महाराष्ट्र पोलीस

सद्रक्षणाय खलनिग्रहणाय

BHANDARA CYBER POLICE

Cyber Awareness Book

सायबर स्मार्ट बना, सुरक्षित रहा!!

www.bhandarapolice.gov.in

भंडारा पोलीस

सुरक्षित भंडारा, आपली व आमची संयुक्त जबाबदारी

https://www.bhandarapolice.gov.in

ही भंडारा जिल्हा पोलीसांची अधिकृत वेबसाईट आहे. या वेबसाईटवर भंडारा जिल्हा पोलीस विभागाशी संबंधित सर्व माहिती, नागरिकांसाठीच्या सेवा, ताज्या घडामोडी व पोलीसांच्या विविध उपक्रमांची माहिती दिलेली आहे.

मुख्य उद्देशः

- जिल्ह्यातील कायदा व सुव्यवस्था संबंधित माहिती देणे
- सुरक्षा सूचना व जनजागृती मोहिमा पोहोचवणे
- तक्रार नोंदणी, आपत्कालीन संपर्क क्रमांक, व पोलिस स्टेशनांची माहिती उपलब्ध करणे
- नवीन उपक्रम (उदा. क्यूआर कोड आधारित उपक्रम, नशा विरोधी मोहिमा) दर्शविणे
- सोशल मीडियावरील अधिकृत अपडेट्स एकत्रित करणे

थोडक्यात, ही वेबसाईट भंडारा जिल्हा पोलीसांचा अधिकृत जनसंपर्क आणि माहितीचा ऑनलाईन प्लॅटफॉर्म आहे.

वरील QR Code भंडारा पोलिसांचे वेबसाइट चे आहे, आपल्या मोबाईल मधे स्कॅन करा.

https://www.bhandarapolice.gov.in

Address : Bhandara Police Headquarters, Police Campus, Ganeshpur, Maharashtra, 441904.

पत्रव्यवहारासाठी पत्ता : भंडारा पोलीस मुख्यालय, भंडारा, महाराष्ट्र, 441904.

भंडारा पोलीस सायबर बॉट 7447470100

आपात्कालीन क्रमांक 112 नियंत्रण कक्ष 07184-252400

नियंत्रण कक्ष 07184-256646 व्हॉटसअँप नं. 9405841100

संजय वामन सावकारे

मंत्री
वस्त्रोद्योग
महाराष्ट्र राज्य

सत्यमेव जयते

भंडारा जिल्ह्याचे पालकमंत्री म्हणून, "सायबर अवेअरनेस बुक" या पुस्तकाचे प्रकाशन हे एक अत्यंत स्तुत्य आणि दूरदृष्टीचे पाऊल आहे. आजच्या काळात डिजिटल तंत्रज्ञानाचा वापर मोठ्या प्रमाणात वाढत असताना, सायबर गुन्ह्यांचे प्रमाणही दिवसेंदिवस वाढत आहे. हे गुन्हे आर्थिक फसवणूक, डेटा चोरी आणि सामाजिक माध्यमांद्वारे होणाऱ्या छळासारख्या अनेक रूपांमध्ये समोर येत आहेत.

सायबर गुन्हेगार कोणत्या पद्धती वापरतात, जसे की डिजिटल अटक, फिशिंग, हॅकिंग आणि ऑनलाइन फसवणूक, याची माहिती दिली आहे. तसेच, यापासून बचावासाठी आवश्यक असलेले उपाय आणि टिप्सही यात समाविष्ट आहेत, ज्यात मजबूत पासवर्ड वापरणे, अनोळखी लिंक्सवर क्लिक न करणे आणि गोपनीय माहिती शेअर न करणे यांचा समावेश आहे. हे पुस्तक केवळ माहितीच देत नाही, तर नागरिकांना सायबर साक्षर बनवून त्यांना डिजिटल युगात सुरक्षित राहण्यासाठी सक्षम बनवते. या पुस्तिकेद्वारे नागरिकांना या गुन्ह्यांपासून स्वतःचे आणि आपल्या कुटुंबाचे संरक्षण कसे करावे, याचे सखोल मार्गदर्शन मिळते.

मला खात्री आहे की, या पुस्तकातील मार्गदर्शनामुळे आणि सूचनांमुळे भंडारा जिल्ह्यातील नागरिकही सायबर गुन्ह्यांपासून सुरक्षित राहतील आणि हे पुस्तक समाजासाठी एक मौल्यवान साधन ठरेल. मी सर्व नागरिकांना हे पुस्तक वाचून सायबर सुरक्षिततेविषयी जागरूक होण्याचे आवाहन करतो.

(संजय सुशिला वामन सावकारे)

दालन क्र. : २०२ (उत्तर बाजू), ३ रा मजला, मंत्रालय, मुख्य इमारत, मादाम कामा रोड, मुंबई ४०० ०३२
दूरध्वनी : ०२२-२२८४२७९१ / ०२२-२२८४२७२०

श्री. नूरुल हसन, भा.पो.से.
पोलीस अधीक्षक, भंडारा.

