इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

G20 भारत 2023 INDIA
वसुधैव कुटुम्बकम्
ONE EARTH • ONE FAMILY • ONE FUTURE

आज़ादी का अमृत महोत्सव

सायबर सुरक्षा

जनजागृती पुस्तिका

डिजिटल नागरीकांसाठी आणि
डिजिटल उपक्रम

द्वारे

भारतीय संगणक इमर्जन्सी रिस्पॉन्स टीम

certin
Enhancing Cyber Security in India

च्या प्रसंगी

राष्ट्रीय सायबर सुरक्षा जागरूकता महिना (1-31 ऑक्टोबर)

NCSAM, 2023 NCSAM, 2023

"आमचे जग सुरक्षित करा"

निर्देशांक

प्रस्तावना

इंडियन कॉम्प्युटर इमर्जन्सी रिस्पॉन्स टीम (CERT-In) ही भारत सरकारच्या इलेक्ट्रॉनिक्स आणि माहिती तंत्रज्ञान मंत्रालयाच्या (MeitY), भारतीय सायबर स्पेस सुरक्षित करण्याच्या उद्देशाने स्थापन केलेली एक सरकारी संस्था आहे.

CERT-In घटना प्रतिबंध आणि प्रतिसाद सेवा तसेच सुरक्षा गुणवत्ता व्यवस्थापन सेवा प्रदान करते.

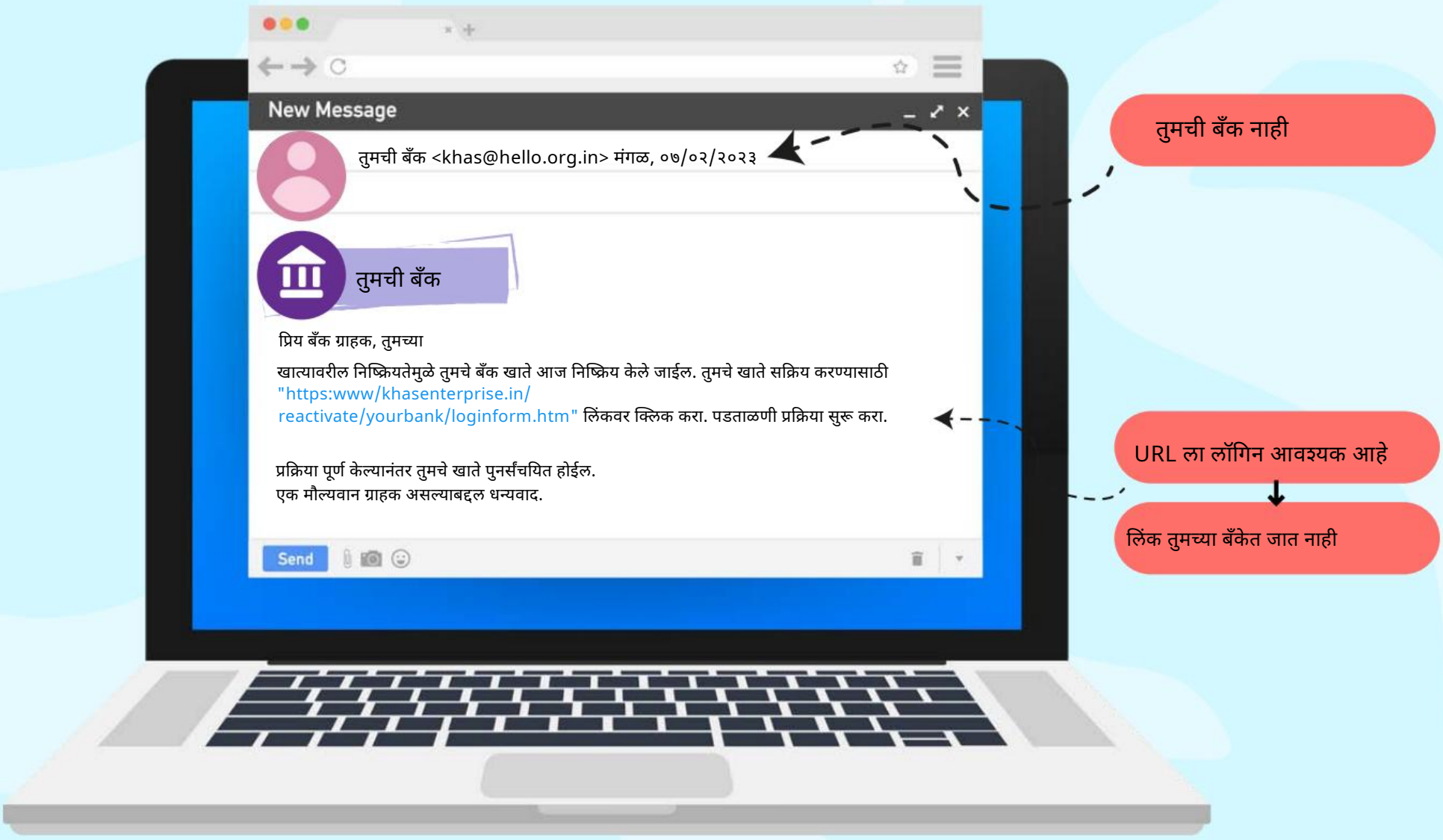
CERT-In ला माहिती तंत्रज्ञान कायदा, 2000 (सुधारणा 2008) च्या कलम 70B अंतर्गत घटना प्रतिसादासाठी राष्ट्रीय एजन्सी म्हणून नियुक्त करण्यात आले आहे. CERT-In च्या सेवांचा एक भाग म्हणून, सायबर सुरक्षेच्या क्षेत्रात जागरुकता निर्माण करण्यासाठी तसेच विविध भागधारकांना प्रशिक्षण / तांत्रिक ज्ञान अपग्रेड करण्यासाठी, CERT-In ऑक्टोबर 2023 मध्ये राष्ट्रीय सायबर सुरक्षा जागरूकता महिना (NCSAM) पाळत आहे. नागरिकांसाठी तसेच तांत्रिकसाठी विविध कार्यक्रम आणि उपक्रमांचे आयोजन

