सायबर जागरूकता

सायबर सिक्युरिटी हा सध्या चर्चेचा विषय आहे. सायबर सुरक्षा म्हणजे डिजिटल माहिती, संगणकप्रणाली, नेटवर्क आणि इलेक्ट्रॉनिक डेटाचे अनधिकृत प्रवेश, वापर, प्रकटीकरण, व्यत्यय, बदल किंवा विनाशयापासून संरक्षण करण्यासाठी डिझाइन केलेल्या पद्धती, तंत्रज्ञान आणि प्रक्रियांचा संदर्भ आहे. या मध्ये मालवेअर,व्हायरस,ट्रोजन,फिशिंग, रॅन्समवेअर आणि इतर प्रकारच्या सायबर धोक्यांपासून संरक्षण समाविष्ट आहे.

प्रभावी सायबर सुरक्षा उपाय गोपनीयता, अखंडता आणि संवेदनशील माहितीची उपलब्धता सुनिश्चित करतात आणि वैयक्तिक किंवा संस्थात्मक सुरक्षेशी तडजोड करू शकतील अशा सायबर हल्ल्यांना प्रतिबंधित करतात. प्रभावी सायबर सुरक्षा उपायांमध्ये तंत्रज्ञान, धोरणे आणि वापरकर्ता जागरूकता यांचा समावेश असतो.

खालील कारणांमुळे आजच्या डिजिटल युगात सायबर सुरक्षा महत्त्वाची आहे:

1. संवेदनशील माहितीचे संरक्षण:
2. आर्थिक नुकसान रोखणे:
3. गोपनीयतेची देखभाल:
4. गंभीर पायाभूत सुविधांचे संरक्षण:
5. व्यवसाय सातत्य:
6. राष्ट्रीय सुरक्षा:
7. बौद्धिकसंपत्तीचे संरक्षण:
8. नियमांचे पालन:
9. प्रतिष्ठा आणि विश्वास:
10. विकसित होणारे धोके:

सायबर सुरक्षा वैयक्तिक, आर्थिक आणि गोपनीय डेटाचे अनधिकृत प्रवेश आणि चोरी पासून संरक्षण करण्यात मदत करते. सायबर हल्ल्यांमुळे लक्षणीय आर्थिक नुकसान, प्रतिष्ठेचे नुकसान आणि कायदेशीर दायित्वे होऊ शकतात. हे सुनिश्चित करते की वैयक्तिक माहिती खाजगी राहते आणि दुर्भावना पूर्ण हेतूंसाठी तिचा वापर केला जात नाही. पॉवरग्रिड, आरोग्यसेवा प्रणाली आणि वाहतूक नेटवर्क यासारख्या महत्त्वपूर्ण पायाभूत सुविधांच्या सुरक्षेसाठी हे आवश्यक आहे. हे अखंडित व्यवसाय ऑपरेशन्स सुनिश्चित करण्यात मदत करते आणि डाउनटाइम कमी करते. राष्ट्रीय सुरक्षेचे रक्षण करण्यासाठी आणि सायबर हेरगिरी रोखण्यासाठी हे महत्त्वाचे आहे. हे बौद्धिक संपदा, व्यापारगुपिते आणि मालकीची माहिती संरक्षित करण्यात मदत करते. हे संस्थांना डेटासंरक्षण नियमांचे पालन करण्यास आणि कायदेशीर परिणाम टाळण्यास मदत करते. हे ग्राहकांचा विश्वास राखण्यात मदत करते आणि संस्थेच्या प्रतिष्ठेचे रक्षण करते. AI-शक्तीचे हल्ले, IoT असुरक्षा आणि सामाजिक अभियांत्रिकी रणनीती यासारख्या उदयोन्मुख धोक्यांपासून पुढे राहण्यासाठी हे आवश्यक आहे.

काही सुरक्षितता टिप्स.....

पासवर्ड सुरक्षा:

सायबरहल्ल्यांपासून स्वतःचे संरक्षण करा:

येथे काही पासवर्ड संरक्षण टिप्स आहेत:

1. मजबूत पासवर्ड वापरा: अप्परकेस आणि लोअरकेस अक्षरे, संख्या, अल्फान्यूमेरिक आणि विशेषवर्ण मिक्स करा. प्रत्येक खात्यासाठी वेगवेगळे पासवर्ड वापरा. नावे, वाढदिवस किंवा सामान्यवाक्ये, ठिकाणे यांसारखे सहज अंदाज लावता येणारे शब्द वापरू नका. ठराविक अंतराने पासवर्ड अपडेट करा.
2. पासवर्ड ची लांबी: आदर्शपणे 12 किंवा अधिकवर्ण.
3. पासवर्ड पुन्हा वापरू नका: एकाधिक खात्यांमध्ये एकच पासवर्ड पुन्हा वापरू नका.
4. द्वि-घटकप्रमाणीकरण (2FA): OTP किंवा बायोमेट्रिक सारख्या सुरक्षेचा अतिरिक्त स्तर जोडण्यासाठी शक्य असेल तेव्हा 2FA सक्षम करा.
5. फिशिंग स्कॅम टाळा: पासवर्ड रीसेट किंवा लॉगिनसाठी विचारणा-या ईमेल किंवा लिंक्स पासून सावध रहा.
6. पासवर्ड खाजगी ठेवा किंवा ते प्रवेशयोग्य ठिकाणी लिहू नका.