आज “सायबर अवेयरनेस बुक” पुस्तक प्रकाशित करताना मला अतिशय आनंद होत आहे. या पुस्तकाच्या प्रकाशनाचा निर्णय आम्ही बराच आधी घेतला होता, आणि त्यामागील मुख्य उद्देश असा आहे की हे पुस्तक जास्तीत जास्त लोकांपर्यंत पोहोचावे, त्यांनी ते मनापासून वाचावे आणि सायबर सुरक्षेबाबत जागरूक व्हावे.

Indian Cyber Crime Coordination Centre (I4C) हा गृहमंत्रालयाने देशपातळीवर सुरू केलेला महत्त्वपूर्ण उपक्रम आहे. त्यांच्या मार्गदर्शनाखाली महाराष्ट्र सायबर हे सायबर फसवणूक रोखण्यासाठी सातत्याने प्रयत्नशील आहे. भंडारा सायबर पोलीस हे महाराष्ट्र सायबर यांच्या सूचनांनुसार आणि मार्गदर्शनानुसार कार्यरत असून, नागरिकांना सायबर गुन्ह्यांपासून वाचविण्यासाठी कटिबद्ध आहे.

माझी मनापासून इच्छा आहे की हे मासिक भंडारा जिल्ह्यातील प्रत्येक नागरिकापर्यंत पोहोचावे. या पुस्तकातून प्रेरणा घेऊन नागरिक सायबर फसवणुकीपासून स्वतःचे संरक्षण करतील आणि इतरांनाही जागरूक करतील, अशी मला खात्री आहे.

“जागरूक नागरिक हेच सायबर गुन्ह्यांवर खरा उपाय आहे.”
“चला, आपण सर्व मिळून सायबर सुरक्षित भारत घडवूया.”

Bhandara Cyber Police

सायबर फसवणुकीचा नवा प्रकार: बँक खात्यांवर हल्ला!

बँकिंग संबंधित समस्यांमध्ये मदत करण्याच्या बहाण्याने फसवणूक करणारे सायबर गुन्हेगार, पीडितांना त्यांच्या नोंदणीकृत मोबाईल नंबरवरून एका विशिष्ट नंबरवर (बँकेनुसार नंबर बदलतो) एक अल्फान्यूमेरिक लिंक (alphanumeric link) फॉरवर्ड करण्यास सांगतात. एकदा हे केले की, सायबर गुन्हेगार त्यांच्या स्वतःच्या मोबाईल फोनवर Wi-Fi चा वापर करून, सिम बाइंडिंग प्रक्रिया टाळून पीडितेचे युपीआय वॉलेट (UPI wallet) इन्स्टॉल करतात. यामुळे त्यांना नोंदणीकृत मोबाईल नंबरशी जोडलेल्या पीडितेच्या बँक खात्यांमध्ये प्रवेश मिळतो.

फसवणूक करणारे लोकांना केवायसी (KYC) किंवा आधार (Aadhaar) अपडेट करण्याच्या बहाण्याने कॉल करतात. त्यानंतर, ते पीडितेला एक अल्फान्यूमेरिक लिंक आणि ओटीपी (OTP) बँकेशी संबंधित एका विशिष्ट नंबरवर शेअर करण्यास सांगतात.

पीडित लिंक आणि OTP सामायिक करतो

फसवणूक करणारे संबंधित बँक खात्यातील UPI वॉलेटमध्ये प्रवेश मिळवतात. फसवणूक करणारे MPIN देखील सेट करतात.

शिकारदाराचे बँक खात्यातील पैसे फसवणूक करून घेतले, तोपर्यंत त्याचे खातं ब्लॉक होत नाही.

फसवणूक करणारे शिकारदाराचे खाते स्वतः च्या खात्यासारखे वापरतात.

सूचना :- बँक/आरबीआय अधिकारी असल्याचा दावा करणाऱ्या कोणत्याही व्यक्तीने दिलेल्या ओटीपी किंवा लिंकवर कधीही विश्वास ठेवू नका आणि ती कोणासोबतही शेअर करू नका.आजकाल फसवणूक करणारे लोक गूगल सर्चमधून एअरलाईन्स/ई-कॉमर्स कंपन्यांचे कस्टमर केअर नंबर मिळवून फ्लाइटचे वेळापत्रक बदलण्यासाठी किंवा रिफंड मिळवण्यासाठी लोकांना कॉल करत आहेत आणि त्यांच्या सूचनांचे पालन केल्यास तुम्ही फसवणुकीचे शिकार होऊ शकता. असे कधीही करू नका.

Bhandara Cyber Police

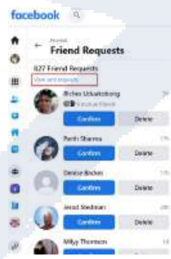
सोशल मीडियावर फसवणुकीचा नवा फंडा: तुमच्या मित्रांच्या नावाने मागताहेत पैसे!

