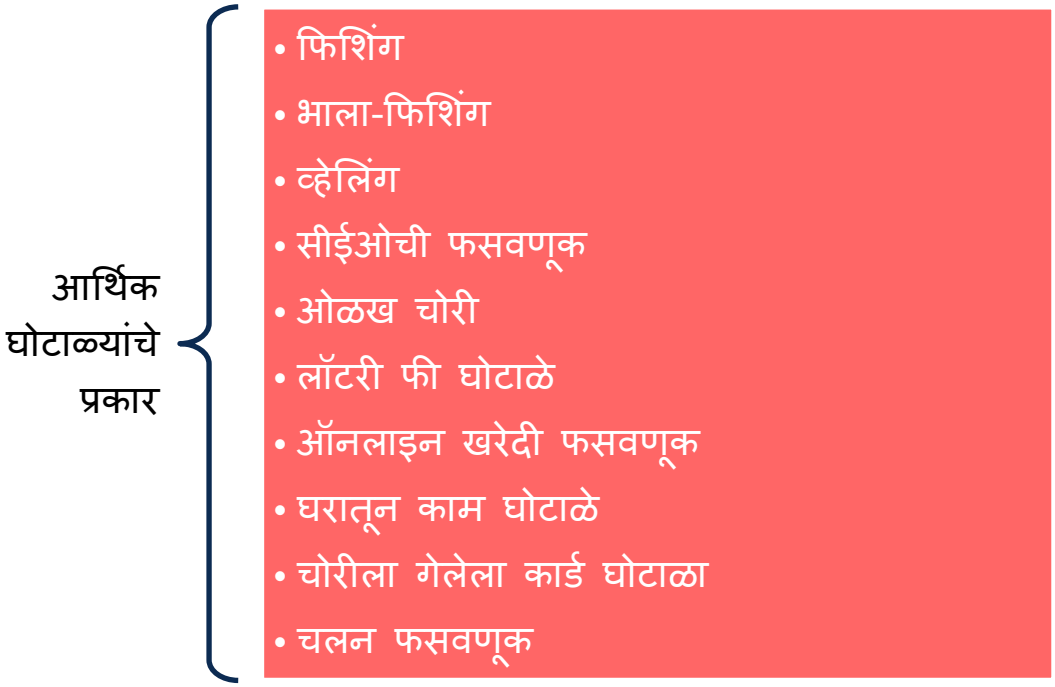
वन-रिंग घोटाळा कसा कार्य करतो:

- घोटाळे करणारा आंतरराष्ट्रीय प्रीमियम दर क्रमांक (IPRN) नियुक्त करतो.
- स्कॅमर तुम्हाला एक रिंग देईल आणि नंतर कॉल डिस्कनेक्ट करेल.
- तुम्हाला वाटेल की तुमचा एक महत्त्वाचा कॉल चुकला आणि त्याच नंबरवर परत कॉल कराल.
- तुमचा कॉल घेतला जाईल पण, दुसऱ्या बाजूने तुमच्याशी कोणीही बोलणार नाही.
- कोणतेही उत्तर न मिळाल्यानंतर, तुम्ही तुमचा कॉल डिस्कनेक्ट कराल.
- कॉल केल्यानंतर, तुम्हाला कळेल की तुम्ही आंतरराष्ट्रीय कॉल करण्यासाठी मोठ्या प्रमाणात पैसे गमावले आहेत.

वन-रिंग स्कॅमपासून सुरक्षित राहण्यासाठी:



आर्थिक घोटाळ्यांचे प्रकार



फिशिंग हा डिजिटल माध्यमाद्वारे केलेला हल्ला आहे जो क्रेडिट कार्ड क्रमांक, बँक माहिती इ. यांसारखी वैयक्तिक माहिती उघड करण्यासाठी एखाद्या व्यक्तीचे पैसे किंवा ओळख चोरण्याचा प्रयत्न करतो..

स्पिअर-फिशिंग हा फिशिंगचा एक प्रकार आहे जो अतिशय विशिष्ट आणि वैयक्तिकृत संदेश वापरून एखाद्या व्यक्तीचे पैसे किंवा ओळख चोरण्याचा प्रयत्न करतो.

भाला-फिशिंग प्रमाणेच, व्हेलिंग उच्च-प्रोफाइल, प्रसिद्ध आणि श्रीमंत व्यक्ती जसे की सीईओ आणि सेलिब्रिटींना लक्ष्य करते.

सीईओच्या फसवणुकीत, फसवणूक करणारे तुम्ही ज्या कंपनीसाठी काम करता त्या कंपनीचे सीईओ किंवा अन्य अधिकारी असल्याचे भासवतात आणि तुम्हाला पैसे पाठवण्यास सांगतात किंवा त्यांना तुमच्या संवेदनशील माहितीमध्ये प्रवेश देण्यास सांगतात..

ओळख चोरीमध्ये, **फसवणूक करणारे** तुमची वैयक्तिक माहिती जसे की नाव, पत्ता, ईमेल पत्ता तसेच क्रेडिट कार्ड किंवा खाते माहिती लक्ष्य करतात. त्यानंतर ते तुमच्या नावाखाली ऑनलाइन वस्तू मागवतात आणि तुमची क्रेडिट कार्ड माहिती वापरून पैसे देतात.

लॉटरी शुल्क घोटाव्यामध्ये, तुम्हाला एक सूचना मिळते की तुम्ही लॉटरी जिंकली आहे आणि तुम्हाला तुमच्या बक्षीसावर दावा करण्यासाठी फी जमा करण्यास सांगितले जाते..

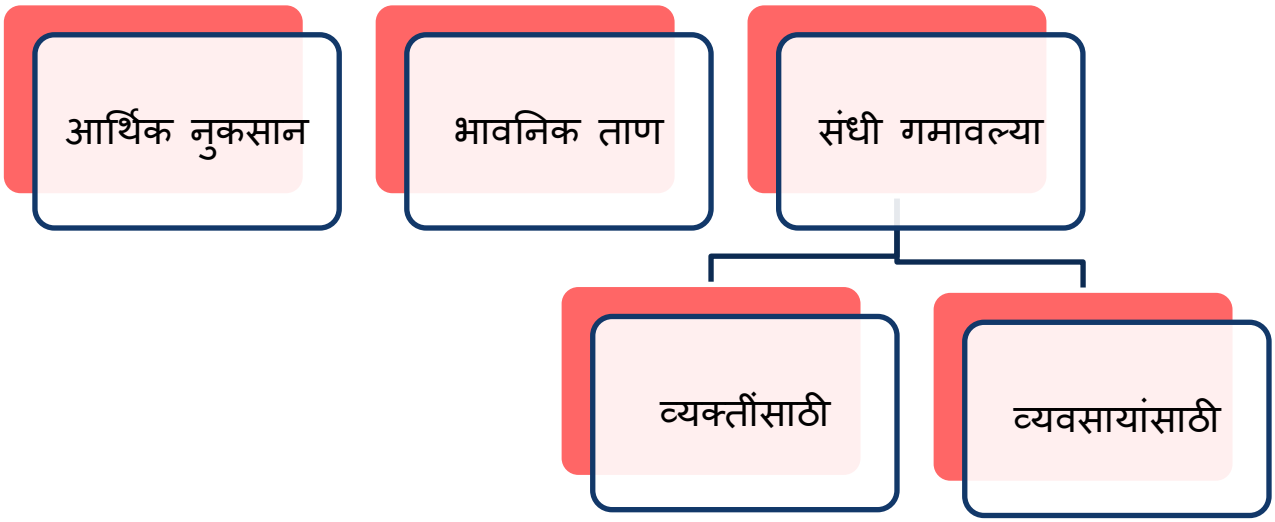
ऑनलाइन शॉपिंगच्या फसवणुकीत, बनावट शॉपिंग पोर्टल आकर्षक किमतीत उत्पादने दाखवते. एकदा पेमेंट केल्यावर, तुम्हाला बनावट उत्पादन किंवा कोणतेही उत्पादन मिळत नाही.

वर्क फ्रॉम-होम घोटाव्यांमध्ये, फसवणूक करणारे लोक घरून काम करून चांगला पगार मिळवतील असे आश्वासन देऊन फसवणूक करतात. ते नोकरी शोधणाऱ्यांना ठराविक रक्कम जमा करण्यास सांगतात. पैसे जमा झाल्यानंतर नोकरदारांचा माग काढला जात नाही.

डेबिट/क्रेडिट कार्ड घोटाळा होतो जेव्हा एखादी व्यक्ती तुमची डेबिट/क्रेडिट कार्ड माहिती तुमच्या माहितीशिवाय आर्थिक व्यवहारांसाठी बेकायदेशीरपणे वापरते..

इनव्हॉइस फसवणुकीत, फसवणूक करणारे पुरवठादार म्हणून व्यवसायाला लक्ष्य करतात आणि ज्या बँक खात्यात पावत्या भरल्या जातात त्या खात्याचे तपशील अपडेट करण्यास सांगतात.

आर्थिक घोटाव्यांचे परिणाम



ऑनलाइन आर्थिक घोटाव्यांपासून सुरक्षित राहणे:

- सर्व वैयक्तिक माहिती, ओळखपत्र आणि बँक कार्ड नेहमी सुरक्षित ठेवा.
- तुमचे पिन क्रमांक गोपनीय ठेवा.
- तुमचे पिन नंबर लिहून ठेवू नका किंवा ते बँक कार्ड्समध्ये साठवू नका.
- कोणत्याही व्यक्तीला बँक खात्याचे तपशील किंवा इतर सुरक्षा माहिती कधीही देऊ नका.
- जे लोक ते तुमच्या वतीने बँकेत ठेवण्याची ऑफर देतात त्यांना तुमचे पैसे कधीही देऊ नका
- तुमचे एटीएम कार्ड इतर कोणालाही वापरू देऊ नका.
- संशयास्पद व्यवहारांसाठी मासिक क्रेडिट कार्ड स्टेटमेंट आणि इतर बँक स्टेटमेंट काळजीपूर्वक तपासा.
- तुमचे कार्ड चोरीला गेल्याची किंवा हरवल्याची त्वरित तक्रार करा.
- इंटरनेटवर पेमेंट करण्यासाठी तुमचे कार्ड वापरताना काळजी घ्या.
- तुमचे कार्ड पडताळणी मूल्य (CVV) फक्त सुरक्षित पेमेंट वेबसाइटवरच उघड करा
- कोणत्याही आर्थिक करारावर डिजिटल स्वाक्षरी करताना काळजी घ्या.

- परदेशातील बँकेत मोठ्या प्रमाणात पैसे ठेवण्यासाठी तुमच्या मदतीसाठी विचारणा करणारे कॉल, पत्र, ई-मेल किंवा फॅक्स यांच्यापासून सावध रहा.
- स्पॅम किंवा अनपेक्षित ई-मेल्सना उत्तर देऊ नका जे तुम्हाला नोकरी किंवा इतर काही फायद्याचे आश्वासन देतात.

तुमच्या ऑनलाइन बँकिंग तपशीलाशी तडजोड झाली असल्यास, खालील उपाय करा ...