लक्षात ठेवा, मजबूत पासवर्ड ही सायबर धोक्यांपासून बचावाची पहिली पायरी आहे!

सायबर धोक्याचे प्रकार:

मालवेअर, "Malicious सॉफ्टवेअर" हे संगणक प्रणाली किंवा त्याच्या वापरकर्त्याचे नुकसान करण्यासाठी किंवा शोषण करण्यासाठी डिझाइन केलेले कोणतेही सॉफ्टवेअर संदर्भित करते.

मालवेअरच्या प्रकारांमध्ये हे समाविष्ट आहे:

1. व्हायरस: प्रतिकृती तयार करतात आणि इतर फाइल्स किंवा सिस्टम मध्ये पसरवतात.
2. ट्रोजन्स: अनधिकृत प्रवेशास अनुमती देऊन, कायदेशीर सॉफ्टवेअर म्हणून भासवतात.
3. स्पायवेअर: गुप्तपणे निरीक्षण करतात आणि वापरकर्त्याचा डेटा गोळा करतात.
4. रॅन्समवेअर: माहिती एनक्रिप्ट करतात व डिक्रिप्शनसाठी देयकाची मागणी करतात.
5. ॲडवेअर: तुम्ही मोबाईल फोन किंवा लॅपटॉप वापरत असताना नको असलेल्या जाहिराती दाखवतात.
6. वर्म्स: स्वत:ची प्रतिकृती बनवतात आणि मानवी संवादाशिवाय पसरवतात.
7. रूटकिट्स: मालवेअर किंवा अनधिकृत प्रवेश लपवतात.
8. की लॉगर्स: पासवर्ड टाकताना अनेकदा संवेदनशील माहिती चोरण्यासाठी कीस्ट्रोक रेकॉर्ड करतात.

मालवेअर याद्वारे सिस्टम मध्ये प्रवेश करू शकतात:

1. ई-मेल संलग्नक किंवा संक्रमित ईमेल लिंक
2. संक्रमित सॉफ्टवेअर डाउनलोड
3. असुरक्षित नेटवर्क कनेक्शन
4. संक्रमित बाह्य उपकरणे (उदा. USB ड्राइव्हस्,)
5. शोषित प्रणाली असुरक्षा

मालवेअर पासून संरक्षण करण्यासाठी, हे करा:

1. अँटीव्हायरस सॉफ्टवेअर वापरा
2. सिस्टम आणि सॉफ्टवेअर अद्ययावत ठेवा
3. संशयास्पद डाउनलोड आणि लिंक टाळा
4. मजबूत पासवर्ड वापरा आणि फायरवॉल सक्षम करा
5. महत्त्वाच्या डेटाचा नियमित बॅकअप घ्या
6. केवळ अधिकृत/विश्वसनीय स्रोतावरून ॲप डाउनलोड करा व त्याची खात्री करा.

लक्षात ठेवा, मालवेअर संक्रमण टाळण्यासाठी दक्षता आणि सावधगिरी ही गुरुकिल्ली आहे!

मनोवैज्ञानिक युक्त्या म्हणजे हल्लेखोर फायदेशीर ऑफर देऊन वापरकर्त्याच्या मनाशी खेळतात. एकदा अडकल्यावर, हल्लेखोर एकतर पैसे चोरून किंवा संवेदनशील वैयक्तिक माहिती (नाव, आधार तपशील, बँकखाते तपशील इ.) चोरून वापरकर्त्याचे शोषण करू शकतात किंवा इतर कोणत्याही प्रकारे वापरकर्त्याला हानी पोहोचवू शकतात. या प्रकारच्या हल्ल्याचा संपूर्ण आधार म्हणजे बनावट ई-मेल, कॉल किंवा एसएमएस पाठवून वापरकर्त्याला त्यांच्या जाळ्यात अडकवणे.

फिशिंग हे फसवे ई-मेल पाठवण्याची कृती आहे जी एखाद्या वैधस्त्रोता कडून दिसते, उदाहरणार्थ, बँक, भर्तीकर्ता किंवा क्रेडिट कार्ड कंपनी इ. संवेदनशील वैयक्तिक माहिती, बँकखाते तपशील इत्यादी मिळवण्याच्या प्रयत्नात हे केले जाते.
विशिंग हे फिशिंग सारखेच आहे.परंतु, या प्रकारच्या गुन्ह्यात ई-मेल ऐवजी, फसवणूक करणारा संवेदनशील वैयक्तिक आणि आर्थिक माहिती मिळविण्यासाठी टेलिफोनचा वापर करतो.

स्मिशिंग हे फिशिंग चे एसएमएस समतुल्य आहे.हे फसवे मजकूर संदेश पाठवण्यासाठी एसएमएस वापरते.एसएमएस प्राप्तकर्त्याला वेबसाइट/वेबलिंक ला भेट देण्यास किंवा फोन नंबर वर कॉल करण्यास सांगतो.त्या नंतर वापरकर्त्याला संवेदनशील वैयक्तिक माहिती, डेबिट/क्रेडिट कार्ड तपशील किंवा पासवर्ड इत्यादी प्रदान करून फसवले जाते.

फिशिंग, विशिंग आणि स्मिशिंग हे वापरकर्त्याचे पैसे चोरण्यासाठी किंवा वापरकर्त्याला इतर कोणतेही नुकसान करण्याच्या प्रयत्नात केले जाते.