फसवणूकदार Facebook आणि Instagram सारख्या लोकप्रिय सोशल मीडिया प्लॅटफॉर्मवरील खात्यांना लक्ष्य करत आहेत. ते असे करतात की, लक्ष्य प्रोफाइलसारखेच एक बनावट खाते तयार करतात आणि लक्ष्य प्रोफाइलच्या मित्रांना काही वैद्यकीय आपत्कालीन परिस्थितीचे कारण देत तातडीने पैसे हस्तांतरित करण्याची विनंती करतात. लक्ष्य प्रोफाइलचे मित्र त्यांना त्यांचाच मित्र समजून पैसे हस्तांतरित करतात. लक्ष्य प्रोफाइलला याबद्दल माहिती मिळेपर्यंत, त्यांचे अनेक मित्र या फसवणुकीचे बळी ठरलेले असतात. लक्ष्य खाते हॅक करूनही अशीच फसवणूक केली जाते.

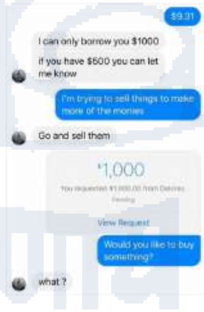
फसवणूक करणारे त्यांचे टार्गेट ची समान सोशल मीडिया प्रोफाइल बनवतात

ओरिजिनल फेसबुक प्रोफाइल

सामान्य प्रदर्शित चित्र वापरून खोटी फेसबुक प्रोफाईल तयार करण्यात येते



त्याचा Friend List मधुन त्यांचे ओळखी च्या लोकांना Friend Request पाठवतात



फसवणूक करणारे बनावट खात्याच्या मित्र सूचीतील लोकांशी मेसेंजरद्वारे संपर्क साधतो आणि काही वैद्यकीय आपत्कालीन स्थितीचे कारण देऊन पैशांची मागणी करतो. तो पैसे पाठवण्यासाठी फोनपे/गुगल पे/पेटीएम खाते किंवा बँक खाते क्रमांक देतो.

जर कोणी आपल्या मित्राची खात्री करून न घेता पैसे पाठवले, तर तो/ती फसवणुकीचा बळी ठरतो/ठरते.

तुमच्या सोशल मीडियासाठी महत्त्वाचे सुरक्षा उपाय

- तुमची गोपनीयता सेटिंग्ज "फक्त माझे मित्र" (My Friends Only) अशी ठेवा.
- फेसबुक, व्हॉट्सॲप किंवा इतर सोशल मीडिया खात्याद्वारे पैशांची मागणी झाल्यास, पैसे हस्तांतरित करण्यापूर्वी संबंधित व्यक्तीला प्रत्यक्ष भेटून किंवा फोन करून मेसेजची सत्यता पडताळून पाहा.
- तुमच्या सर्व सोशल मीडिया खात्यांसाठी दोन-घटक प्रमाणीकरण (2-Step Verification) चालू करा.
- तुमचा पासवर्ड मजबूत ठेवा आणि त्याची गोपनीयता राखा.

Bhandara Cyber Police

बँक/आरबीआय अधिकारी असल्याचे भासवून फसवणूक

आजकाल सायबर गुन्हेगार बँक किंवा आरबीआयचे (RBI) अधिकारी असल्याचे भासवून लोकांना फोन करतात. ते सांगतात की, त्यांचे एटीएम कार्ड ब्लॉक झाले आहे, किंवा त्यांचे केवायसी (KYC) अपडेटेड नाही, अथवा त्यांचे आधार कार्ड त्यांच्या बँक खात्याशी जोडलेले नाही, ज्यामुळे त्यांचे खाते ब्लॉक केले जाईल.

त्यानंतर, केवायसी अपडेट करण्याच्या, बँक खाते आधारशी जोडण्याच्या किंवा एटीएम कार्डच्या सेवा पुन्हा सुरू करण्याच्या/नवीन एटीएम कार्ड सक्रिय करण्याच्या बहाण्याने, ते पीडितांकडून त्यांच्या बँक खात्याशी संबंधित माहिती विचारतात. यामध्ये एटीएम कार्ड नंबर, सीव्हीव्ही (CVV) नंबर, ओटीपी (OTP) इत्यादी तपशीलांचा समावेश असतो. एकदा ही माहिती पीडिताने शेअर केली की, त्याच्या बँक खात्यातून पैसे काढून घेतले जातात.

फसवणूक करणारे बँक/आरबीआय अधिकारी असल्याचे भासवून फोन करतात.

केवायसी/आधार अपडेट करण्याच्या किंवा नवीन एटीएम कार्ड सक्रिय करण्याच्या बहाण्याने, फसवणूक करणारे एटीएम कार्ड नंबर आणि ओटीपी (OTP) मागतात.

पीडित एटीएम कार्ड नंबर आणि (CVV) शेअर करतो/करते.

पीडित त्याच्या मोबाईल वर आलेला ओटीपी (OTP) शेअर करतो.

फसवणूक करणारे तात्काळ पैसे ई-वॉलेट (e-wallet) किंवा युपीआय (UPI) खात्यांमध्ये किंवा त्यांचे बँक खाते मध्ये हस्तांतरित करतात किंवा त्वरित खरेदी करतात.

महत्त्वाची सूचना: तुमची बँक कधीही तुमच्या कार्ड नंबर/CVV नंबर/OTP साठी विचारणार नाही.