1. तुमच्या बँकेला ताबडतोब सूचित करा
2. तुमचे क्रेडिट/डेबिट कार्ड किंवा UPI ॲप ब्लॉक करा
3. नेट बँकिंगसाठी तुमचे पासवर्ड बदला
4. तुमचे UPI, डेबिट कार्ड आणि क्रेडिट कार्ड पिन बदला
5. वर्तमान डेबिट/क्रेडिट कार्ड रद्द करा आणि बदलण्यासाठी विचारा
6. एक नवीन सुरक्षा वैशिष्ट्य सेट करा (मल्टी-स्टेप ऑथेंटिकेशन)

संदर्भ वाचन:

- आर्थिक फसवणुकीबद्दल अधिक: https://cybercrime.gov.in/pdf/Financial%20Fraud%20Brochures%20final.pdf

मॉड्यूल 3
सामाजिक माध्यमे

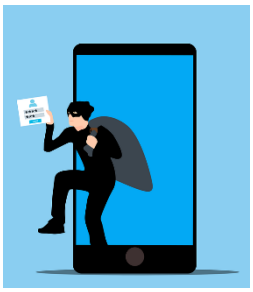
मोठ्या प्रमाणावर वापरले जाणारे सोशल मीडिया प्लॅटफॉर्म

- व्हॉट्सॲप
- इंस्टाग्राम
- फेसबुक
- ट्विटर
- शेअरचॅट
- स्नॅपचॅट

सोशल मीडिया प्लॅटफॉर्म वापरकर्त्यांना चित्रे प्रदर्शित करण्यास आणि सार्वजनिकरित्या पोस्ट करण्यास सक्षम करतात. फसवणूक करणारे वापरकर्त्याच्या माहितीशिवाय गुप्तपणे माहिती गोळा करतात. गोळा केलेल्या माहितीसह, फसवणूक करणारे नंतर वेगवेगळ्या मार्गांनी वापरकर्त्यांशी संपर्क साधतात.

विविध मार्ग ज्याद्वारे फसवणूक करणारे सोशल मीडिया वापरकर्त्यांना फसवतात:

सामाजिक अभियांत्रिकी



या हल्ल्यात अनधिकृत प्रवेश, नेटवर्क आणि आर्थिक फायदा मिळवण्यासाठी हेराफेरीचा समावेश आहे. फसवणूक करणारे व्यवहार किंवा पैसे ट्रान्सफर करण्यासाठी स्वतःला बँकेचे किंवा अन्य संस्थेचे अस्सल प्रतिनिधी म्हणून दाखवून वापरकर्त्याला फसवतात.

स्वतःचे रक्षण करण्यासाठी, कधीही व्यवहार करू नका किंवा फोन कॉलवर आधारित बँक तपशील देऊ नका.

सोशल मीडिया फिशिंग

फिशिंगचा उद्देश वैयक्तिक डेटा प्राप्त करणे किंवा वापरकर्त्याच्या सोशल मीडिया खात्यांमध्ये प्रवेश करणे आहे.

तोतयागिरी

या घोटाळ्यात, फसवणूक करणारे लोक संवेदनशील माहिती चोरण्यासाठी वापरकर्त्याद्वारे विश्वास ठेवू शकेल अशी एखादी व्यक्ती असल्याचे भासवतात.

सोशल मीडिया स्क्रॅपिंग

हे सोशल मीडिया फिशिंग आणि तोतयागिरीचे उदाहरण आहे. वैयक्तिक माहिती पुनर्प्राप्त करण्यासाठी फसवणूक करणारे ग्राहक एक्झिक्युटिव्ह म्हणून बनावट कॉल करतात. त्यात नावे, जन्मतारीख, वैयक्तिक फोटो आणि स्थान समाविष्ट आहे. फसवणूक करणारे ही माहिती भविष्यात डेटा/ओळख चोरीसाठी वापरतात

सोशल मीडिया स्क्रॅपिंगपासून स्वतःचे रक्षण करण्यासाठी:

- तुमचे वैयक्तिक तपशील कधीही शेअर करू नका
- अशा कॉल्सबद्दल ताबडतोब तक्रार करा
- संशयास्पद प्रोफाइलचा अहवाल द्या आणि ब्लॉक करा

डेटा चोरी

या घोटाळ्यात फसवणूक करणारे अवैधरित्या गोपनीय माहिती हस्तांतरित करतात. मालवेअर सामान्यत: लाइक बटण, ऑडिओ क्लिप, व्हिडिओ किंवा सोशल मीडियावरील लिंक्समध्ये प्रच्छन्न केले जाऊ शकते.

फसवणूक आणि फेक न्यूज

या घोटाळ्यात, फसवणूक करणारे काही अपप्रचार करून वापरकर्त्यांची दिशाभूल करण्यासाठी खोटी माहिती पसरवतात.

फसव्या कॉल्स आणि मेसेजपासून स्वतःचे रक्षण करण्यासाठी, आपण केले पाहिजे:

- नेहमी फोटो आणि मीडिया काळजीपूर्वक तपासा.
- विश्वसनीय स्त्रोतांकडून माहिती सत्यापित करा.
- बेकायदेशीर आणि धोकादायक संभाषण गटांना ब्लॉक करा आणि तक्रार करा.
- अवांछित गटांमध्ये सामील होण्यापासून रोखण्यासाठी गट गोपनीयता सेटिंग्ज वापरा.

एनक्रिप्टेड बॅकअप

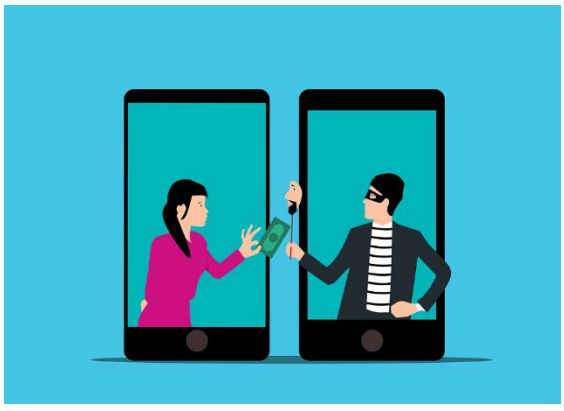
या घोटाळ्यात, डेटा अल्गोरिदमद्वारे एन्कोड केलेला नाही आणि कोणीही वाचू शकतो.

बनावट खाती ओळखण्यासाठी, सोशल मीडियावर फसवणूक करणाऱ्याचे खालील वर्तन पहा:

- कॉल आणि मीटिंग टाळतो
- ऑनलाइन उपस्थिती नाही
- मर्यादित मित्र/अनुयायी
- अगदी अलीकडील प्रोफाइल
- व्यावसायिक चित्रे
- चोरलेली चित्रे
- पैसे मागतो
- स्पष्ट प्रतिमा किंवा व्हिडिओ विचारतो

सोशल मीडिया फ्रॉडचा सर्वात सामान्य प्रकार म्हणजे **कॅटफिशिंग**.

कॅटफिशिंग हा ऑनलाइन फसवणुकीचा एक प्रकार आहे. फसवणूक करणारा बनावट ओळख वापरून दुसरे कोणीतरी असल्याचे भासवतो आणि प्रेमसंबंध निर्माण करून सोपे लक्ष्य फसवतो.



- बनावट ओळखीचे समर्थन करण्यासाठी, एक मांजर-फिशर तयार केलेल्या कथा आणि बनावट फोटो वापरतो.
- एक मांजर-फिशर सहसा पैसे आणि वैयक्तिक माहिती विचारतो

सर्व सोशल मीडिया प्लॅटफॉर्ममध्ये वापरकर्त्याला दुसऱ्या त्रासदायक किंवा बनावट वापरकर्त्यापासून संरक्षण देण्याच्या समान कार्यासह **"रिपोर्ट" आणि "ब्लॉक"** ची वैशिष्ट्ये आहेत.

ब्लॉक

संपर्क अवरोधित केल्याने वापरकर्त्याकडून संदेश प्राप्त करणे अक्षम होते.

अहवाल द्या

जर एखाद्या वापरकर्त्याद्वारे किंवा गटाद्वारे अटी आणि शर्तींचे उल्लंघन केले जात असेल अहवाल देणे कंपनीला सूचित करण्यात मदत करते

व्हॉट्सॲपचे फायदे आहेत:

- कोणत्याही पॉप-अप जाहिराती नाहीत
- वापरण्यास सोप
- कोणतीही शुल्क संदेश सेवा नाही
- मीडिया, स्थान आणि स्थिती शेअरिंग
- समूह सामूहिक संवाद सक्षम करतात
- व्हिडिओ कॉलिंग

व्हॉट्सॲपचे तोटे आहेत:

- अनेक गोपनीयतेच्या समस्या आहेत
- पुष्कळ असत्यापित माहितीची देवाणघेवाण आहे
- व्हाट्स एप्प खूप व्यसन आहे

सोशल मीडिया शिष्टाचार:

सोशल मीडिया शिष्टाचार ही मार्गदर्शक तत्त्वे आहेत जी सोशल मीडिया प्लॅटफॉर्म आणि वापरकर्ते ऑनलाइन प्रतिष्ठा जपण्यासाठी वापरतात.

सोशल मीडिया करा

- ज्ञात संपर्कांशी संवाद साधा
- परवानगीसाठी विचारा आणि सीमांचा आदर करा
- गट नियंत्रणे वापरा
- फक्त योग्य फोटो आणि व्हिडिओ शेअर करा
- योग्य फोटो आणि व्हिडिओ पोस्ट करा
- सोशल मीडिया प्लॅटफॉर्मच्या मार्गदर्शक तत्त्वांचे अनुसरण करा.

सोशल मीडिया करू नका

- इतर वापरकर्त्यांना स्पॅम करा
- इतरांची वैयक्तिक माहिती वापरा किंवा शेअर करा
- मोठ्या प्रमाणात संदेश
- अपशब्द वापरा
- खोट्या बातम्या आणि दिशाभूल करणारी माहिती वाढवा
- ओव्हर-शेअर

व्हॉट्सॲप डॉस:

- ✓ प्रोफाईल फोटो, स्थिती आणि तुमच्या ओळखीच्या संपर्कांबद्दलच्या माहितीची दृश्यमानता मर्यादित करा.
- ✓ यादृच्छिक गटांमध्ये जोडले जाणे टाळण्यासाठी गट गोपनीयता सेटिंग्ज वापरा.
- ✓ एंड-टू-एंड एन्क्रिप्शन वापरा..
- ✓ चॅटमधील लाईव्ह लोकेशन बंद करा.
- ✓ तुमच्याकडे जाण्याचा प्रयत्न करणाऱ्या अज्ञात वापरकर्त्यांना ब्लॉक करा.

व्हाट्स एप्प करू नका

- तुमची वैयक्तिक माहिती अनोळखी व्यक्तींसोबत शेअर करा.
- तुमची गोपनीयता सेटिंग सार्वजनिक वर सेट करा.
- इतर वापरकर्त्याच्या गोपनीयतेचा अनादर करा.