<u>सोशल मीडिया फसवणूक</u>: · फसवणूक करणारे खोटी किंवा खोटी माहिती पसरवण्यासाठी वापरकर्त्याच्या बनावट प्रोफाइलचा वापर करतात. आर्थिक लाभ मिळविण्यासाठी वापरकर्त्याच्या इतर मित्रांना मित्रविनंती पाठवतात. पीडिताची प्रतिष्ठा खराब करणे.

वरील सोशल मीडिया फसवणूक टाळण्यासाठी : · तुमची वैयक्तिक माहिती जसे की पत्ता, मोबाइल नंबर, वैयक्तिक मेल आयडी आणि इतर संवेदनशील ओळख संबंधित माहिती सोशलमीडिया वर शेअर करणे टाळा. तुमची वैयक्तिक छायाचित्रे सोशल मीडिया अकाउंटवर सार्वजनिकपणे ऑनलाइन शेअर करू नका. योग्य पडताळणी आणि पुष्टीकरणाशिवाय कधी ही मित्रविनंत्या स्वीकारू नका.सोशल मीडिया खात्यांसाठी बहु-घटक प्रमाणीकरण सक्षम करा.सार्वजनिक शोधांमधून प्रोफाइल दृश्यमानता अक्षम करा. प्रत्येक सत्रानंतर लॉगआउट करा. सोशल मीडिया क्रेडेन्शियल्स कधीही कोणाशीही शेअर करू नका. सोशल मीडिया प्रोफाइलची गोपनीयता सेटिंग्ज अत्यंत प्रतिबंधित स्तरावर ठेवा, विशेषतः सार्वजनिक पाहण्यासाठी. छायाचित्रे, व्हिडिओ, स्टेटस, कमेंट्स इत्यादी शेअर करताना जास्तीत जास्त सावधगिरी बाळगा. गुन्हेगार वापरकर्त्याच्या पोस्ट आणि प्रोफाइल वरून वापरकर्त्यां बद्दल पुरेशी माहिती गोळा करू शकतात. तुमच्या सोशलमीडिया गोपनीयता सेटिंग्जचे पुनरावलोकन करा आणि कुटुंब आणि ओळखीच्या मित्रांपुरते मर्यादित करा. सावध राहा

'डिजिटल अटक अटॅक'**<u>(Digital Arrest):</u>**

या अंतिम वापरकर्त्याला (पीडित) कॉल येतो ज्यामध्ये हल्लेखोर, पीडितेवर/व्यक्तीला दबाव आणतात आणि दावा करतात की तो/ती पोलीस-सीबीआय-ईडी अधिकारी आहेत आणि पीडितेला/व्यक्तीला कळवतात की त्याच्या नातेवाईकाने गुन्हा/हल्ला केला आहे आणि पीडितेने सांगितले की नातेवाईक पोलिस/सीबीआय अंतर्गत आहेत. कोठडी , त्याच्या/तिच्या शिक्षेतून मुक्त होण्यासाठी पीडिताला यादच्छिक पैसे देण्यास सांगणे / काही वेळा आभासी पैसे (जसे बिट कॉईन) तसेच पीडितांची वैयक्तिक माहिती विचारणे खाते तपशील. हल्लेखोर पीडितेला व्हिडिओ कॉल करतात ज्यामध्ये पोलिस कार्यालय/सीबीआय/ईडी कार्यालय/कोर्ट रूमची अचूक व्यवस्था तयार केली जाते. पैसे मिळेपर्यंत/पीडीत सापळे होईपर्यंत, हल्लेखोर पीडिताला स्काईप किंवा टीम कॉलद्वारे व्हिडिओ कॅमेऱ्यासमोर ऑनलाइन उपस्थित राहण्यास लावतात. व्हिडिओ कॉलद्वारे, हल्लेखोरांनी पीडितेला सांगितले की जोपर्यंत पीडित हल्लेखोराला रक्कम देत नाहीत तोपर्यंत तो/ती ऑनलाइन अटकेत आहे. त्यामुळे पीडितांना 3-4 दिवस सतत ऑनलाइन कॅमेऱ्यासमोर बसावे लागते. शेवटी बळी हल्लेखोरांना खोटी प्रार्थना करतात आणि हल्लेखोराला हवे ते पैसे हस्तांतरित करतात. हे अगदी ऑनलाइन छळवणुकीसारखे आहे.

<u>अलीकडील 'डिजिटल अटक अटॅक' घटना आहेत</u> :- डिजिटल अटकेनंतर जवळपास 4 दिवसांपासून छळलेल्या प्रसिद्ध डॉक्टरांसोबत, सीबीआय अधिकारी म्हणून दाखवलेल्या व्यक्ती ने सांगितले की सायबर गुन्हेगारांना तिने 2.81 कोटी रुपये हस्तांतरित केले, अचूक ऑनलाइन कोर्ट रूम सेटअप तयार केला गेला, डॉक्टरांचे बँक खाते असा दावा करतात रुपये मनी लॉंड्रिंगमध्ये वापरण्यात आला होता, त्यानंतर तिला ताबडतोब पोलिसांकडे अटक करण्यास सांगितले, एकदा ती पोलिसात हजर राहू शकली नाही आणि चौकशीत ती जबरदस्तीने होती काही दिवसांपासून 'स्काईप व्हिडिओ कॉल'समोर डिजिटल अटक.