"आमचे जग सुरक्षित करा" या थीमसह भारतातील सायबर समुदाय.

डिजिटल नागरीक आणि डिजिटल एंटरप्रायझेससाठी ही जागरूकता पुस्तिका CERT-In च्या जागरूकता उपक्रमांचा एक भाग म्हणून वापरकर्त्यांना विविध सायबर सुरक्षा हल्ल्यांपासून आणि सायबर गुन्ह्यांच्या फसवणुकीपासून वाचवण्यासाठी आवश्यक असलेल्या सर्वोत्तम पद्धतींबद्दल शिक्षित करण्यासाठी प्रसिद्ध करण्यात आली आहे.

फिशिंग

फिशिंग ही एक सामान्य पद्धत आहे जी सायबर गुन्हेगार वैयक्तिक माहिती किंवा आर्थिक डेटा सामायिक करण्यासाठी पीडितांना फसवण्यासाठी प्रामाणिक दिसणारे ईमेल किंवा वेबसाइट तयार करून फसवणूक करण्यासाठी वापरतात.



सुरक्षितता टिपा

- URL वर क्लिक करण्यापूर्वी काळजीपूर्वक तपासा.
- निकड दाखवणाऱ्या संदेशांवर कधीही प्रतिक्रिया देऊ नका.
- प्रचारात्मक ऑफरवर विश्वास ठेवू नका ज्या “खूप चांगल्या आहेत”.

- तुम्ही फिशिंगला बळी पडल्यास कायद्याची अंमलबजावणी करणाऱ्या एजन्सींना तक्रार करण्यास अजिबात संकोच करू नका.
- सामान्य प्राप्तकर्त्यांना संबोधित केलेल्या ईमेलमधील ईमेल आयडी सत्यापित करा.
- टायपिंग त्रुटी शोधा (उदा., खाते, ema1l, dep0sit, passw0rd)
- "तुम्ही स्वतःबद्दल काळजी करता?" खराब व्याकरण आणि अव्यावसायिक भाषा पहा.