इंस्टाग्राम डॉस

- तुमच्या फॉलोअर्समध्ये ओळखीच्या लोकांना जोडा.
- योग्य फोटो, व्हिडिओ, माहिती पोस्ट करा.
- इतर वापरकर्त्याच्या गोपनीयतेचा आदर करा.
- फसवणूक करणाऱ्यांसाठी ब्लॉक/रिपोर्ट वापरा.

इंस्टाग्राम करू नका

- सार्वजनिक खात्यांवर संवेदनशील माहिती शेअर करा.
- परवानगीशिवाय दुसऱ्याच्या पोस्टचा वापर करा.
- अनुयायी खरेदी करा.
- इतरांचा अनादर करा

फेसबुक डॉस

- सत्यापित बातम्या आणि माहिती सामायिक करा.
- तुमचा डेटा आणि माहिती सुरक्षित करण्यासाठी गोपनीयता सेटिंग्ज वापरा.
- फक्त योग्य मीडिया शेअर करा.
- ज्ञात वापरकर्त्यांशी संवाद साधा.

फेसबुक करू नका

- असत्यापित बातम्या शेअर करा
- यादृच्छिक लिंकवर क्लिक करा.
- कोणत्याही जाहिरातीवरील बँक खात्याच्या तपशीलासारखी तुमची क्रेडेन्शियल्स भरा

ट्विटर डॉस

- तुमचा डेटा आणि ट्विट्सचा गैरवापर होण्यापासून संरक्षण करण्यासाठी गोपनीयता आणि सुरक्षितता पर्याय वापरा.
- ट्विटद्वारे तुमचे विचार व्यक्त करण्यासाठी योग्य भाषेचा वापर करा.
- केवळ ज्ञात वापरकर्त्यांच्या विनंत्या स्वीकारा.

ट्विटर करू नका

- तुमची मते इतरांवर लादणे.
- असभ्य भाषा वापरा.
- तुमचे थेट स्थान सार्वजनिकपणे शेअर करा.

सोशल मीडिया संवादासाठी खूप उपयुक्त आहे आणि आपल्याला जगाशी अपडेट ठेवतो. पण त्याचा वापर जबाबदारीने करायला हवा. सोशल मीडियावर अनेक मनोरंजक तथ्ये आणि बातम्या उपलब्ध आहेत. त्यांना प्रसारित करण्यापूर्वी आपण सावध असणे आवश्यक आहे..

संदर्भ वाचन:

- सायबर जागरुकता दिवस: https://www.youtube.com/watch?v=6whmq4EwIIo
- सायबर बुलिंग तथ्ये : https://www.youtube.com/watch?v=0Xo8N9qlJtk

मॉड्यूल 4
ओळख चोरी

संकेतशब्द आणि प्रमाणीकरण

पासवर्ड हा प्रमाणीकरण प्रक्रियेदरम्यान वापरकर्त्याची ओळख सत्यापित करण्यासाठी वापरल्या जाणाऱ्या वर्णांची एक स्ट्रिंग आहे.

पासवर्ड तुमच्या स्मार्ट डिव्हाइसेस आणि वैयक्तिक माहितीवर अनधिकृत प्रवेशापासून प्रथम संरक्षण प्रदान करतात.

- पासवर्डमध्ये किमान दहा वर्ण असावेत आणि त्यात वर्णांचे संयोजन असावे जसे की:

विशेष वर्ण	अप्पर-केस आणि लोअर-केस अक्षरे	संख्या

- “12345” किंवा “qwerty” सारखे क्रम वापरणे टाळा
- तुम्ही अक्षरांऐवजी एकसारख्या दिसणाऱ्या संख्या वापरू शकता—O ऐवजी शून्य 0 वापरा

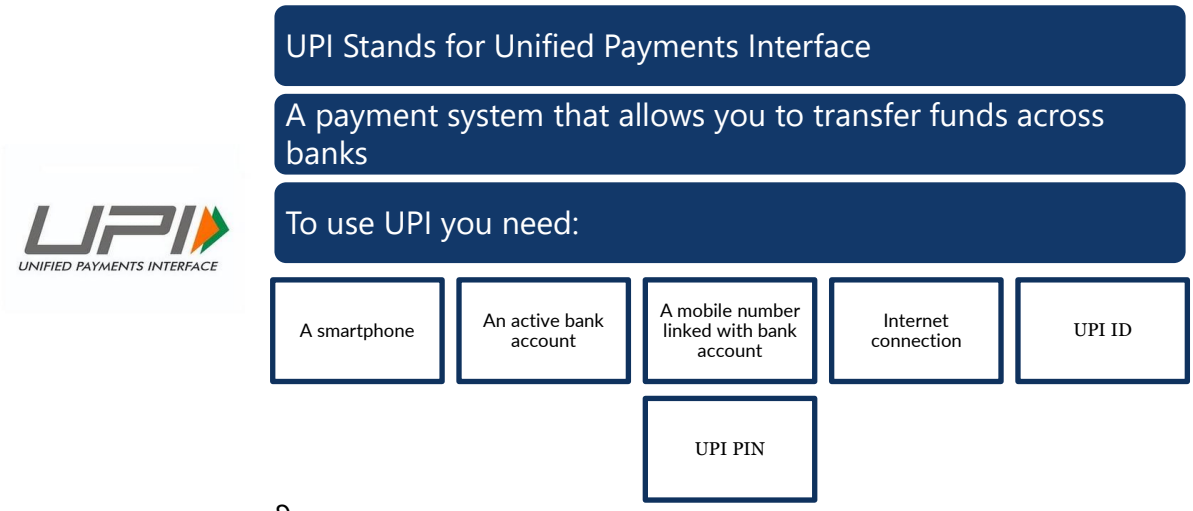
झूम	लिहा	झूम
युक्ती	लिहा	युक्ती
टोपली	लिहा	845KE7
चेंडू	लिहा	8411

- तुम्ही तुमच्या कीबोर्डवरील संख्यांसह नमूद केलेल्या विशेष वर्णांसह संख्या देखील बदलू शकता.

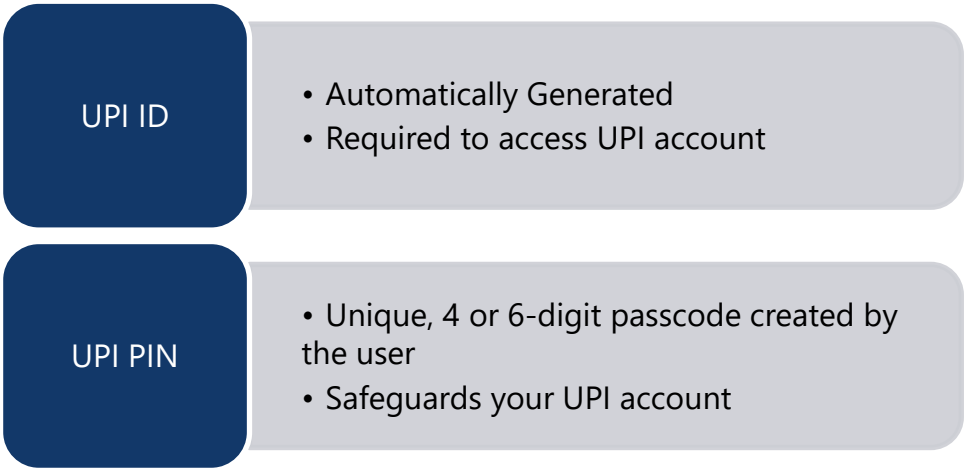
प्रमाणीकरणामध्ये खालील घटकांचा समावेश होतो:

- वापरकर्त्याला माहित असलेली एखादी गोष्ट जसे की पासवर्ड, पिन
- वापरकर्त्याकडे काहीतरी आहे जसे की डेबिट कार्ड आणि क्रेडिट कार्ड
- बायोमेट्रिक वैशिष्ट्यांसारखे वापरकर्त्यासाठी काहीतरी अनन्य

UPI पिन, बँकिंग कार्ड पिन आणि बायोमेट्रिक प्रमाणीकरण



1. UPI प्रमाणीकरण



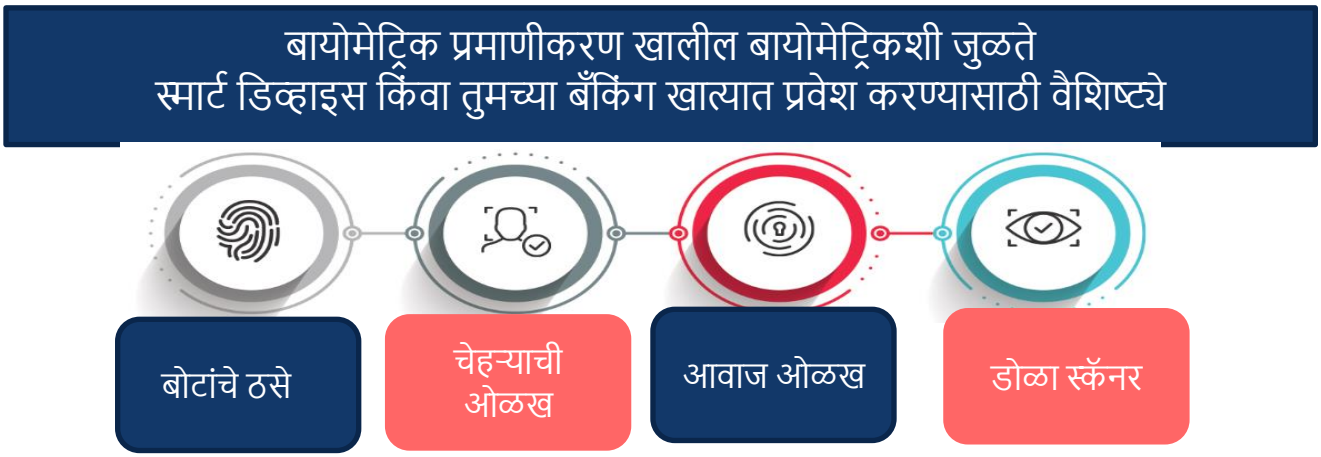
2. बँकिंग कार्ड प्रमाणीकरण

बँकिंग कार्ड पिन मध्ये पिन समाविष्ट आहे:

P	I	N
Personal	Identification	Number

चार-अंकी कोड जो खातेधारकाच्या कार्डसाठी अद्वितीय असतो.