या गोष्टी नेहमी लक्षात ठेवा:

- तुमची बँक तुम्हाला तुमचा एटीएम कार्ड नंबर, CVV, OTP किंवा इतर कोणतीही गोपनीय बँक माहिती फोन कॉल, SMS किंवा WhatsApp वर कधीही विचारणार नाही.
- कोणत्याही परिस्थितीत ही माहिती कोणासोबतही शेअर करू नका.
- तुमचा ई-मेल पत्ता देखील अनोळखी व्यक्तीसोबत शेअर करणे टाळा. कारण, सायबर गुन्हेगार या माहितीचा वापर करून तुमचे इंटरनेट बँकिंग सक्रिय करू शकतात आणि तुमच्या खात्यातून पैसे काढून घेऊ शकतात.

Bhandara Cyber Police

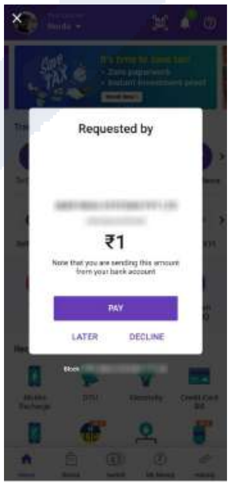
सायबर फसवणुकीचा नवा प्रकार: 'पैसे मिळवा म्हणत पैसे काढून घेणे!!

सायबर भामटे (Cyber Fraudsters) आता लोकांना फसवण्यासाठी नवनवीन युक्त्या वापरत आहेत. ते तुम्हाला गुगल पे (Google Pay), फोनपे (PhonePe) किंवा पेटीएम (Paytm) द्वारे तुमच्या बँक खात्यात पैसे मिळवण्यासाठी डेबिट लिंक्स (debit links) किंवा क्यूआर कोड (QR codes) पाठवतात.

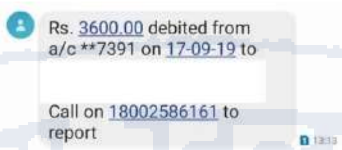
तुम्हाला वाटते की तुम्ही हा कोड स्कॅन केल्यावर किंवा लिंकवर क्लिक केल्यावर तुम्हाला पैसे मिळतील. परंतु, प्रत्यक्षात असे होत नाही! फसवणूक करणारे तुम्हाला 'पैसे मिळवा' असे सांगून पैसे पाठवण्याची विनंती (request money) करणारा क्यूआर कोड किंवा लिंक पाठवतात. त्यामुळे, तुम्ही जेव्हा तो स्कॅन करता किंवा लिंकवर क्लिक करता, तेव्हा तुमच्या खात्यात पैसे जमा होण्याऐवजी, तुमच्या बँक खात्यातून पैसे काढून घेतले जातात (gets debited).

फसवणूक करणारे विक्रेते किंवा कोणत्याही व्यावसायिकाला किंवा इतर व्यक्तीला फोन करतात आणि असे भासवतात की त्यांना पैसे पाठवायचे आहेत आणि त्यासाठी तुमचा Google Pay किंवा PhonePe वर नोंदणीकृत असलेला मोबाईल नंबर मागतात.

ते व्यक्ती नोंदणीकृत मोबाईल नंबर शेअर करतो आणि त्याला 'पै' अशी विनंती करणारी लिंक किंवा क्यूआर कोड मिळतोकिंवा तुमचा पेमेंट अ‍ॅप मध्ये नोटिफिकेशन येते .



त्या व्यक्तीला (पीडिताला) असे भासवले जाते की, ही पेमेंट प्रक्रिया त्याच्या खात्यात पैसे जमा करण्यासाठी (for credit) आहे, पण प्रत्यक्षात मात्र ती त्याच्या खात्यातून पैसे काढण्यासाठी (for debit) असते.



पीडित त्याच्या बँक खात्याशी जोडलेल्या नोंदणीकृत फोन नंबरवर आलेला मजकूर संदेश (टेक्स्ट मेसेज) दुर्लक्षित करतो/करते.

पीडिताला पैसे मिळण्याऐवजी, तो 'पैसे पाठवण्याची विनंती' करणाऱ्या क्यूआर कोड किंवा लिंकद्वारे फसवणूकदारालाच पैसे देऊन बसतो.

सूचना:

- अविश्वसनीय स्त्रोतांकडून आलेली कोणतीही लिंक स्वीकारू नका किंवा त्यावर क्लिक करू नका, तसेच कोणताही क्यूआर कोड स्कॅन करू नका. कारण, ते तुम्हाला चुकीची लिंक/कोड पाठवू शकतात.
- पैसे मिळवण्यासाठी तुम्हाला कधीही MPIN किंवा UPI PIN टाकण्याची गरज नसते. जर तुम्हाला कोणी पैसे पाठवत असेल आणि पिन मागितला, तर समजून जा की ही फसवणूक आहे.