असाच प्रकार आग्राच्या शिक्षकासोबत आहे, मध्य प्रदेशात फसवणूक करणाऱ्या डिजिटल अटकेनंतर शास्त्रज्ञाला ७१ लाख रुपयांची फसवणूक, उद्योगप्रमुखांपैकी एकाला रु. डिजिटल अटक मध्ये 7 कोटी, बेंगळुरू स्थित MNC कार्यकारिणीला 'डिजिटल अटक' मध्ये 51 लाख रुपये आणि बरेच काही गमावले.

इंडियन सायबर क्राइम कोऑर्डिनेशन सेंटर (I4C) नुसार, पोलीस/CBI/ED कधीही व्हिडिओ कॉलद्वारे कोणालाही अटक करत नाही.

QR Code स्कॅम : लोकांना फसविण्यासाठी सायबर भामटे अनेक युक्त्या वापरतात. सायबर सिक्युरिटी कंपन्यांनुसार, हे सायबर गुन्हेगार लोकांना ठगवण्यासाठी फसवे ई-मेल पाठवतात. त्या माध्यमातून फसवणूक करतात. गेल्या काही वर्षात ऑनलाईन खरेदी वाढली आहे. अनेकजण स्वस्त आणि माफक दरात सामान खरेदीसाठी सहज गुगल करतात. त्यात अनेक ऑनलाईन शॉपिंग प्लॅटफॉर्म समोर येतात. काही नावाजलेले तर काही माहिती नसलेले प्लॅटफॉर्म दिसतात. टेलेग्राम, व्हॉट्सअप या माध्यमातूनही ऑनलाईन वस्तू खरेदीसाठीचे मॅसेज येतात. त्यात एखादी वस्तू खरेदी केल्यानंतर ऑनलाईन पेमेंटसाठी QR Code ई-मेल अथवा व्हॉट्सअपवर पाठविण्यात येतो. तो स्कॅन करण्यास सांगण्यात येते. नेमके इथंच या सायबर भामटच्यांचे फावते व ते पैसे काढतात.

मुलांना पासवर्ड सुरक्षिततेबद्दल शिक्षित करा.त्यांची सोशल मीडिया खाती तपासा आणि त्याचा मागोवा ठेवा.

मॉर्फिंग म्हणजे ऑनलाइन उपलब्ध मॉर्फिंग साधने वापरून व्यक्तीचे चित्र बदलणे. मॉर्फ केलेली चित्रे नंतर पीडितांना ब्लॅकमेल करण्यासाठी, बनावट ऑनलाइन प्रोफाइल तयार करण्यासाठी, सेक्सटिंग, सेक्सचॅट्स, अश्लीलसामग्री,नग्नचित्रे इत्यादी साठी वापरतात, मॉर्फिंग पीडिताच्या प्रतिष्ठेला हानी पोहोचवू शकते आणि भावनिक आघात होऊ शकते, मॉर्फिंगकर्त्याकडून धमक्या देखील येऊ शकतात. गुन्हेगार आणि त्यांना ब्लॅकमेल करण्याच्या त्यांच्या प्रयत्नांना बळी पडू शकतात.

सायबर गुन्हेगार सतत सुरक्षा धोके उघड करण्यासाठी नवीन मार्ग शोधत आहेत. ते संगणक प्रणालीवर अनधिकृत प्रवेशाद्वारे संस्थेची मालमत्ता चोरणे, उघड करणे, बदलणे, अक्षम करणे किंवा नष्ट करणे यासाठी सायबर हल्ले करतात. सायबर हल्ल्यामुळे आर्थिक नुकसान आणि व्यवसायात व्यत्यय येऊ शकतो.

डीपफेक्समध्ये वाढ- AI व्युत्पन्न व्हॉइस, व्हिडिओ आणि फोटो स्कॅममुळे चुकीची माहिती फिल्टर करणे हे एक आव्हानात्मक कार्य बनते. हे एआय टूल्स वापरून संपादित किंवा व्युत्पन्न केले जाते आणि जे वास्तविक किंवा अस्तित्वात नसलेल्या लोकांचे चित्रण करू शकते. (फसवणूक प्रतिमा, व्हिडिओ इ.)

अफवा पसरवण्यापलीकडे, सायबर हल्लेखोर आता सार्वजनिक डोमेनमध्ये उपलब्ध असलेल्या प्रतिमा हाताळू शकतात आणि त्या प्रतिमांच्या बनावट स्पष्ट आवृत्त्या पुन्हा पोस्ट करू शकतात. खोट्या प्रतिमा आणि शब्दांमुळे मुले आणि त्यांच्या कुटुंबीयांना महत्त्वपूर्ण, कायमस्वरूपी हानी पोहोचू शकते, त्यांची गोपनीयता, ओळख आणि कल्याण यांना हानी पोहोचू शकते.