3. बायोमेट्रिक प्रमाणीकरण



द्वि-घटक प्रमाणीकरणास 2FA म्हणून देखील संबोधले जाते द्वि-घटक प्रमाणीकरणास 2FA म्हणून देखील संबोधले जाते द्वि-घटक प्रमाणीकरणास 2FA म्हणून संबोधले जाते द्वि-घटक प्रमाणीकरणास 2FA म्हणून

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

देखील संबोधले जाते द्वि-घटक प्रमाणीकरणास 2FA म्हणून देखील संबोधले जाते द्वि-घटक प्रमाणीकरणास 2FA म्हणून देखील संबोधले जाते द्वि-घटक प्रमाणीकरणास 2FA म्हणून देखील संबोधले जाते द्वि-घटक प्रमाणीकरणास 2FA म्हणून देखील संबोधले जाते

द्वि-घटक प्रमाणीकरण

दुर्भावनायुक्त वेबसाइट आणि ॲप्स

द्वि-घटक प्रमाणीकरण पासवर्ड आणि एक-वेळ पासकोड/प्रमाणीकरण कोड वापरते
SMS द्वारे मोबाईल फोन जे प्रविष्ट केल्यावर वापरकर्त्याला शेवटी खात्यात प्रवेश करण्याची परवानगी देते

वापरकर्तानाव प्रविष्ट | प्रमाणीकरण | प्रमाणीकरण प्रविष्ट करा

दुर्भावनायुक्त वेबसाइट आणि ॲप्स

दुर्भावनायुक्त वेबसाइट्स आणि ॲप्स हे सायबर हल्ल्याच्या सर्वात सामान्य प्रकारांपैकी एक आहेत

हॅकर्स तुम्हाला एसएमएस, ईमेल किंवा तुमच्या सोशल मीडिया खात्यांवर प्रदर्शित केलेल्या जाहिरातींद्वारे लिंक पाठवतात

तुम्हाला सतर्क राहण्याची गरज आहे कारण एका क्लिकवर तुमची सर्व वैयक्तिक माहिती हॅकर्सकडे लीक होईल.

दुर्भावनायुक्त वेबसाइट्स तुम्हाला पुढील गोष्टी करण्यासाठी सूचना देऊ शकतात:

- सॉफ्टवेअर/कोणतेही बीजक/फाइल/ॲप डाउनलोड करा
- फाइल सेव्ह करा
- एक कार्यक्रम चालवा

दुर्भावनायुक्त वेबसाइट/ॲप्स कसे कार्य करतात?

दुर्भावनायुक्त लिंक/फाइल/संलग्नक वापरकर्त्याला पाठवले जाते

तुम्ही तुमच्या वॉलेटमध्ये 5000INR बोनस पॉइंट जिंकले आहेत. दावा करण्यासाठी येथे क्लिक करा !!! त्वरा करा लिंक पुढील 15 मिनिटांत कालबाह्य होईल

वापरकर्ता दुव्यावर क्लिक करतो

डिव्हाइसवर एक मालवेअर स्थापित केला आहे जो तुमचा सर्व संवेदनशील डेटा चोरतो.

येथे काही मुद्दे आहेत जे दुर्भावनापूर्ण वेबसाइट आणि ॲपपासून तुमचे डिव्हाइस सुरक्षित करण्यात मदत करतील:

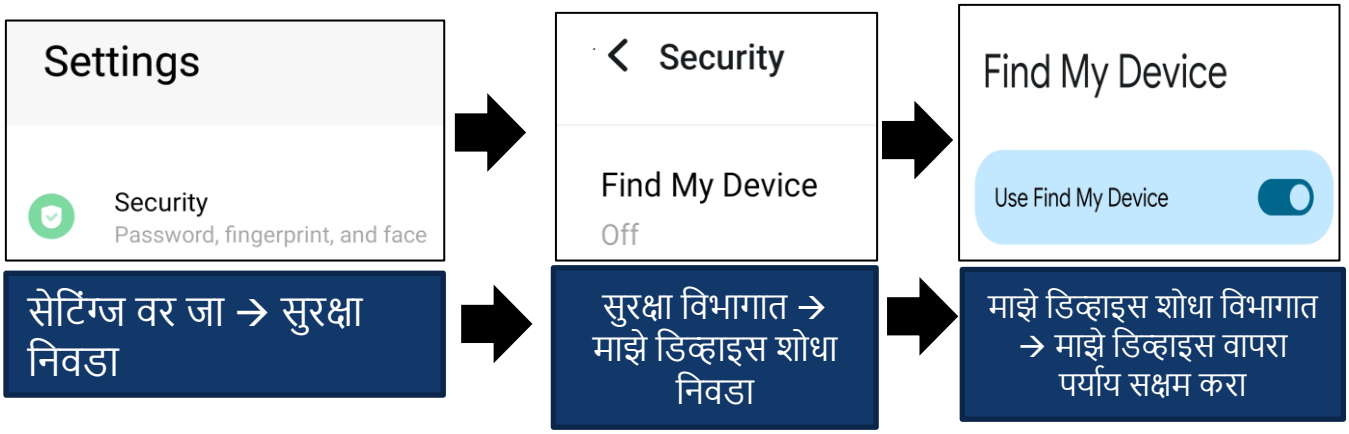
- ईमेलमध्ये एम्बेड केलेल्या लिंकवर कधीही क्लिक करू नका
- कोणत्याही बाह्य तृतीय-पक्ष संदेशातून प्राप्त झालेल्या दुव्यावर कधीही क्लिक करू नका.
- तुमची वैयक्तिक संवेदनशील माहिती विचारणारे कोणतेही यादृच्छिक ॲप कधीही स्थापित करू नका
- कोणतेही ऑनलाइन पेमेंट करताना नेहमी URL मध्ये "https" तपासा.
- URL काळजीपूर्वक वाचा. वेबसाइटच्या स्पेलिंगमध्ये किरकोळ वळण घेतल्यास धोका होऊ शकतो
- बँकेने दिलेल्या लिंकवरून तुमचे बँकिंग ॲप इंस्टॉल करा.
- कोणत्याही वेबसाइटवर प्रवेश करण्यापूर्वी नेहमी URL तपासा.
- केवळ विश्वसनीय वेबसाइटवर खरेदी करा आणि प्राप्त झालेल्या कोणत्याही यादृच्छिक दुव्यांद्वारे नाही.
- विश्वसनीय प्ले स्टोअरमधून सुरक्षित ॲप्स स्थापित करा.
- ईमेल उघडण्यापूर्वी ते तपासा. जर तुम्हाला प्रेषक माहित असेल तरच उघडा.
- तुम्ही कोणत्याही खात्यात ऑनलाइन लॉग इन केले असल्यास, नेहमी खाते सोडण्यापूर्वी लॉग ऑफ करा
- तुमचा अँटीव्हायरस नियमितपणे अपडेट करा.

हरवलेले फोन दूरस्थपणे व्यवस्थापित करणे

फक्त खालील परिस्थितींमध्ये, हरवलेला फोन दूरस्थपणे प्रवेश केला जाऊ शकतो

- फोन चालू आहे
- Google खात्यात साइन इन केले (Android च्या बाबतीत) किंवा iPhone च्या बाबतीत iCloud
- इंटरनेटशी कनेक्ट केलेले
- माझे डिव्हाइस शोधा सक्षम केले आहे

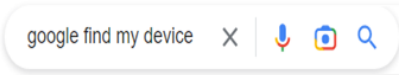
"माझे डिव्हाइस शोधा" पर्याय सक्षम करण्यासाठी तुम्हाला पुढील चरणांचे पालन करणे आवश्यक आहे:



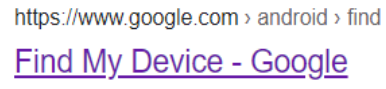
हे तम्हाला तमचा फोन हरवल्यास किंवा चोरीला गेल्यास दरस्थपणे ॲक्सेस करण्याची

तुमचा हरवलेला स्मार्टफोन डेटा दूरस्थपणे पुसून टाकण्यासाठी, तुम्हाला दाखवलेल्या चरणांचे पालन करणे आवश्यक आहे:

Google Chrome उघडा आणि तुमच्या खात्यात साइन इन करा

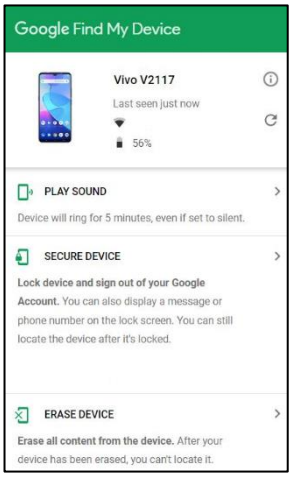


सर्च बारमध्ये Google Find My Device टाइप करा



दाखवलेल्या लिंकवर क्लिक करा. Google Find my device स्क्रीन दिसते..

आता, स्क्रीनवर दाखवल्याप्रमाणे योग्य पर्याय निवडून तुम्ही तुमचे डिव्हाइस सुरक्षित करू शकता किंवा त्यावरील सामग्री मिटवू शकता.



फिशिंग आणि ऑनलाइन फॉर्म

ऑनलाइन फॉर्म आहेत हे आपल्या सर्वांना माहीत आहे:

- अनेक प्रश्न असलेले सर्वेक्षण फॉर्म तयार करण्यासाठी वापरले जाते.
- रिअल-टाइममध्ये सर्वेक्षण परिणामांचे विश्लेषण करण्यासाठी वापरले जाते.
- कोणत्याही डिव्हाइसवरून प्रवेशयोग्य

पण तुमची वैयक्तिक माहिती हॅक करण्यासाठी त्यांचा वापर हॅकर्सकडून अनेकदा केला जातो.

हॅकर्स तुमचा बँक कर्मचारी असल्याचे भासवू शकतात आणि तुम्हाला माहिती देतील की त्यांनी तुम्हाला एक फॉर्म संलग्न केलेला ईमेल पाठवला आहे, तुम्हाला ते भरा आणि लवकरात लवकर पाठवण्यास सांगितले आहे जेणेकरून तुमच्या बचत योजनेचे नूतनीकरण करता येईल.

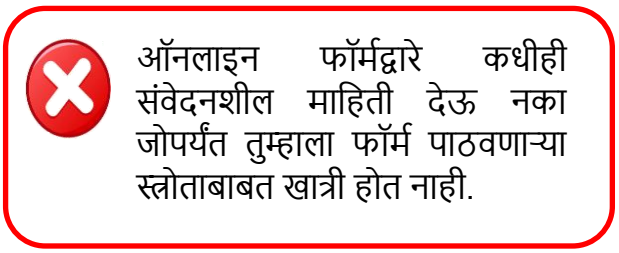
अशा फिशिंग घोटाळ्यांकडे कधीही जाऊ नका. तुम्हाला तुमच्या बँकेतून ऑनलाइन फॉर्म भरण्याची आवश्यकता असल्यास लगेच पुष्टी करा.

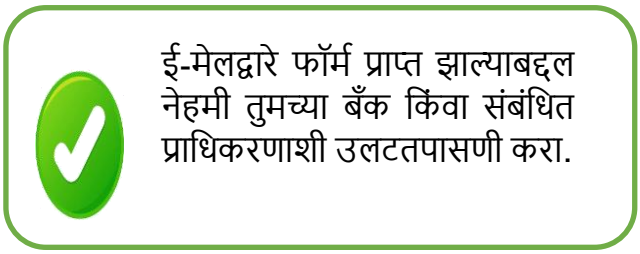
येथे फिशिंग ऑनलाइन फॉर्म ईमेलचा नमुना आहे.