Bhandara Cyber Police

स्क्रीन शेअरिंग ॲप्स वापरून फसवणूक

सायबर फसवणूकदार मदतीचे किंवा एखाद्या कंपनीच्या धोरणाचे कारण देत, पीडितेला क्विक सपोर्ट (Quick Support), टीमव्ह्यूअर (TeamViewer), एनीडेस्क (AnyDesk) इत्यादी स्क्रीन शेअरिंग ॲप्स (Apps) इन्स्टॉल करण्यास सांगतात. अशा प्रकारे ते पीडितेच्या फोनवर नियंत्रण मिळवतात आणि ओटीपी (OTP), एमपीआयएन (MPIN), इंटरनेट बँकिंगचे (Internet Banking) युझरनेम (Username)/पासवर्ड (Password) यांसारख्या बँकिंग क्रेडेन्शियल्सचा (Credentials) ॲक्सेस मिळवतात. त्यानंतर फसवणूकदार त्या क्रेडेन्शियल्सचा वापर करून पीडितेच्या खात्यातून पैसे काढून घेतात. पीडितेला याची जाणीव होईपर्यंत, बरेच पैसे आधीच काढून घेतलेले असतात.

लोक बँक किंवा ई-कॉमर्स प्लॅटफॉर्मचे बनावट कस्टमर केअर नंबर गूगल सर्च इंजिनवर शोधून संपर्क साधतात.

TeamViewer

AnyDesk

फसवणूक करणारा, स्वतःला कस्टमर केअर ऑपरेटर भासवून, पीडितेला वरीलपैकी कोणतेही स्क्रीन शेअरिंग ॲप इन्स्टॉल करण्यास सांगतो आणि त्याला मदत करण्याच्या बहाण्याने पीडितेच्या स्क्रीनचा ॲक्सेस मिळवण्यासाठी कोड शेअर करण्यास सांगतो.

पीडित फसवणूक करणाऱ्यासोबत कोड शेअर करतो.

फसवणूक करणारा पीडितेच्या फोनमध्ये प्रवेश मिळवतो आणि बँकिंग क्रेडेन्शियल्स चोरतो.

फसवणूक करणारा पीडितेने ओटीपी (OTP) शेअर न करताही त्याच्या खात्यात पैसे हस्तांतरित करतो.

सूचना:

- कोणत्याही संस्थेच्या कस्टमर केअर/हेल्प डेस्क प्रतिनिधीने फोन कॉलवर स्क्रीन शेअरिंग ॲप (App) इन्स्टॉल करण्यास सांगितल्यास ते कधीही करू नका.
- बँका/ई-कॉमर्स संस्था (Entities) इत्यादी स्क्रीन शेअरिंगसाठी कधीही तृतीय-पक्ष ॲप्लिकेशन (Third-party application) इन्स्टॉल करण्यास सांगत नाहीत.

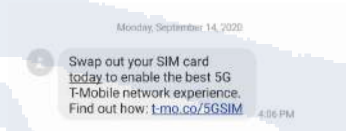
Bhandara Cyber Police

सिम कार्डद्वारे होणारी फसवणूक: कशी ओळखावी आणि टाळावी?

हा एक प्रकारचा Identity Theft चा प्रकार आहे जिथे सायबर गुन्हेगार टेलिकॉम सेवा प्रदात्याकडून (Telecom Service Provider) तुमच्या नोंदणीकृत मोबाईल नंबरसाठी नवीन सिम कार्ड (SIM card) मिळवण्यात यशस्वी होतात. नवीन सिम कार्डच्या मदतीने, फसवणूक करणारे तुमच्या बँक खात्यातून आर्थिक व्यवहारासाठी (financial transaction) आवश्यक असलेला ओटीपी (OTP) आणि इतर गोपनीय तपशील (confidential details) मिळवतात.

सायबर गुन्हेगार कोणत्याही किरकोळ विक्रेत्याकडून (retailer) कोरे सिम कार्ड (blank SIM card) मिळवतात.

सायबर गुन्हेगार टेलिकॉम सेवा प्रदात्याचे (TSP) कस्टमर केअर एक्झिक्युटिव्ह असल्याचा बहाणा करून पीडितेला फोन करतात. ते त्यांना स्वतःच 4G सिम अपग्रेडेशन सुरू करण्यास सांगतात, अन्यथा त्यांच्या सिमच्या सेवा खंडित होतील अशी धमकी देतात.



त्यांच्या फसवणुकीला पुढे नेण्यासाठी, सायबर गुन्हेगार एक सिम नंबर (SIM no.) देतात आणि पीडितेला तो सिम नंबर एसएमएसद्वारे (SMS) कस्टमर केअर नंबरवर पाठवून सेवा सुरू करण्यास सांगतात.

पीडित, फसवणूक करणाऱ्याला टेलिकॉम सेवा प्रदात्याचा (TSP) खरा कस्टमर केअर ऑपरेटर समजून, त्याच्या मोबाईल फोनमधून तो सिम नंबर (SIM no.) फॉरवर्ड करतो.

आता, सायबर गुन्हेगाराला पीडितेच्या मोबाईल नंबरशी जोडलेल्या बँक खात्याच्या सर्व तपशीलांमध्ये प्रवेश मिळवता येतो आणि तो पैसे काढून घेतो.

सूचना:

- फोन कॉलवर कोणत्याही बँक खात्याशी संबंधित किंवा सिमची माहिती कधीही शेअर करू नका.
- सिमच्या मागील बाजूस असलेला २०-अंकी सिम नंबर (SIM number) ही अत्यंत संवेदनशील माहिती आहे.
- जर तुमचा मोबाईल नंबर काही तासांसाठी इनॲक्टिव्ह (inactive) किंवा नेटवर्क क्षेत्राबाहेर (out of range) असेल, तर तात्काळ तुमच्या मोबाईल ऑपरेटरकडे चौकशी करा.
- तुमच्या बँकिंग व्यवहारांसाठी नियमित एसएमएस (SMS) तसेच ईमेल अलर्टसाठी (email alerts) नोंदणी करा. (यामुळे, जरी तुमचे सिम डी-ॲक्टिव्हेट (de-activated) झाले तरी, तुम्हाला ईमेलद्वारे अलर्ट मिळत राहतील).