इच्छा

- बँक/आयकर/गॅस एजन्सी इत्यादी विश्वसनीय स्त्रोतांकडून कॉल करत असल्याची बतावणी करून फसवणूक करणारे पीडिताशी संपर्क साधतात.
- ते पीडितांना बँक खात्याचे तपशील विचारतात आणि डेबिट/क्रेडिट कार्ड, कालबाह्यता तारीख इत्यादींबद्दल आर्थिक माहिती गोळा करतात.
- फसवणूक करणारा पीडितेला रक्कम जमा करण्यासाठी मोबाईलवर पाठवलेला ओटीपी शेअर करण्यास सांगतो.
- पीडितेने ओटीपी शेअर केल्यावर त्यांच्या खात्यातून पैसे कापले जातात.

सुरक्षितता टिपा

- OTP, PIN, CVV, डेबिट/क्रेडिट कार्ड तपशील कधीही कोणाशीही शेअर करू नका.
- पैसे मिळवण्यासाठी कोणताही OTP/UPI पिन शेअर करू नका.
- बँक खाते, क्रेडिट/डेबिट कार्ड तपशील किंवा संवेदनशील माहितीची पुष्टी किंवा शेअर करण्यास सांगणाऱ्या कोणत्याही कॉलला प्रतिसाद देऊ नका.
- बक्षीस/लॉटरी/भेटवस्तू/केवायसी इ. अपडेट करण्यासाठी वैयक्तिक माहिती देऊ नका, शोध इंजिनमध्ये यादृच्छिकपणे आढळलेल्या सेवा प्रदात्यांच्या क्रमांकावर कॉल करू नका
- कारण ते बनावट क्रमांक असू शकतात.
- संस्था/संस्था/बँका इत्यादींच्या अधिकृत वेबसाइटवर उपलब्ध ग्राहक सेवा क्रमांक वापरा.
- कोणतीही घटना घडल्यास, वापरकर्त्याने 1930 वर कॉल करून त्यांच्या खात्याचा पासवर्ड ताबडतोब बदलला पाहिजे किंवा आर्थिक नुकसान टाळण्यासाठी कार्ड ब्लॉक / खाते गोठवावे.
- वापरकर्त्यांनी नियमितपणे बँक आणि क्रेडिट कार्ड स्टेटमेंटचे पुनरावलोकन करावे आणि कोणत्याही अनियमिततेची तक्रार करावी.
- वैयक्तिक माहिती सामायिक करण्यास किंवा मदत करण्याच्या बहाण्याने कोणतेही रिमोट ऍक्सेस ॲप्स स्थापित करण्यास सांगणाऱ्या कॉलपासून सावध रहा.

दुर्भावनायुक्त मोबाइल अर्ज

संक्रमित मोबाईल ऍप्लिकेशन्समध्ये मालवेअर असू शकतो जे तुमचा डेटा, लॉगिन क्रेडेन्शियल्स चोरू शकतात आणि प्रीमियम सेवांसाठी ऑटोसबस्क्राइब करू शकतात.

सुरक्षितता टिपा

- कोणतेही मोबाइल ॲप्लिकेशन डाउनलोड करण्यापूर्वी प्ले स्टोअरवरील प्ले प्रोटेक्ट फीचर तपासा.
- नेहमी वैध वेबसाइट किंवा अधिकृत ॲप स्टोअर सारख्या विश्वसनीय स्त्रोतांकडूनच अनुप्रयोग डाउनलोड करा.
- एसएमएस, ईमेल, सोशल मीडिया मेसेजवरून ॲप्स डाउनलोड करणे टाळा.
- अनुप्रयोग स्थापित करताना कोणत्याही नवीन परवानग्या देण्याबाबत सावधगिरी बाळगा.
- कोणतेही मोबाइल अनुप्रयोग स्थापित करण्यापूर्वी वापरकर्त्यांच्या पुनरावलोकने आणि टिप्पण्यांकडे लक्ष द्या.

मालवेअर

मालवेअर हा दुर्भावनापूर्ण कोडचा एक तुकडा आहे जो एखाद्या ऍप्लिकेशनमध्ये, प्रोग्राममध्ये किंवा सिस्टममध्ये धोक्याच्या कलाकारांद्वारे समाविष्ट केला जातो. ते तुमच्या सिस्टमला संक्रमित करू शकतात आणि दुर्भावनापूर्ण ऑपरेशन करू शकतात.