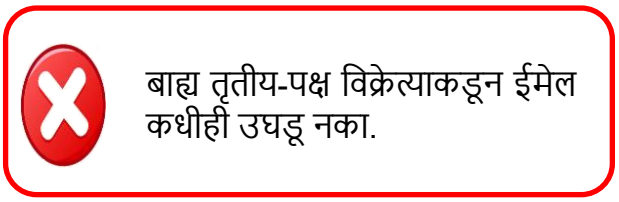
Attention: Urgent | External email प्रिय खातेधारक हे तुम्हाला सूचित करण्यासाठी आहे की तुमच्या KYC संदर्भात काही माहिती गहाळ आहे. कृपया संलग्न केलेला फॉर्म भरा आणि आजपर्यंत सबमिट करा अन्यथा पुढील सूचना मिळेपर्यंत तुमचे खाते गोठवले जाईल आणि तुम्ही या खात्यातून कोणतेही आर्थिक व्यवहार करू शकणार नाही. तुमचे खाते अपडेट करण्यासाठी कृपया खालील लिंक वर क्लिक करा: Update Now आम्ही तुमच्या गोपनीयतेचा आदर करतो! Thanks and Regards MSN20002 Unnamed 555555.png	तपशील भरा: पहिले नाव:* आडनाव:* पत्ता 1:* पत्ता 2: ई - मेल आयडी:* नोंदणीकृत मोबाईल क्रमांक:* आधार क्रमांक:*

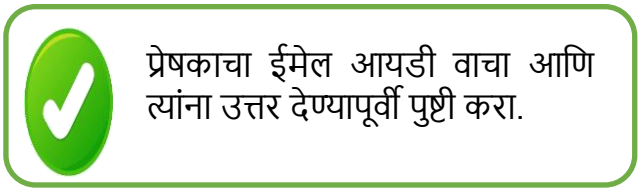
फिशिंग फॉर्म ई-मेल

सुरक्षित राहण्यासाठी ऑनलाइन फॉर्मचे काय आणि काय करू नका:





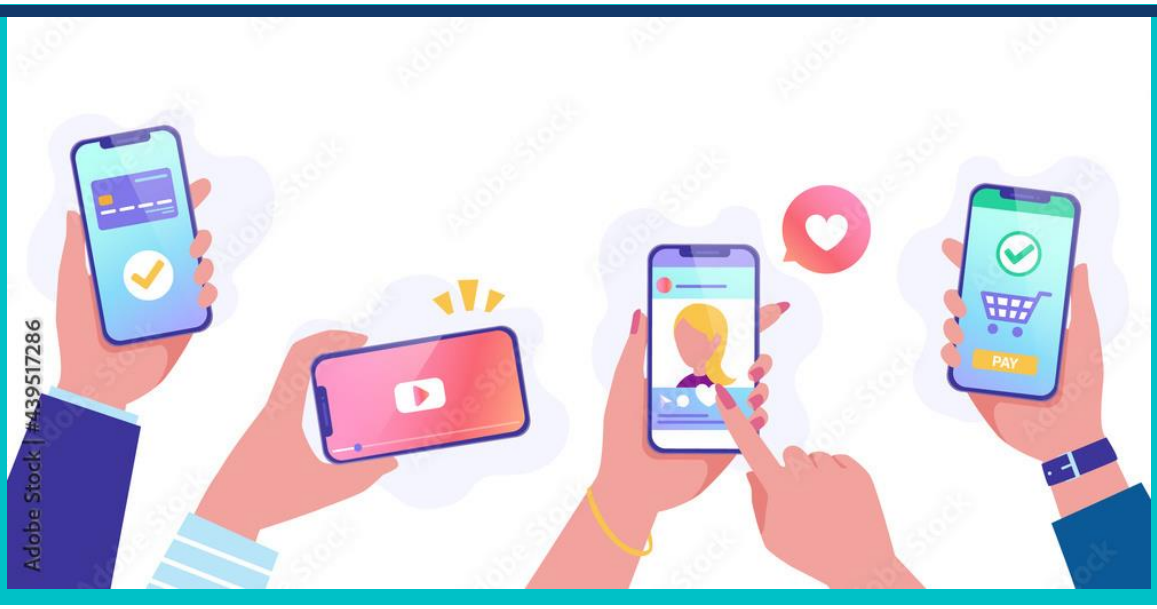




संदर्भ वाचन:

- **तुमचा UPI पिन कसा रीसेट करायचा :** https://www.youtube.com/watch?v=ZoEqpKF_Sjw
- **तुमचे Instagram खाते द्वि-घटक प्रमाणीकरणासह सुरक्षित करणे:** https://help.instagram.com/566810106808145
- **तुमचे Facebook खाते दोन घटक प्रमाणीकरणासह सुरक्षित करणे :** https://www.facebook.com/help/148233965247823
- **हरवलेला आयफोन दूरस्थपणे व्यवस्थापित करणे :** https://support.apple.com/en-in/guide/security/secc46f3562c/web
- **मालवेअर संसर्गासाठी वेबसाइट कशी तपासायची :** https://www.sitelock.com/blog/check-website-for-malware/
- **तुमच्या स्मार्टफोनला संभाव्य हानी असलेले दुर्भावनायुक्त ॲप्स:** https://www.91mobiles.com/hub/malicious-apps-malware-google-play-store/

मॉड्यूल 5
इंटरनेट स्मार्ट असणे



सुरक्षित ब्राउझिंग टिपा:

असे काही मार्ग आहेत ज्याद्वारे ऑनलाइन ब्राउझिंग सुरक्षित असू शकते.

इंटरनेट स्मार्ट व्हा

- काळजीपूर्वक शेअर करा

  बातम्या वेगाने पसरतात. याचे लोकांवर काय परिणाम होतील याचा आधीच विचार करणे गरजेचे आहे.

- **जबाबदारीने संवाद साधा**
  - समोरासमोर संवादाप्रमाणेच ऑनलाइन संप्रेषणाद्वारे विचारशील सामायिकरण वाढवा.
  - योग्य संवादासाठी फॉर्म मार्गदर्शक तत्त्वे.
  - कुटुंब आणि मित्रांचे तपशील सुरक्षित करा.
- **इंटरनेट सतर्क रहा**
  - खोट्या बातम्यांना बळी पडू नका.
  - लोकांना समजून घेण्यात मदत करणे महत्त्वाचे आहे
    - खरे काय आणि खोटे काय हा ऑनलाइन सुरक्षिततेचा एक अतिशय महत्त्वाचा धडा आहे.

      ऑनलाइन लोक आणि परिस्थिती नेहमी जशी दिसते तशी नसते.
- **इंटरनेट मजबूत व्हा**

  - तुमचे रहस्य सुरक्षित करा
  - गोपनीयता आणि सुरक्षितता या ऑनलाइन तितक्याच महत्त्वाच्या आहेत जितक्या ऑफलाइन आहेत.
  - वैयक्तिक माहितीचे रक्षण केल्याने वापरकर्त्याला त्यांच्या डिव्हाइसेस, प्रतिष्ठा आणि संबंधांचे नुकसान टाळण्यास मदत होते.
- **इंटरनेट सारखे व्हा**
  - दयाळू असणे छान आहे
  - इंटरनेट हे सकारात्मकता तसेच नकारात्मकता पसरवण्याचे एक शक्तिशाली साधन आहे. वापरकर्ता "आपल्याला जसे वागवायचे आहे तसे इतरांशी वागवा" ही संकल्पना त्यांच्या ऑनलाइन कृतींमध्ये घेऊ शकतो, इतरांवर सकारात्मक प्रभाव निर्माण करतो आणि अयोग्य वर्तन दूर करतो..

- **इंटरनेट धाडसी व्हा**
    - घरात आणि सार्वजनिक ठिकाणी खुले संवाद वाढवून वापरकर्ते एकमेकांना शंकास्पद गोष्टींबद्दल बोलण्यास सोयीस्कर बनवू शकतात.

स्मार्ट ब्राउझिंग:

हॅकर्स सोशल प्रोफाइलवरून गोळा केलेल्या माहितीच्या आधारे फिशिंग स्कॅम तयार करू शकतात. घोटाळ्यांपासून स्वतःचे संरक्षण करण्यासाठी येथे काही SMART टिपा आहेत.

एस-सुरक्षित	**एम-बैठक**	**ए-विचारा**	**आर-विश्वासार्ह**	**टी-सांगा**
सुरक्षित राहण्यासाठी, तुमची वैयक्तिक माहिती कधीही अनोळखी व्यक्तींसोबत ऑनलाइन शेअर करू नका.	तुम्ही वैयक्तिकरित्या ओळखत असलेल्यांनाच भेटा. तुम्ही ऑनलाइन भेटलेल्या कोणत्याही अनोळखी व्यक्तीला कधीही भेटू नका.	सुरक्षिततेबद्दल शंका असल्यास, एखाद्या जाणकार व्यक्तीला मदतीसाठी विचारा. अनोळखी व्यक्तींकडून कधीही फ्रेंड रिक्वेस्ट स्वीकारू नका किंवा ईमेल उघडू नका.	कोणतीही वेबसाइट वापरण्यापूर्वी किंवा कोणतेही ॲप डाउनलोड करण्यापूर्वी विश्वसनीयता तपासणे आवश्यक आहे	तुमच्या ऑनलाइन खात्यावर आढळलेल्या कोणत्याही बेकायदेशीर हालचालींबद्दल संबंधित अधिकाऱ्यांना सांगा

- तुमची वैयक्तिक माहिती जसे की प्रवास योजना किंवा कुटुंबाचे तपशील शेअर करू नका. हॅकर्स त्या पोस्टमधील माहिती तुमच्या विरोधात वापरू शकतात
- तुमचा ई-मेल आणि संपर्क क्रमांक ऑनलाइन पोस्ट, शेअर किंवा ट्विट करू नका.
- अनोळखी व्यक्तींच्या फ्रेंड रिक्वेस्ट स्वीकारू नका.
- तुमच्या वर्कस्टेशनमधील फोटो शेअर करताना, तुमच्या कॉम्प्युटर सिस्टीममधून काहीही उघड होत नाही याची खात्री करा.
- नेहमी वेगवेगळ्या सोशल मीडिया प्लॅटफॉर्मवर भिन्न प्रोफाइल चित्रे वापरण्याचा प्रयत्न करा.

सुरक्षित ब्राउझिंग साधने

फायरवॉल: फायरवॉल हे एक सॉफ्टवेअर आहे जे नेटवर्कमध्ये अनधिकृत प्रवेश रोखण्यासाठी आणि सुरक्षा धोके कमी करण्यासाठी काही नियम वापरून रहदारीची तपासणी करण्यासाठी प्रथम संरक्षण लाइन म्हणून कार्य करते..

अँटीव्हायरस:

संगणक व्हायरस हा एक दुर्भावनापूर्ण कोड किंवा प्रोग्राम आहे जो स्वतःची प्रतिकृती बनवतो आणि संगणकाच्या कार्यपद्धतीमध्ये अडथळा आणण्यासाठी डिझाइन केलेले आहे. व्हायरस एखाद्या वैध प्रोग्राममध्ये स्वतःला घालून किंवा संलग्न करून ऑपरेट करतो. व्हायरसमध्ये डेटा खराब करून किंवा नष्ट करून सिस्टम सॉफ्टवेअरला नुकसान किंवा हानी पोहोचवण्याची क्षमता असते

.

अँटी-व्हायरस हा व्हायरस आणि वर्म्स सारख्या मालवेअरद्वारे संसर्ग टाळण्यासाठी आपल्या संगणकावर किंवा मोबाइल डिव्हाइसवर स्थापित केलेला सुरक्षा प्रोग्राम आहे.