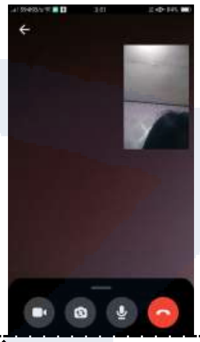
Bhandara Cyber Police

ऑनलाइन लैंगिक खंडणी(Sextortion)

सोशल मीडियावर (उदा. फेसबुक, इन्स्टाग्राम, स्नॅपचॅट इत्यादी) होणारे सेक्स्टॉर्शन (Sextortion) हा एक गंभीर ऑनलाइन गुन्हा आहे. यात सायबर गुन्हेगार महिला असल्याचे भासवून पीडितांशी लाइव्ह व्हिडिओ चॅट करतात. या फसवणुकीत, सायबर गुन्हेगार पीडिताला अश्लील स्थितीत व्हिडिओ कॉल करण्यासाठी पटवून घेतात. त्यानंतर, ते त्या व्हिडिओ कॉलचे स्क्रीनशॉट घेतात किंवा स्क्रीन रेकॉर्डिंग करतात. पुढे, मागणी केलेले पैसे न दिल्यास, हे सायबर गुन्हेगार पीडितेला धमकावतात की, अश्लील स्थितीतील फोटो किंवा व्हिडिओ विविध ऑनलाइन प्लॅटफॉर्मवर व्हायरल करतील.

सायबर गुन्हेगार कोणत्याही किरकोळ विक्रेत्याकडून (retailer) कोरे सिम कार्ड (blank SIM card) मिळवतात.

अनेकदा सायबर गुन्हेगार पीडितांना विविध प्रकारचे व्हिडिओ चॅट ॲप्लिकेशन्स डाउनलोड करण्याचा सल्ला देतात.



अनेक चॅटनंतर, सायबर गुन्हेगार पीडितेला व्हिडिओ कॉलिंगसाठी येण्यास पटवून घेतो.सायबर गुन्हेगार पीडितेला नग्न होण्यासाठी फसवतो आणि त्यानंतर चालू असलेल्या व्हिडिओ कॉलचे स्क्रीनशॉट किंवा स्क्रीन रेकॉर्डिंग सेव्ह (save) करतो, ज्यात पीडित नग्न असतो.

सायबर गुन्हेगार पीडितेला ब्लॅकमेल करण्यास सुरुवात करतो आणि पैसे उकळतो, अन्यथा नग्न फोटो वेबसाईट(Websites), यूट्यूब (YouTube) इत्यादींवर अपलोड करण्याची धमकी (threatens) देतो.

व्यक्ती भीतीने पैसे पाठवते आणि ब्लॅकमेलिंग (blackmailing) व खंडणीचा (extortion) बळी ठरते.

<u>सूचना:</u>

- फेसबुकवर किंवा इतर कोणत्याही सोशल मीडिया प्लॅटफॉर्मवर अनोळखी लोकांशी कधीही व्हिडिओ कॉल करू नका
- सोशल मीडिया प्लॅटफॉर्मवर अनोळखी लोकांशी मैत्री करणे टाळा.

बनावट सोशल मीडिया प्रोफाईलद्वारे होणारा फसवणूक

सायबर गुन्हेगार सोशल मीडियावरून पीडितेचे फोटो मिळवतात, ते मॉर्फ (बदलून) करतात आणि सोशल मीडिया प्लॅटफॉर्मवर अपलोड करतात. त्यानंतर, ते मॉर्फ केलेले फोटो सोशल मीडियावरून काढण्यासाठी पैशांची मागणी करतात. पीडित या जाळ्यात अडकतो आणि पैसे ट्रान्सफर करतो.

पीडित व्यक्ती, फ्रेंड रिक्वेस्ट पाठवणारे कोण आहेत हे न तपासताच, साधारणपणे सर्व फ्रेंड रिक्वेस्ट स्वीकारतो. पीडिताच्या खात्याच्या कमकुवत गोपनीयता सेटिंग्जमुळे (poor privacy settings), सोशल मीडिया प्लॅटफॉर्मवरील त्याचे/तिचे फोटो (photographs) किंवा पोस्ट (posts) सर्वांना दिसतात, ज्याचा फायदा सायबर गुन्हेगार घेतात.

सायबर गुन्हेगार पीडिताचे फोटो डाउनलोड करतात आणि पीडिताची बनावट ओळख (impersonating the victim) वापरून बनावट खाते (fake account) तयार करतात. त्यानंतर, ते मॉर्फ केलेले अश्लील फोटो (morphed obscene photographs) इत्यादी अपलोड करून पीडिताला छळतात (harassing the victim).