"मालवेअर दर्शविणारी प्रमुख चिन्हे"

सुरक्षितता टिपा

- अज्ञात स्त्रोतांकडून संशयास्पद ईमेल, लिंक आणि साइटवर क्लिक करणे टाळा.
- तुम्ही कोणत्याही दुर्भावनायुक्त लिंकवर क्लिक करताच, तुमचा मोबाईल हॅक होऊ शकतो किंवा तुमचा डेटा चोरीला जाऊ शकतो.
- फक्त सुरक्षित आणि अधिकृत वेबसाइट ब्राउझ करा.
- तुमचे संगणक सॉफ्टवेअर/ब्राउझर नेहमी अद्ययावत ठेवा.
- तुमच्या डेटाचा नियमित बॅकअप ठेवा.
- वेबसाइट्सवर दिसणाऱ्या दुर्भावनापूर्ण जाहिराती ब्लॉक करण्यासाठी पॉप-अप/ ॲड-ब्लॉकरसारखे सॉफ्टवेअर इन्स्टॉल करा.
- तुमच्या डिव्हाइसमध्ये अँटीव्हायरस आणि अँटीमालवेअर सोल्यूशन्स इंस्टॉल करा आणि ते अपडेट ठेवा.
- वास्तविक दुवा शोधण्यासाठी प्रतिमा/लिंकवर फिरवा.
- चॅट किंवा सोशल मीडिया पोस्टवर मिळालेल्या लिंकद्वारे कोणतेही ॲप्स इन्स्टॉल करू नका.

सोशल मीडिया फसवणूक

- इंटरनेट बँकिंग किंवा UPI ट्रान्सफर यांसारख्या, त्यांच्या नियंत्रणाखालील खात्यांमध्ये ऑनलाइन पेमेंट करण्यासाठी संशय नसलेल्या वापरकर्त्यांना फसवण्यासाठी स्कॅमर "बॉट्स" वापरतात.

- फसवणूक करणारे पीडितेच्या बनावट प्रोफाइलचा वापर करतात: खोटी किंवा

  बनावट माहिती पसरवण्यासाठी. १.

  2. आर्थिक लाभ मिळविण्यासाठी पीडितेच्या इतर मित्रांना मित्र विनंती पाठवते.

  पीडिताची प्रतिष्ठा खराब करणे. 3.

सुरक्षितता टिपा

- तुमची वैयक्तिक माहिती जसे की पत्ता, मोबाइल नंबर, वैयक्तिक मेल आयडी आणि इतर संवेदनशील ओळख संबंधित माहिती सोशल मीडियावर शेअर करणे टाळा.

- तुमची वैयक्तिक छायाचित्रे सोशल मीडिया अकाउंटवर सार्वजनिकपणे ऑनलाइन शेअर करू नका.

- योग्य पडताळणी आणि पुष्टीकरणाशिवाय कधीही मित्र विनंत्या स्वीकारू नका.

- जोपर्यंत तुम्ही स्त्रोताची सत्यता पडताळत नाही तोपर्यंत संशयास्पद लिंकवर क्लिक करू नका किंवा संदेशांद्वारे प्राप्त झालेले कोणतेही ॲप डाउनलोड करू नका.
- वेगवेगळ्या सोशल मीडिया खाती आणि ईमेलसाठी वेगवेगळे पासवर्ड वापरा.

- सोशल मीडिया खात्यांसाठी बहु-घटक प्रमाणीकरण सक्षम करा.
- सार्वजनिक शोधांमधून प्रोफाइल दृश्यमानता अक्षम करा.
- प्रत्येक सत्रानंतर लॉग आउट 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 वापरकर्त्यांच्या पोस्ट आणि प्रोफाइलमधून वापरकर्त्यांबद्दल पुरेशी माहिती गोळा करू शकतात.

हल्ले लक्ष्यीकरण ज्येष्ठ नागरिक

फसवणूक करणारे ज्येष्ठ नागरिकांना लक्ष्य करतात कारण ते ऑनलाइन आर्थिक घोटाळे आणि फसवणुकीसाठी अधिक असुरक्षित असतात.