तुमच्या डिव्हाइस किंवा सिस्टममध्ये अँटी-व्हायरस स्थापित करण्याचे फायदे आहेत:

- व्हायरस शोधणे, अवरोधित करणे आणि काढून टाकणे.
- ओळख चोरीला प्रतिबंध करणे आणि फिशिंग अवरोधित करणे.
- दुर्भावनायुक्त वेबसाइट्स आणि लिंक्सबद्दल चेतावणी.
- सुरक्षित पासवर्ड एन्क्रिप्शनसह ऑनलाइन खाती सुरक्षित ठेवणे.
- संगणक सुरळीत चालणे.

इंटरनेट हे माहितीचे जटिल मिश्रण आहे, विचलित करणाऱ्या जाहिराती, धोकादायक मालवेअर आणि फसवणूक करणाऱ्या क्लिक-बेट लिंक्स ज्यामुळे संशय नसलेल्या वापरकर्त्यांना सायबर दुःस्वप्न होऊ शकते. मालवेअर आणि इतर ब्राउझर-आधारित हल्ल्यांबद्दल काळजी न करता वेबच्या अवघड भूभागावर नेव्हिगेट करण्यासाठी, ब्राउझर विक्रेते अनेक उपयुक्त सुरक्षा वैशिष्ट्ये प्रदान करतात.

इंटरनेटवर सुरक्षिततेसाठी ब्राउझरद्वारे ऑफर केलेली वैशिष्ट्ये

- Google Chrome द्वारे सुरक्षित ब्राउझिंग वैशिष्ट्य
- मायक्रोसॉफ्ट द्वारे स्मार्टस्क्रीन फिल्टर
- Mozilla Firefox द्वारे फिशिंग फिल्टर

- ही वैशिष्ट्ये फिशिंग हल्ल्यांपासून आणि मालवेअरपासून संगणकांचे संरक्षण करण्यात मदत करतात.

येथे काही पायऱ्या आहेत ज्या तुम्हाला ऑनलाइन सुरक्षित ठेवू शकतात आणि ऑनलाइन संरक्षणात्मक कवच तयार करण्यात मदत करू शकतात.

- **संवेदनशील ब्राउझिंग**: बँक व्यवहारांसाठी आम्ही अनेकदा कॅफे इत्यादींमध्ये खुले नेटवर्क वापरतो. सायबर गुन्हेगार एका सेकंदात तुमचे बँक तपशील कॉपी करतात आणि तुमचे कष्टाने कमावलेले पैसे लुटतात.

- **स्पॅम संदेश शोधणे आणि टाळणे सोपे आहे**: या संदेशांमध्ये 'RBI कडून संदेश' किंवा 'तुमची मदत आवश्यक आहे' इत्यादी शब्द वापरले जातात. तुम्हाला ते टाळावे लागेल आणि तुम्ही अशा संशयास्पद लिंक्स उघडू नयेत.

- **मजबूत पासवर्ड क्रॅक करणे कठीण आहे**: प्रत्येक वेगळ्या ऑनलाइन खात्यासाठी नेहमी वेगवेगळे पासवर्ड वापरण्याचा प्रयत्न करा. वेबसाइट्सच्या पासवर्ड पॉलिसीनुसार तुम्ही तुमचे पासवर्ड नेहमी सेट केले पाहिजेत. पासवर्ड अल्फा-न्यूमेरिक असावेत आणि त्यांना मजबूत करण्यासाठी विशेष वर्ण असावेत.

- **तुमची खाती/सत्रांमधून साइन आउट करा** : आम्ही साधारणपणे आमच्या मेल किंवा सोशल मीडिया खात्यांमध्ये किंवा आमच्या डिव्हाइसेसवरील बँकिंग सत्रांमध्ये लॉग इन करतो. पण हे आपल्या सायबर सुरक्षेलाही धोका ठरू शकते. तुमच्या खात्यांमधून नेहमी लॉग आउट करा आणि तुमच्या डिव्हाइसवर तुमच्या बँक लॉगिन करा.

- **सोशल मीडियावरील सुरक्षा**: आजकाल फेसबुक किंवा इंस्टाग्राम आणि इतर सोशल साइट्सवर चित्रे अपलोड करणे खूप सामान्य आहे, परंतु या प्रतिमांचा गैरवापर होऊ शकतो. तुमचा ऑनलाइन डेटा स्टॉकर्स आणि इतर जोखमींपासून सुरक्षित ठेवण्यासाठी, तुम्ही तुमची खाते सेटिंग्ज सार्वजनिक ते खाजगीमध्ये बदलली पाहिजेत.

- **डेटा बॅक-अप**: नेहमी भौतिक ड्राइव्ह किंवा ऑनलाइन स्टोरेज म्हणजेच क्लाउड स्टोरेजच्या मदतीने तुमच्या डेटाचा बॅकअप घ्या. अशा प्रकारे, तुमच्या डिव्हाइसला काहीही झाले तर तुमचा डेटा सुरक्षित राहील.

- **बसाइट्सची सुरक्षितता चेतावणी** : McAfee Site Advisor सारखे अनेक साइट सुरक्षा विस्तार तुम्हाला वेबसाइट ब्राउझ करण्याच्या सुरक्षिततेबद्दल चेतावणी देतात.

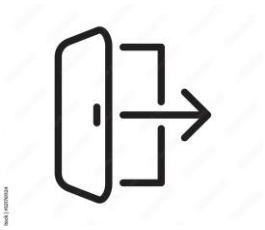
सार्वजनिक आणि मोफत वाय-फाय

सार्वजनिक वाय-फाय असुरक्षित आणि धोकादायक आहे. सार्वजनिक वाय-फायच्या असुरक्षित कनेक्शनपासून काही संभाव्य धोके

- मधल्या हल्ल्यात माणूस
- एनक्रिप्ट न केलेले नेटवर्क
- मालवेअर वितरण
- व्हायरस
- वर्म्स
- ट्रोजन घोडे
- रॅन्समवेअर
- ॲडवेअर
- स्नूपिंग आणि स्निफिंग
- वैयक्तिक माहितीची चोरी
- लॉगिन क्रेडेन्शियल्स
- आर्थिक माहिती
- वैयक्तिक माहिती
- चित्रे
- सत्र अपहरण

सार्वजनिक वाय-फाय वापरताना सुरक्षित राहणे

टाळा	वापरा	उघडा	सक्षम करा	वापरा
				
संवेदनशील कागदपत्रे/फाईल्स उघडत आहे	सार्वजनिक वाय-फाय वर एनक्रिप्शन वापरून VPN सुरक्षित कनेक्शन	फक्त https वेबसाइट्स	सुरक्षित ब्राउझर सेटिंग्ज	एक गोपनीयता स्क्रीन

बंद कर	वापरा	खात्री करा	लक्षात ठेवा
			
फाइल शेअरिंग	द्वि-घटक प्रमाणीकरण	तुमची ऑपरेटिंग सिस्टम आणि ब्राउझर अद्ययावत आहेत	सार्वजनिक वाय-फाय मधून लॉग आउट करण्यासाठी

सायबर गुन्ह्यांचे प्रकार:

• कॉपीराइटचे उल्लंघन करणे: परवानगीशिवाय एखाद्याचे कॉपीराइट केलेले कार्य वापरणे. उदाहरणार्थ, कंपनीच्या वेबसाइटवरील प्रतिमा वापरणे आणि ती आपल्या वैयक्तिक खात्यावर पोस्ट करणे.

• रॅन्समवेअर हल्ले: रॅन्समवेअर हा मालवेअर आहे जो आक्रमणकर्त्याला खंडणी फी भरेपर्यंत डेटा किंवा डिव्हाइस कूटबद्ध करून प्रकाशित करण्याची धमकी देतो किंवा त्याचा प्रवेश अवरोधित करतो.

• बेकायदेशीर जुगार: ऑनलाइन जुगारामध्ये इंटरनेटवर कॅसिनो किंवा खेळांवर सट्टेबाजी करणे समाविष्ट आहे.

• सायबर हेरगिरी: सायबर हेरगिरी म्हणजे स्पर्धेमध्ये फायदे मिळविण्यासाठी संगणक उपकरणांमधून किंवा त्याद्वारे डेटा, संवेदनशील माहिती किंवा बौद्धिक संपत्तीची हेतुपुरस्सर चोरी करणे. उदाहरणार्थ, राजकीय पक्ष निवडणुकीदरम्यान प्रतिस्पर्ध्यांचा डेटा चोरतात.

• ईमेल आणि इंटरनेट फसवणूक

• ओळख फसवणूक

• आर्थिक किंवा कार्ड पेमेंट डेटाची चोरी

• क्रिप्टोजॅकिंग: क्रिप्टोजॅकिंग हा सायबर गुन्ह्यांचा एक प्रकार आहे ज्यामध्ये लोकांच्या डिव्हाइसेसचा (संगणक, स्मार्टफोन, टॅबलेट किंवा अगदी सर्व्हर) सायबर गुन्हेगारांकडून क्रिप्टोकरन्सीसाठी माझ्याकडे अनधिकृतपणे वापर करणे समाविष्ट आहे. सायबर गुन्ह्यांच्या अनेक प्रकारांप्रमाणे, नफा हा हेतू आहे, परंतु इतर धोक्यांपेक्षा वेगळे, ते पीडितापासून पूर्णपणे लपवून ठेवण्यासाठी डिझाइन केलेले आहे.

• सायबर एक्सटॉर्शन: सायबर एक्सटॉर्शन हा एक गुन्हा आहे ज्यामध्ये हल्ला किंवा हल्ल्याची धमकी आणि हल्ला थांबवण्याच्या बदल्यात पैशाची मागणी किंवा इतर काही प्रतिसाद यांचा समावेश आहे.