केंद्रीय गृहमंत्री अमित शाह यांनी जाहीर केले आहे की भारतातील वाढत्या सायबर धोक्यांचा सामना करण्यासाठी पुढील पाच वर्षांमध्ये 5,000 सायबर कमांडो पूर्णपणे प्रशिक्षित आणि तैनात केले जातील. I4C (इंडियन सायबर क्राइम कोऑर्डिनेशन सेंटर) च्या स्थापनादिनानिमित्त, शहा यांनी राष्ट्रीय सुरक्षेसाठी महत्त्वपूर्ण म्हणून सुरक्षित सायबर स्पेसच्या गरजेवर भर दिला आणि म्हटले की देशाची प्रगती मजबूत सायबर सुरक्षा सुनिश्चित करण्यापासून अविभाज्य आहे. भारताच्या डिजिटल संरक्षणास बळकट करून देशभरातील सायबर हल्ल्यांना त्वरेने संबोधित करण्यासाठी आणि त्यांना रोखण्यासाठी कमांडो सज्ज असतील. सायबर हल्ल्यांना जलद प्रतिसाद आणि प्रतिबंध, किमान नुकसान आणि गंभीर डिजिटल पायाभूत सुविधांमध्ये व्यत्यय सुनिश्चित करणे हे त्यांचे ध्येय असेल. बँका आणि आर्थिक मध्यस्थांच्या सहकार्याने विकसित केलेली

त्याची रजिस्ट्री राज्ये, केंद्रशासित प्रदेश आणि कायद्याची अंमलबजावणी करणाऱ्या एजन्सींसाठी अशा गुन्ह्यांमध्ये सहभागी असलेल्या संशयितांपर्यंत पोहोचण्यासाठी आणि त्यांचा मागोवा घेण्यासाठी केंद्रीय भांडार असेल, ज्यामुळे फसवणूक जोखीम व्यवस्थापन वाढेल.

तुम्हाला सुरक्षित ठेवण्यासाठी टिप्स.....

1. तुमची सिस्टीम/डिव्हाइस (डेस्कटॉप, लॅपटॉप, मोबाईल) नेहमी नवीनतम पॅचसह अपडेट ठेवा.
2. नवीनतम आवृत्तीसह अँटी-व्हायरस सारख्या सुरक्षा सॉफ्टवेअरद्वारे सिस्टम/डिव्हाइसचे संरक्षण करा.
3. नेहमी फक्त ज्ञात, विश्वसनीय स्त्रोतांकडून सॉफ्टवेअर डाउनलोड करा. तुमच्या सिस्टम/डिव्हाइस वर पायरेटेड सॉफ्टवेअर कधीही वापरू नका.
4. सर्व उपकरणे/खाती मजबूत पिन किंवा पासकोडद्वारे संरक्षित असल्याची खात्री करा.
5. पासवर्ड कधीही कोणाशीही शेअर करू नका.
6. तुमचा नेट-बँकिंग पासवर्ड, वनटाईम पासवर्ड (ओटीपी), एटीएम किंवा फोन बँकिंग पिन, सीव्हीव्ही नंबर इत्यादी कोणत्याही व्यक्ती सोबत शेअर करू नका, जरी तो /ती बँकेचा कर्मचारी किंवा प्रतिनिधी असल्याचा दावा करत असेल आणि अशाप्रकारची तक्रार नोंदवा.
7. तुमच्या वाय-फाय राउटर वरील डीफॉल्ट प्रशासक पासवर्ड नेहमी फक्त तुम्हाला माहीत असलेल्या मजबूत पासवर्ड मध्ये बदला. याव्यतिरिक्त, नवीनतम एन्क्रिप्शन वापरण्यासाठी नेहमी तुमचे वायरलेस नेटवर्क कॉन्फिगर करा (कोणत्याही शंकाअसल्यास तुमच्या नेटवर्क सेवाप्रदात्याशी संपर्क साधा).
8. सार्वजनिक Wi-Fi द्वारे ब्राउझ करताना सावधगिरी बाळगा आणि वैयक्तिक लॉगइन करणे टाळा
9. सार्वजनिक संगणकावरून नेट-बँकिंग सुविधे मध्ये प्रवेश करण्यासाठी नेहमी व्हर्च्युअल कीबोर्ड वापरा; आणि ऑनलाइन व्यवहार पूर्ण झाल्यानंतर बँकिंग पोर्टल/वेबसाइट वरून लॉगआउट करा. ऑनलाइन बँकिंग प्रक्रिया पूर्ण झाल्यानंतर वेब ब्राउझर (इंटरनेट एक्सप्लोरर, क्रोम, फायरफॉक्स इ.) वरून ब्राउझिंग इतिहास हटवण्याची खात्री करा.
10. सर्व ई-मेल संलग्नक (Attachments) उघडण्यापूर्वी व्हायरस साठी स्कॅन करा. अज्ञात किंवा अविश्वासू स्त्रोतांकडून ई-मेल मध्ये प्राप्त झालेले ई-मेल संलग्नक डाउनलोड करणे टाळा.
11. ओळखीचा पुरावा कागदपत्रे शेअर करताना सावधगिरी बाळगा, खास करून तुम्ही ज्या कंपनीशी / व्यक्तीसोबत माहिती शेअर करत आहात त्याची सत्यता पडताळून घ्या .
12. तुमच्या सेल फोनचा IMEI कोड लक्षात ठेवा आणि तो सुरक्षित ठिकाणी ठेवा. सेलफोन चोरीला गेल्यास ऑपरेटर IMEI कोड वापरून फोन ब्लॅकलिस्ट/ब्लॉक/ट्रेस करू शकतो.
13. एटीएम वापरण्यापूर्वी स्किमर्स किंवा तुमच्या पिनचे निरीक्षण करणाऱ्या लोकांसाठी तुमच्या परिसराचे

निरीक्षण करा.