सूचना:

- सोशल मीडिया साइट्सवर तुमच्या पोस्ट्स, फोटो कोण पाहू शकेल किंवा तुम्हाला कोण फ्रेंड रिक्वेस्ट पाठवू शकेल, हे नियंत्रित करण्यासाठी गोपनीयता सेटिंग्ज वापरा. तुमच्या प्रोफाइलवरील प्रवेश मर्यादित ठेवा.
- तुमची वैयक्तिक माहिती, फोटो आणि व्हिडिओ केवळ तुमच्या विश्वासू मित्रांना (trusted ones) दिसतील याची खात्री करा. अनोळखी व्यक्तींसोबत सोशल मीडियावर मैत्री करणे टाळा.
- ऑनलाइन काहीही पोस्ट किंवा शेअर करण्यापूर्वी दोनदा विचार करा. कारण ती माहिती कायमस्वरूपी ऑनलाइन राहू शकते आणि भविष्यात तुम्हाला त्रास देण्यासाठी वापरली जाऊ शकते.
- तुमच्या मुलांना सायबरबुलिंग (Cyberbullying) हा शिक्षेस पात्र गुन्हा आहे याची जाणीव करून द्या, जेणेकरून ते स्वतः सायबरबुलिंगमध्ये सहभागी होणार नाहीत आणि कोणालाही त्यांना त्रास देऊ देणार नाहीत.
- तुम्हाला त्रासदायक वाटणाऱ्या कमेंट्स, मेसेज आणि फोटोंची तक्रार करा आणि संबंधित सोशल मीडिया प्लॅटफॉर्मला ती काढण्याची विनंती करा. 'अनफ्रेंड (unfriending)' करण्याव्यतिरिक्त, तुम्ही अशा लोकांना पूर्णपणे ब्लॉक करू शकता, जेणेकरून ते तुमचे प्रोफाइल पाहू शकणार नाहीत किंवा तुमच्याशी संपर्क साधू शकणार नाहीत.

लॉटरी/बक्षीस लागल्याची फसवणूक

सायबर फसवणूकदार ईमेल/एसएमएस (e-mails/SMSs) पाठवून प्राप्तकर्त्याला (पीडित व्यक्तीला) कळवतात की त्याला/तिला लाखो रुपये (lottery) किंवा बक्षीस (prize) लागले आहे. प्राप्तकर्त्याला फक्त त्यांच्या ईमेल/मोबाईल फोनवर पाठवलेल्या लिंकवर क्लिक (click) करण्यास सांगितले जाते किंवा त्यांना बक्षीसाची रक्कम कशी हवी आहे हे विचारले जाते. मात्र, जेव्हा प्राप्तकर्ता सकारात्मक प्रतिसाद देतो, तेव्हा बक्षीसाची रक्कम मिळवण्यासाठी त्याला नोंदणी शुल्क (registration), शिपमेंट (shipment), सेवा शुल्क (service charges), जीएसटी (GST) इत्यादींच्या नावाखाली एकामागून एक पैसे भरण्यास सांगितले जाते. अशा प्रकारे, प्राप्तकर्त्याला फसवणूक लक्षात येईपर्यंत तो फसवणूकदारांना पैसे देत राहतो.

फसवणूक करणारे ईमेल/एसएमएस/कॉलद्वारे (email/SMS/call) पीडित व्यक्तीला लॉटरी लागल्यामुळे मिळालेल्या बक्षीस रकमेची (prize money) माहिती देतात.

जर पीडित व्यक्तीने सकारात्मक प्रतिसाद दिला, तर फसवणूक करणारे त्याला/तिला बक्षीसाची रक्कम कशी मिळवायची आहे असे विचारतात. बक्षीस मिळवण्याची पद्धत सांगितल्यावर, ते बक्षीसाची रक्कम देण्यासाठी नोंदणी/शिपमेंट/सेवा शुल्क, जीएसटी (GST) इत्यादींची मागणी करतात.

ती व्यक्ती या जाळ्यात अडकते आणि फसवेगिरी करणाऱ्याला पैसे थोडे थोडे करून पाठवत राहते, जोपर्यंत तिला/त्याला फसवणूक झाल्याचे कळत नाही.

सूचना:

- तुम्हाला लॉटरी किंवा बक्षीस लागल्याचे सांगणारे किंवा तुमची वैयक्तिक किंवा आर्थिक माहिती मागवणारे कॉल्स, एसएमएस किंवा ईमेल यांना कधीही प्रतिसाद देऊ नका.
- तुमच्या ईमेल अकाउंटमध्ये योग्य स्पॅम फिल्टर (spam filters) असल्याची खात्री करा, जेणेकरून तुम्हाला अनावश्यक ईमेल मिळणार नाहीत.
- एक सोपा नियम नेहमी लक्षात ठेवा: जास्त परताव्याच्या, बक्षीस जिंकण्याच्या किंवा लॉटरी लागण्याच्या आमिषाने अनोळखी व्यक्तींना किंवा संस्थांना कधीही पैसे ट्रान्सफर (transfer funds) करू नका.