ज्येष्ठ नागरिकांनी ऑनलाइन असताना सावधगिरी बाळगणे आवश्यक आहे.

ज्येष्ठ नागरिकांना लक्ष्य करून आर्थिक फसवणूक

- फसवणूक करणारे ज्येष्ठ नागरिकांना लक्ष्य करतात कारण ते ऑनलाइन आर्थिक घोटाळे आणि फसवणुकीसाठी अधिक असुरक्षित असतात.
- ज्येष्ठ नागरिकांनी ऑनलाइन असताना सावधगिरी बाळगली पाहिजे.
- फसवणूक करणारे पीडितांना त्यांचे पैसे चोरण्यासाठी जन्मतारीख, क्रेडिट किंवा डेबिट कार्ड क्रमांक, पासवर्ड, ओटीपी इत्यादी वैयक्तिक संवेदनशील माहिती प्रदान करतात.

- बनावट विमा योजना, कमी किमतीची औषधे, कार्ड नूतनीकरण, केवायसी पडताळणी, मोफत भेटवस्तू आणि ऑफरद्वारे फसवणूक करणारे ज्येष्ठ नागरिकांना लक्ष्य करतात.
- फसवणूक करणारे वयोवृद्ध लोकांच्या एकटेपणाचा गैरफायदा घेतात आणि त्यांना खोटे नाते जोडून फसवतात.

- फसवणूक करणारे ज्येष्ठ नागरिकांना लक्ष्य करण्यासाठी आणि त्यांना पैसे देण्यासाठी किंवा बँकिंग क्रेडेन्शियल्स/ओटीपी/पिन शेअर करण्यासाठी पटवून देण्यासाठी बनावट सोशल मीडिया खाती तयार करतात.

सुरक्षितता टिपा

- वैयक्तिक संवेदनशील माहिती मागणाऱ्या बँका किंवा इतर संस्थांमधून फसवणूक करणाऱ्यांपासून सावध रहा.

- फोन किंवा इंटरनेटवर OTP, वापरकर्तानाव, पासवर्ड, क्रेडिट/डेबिट कार्ड तपशील, पिन कधीही शेअर करू नका.

- अज्ञात स्त्रोतांकडून कोणत्याही लिंक/अटॅचमेंटवर कधीही क्लिक किंवा डाउनलोड करू नका.
- तुम्हाला माहिती नसेल तर ऑनलाइन खरेदी करणे टाळा.
- तुमच्या मोबाईल/लॅपटॉप/कॉम्प्युटरमध्ये प्रवेश करण्यासाठी नेहमी लॉक, पिन, पासवर्ड किंवा फिंगरप्रिंट ठेवा.

- तुमच्या ईमेल, बँकिंग आणि सोशल मीडिया खात्यांवर बहु-घटक प्रमाणीकरण सक्षम करा.

- अनोळखी व्यक्तींसोबत आणि सोशल मीडियावर संवेदनशील वैयक्तिक माहिती कधीही शेअर करू नका.

- फोनवर धर्मादाय योगदान देणे टाळा.
- नेहमी लक्षात ठेवा की बँका किंवा इतर वित्तीय संस्था कधीही तुमचे वापरकर्तानाव/पासवर्ड, ओटीपी, पिन, क्रेडिट/डेबिट कार्ड तपशील विचारत नाहीत.

हल्ले लक्ष्यीकरण

मुले

सायबर गुंडगिरी हा छळाचा एक प्रकार आहे ज्यामध्ये इतर कोणाबद्दल नकारात्मक, हानीकारक, खोटी किंवा वाईट सामग्री पाठवणे, पोस्ट करणे किंवा सामायिक करणे समाविष्ट आहे. यात लाजिरवाणे किंवा अपमानास कारणीभूत असलेल्या एखाद्या व्यक्तीबद्दल वैयक्तिक किंवा खाजगी माहिती सामायिक करणे समाविष्ट असू शकते.

सुरक्षितता टिपा

- तुमच्या सोशल मीडिया गोपनीयता सेटिंग्जचे पुनरावलोकन करा आणि कुटुंब आणि ज्ञात मित्रांपुरते मर्यादित करा.