14. सुरक्षित इंटरनेट पद्धती आणि नेटिकेट्स बद्दल तुमचे मित्र आणि कुटुंबीयांशी नियमितपणे चर्चा करा! त्यांना सायबर गुन्हे आणि सुरक्षित सायबर पद्धतींबद्दल अधिक जाणून घेण्यासाठी प्रवृत्त करा.

15. तुमचे कार्ड किंवा बँक खात्याचे तपशील तुमच्या ई-वॉलेटमध्ये सेव्ह करू नका कारण यामुळे सुरक्षा उल्लंघनाच्या बाबतीत चोरी किंवा फसव्या व्यवहारांचा धोका वाढतो.

15. तुमच्या मोबाईल नंबरमध्ये बदल झाल्यास मोबाईल नंबर तुमच्या शाखेत वेळोवेळी अपडेट करा जेणेकरून नियमित एसएमएस अपडेट मिळतील.

16. सुरक्षित व्यवहारांसाठी फक्त अधिकृत मोबाइल ॲप्स वापरा.

17. तुमची तडजोड झाली आहे असे तुम्हाला वाटत असल्यास, अधिकाऱ्यांना ताबडतोब कळवा.

18. जर ते तुम्हाला सांगत असतील की तुम्ही 'डिजिटल अरेस्ट' मध्ये आहात, आणि कुणालाही कॉल करू नका, जिथे आहात तिथून हलू नका पुढचे ४८ तास ! तर याला प्रतिसाद देऊ नका. हा स्कॅम आहे.

19. जर ते तुम्हाला सांगत असतील की तुमच्यासाठी पाठवलेल्या किंवा तुम्ही पाठवलेल्या एखाद्या पॅकेजमध्ये ड्रग्ज सापडली आहेत, तर प्रतिसाद देऊ नका. हा स्कॅम आहे. (लक्षात ठेवा.... कर नाही तर डर कशाची) हे विसरू नका !

20. जर ते म्हणाले की तुमचा मुलगा / मुलगी ऍक्सीडेन्ट मध्ये सापडला असून आता आमच्या हॉस्पिटल मध्ये आहे, पंधरा मिनिटात ऑपरेशन करावे लागेल, तर तोवर टोकन मनी म्हणून अमुक इतके पैसे पाठवा ! तर अजिबात पाठवू नका ! हा स्कॅम आहे. त्यासाठी आधी मुलाला कॉल करून खात्री करून घ्या. मग कळेल की तो तर ऑल रेडी सेफ आहे..... कॉलेजात / कँटीन मध्ये !

21. जर ते तुमच्याशी व्हॉट्सअँप किंवा एसएमएसद्वारे संपर्क साधत असतील, तर प्रतिसाद देऊ नका. हा स्कॅम आहे. (शक्यतो अननोन नम्बरवरून आलेले कोणतेही कॉल अटेंड करू नका ! व्हिडीओ कॉल तर मुळीच करू नका अटेंड

22. जर कोणी म्हणत असेल की ते स्विगी किंवा झोमॅटोवरून फोन करत आहेत आणि तुम्हाला 1 किंवा इतर कोणताही नंबर काहीही दाबून तुमच्या पत्त्याची पुष्टी करण्याची आवश्यकता असेल तर प्रतिसाद देऊ नका. हा स्कॅम आहे.

23. व्हिडिओ मोडवर कोणत्याही कॉलला कधीही उत्तर देऊ नका. त्यासाठी वाटलं तर अशावेळी तुमच्या मोबाईलचा स्क्रीन छताकडे धरून पहा. समोरून कोण कसल्या अवस्थेत (न्यूड टाईप) बोलत असेल तर तुम्हाला ते दिसेल पण त्यांना तुम्ही दिसणार नाही त्यामुळे नंतर होणारे इमोशनल ब्लॅक मेल थांबेल ! नंतर त्या नंबरला लगेच ब्लॉक करा !

24. जरी तुम्हाला सर्वोच्च अधिकारी पोलिस (डिपार्टमेंट), सी. बी. आय., ई. डी., आय. टी. विभागाकडून नोटीस पाठवली आहे असं कॉल / मेसेज करून सांगितलं असलं तरी पॅनिक होऊ नका ! संबंधित खात्याच्या अधिकृत वेबसाईटवर जाऊन त्याची आधी खात्री करून घ्या. कारण या विभागातर्फे असे कधीही कॉल / मेसेज करून नोटीस पाठवली जात नाही. अधिकृत पोस्टातर्फे तरी येते किंवा त्यांची माणसे फिजिकली नोटीस घेऊन येतात. हे विसरू नका !

25. 'सोप्या कर्जाच्या' ॲप्सच्या जाळ्यात अडकू नका. तुम्ही परत करू शकत नाही अशी अनेक कर्जे घेण्यासाठी ते हळूहळू तुम्हाला फसवतात. कधीकधी, ते मोठ्या परताव्याचे आश्वासन देतात आणि तुम्हाला गुंतवणुकीसाठी कर्ज देतात. कधीही नफा मिळत नाही. तुम्ही गुंतवलेले पैसे गेले आहेत. तुम्ही केवळ काही घोटाळ्यात गुंतवणूक करण्यासाठी कर्ज घेता. तुमची "गुंतवणूक" नष्ट होईल परंतु कर्ज आणि व्याज भरण्यासाठी तुम्ही जबाबदार असाल.
अशा रीतीने फसवणूक झालेल्या अनेक तरुणांनी शेवटी आत्महत्या केल्यात. इतकं हे भीषण आहे.