हॅकर्सपासून तुमचे डिव्हाइस संरक्षित करण्याच्या पद्धती:

- फायरवॉल वापरा
- अँटी-व्हायरस स्थापित करा
- मजबूत पासवर्ड वापरा
- अद्ययावत ब्राउझर वापरा
- तुमचे नेटवर्क सुरक्षित करा
- द्वि-घटक प्रमाणीकरण वापरा
- ॲप्स आणि वैयक्तिक माहितीसाठी सुरक्षा पिन वापरा

संदर्भ वाचन:

- **वैयक्तिक गोपनीयता: इंटरनेटवर सुरक्षित ब्राउझिंगसाठी शीर्ष 12 टिपा:** https://cybersecurityventures.com/12-tips-for-safer-browsing/
- **महिला आणि मुलींना ऑनलाइन सुरक्षित राहण्यास मदत करण्यासाठी 5 टिपा:** https://www.globalcitizen.org/en/content/tips-to-help-women-girls-stay-safe-online/
- **सार्वजनिक वायफाय सुरक्षा धोके कसे टाळायचे:** https://www.kaspersky.co.in/resource-center/preemptive-safety/public-wifi-risks

मॉड्यूल 6

डिजिटल अधिकार, कायदे आणि निवारण यंत्रणा

डिजिटल सिटिझन:

डिजिटल नागरिक म्हणजे इंटरनेट आणि इतर डिजिटल तंत्रज्ञानाचा वापर जबाबदारीने करणारी व्यक्ती

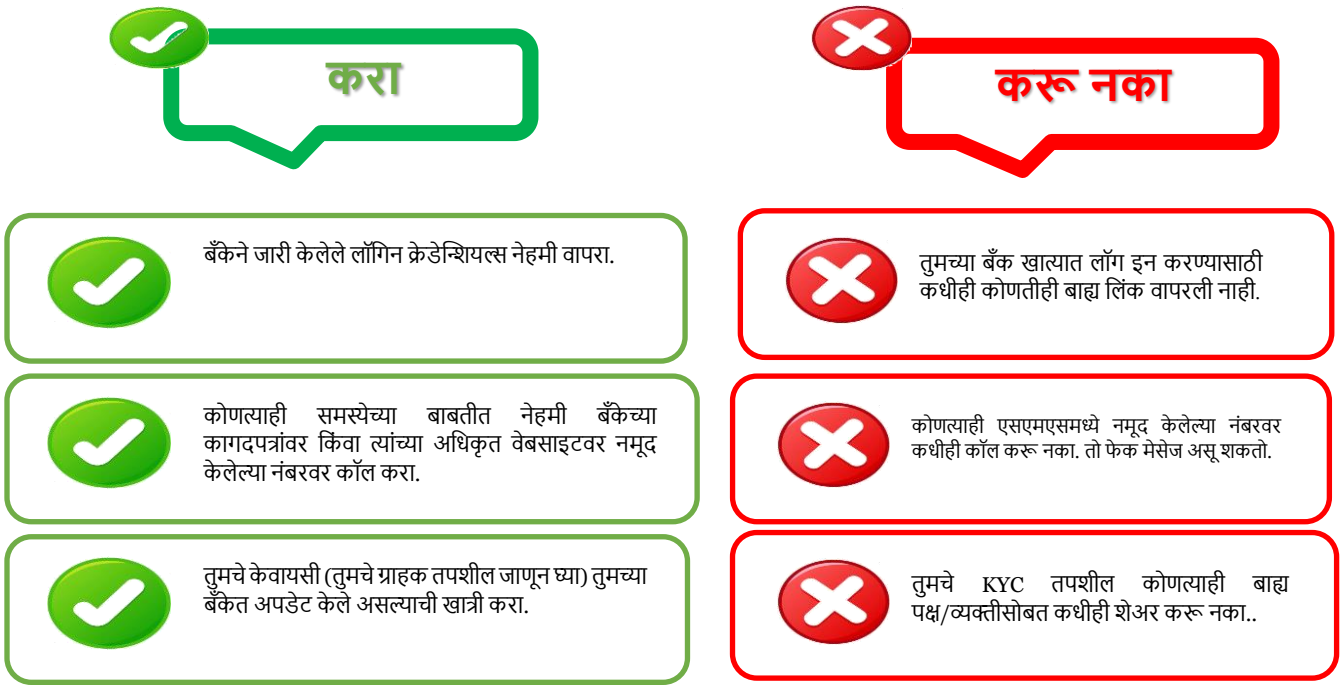
डिजिटल नागरिकांची भूमिका:

- तुमची वैयक्तिक माहिती संरक्षित करा
- तुमचा डिजिटल फूटप्रिंट काळजीपूर्वक व्यवस्थापित करा (एखाद्या विशिष्ट व्यक्तीची माहिती जी त्यांच्या ऑनलाइन क्रियाकलापाच्या परिणामी इंटरनेटवर अस्तित्वात आहे)
- ऑनलाइन व्यवहार कायद्यांचे पालन करा
- बेकायदेशीर क्रियाकलापांसाठी उभे रहा
- डिजिटल नागरिक म्हणून तुमचे हक्क जाणून घ्या

वैयक्तिक माहिती शेअर करताना जबाबदार स्मार्ट डिजिटल नागरिक व्हा:

एस-सुरक्षित	एम-बैठक	ए-विचारा	आर-विश्वासार्ह	T-Tell
ऑनलाइन सुरक्षित राहण्यासाठी, तुमची वैयक्तिक माहिती कधीही अनोळखी व्यक्तींसोबत ऑनलाइन शेअर करू नका.	तुम्ही वैयक्तिकरित्या ओळखत असलेल्यांनाच भेटा. तुम्ही ऑनलाइन भेटलेल्या कोणत्याही अनोळखी व्यक्तीला कधीही भेटू नका.	सुरक्षिततेबद्दल शंका असल्यास, एखाद्या जाणकार व्यक्तीला मदतीसाठी विचारा. अनोळखी व्यक्तींकडून कधीही फ्रेंड रिक्वेस्ट स्वीकारू नका किंवा ईमेल उघडू नका.	कोणतीही वेबसाइट वापरण्यापूर्वी किंवा कोणतेही ॲप डाउनलोड करण्यापूर्वी विश्वसनीयता तपासणे आवश्यक आहे	तुमच्या ऑनलाइन खात्यावर आढळलेल्या कोणत्याही बेकायदेशीर हालचालींबद्दल संबंधित अधिकाऱ्यांना सांगा

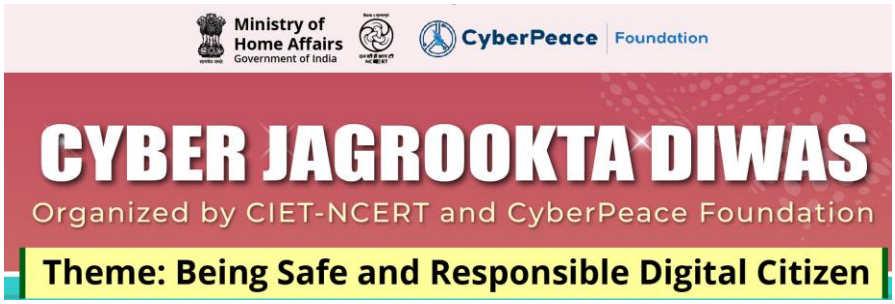
बँक खाते ऑनलाइन वापरताना जबाबदाऱ्या



डिजिटल नागरिकांच्या जबाबदाऱ्यांकडे सरकारचा पुढाकार:

शाळा आणि महाविद्यालयातील विद्यार्थी, शिक्षक आणि पालकांमध्ये जागरूकता निर्माण करण्यासाठी प्रत्येक महिन्याच्या पहिल्या बुधवारी "सायबर जागृत दिवस" साजरा करण्याचा प्रस्ताव आहे.

- डिजिटल नागरिकांचे हक्क आणि जबाबदाऱ्यांबद्दल जागरूकता निर्माण करण्यासाठी पुढाकार घेतला



डिजिटल नागरिकांचे हक्क:

• **प्रवेशाचा अधिकार**: प्रत्येक नागरिकाला इंटरनेट वापरण्याचा अधिकार आहे. मतस्वातंत्र्यासाठी हा अत्यावश्यक हक्क मानला जातो. भारताच्या सर्वोच्च न्यायालयाच्या म्हणण्यानुसार, इंटरनेटचा वापर हा मूलभूत मूलभूत अधिकार आहे

- **अभिव्यक्ती, माहिती आणि संप्रेषण स्वातंत्र्याचा अधिकार**: प्रत्येक नागरिकाला सोशल मीडिया नेटवर्कचा वापर व्यक्त करण्यासाठी, कोणतीही माहिती मिळविण्यासाठी किंवा संवाद साधण्याचा अधिकार आहे..

• **गोपनीयता आणि डेटा संरक्षणाचा अधिकार**: वापरकर्त्यास सोशल मीडियावर सादर केलेल्या त्यांच्या वैयक्तिक माहितीचे संरक्षण करण्याचा अधिकार आहे. सर्व सोशल मीडिया प्लॅटफॉर्मसाठी गोपनीयता आणि डेटा संरक्षण सेटिंग प्रदान करणे बंधनकारक आहे जसे की वापरकर्ता तुमचे प्रोफाइल कोण पाहू शकतो किंवा त्यांचे प्रोफाइल खाजगी ठेवू शकतो..

- **संरक्षणाचा अधिकार**: सरकारने सोशल मीडिया प्लॅटफॉर्मद्वारे इंटरनेट वापरकर्त्यांचे संरक्षण सुनिश्चित केले पाहिजे. तसेच, 1930 वर कॉल करून इंटरनेटवरील कोणत्याही बेकायदेशीर क्रियाकलापाची तक्रार करण्यासाठी वापरकर्त्यांना सायबर सेलमध्ये सहज प्रवेश आहे..

नागरिकांच्या ऑनलाइन सुरक्षिततेसाठी डिजिटल साधने – ऑनलाइन व्यवहार

- भारत इंटरफेस फॉर मनी-युनिफाइड पेमेंट्स इंटरफेस (BHIM-UPI)
- तात्काळ पेमेंट सेवा (IMPS)
- प्री-पेड पेमेंट इन्स्ट्रुमेंट्स (PPIS)
- नॅशनल इलेक्ट्रॉनिक टोल कलेक्शन (NETC)
- रिअल-टाइम ग्रॉस सेटलमेंट (RTGS)

ॲप्स डाउनलोड करण्यासाठी, खालील सुरक्षित ऑनलाइन स्टोअर्स वापरा:

GET IT ON Google Play

Download on the App Store

बेकायदेशीर सायबर क्रियाकलाप:

सर्वात सामान्य बेकायदेशीर सायबर क्रियाकलाप आहेत:

- **सायबरस्टॉकिंग** - सायबरस्टॉकिंग म्हणजे इलेक्ट्रॉनिक मीडिया वापरून कोणत्याही व्यक्तीचा पाठलाग करणे. यात हे समाविष्ट आहे:
  - o सायबरस्टॉकिंग - सायबरस्टॉकिंग म्हणजे इलेक्ट्रॉनिक मीडिया वापरून कोणत्याही व्यक्तीचा पाठलाग करणे. यात हे समाविष्ट आहे:
  - o ओळख चोरीच्या उद्देशाने माहिती मिळवणे.
  - o अवांछित, भयावह, किंवा अश्लील ईमेल किंवा संदेश पाठवणे.
  - o सोशल मीडियावर त्रास देणे किंवा धमकावणे.ओळख चोरीच्या उद्देशाने माहिती मिळवणे.
  - o अवांछित, भयावह, किंवा अश्लील ईमेल किंवा संदेश पाठवणे.
  - o सोशल मीडियावर त्रास देणे किंवा धमकावणे.
- **गोपनीयता/गोपनीयतेचे उल्लंघन आणि उल्लंघन**

o यामध्ये व्यक्तीच्या संमतीशिवाय सोशल मीडिया/कोणत्याही प्लॅटफॉर्मवर कोणतीही खाजगी माहिती किंवा प्रतिमा प्रकाशित करणे किंवा प्रसारित करणे समाविष्ट आहे.

o कायद्याने आवश्यक असेल तेव्हाच, बँका आणि सोशल मीडिया प्लॅटफॉर्म एखाद्याची वैयक्तिक माहिती शेअर करू शकतात.