- मुलांना पासवर्ड सुरक्षिततेबद्दल शिक्षित करा.
- त्यांचे सोशल मीडिया खाते तपासा आणि त्याचा मागोवा ठेवा.
- ते ट्रॅक करण्यायोग्य स्थानासारखी सहज ओळखता येणारी माहिती शेअर करत नाहीत याची खात्री करा.

- सोशल मीडियावरील नियमित व्यस्तता थांबवा.
- सोशल मीडियावर अनोळखी व्यक्तींकडून "फ्रेंड रिक्वेस्ट" स्वीकारू नका.
- धमकावल्यावर साइट लॉग ऑफ करा, चॅट/संदेश/ई-मेल सेव्ह करा आणि तुमचा विश्वास असलेल्या तुमच्या पालकांना/शिक्षकांना/वडिलांना कळवा.
- प्रतिसाद देऊ नका. ई-मेल/संदेश अवरोधित करा.
- ऑनलाइन शेअर करण्यापूर्वी नीट विचार करा.
- गोपनीयता सेटिंगचा वापर करा आणि तुम्ही ऑनलाइन करत असलेल्या पोस्ट नियंत्रित करा.
- तुमचा पासवर्ड कधीही शेअर करू नका. तुमचे मित्रही तुमच्या पासवर्डचा गैरवापर करू शकतात.

- ऑनलाइन इतरांशी दयाळूपणे वागणे तुम्हाला सुरक्षित ठेवण्यात मदत करेल.
- तुम्हाला ऑनलाइन मिळणाऱ्या कोणत्याही संदेश/पोस्टबद्दल तुमचा विश्वास असलेल्या प्रौढ व्यक्तीशी बोला. ते तुम्हाला गुंडगिरीपासून मुक्त करण्यात मदत करू शकतात.

हल्ले लक्ष्यीकरण महिला

- मॉर्फिंग म्हणजे ऑनलाइन उपलब्ध मॉर्फिंग साधने वापरून व्यक्तीचे चित्र बदलणे किंवा बदलणे. अल्पवयीन मुली आणि स्त्रिया सहसा ऑनलाइन गुन्हेगारांच्या हातून बळी पडतात, जे ऑनलाइन पोस्ट केलेले त्यांचे छायाचित्र वापरतात आणि चित्रांचे मॉर्फिंग करून या प्रतिमांचा दुरुपयोग करतात.

- मॉर्फ केलेली चित्रे नंतर पीडितांना ब्लॅकमेल करण्यासाठी, बनावट ऑनलाइन प्रोफाइल तयार करण्यासाठी, सेक्सटिंग, सेक्स चॅट्स, अश्लील सामग्री, नग्न चित्रे इत्यादीसाठी वापरतात, मॉर्फिंग पीडिताच्या ऑनलाइन प्रतिष्ठेला हानी पोहोचवू शकते आणि भावनिक आघात होऊ शकते, कडून धमक्या देखील येऊ शकतात. गुन्हेगार आणि त्यांना

- ब्लॅकमेल करण्याच्या त्यांच्या प्रयत्नांना बळी पडू शकतात.

सुरक्षितता टिपा

- सोशल मीडिया खात्यांवर तुमची सुरक्षा आणि गोपनीयता वैशिष्ट्ये सक्षम करा तुमची वैयक्तिक चित्रे कधीही सोशल मीडिया खात्यांवर
- सार्वजनिकपणे ऑनलाइन शेअर करू नका. चित्रे शेअर करताना वॉटरमार्क वापरा तुमच्या सोशल मीडिया खात्यांसाठी मजबूत पासवर्डसह मल्टी-
- फॅक्टर ऑथेंटिकेशन सक्षम करा.
-

- घटनेचा नंतर संदर्भ देण्यासाठी पुरावे आणि स्क्रीन शॉट्स जतन करा.

- शांतपणे दु:ख सहन करू नका, आपण एकटे नाही हे जाणून घ्या, विश्वासार्ह कुटुंब आणि मित्रांकडून मदत घ्या.