26. समभाग (शेयर्स) किंवा क्रिप्टोकरन्सी खरेदी करण्याचा सल्ला देणाऱ्या कोणत्याही कॉल/संदेशांना प्रतिसाद

देऊ नका. असा साठा खरेदी करू नका कारण "निश्चित नफा" अपेक्षित आहे. जो तुम्हाला भासवला जातो पण रियल मध्ये कधीही तो तुम्हाला मिळत नाही. उलट जे पैसे गुंतवले ते सगळे घेऊन हे भामटे फरार होतात.

27. "वर्क फ्रॉम होम" करण्याचे आश्वासन देणाऱ्या कॉल/संदेशांना शक्यतो प्रतिसाद देऊ नका. ते तुम्हाला जाळ्यात अडकवतात, तुम्हाला "नफा" दर्शविताना "गुंतवणुकीसाठी" पैसे पाठवतात. कधीही नफा मिळत नाही. हा स्कॅम आहे.
28. जर कोणी तुम्हाला फोन करून सांगितले की त्यांनी चुकून तुमच्या यू. पी. आय. आयडीवर पैसे पाठवले आहेत आणि त्यांना फक्त त्यांचे पैसे परत हवे आहेत, तर प्रतिसाद देऊ नका. हा स्कॅम आहे. तुमच्याकडे ते शंभर रुपये पाठवतील आणि लिंक अथवा क्यू आर कोड देतील आणि सांगतील की इथे रिटर्न करा ! ते अजिबात करू नका ! त्यातून तुमचा फोन हॅक करून तुमचे अकाउंट "रिकामे" करण्याचा हा स्कॅम आहे
29. आंतरराष्ट्रीय कॉल प्राप्त करताना, तुमच्या फोनवर भारतीय क्रमांक किंवा कोणताही क्रमांक दिसत नसल्यास, कृपया DoT संचार पोर्टल https://sancharsaathi.gov.in किंवा टोल फ्री क्रमांक 1800110420/1963 वर कळवा
30. कोणतेही न्यायालय/पोलिस स्टेशन/सरकारी तपासणी एजन्सी तुम्हाला फोन करून माहिती देत नाहीत किंवा आदेश काढून बोलवू पण शकत नाहीत. -ते कागदी पद्धतीने सरकारी नियमात राहून काम करतात.
31. अपनी शिकायत सबसे पहले, बैंक/एनबीएफसी/भुगतान प्रणाली सहभागी/क्रेडिट सूचना कंपनी के पास दर्ज करें। 30 दिनों में समाधान न मिलने पर cms.rbi.org.in पर शिकायत दर्ज करें। -RBI
32. आरबीआई द्वारा विनियमित बैंक/ एनबीएफसी के साथ ऋण देने वाले डिजिटल ऐप्स की जुड़ाव का आधिकारिक वेबसाइट पर पता लगाकर ही उनका सत्यापन करें। एसएमएस या सोशल मीडिया से मिलने वाले लिंक से डाउनलोड करने से बचें। -RBI
33. किसी भी लेनदेन के लिए फिंगरप्रिंट का उपयोग करने से पहले यह सुनिश्चित करें कि डिवाइस पर कोई पारदर्शी फिल्म नहीं है। ऑपरेटर की आईडी सत्यापित करें। लेनदेन की रसीद मांगें। -RBI
34. रहें साइबर सुरक्षित! अपने डिवाइस को बॉटनेट संक्रमण और मालवेयर से सुरक्षित करने के लिए, सीईआरटी-इन, भारत सरकार https://www.csk.gov.in पर "फ्री बॉट रिमूवल टूल" डाउनलोड करने की सलाह देता है - दूरसंचार विभाग
35. . कैशबैक, आकर्षक रिटर्न, तुरंत लोन, नौकरी के ऑफर या पैसे के अनुरोध वाले अज्ञात लिंक पर क्लिक न करें। -RBI
36.आरबीआई/ बैंक कभीभी लोगो से व्यक्तिगत जानकारी / बैंक का विवरण नहीं मांगता है।आर बी आई के नकली लोगो और संदेशों से सावध रहें।

सायबर फसवणुकीची तक्रार कुठे करावी?

1. ताल्काळ जवळच्या पोलीस स्टेशनला भेट द्या व तक्रार दाखल करा.
2. सायबर गुन्ह्यांच्या तक्रारी ऑनलाइन करण्यासाठी, नॅशनल सायबर क्राईम रिपोर्टिंग पोर्टलला भेट द्या. या पोर्टलवर https://cybercrime.gov.in वर प्रवेश करता येईल

तुम्ही हेल्पलाइन नंबर 1930 डायल करून तक्रार दाखल करू शकता.

3. तुमची संवेदनशील वैयक्तिक माहिती किंवा बँक तपशील विचारणारा फसवणूक एसएमएस, ई-मेल, लिंक, फोन कॉल मिळाल्यास किंवा आढळल्यास, कृपया www.reportphishing.in ला भेट देऊन महाराष्ट्र सायबरच्या वेब पोर्टलवर त्याची तक्रार करा.