- **व्हॉय्युरिझम**
  - खाजगी कृत्यांमध्ये गुंतलेल्या व्यक्तीच्या प्रतिमा किंवा व्हिडिओ त्यांच्या संमतीशिवाय पाहणे, कॅप्चर करणे किंवा शेअर करणे याचा संदर्भ आहे.
  - हे IPC कलम 354 (C) अंतर्गत दंडनीय कृत्य आहे.
  - याची तात्काळ सायबर सेल/महिला सेल/नजीकच्या पोलीस स्टेशनला तक्रार करावी
- **सायबरस्टॉकर्सपासून स्वतःचे रक्षण करण्यासाठी पायऱ्या आहेत::**
  - सायबर सेल/महिला सेलला अहवाल द्या
  - त्यांना ब्लॉक करा
  - कुटुंबातील सदस्यांना काय चालले आहे ते सांगा
  - तुमच्या खात्यावर गोपनीयता फिल्टर सेट करा
  - सर्व पुरावे जतन करा
  - त्यांना थांबायला सांगा

बेकायदेशीर डिजिटल क्रियाकलापांसाठी कायदेशीर तरतुदी

भारतीय दंड संहितेनुसार, 1860 खालील काही कायदेशीर तरतुदी आहेत

कलम	बेकायदेशीर क्रियाकलाप	शिक्षा
कलम 354A	• महिलांच्या संमतीशिवाय लैंगिक सामग्री दाखवणे किंवा शेअर करणे • लैंगिक अनुकूलतेसाठी विचारणे • लैंगिक टिप्पणी/संदेश पोस्ट करणे/पाठवणे	• तीन वर्षांपर्यंत वाढू शकेल अशा मुदतीसाठी सश्रम कारावास, किंवा दंड, किंवा दोन्ही..
कलम 354C	• व्हॉय्युरिझम	• प्रथम दोषी आढळल्यास दंड तसेच तीन वर्षांपर्यंत कारावास • त्यानंतरच्या दोषींवर सात वर्षे
कलम 354D	• सायबरस्टॉकिंग	• पहिल्या गुन्ह्यासाठी तीन वर्षांपर्यंत कारावास • त्यानंतरच्या दोषी आढळल्यास दंड आणि पाच वर्षांच्या कारावासास पात्र

माहिती तंत्रज्ञान कायदा, 2008 नुसार खालील काही कायदेशीर तरतुदी आहेत

IT ACT चे कलम	बेकायदेशीर क्रियाकलाप	शिक्षा
कलम 66E	• गोपनीयतेचे उल्लंघन • कोणत्याही व्यक्तीच्या खाजगी क्षेत्राची प्रतिमा त्यांच्या संमतीशिवाय कॅप्चर करणे, प्रकाशित करणे किंवा प्रसारित करणे	• कारावास, जो तीन वर्षांपर्यंत वाढू शकतो, आणि/किंवा दंड.
कलम 66C	• ओळख चोरी • सायबर हॅकिंग • इलेक्ट्रॉनिक स्वाक्षरीचा गैरवापर	• कारावास जो तीन वर्षांपर्यंत वाढू शकतो • एक लाख रुपयांपर्यंतचा दंड
कलम 67	• अश्लील सामग्रीचे प्रकाशन किंवा प्रसारण.	• तीन वर्षांपर्यंत कारावास आणि प्रथम दोषी आढळल्यास दंड • दुसऱ्यांदा दोषी आढळल्यास पाच ते सात वर्षे आणि दंड

कॉपीराइट कायद्यानुसार, जेव्हा तुम्ही तुमचे सर्जनशील कार्य सोशल मीडियावर पोस्ट करता, तेव्हा त्याचे कॉपीराइट तुमच्या मालकीचे असते. तुमच्या परवानगीशिवाय कोणीही काम वापरू शकत नाही किंवा प्लॅटफॉर्म मालकी घेत नाही.

बेकायदेशीर डिजिटल क्रियाकलापांसाठी निवारण यंत्रणा

तुम्ही कोणत्याही सायबर बेकायदेशीर क्रियाकलापाविरुद्ध तुमची तक्रार खालील ठिकाणी नोंदवू शकता:

- नॅशनल सायबर क्राईम रिपोर्टिंग पोर्टल
  - https://cybercrime.gov.in/Default.aspx
- नॅशनल सायबर क्राईम रिपोर्टिंग हेल्पलाइन नंबर -1930 (सकाळी 9.00 ते संध्याकाळी 6)
  - https://ncrb.gov.in/en/node/2318
- उमंग (न्यू-एज गव्हर्नन्ससाठी युनिफाइड मोबाईल ऍप्लिकेशन)
  - https://web.umang.gov.in/landing/department/cybercrime-reporting-portal.html
- सायबर पोलीस पोर्टल
  - https://cyberpolice.nic.in/

सायबर क्राईम पोर्टलवर तक्रार नोंदवण्याचे टप्पे:

1. लिंकवर जा: https://cybercrime.gov.in/

2. वेबसाइटच्या खालील विभागात स्क्रोल करा आणि नंतर तक्रार दाखल करा बटणावर क्लिक करा

3. अनामितपणे अहवाल द्या बटणावर क्लिक करा

4. फॉर्मचे सर्व विभाग भरा आणि पुढील प्रक्रियेसाठी सबमिट करा. तुमच्याकडे पुरावे कागदपत्रे तयार असल्याची खात्री करा जसे की स्क्रीनशॉट.

5. तुमची तक्रार नोंदवली जाईल. तुम्ही कोणत्याही मदतीसाठी 1930 वर कॉल करू शकता किंवा तक्रार नोंदवू शकता

संदर्भ वाचन:

• सायबर जागरुकता दिवसाबद्दल अधिक जाणून घेण्यासाठी खालील लिंक्सचा संदर्भ घ्या:

सायबर जागरुकता (जागरूकता) दिवस (दिवस 1 - दिवस 5)

• सोशल मीडिया प्लॅटफॉर्मचा सुरक्षित वापर अधिक जाणून घेण्यासाठी खालील लिंक्सचा संदर्भ घ्या:

सोशल मीडिया प्लॅटफॉर्म वापरताना काळजी घ्या

• ऑनलाइन सायबर गुन्ह्यांची तक्रार कशी करावी हे जाणून घेण्यासाठी खालील लिंक्सचा संदर्भ घ्या:

सायबर क्राईम हेल्पलाइन नंबर

• भारतात ई-कॉमर्स कायदे आणि नियम कसे आहेत हे जाणून घेण्यासाठी खालील लिंक्सचा संदर्भ घ्या:
भारतातील ई-कॉमर्स कायदे आणि नियम

• माझा ऑनलाइन व्यवहार सुरक्षित आहे की नाही हे मी कसे सांगू शकतो हे जाणून घेण्यासाठी खालील लिंक्सचा संदर्भ घ्या?
माझे ऑनलाइन व्यवहार सुरक्षित आहे

सुचवलेले व्यावहारिक उपक्रम

आता तुम्ही डिजिटल सेफ्टी अँड सिक्युरिटी प्रोग्रामचे ऑनलाइन लर्निंग मॉड्युल्स पूर्ण केले आहेत, कृपया या ॲक्टिव्हिटींचा सराव करून पहा आणि तुमच्या वास्तविक जीवनात ते लागू करा. आम्हाला आशा आहे की या उपक्रमांमुळे तुमच्या शिक्षणाला बळकटी मिळेल.

1. तुमच्या सर्व सोशल मीडिया, बँकिंग, ई-कॉमर्स आणि ईमेल खात्यांसाठी अद्वितीय आणि मजबूत 10-वर्णांचे ASCII पासवर्ड तयार करा
2. दररोज आपल्या डेटाचा बॅकअप घ्या किंवा स्वयंचलित बॅक-अप सुविधा सेट करा
3. तुमचे ऑपरेटिंग सिस्टम सॉफ्टवेअर नियमितपणे तपासा आणि अपडेट करा (Windows/IoS/Android)
4. इंटरनेट ब्राउझ करताना गुप्त मोड वापरा आणि त्यात काय वेगळे आहे ते शोधा
5. तुमच्या बँक वेबसाइटवर सुरक्षित आर्थिक व्यवहार सुलभ करण्यासाठी बँकिंग आणि पेमेंट संरक्षण सक्षम करण्यासाठी तुमचे अँटी-व्हायरस सॉफ्टवेअर सेट करा
6. लहान मुले तुमची डिव्हाइस वापरतात तेव्हा धोकादायक आणि आक्षेपार्ह वेबसाइट ब्लॉक करण्यासाठी पालक नियंत्रण सक्षम करण्यासाठी तुमचे अँटीव्हायरस सॉफ्टवेअर सेट करा
7. तुमच्या फोनवरील अनोळखी नंबरवरून आलेले कॉलचे बारकाईने निरीक्षण करा आणि ते आंतरराष्ट्रीय अनोळखी नंबरवरून आले असल्यास उत्तर देऊ नका
8. आधार/पॅनच्या फक्त स्वाक्षरी केलेल्या छायाप्रती सबमिट करा आणि त्या तारखेचाही उल्लेख करा, ज्याला तुम्ही फोटोकॉपी जमा करत आहात आणि त्या सबमिट करण्याचा उद्देश.
9. डिजीलॉकर खाते तयार करा आणि तुमचे आधार, पॅन, ड्रायव्हिंग लायसन्स आणि शैक्षणिक प्रमाणपत्रे अपलोड करा
10. स्वतःला गटांमध्ये जोडले जाण्यापासून रोखण्यासाठी WhatsApp वर सेटिंग्ज बदला
11. अनोळखी व्यक्ती (किंवा नंबर) तुम्हाला वारंवार मेसेज पाठवत असल्यास WhatsApp वरील “ब्लॉक” वैशिष्ट्य वापरून पहा
12. Facebook/Instagram/इतर सोशल मीडिया सेटिंग्ज खाजगी वर बदला
13. तुमच्या मेल आयडीसाठी 2-फॅक्टर ऑथेंटिकेशन तयार करा
14. तुमच्या Google खाते/IoS खात्यावर माझा फोन शोधा सक्षम करा
15. तुमच्या वेब ब्राउझरवर सुरक्षा वैशिष्ट्ये सक्षम करा (Google Chrome/Microsoft Edge/Mozilla Firefox/Opera/IoS)
16. आठवड्यातून एकदा तुमच्या डिव्हाइसवरून ब्राउझिंग इतिहास हटवा
17. सायबरस्टॉकिंग किंवा कोणत्याही बेकायदेशीर सायबर क्रियाकलापांचा अनुभव घेत असलेल्या कोणालाही/लहान मुलांना पहा, समर्थन द्या आणि मदत करा
18. नॅशनल सायबर क्राईम रिपोर्टिंग पोर्टलवर सामायिक केलेल्या विविध सेवा आणि सावधगिरींचे अन्वेषण करा (https://cybercrime.gov.in/Default.aspx)
19. उमंग वेबसाइट एक्सप्लोर करा (https://web.umang.gov.in/landing/department/cybercrime-reporting-portal.html)
20. राष्ट्रीय महिला आयोगाच्या पोर्टलवर निवारणासाठी विविध सेल एक्सप्लोर करा (http://ncw.nic.in/ncw-cells)

नोट्स