- तुम्ही तुमचे फेक प्रोफाईल किंवा सोशल मीडियावर अशा कोणत्याही आक्षेपार्ह पोस्ट पाहिल्यास, संबंधित सोशल मीडिया मदत केंद्राला कळवा.

हल्ले लक्ष्यीकरण अपंग व्यक्ती

फसवणूक करणाऱ्या व्यक्ती बहुधा अपंग लोकांची फसवणूक करण्यासाठी अधिकृत प्रतिनिधी म्हणून दाखवतात. हे स्कॅमर पीडिताला कॉल करतील किंवा ईमेल करतील आणि त्यांची वैयक्तिक माहिती विचारतील.

फसवणूक करणारे अनेकदा त्यांना आश्वासक संधी देतात जसे की घरून काम करण्याची आणि अतिरिक्त कमाई करण्याची संधी.

सुरक्षितता टिपा

- कोणत्याही अनोळखी व्यक्तीशी किंवा व्यवसायाशी ऑनलाइन किंवा फोनवर गुंतण्यापूर्वी कोणतीही गोपनीय माहिती सामायिक केली जात नाही याची खात्री करून घ्या की कोणत्याही संप्रेषणाच्या शेवटी कोण आहे याची पुष्टी केल्याशिवाय.

- वेगवेगळ्या प्रकारच्या धमक्यांबद्दल जागरुक रहा आणि स्पॉट करायला शिका
  एक घोटाळा.
- तुम्ही बळी पडल्यास 1930 वर कॉल करा कोणत्याही
- संशयास्पद लिंक्स आणि संलग्नकांवर क्लिक करू नका.
- चॅट्स, ई-मेल आणि सोशल मीडिया प्लॅटफॉर्मद्वारे प्राप्त झालेले कोणतेही ॲप्लिकेशन डाउनलोड करू नका.

हल्ले लक्ष्यीकरण संघटना

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

सुरक्षितता टिपा

- तुम्हाला तुमची वैयक्तिक/संवेदनशील माहिती प्रविष्ट करण्यास सांगणाऱ्या ईमेल, मजकूर संदेश इत्यादीद्वारे प्राप्त झालेल्या थेट लिंकवर क्लिक करू नका.
- सार्वजनिक नेटवर्क वापरणे टाळा.
- कोणत्याही वेबसाइट किंवा सेवांमध्ये पासवर्डचा पुनर्वापर टाळा.
- मेल हटवण्याऐवजी तुमच्या कामाच्या ठिकाणी कोणत्याही संशयास्पद ईमेलची तक्रार करा.

- पासवर्ड व्यवस्थापन साधनामध्ये गुंतवणूक करा, कारण एकाधिक पासवर्ड लक्षात ठेवणे कठीण आहे.

- कर्मचारी जेव्हा संस्था सोडतात तेव्हा नेहमी पासवर्ड बदला.
- मल्टी-फॅक्टर ऑथेंटिकेशन लागू करा.
- तुमचे सॉफ्टवेअर अद्ययावत ठेवा.
- डेटा एन्क्रिप्ट करण्यासाठी सुरक्षित फाइल-सामायिकरण उपाय वापरा.
- अपडेटेड अँटीव्हायरस आणि अँटी-मालवेअर सोल्यूशन्स वापरा.
- तुमचे कनेक्शन एनक्रिप्ट करण्यासाठी आणि तुमची खाजगी माहिती संरक्षित करण्यासाठी VPN वापरा.

- महत्त्वाच्या डेटाचा बॅकअप घ्या.

नेहमी मजबूत आणि जटिल पासवर्ड वापरा

**** कमकुवत

******** मध्यम

********** मजबूत

" संकेतशब्द मजबूत, सुरक्षितता मजबूत"

सुरक्षितता टिपा

- तुमच्या पासवर्डचा भाग म्हणून तुमचे नाव, वय, वाढदिवस, फोन नंबर, पत्ता, ठिकाण किंवा इतर कोणतीही संवेदनशील वैयक्तिक माहिती कधीही वापरू नका.
- प्रत्येक खात्यासाठी अद्वितीय पासवर्ड वापरा.
- अप्पर केस, लोअर केस, संख्या आणि चिन्हे मिसळून लांब पासवर्ड बनवा.
- तुमचा पासवर्ड कोणाशीही शेअर करू नका.
- बहु-घटक प्रमाणीकरण सक्षम करा.
- नियमितपणे पासवर्ड बदला.