4. https://www.cert-in.org.in/ वर CERT-IN द्वारे जारी केलेल्या नवीनतम सूचनांचा संदर्भ घ्या
5. खालील चॅनेल वापरून CERT-IN ला कोणत्याही प्रतिकूल क्रियाकलाप किंवा अवांछित वर्तनाची तक्रार कराE-mail : incident@cert-in.org.in

• हेल्पडेस्क : 91 1800 11 4949 घटनेची माहिती देताना खालील माहिती (शक्यतेवढी) द्या.

- घटना घडण्याची वेळ
- प्रभावित प्रणाली/नेटवर्क संबंधित माहिती
- लक्षणे दिसली

1. हरवलेल्या किंवा चोरीला गेलेल्या मोबाईलची तक्रार करण्यासाठी, पोलिसां कडे प्रथम माहितीअहवाल (FIR) दाखल करा. एफ आय आर दाखल केल्यानंतर, हेल्पलाइन क्रमांक 14422 द्वारे दूरसंचार विभागाला (DoT) कळवा किंवा पडताळणी नंतर https://ceir.gov.in वर भेट देऊन सेंट्रल इक्विपमेंट आयडेंटिटी रजिस्टर (CEIR) पोर्टलवर ऑनलाइन अनुपालन दाखल करा. DoT फोन ब्लॅकलिस्ट करेलआणि त्याला पुढील वापरा पासून ब्लॉक करेल. याव्यतिरिक्त, जर कोणी वेगळे सिम कार्ड वापरून डिव्हाइस वापरण्याचा प्रयत्न केला, तर सेवापुरवठादार नवीन वापरकर्त्याची ओळख करून पोलिसांना कळवेल.
2. हॉटलिस्ट कार्ड साठी तुम्ही खाली नमूद केलेल्या कोणत्याही चरणांचे अनुसरण करू शकता:

अ) आमच्या बँकेत नोंदणीकृत मोबाईल क्रमांकावरून "9223110011" डायल करा. 2-3 रिंग नंतर कॉल डिस्कनेक्ट होईल, सिस्टम कार्ड हॉटलिस्ट करेल

आ) ग्राहक थेट 1800223131/ 022-68778900 वर कॉल करू शकतो आणि डेस्कचे व्यवस्थापन करणाऱ्या कर्मचाऱ्याने विचारलेल्या आवश्यक क्रेडेंशियल प्रदान करून कार्ड हॉटलिस्ट करण्यासाठी विनंती नोंदवू शकतो.

इ) जर कार्डधारकाने आमच्या मोबाईल बँकिंग सेवांचा लाभ घेतला असेल, तर तो कार्ड हॉटलिस्ट पर्याय निवडून कार्ड हॉटलिस्ट करू शकतो.

ई) आवश्यक कारवाई साठी ग्राहक hotlist@abhyudayabank.net वर ईमेल देखील करू शकतात.

अनधिकृत इलेक्ट्रॉनिक व्यवहाराबाबत मूळ शाखेकडे लेखी तक्रार नोंदवा.

इलेक्ट्रॉनिक व्यवहारांच्या संदर्भातअभ्युदय बँकेचे तक्रार निवारण धोरण

बँकेचा स्वतंत्रग्राहक तक्रार निवारण कक्ष आहे (संपर्ककमांक 022- 27890636, 022- 7890638, ईमेल पत्ता atmrecon@abhyudayabank.net इलेक्ट्रॉनिक ट्रान्झॅक्शन चॅनल सहग्राहकांच्या तक्रारीं चे त्वरित निवारण करण्यासाठी. सेलसमस्यांचे निराकरण करण्यासाठी समस्या सोडवतो. NPCI विवाद व्यवस्थापन योजनेद्वारे चुकीचे/ फसवे डेबिटआणि क्रेडिट्स.

कोणत्याही इलेक्ट्रॉनिक पेमेंट पर्याया बाबत तक्रारअसल्यासअभ्युदय बँकेच्या कोणत्याही शाखेत जाऊन याप्रकरणाच्या तपशीलासह लेखी तक्रार दाखल करू शकतात. तक्रारदाराने सोबत पासबुकआणिअधिकृत पणे वैधओळखपत्र आणि पासपोर्ट आकाराचा फोटो सोबत आणावा. ग्राहकाच्या खात्यातून फसव्या डेबिट किंवा पैसे काढण्याच्या बाबतीत, ग्राहकाने पोलिस तक्रार किंवा एफआयआर

दाखल करावा.

तथापि, ग्राहकाने एफ आय आर दाखल करणे ही पूर्व अट नाही परंतु अभ्युदय बँकेच्या कोणत्याही शाखेने तक्रार स्वीकारण्यासाठी पोलिस तक्रार (पोचपावती) नोंदवणे अनिवार्य आहे.ज्याशाखेकडे तक्रार दाखल केली आहे ती प्रथम समस्येचे मूल्यांकन करेल, स्वाक्षरीसह असलेल्या तक्रार पत्रावर संबंधित माहिती रेकॉर्ड करेलआणि ती त्वरित ATM-RECON विभाग वाशी कडे पाठवेल, जे सध्या ग्राहक तक्रार निवारण कक्ष म्हणून कार्यरत आहे.

****