मूलभूत सायबर स्वच्छता

सर्वोत्तम पद्धती

- अस्सल सॉफ्टवेअर वापरा
- तुमचे सॉफ्टवेअर अद्ययावत ठेवा
- संशयास्पद ईमेल उघडणे टाळा
- संशयास्पद लिंक्स/ संलग्नकांवर क्लिक करण्यापूर्वी विचार करा
- अपडेटेड अँटी-व्हायरस आणि अँटी-मालवेअर वापरा
- अद्ययावत ब्राउझर वापरा
- मजबूत पासवर्ड वापरा आणि ते नियमितपणे बदला
- तुमचे पासवर्ड कोणाशीही शेअर करू नका
- मल्टी-फॅक्टर ऑथेंटिकेशन सक्षम करा
- सुरक्षित व्यवहारांसाठी सार्वजनिक वाय-फाय नेटवर्क वापरणे टाळा
- तुमच्या डेटाचा नियमित बॅकअप घ्या

सूचना/सूचना

सूचना:

भेट द्या: https://www.csk.gov.in/alerts/Monti_ransomware.html https://www.csk.gov.in/alerts/Nitrogen_malware.html https://www.csk.gov.in/alerts/ Daam_android_botnet.html

सल्ला:

भेट द्या: https://www.cert-in.org.in CERT-In

Advisory CIAD-2021-0004 : डेटा भंग/डेटा लीक रोखणे

CERT-इन सल्लागार CIAD-2022-0026 : पासवर्ड व्यवस्थापन आणि सुरक्षा

CERT-इन सल्लागार CIAD-2022-0003 : ट्विटर सुरक्षित करणे
खाती

सायबरस्वच्छतकेंद्र

सुरक्षा साधने

फ्री बॉट रिमूव्हल टूल- मायक्रोसॉफ्ट विंडोजसाठी

- eScan अँटीव्हायरस
- K7 सुरक्षा
- जलद बरे

मोफत बॉट रिमूव्हल टूल - Android साठी

- eScan अँटीव्हायरस

मोफत मोबाइल सुरक्षा अनुप्रयोग - Android साठी

- म-कवच २

इतर संबंधित साधने:

- यूएसबी प्रतिरोध
- AppSamvid
- ब्राउझर JSGuard

मला स्कॅन करा

सायबर सुरक्षेचा अहवाल द्या सीईआरटी-इनची घटना

CERT-In ला सायबर सुरक्षा घटनांचा अहवाल देण्यासाठी: वेबसाइटला भेट द्या: https://www.cert-in.org.in

ईमेल: घटना@cert-in.org.in टोल फ्री फोन: +91-1800-11-4949 फोन:

+91-11-24368551

माहिती डेस्क

टोल फ्री फॅक्स: +91-1800-11-6969

फॅक्स: +91-11-24368546

I4C ला सायबर फसवणूक आणि गुन्ह्याची तक्रार करण्यासाठी: वेबसाइटला भेट द्या:

https://www.cybercrime.gov.in कॉल: 1930

सायबर सुरक्षेच्या क्षेत्रात CERT-In सह असुरक्षा आणि सहयोगाची तक्रार करण्यासाठी: वेबसाइटला भेट द्या: https://www.cert-in.org.in ईमेल: vdisclose@cert-in.org.in collaboration@cert-in.org.in

फोन: +11-22902600 विस्तार: 1012, +91-11-24368572 प्रशिक्षण/जागृती कार्यक्रमांसाठी:

ईमेल: training@cert-in.org.in

@IndianCERT चे अधिकृत सोशल मीडिया हँडल

https://www.facebook.com/IndianCERT/

https://twitter.com/IndianCERT

https://www.kooapp.com/profile/IndianCERT

https://www.pixstory.com/user/indiancert/9280

मला स्कॅन करा

www.cert-in.org.in

मला स्कॅन करा

www.csk.gov.in