Bhandara Cyber Police

"ज्यूस जॅकिंग" (Juice Jacking)

ज्यूस जॅकिंग हा एक सायबर हल्ला आहे जिथे सार्वजनिक USB चार्जिंग पोर्ट (उदा. विमानतळ, रेल्वे स्टेशन, बस स्टॉप, हॉटेल्स किंवा इतर सार्वजनिक ठिकाणी उपलब्ध असलेले) हॅकर्सकडून बदलले जातात किंवा त्यात मालवेअर (हानिकारक सॉफ्टवेअर) इन्स्टॉल केले जाते. जेव्हा तुम्ही तुमचा फोन किंवा इतर डिव्हाइस अशा पोर्टला चार्ज करण्यासाठी कनेक्ट करता, तेव्हा हॅकर्स तुमच्या डिव्हाइसमधील डेटा (उदा. पासवर्ड, बँक खात्याची माहिती, फोटो, संपर्क) चोरू शकतात किंवा तुमच्या डिव्हाइसवर मालवेअर इन्स्टॉल करू शकतात. यामुळे तुमची आर्थिक फसवणूक किंवा वैयक्तिक माहितीची चोरी होऊ शकते.

हॅकर्स डेटा केबल वापरून USB पोर्टद्वारे डेटा चोरण्यासाठी त्याच चार्जिंग पॉइंटचा वापर करतात. जसे की सार्वजनिक USB चार्जिंग पोर्टचा वापर करून स्मार्टफोन किंवा इतर उपकरणांमधून डेटा चोरला जातो.

मिळाल्यावर सायबर गुन्हेगार तुमची ओळख चोरून आर्थिक फसवणूक करू शकतात. ते तुमचे ऑनलाइन खाते हॅक करतात, किंवा मालवेअरद्वारे तुमच्या डिव्हाइसवर नियंत्रण मिळवून रॅन्समवेअर, हेरगिरी करू शकतात. हा डेटा फिशिंग हल्ल्यांसाठी वापरण्यात येऊ शकते. थोडक्यात, त्यांचा उद्देश तुमच्या माहितीचा गैरवापर करून पैसे कमावणे किंवा हॅक केलेला फोन वाईट कृत्यांसाठी वापरणे हा असतो.

सूचना:

- रेल्वे स्टेशन, विमानतळ, बस स्टँड, मॉल किंवा हॉटेलसारख्या सार्वजनिक ठिकाणी उपलब्ध असलेले USB चार्जिंग पोर्ट वापरणे पूर्णपणे टाळा. हे पोर्ट हॅकर्सनी छेडछाड केलेले असू शकतात.
- नेहमी तुमचा स्वतःचा वॉल चार्जर थेट AC आउटलेटमध्ये लावून फोन चार्ज करा, किंवा पूर्ण चार्ज केलेली पॉवर बँक सोबत ठेवा.
- अनोळखी USB पोर्टला कनेक्ट करताना, तुमच्या डिव्हाइसवर विचारल्यास नेहमी "फक्त चार्ज करा" (Charge Only) हा पर्याय निवडा.
- तुमच्या फोनचे ऑपरेटिंग सिस्टम आणि ॲप्स नवीनतम सुरक्षा पॅचसाठी नियमितपणे अपडेट करत रहा.
- जर तुम्हाला सार्वजनिक ठिकाणी फोन चार्ज करायचाच असेल, तर फक्त भिंतीवरील सॉकेटमध्ये तुमचा स्वतःचा चार्जर लावून फोन चार्ज करा. USB पोर्टऐवजी थेट AC आउटलेट वापरा, कारण AC आउटलेटमधून फक्त वीज येते, डेटा ट्रान्सफर होत नाही.

फेक जॉब ऑफर्स: पैसे मागितल्यास सावधान, ही सायबर फसवणूक!

साइबर गुन्हेगार ऑनलाइन फेक वेबसाइट्सद्वारे विविध प्लॅटफॉर्मवरील फेक नोकरीच्या अटी जाहिरात करतात. नोकरीच्या शोधात असलेल्या व्यक्ती या फेक नोकरीच्या अटींवरुन जातात आणि साइबर गुन्हेगारांशी संपर्क साधतात. साइबर गुन्हेगारांना संपर्क केल्यावर, त्या व्यक्तीला नोकरी मिळविण्यासाठी त्यांच्या सेवा मिळविण्याकरिता नोंदणी फी किंवा अग्रिम भरणा (जो ते परतफेडीच्या दावे करतात) देण्यास सांगितले जाते. व्यक्ती पैसे हस्तांतरित करते आणि नोकरी मिळविण्यासाठी ठगाच्या मार्गदर्शक तत्त्वांचे अनुसरण करते आणि साइबर गुन्ह्यात बळी पडते. काही प्रकरणांमध्ये, एक फेक वेबसाइट आर्थिक माहिती एका फेक पेमेंट चॅनलद्वारे उकळते.

फसवणूक करणारे हुबेहूब दिसणाऱ्या खोट्या वेबसाइट्स, आकर्षक जाहिराती आणि भरमसाठ पगाराची प्रलोभने देऊन लोकांना जाळ्यात ओढतात.

ते स्वतःला एचआर मॅनेजर भासवतात, खोट्या मुलाखती घेतात, जेणेकरून पीडिताला खरी नोकरी मिळाल्याचा पूर्ण विश्वास वाटेल.

पीडित निवडला गेल्याचे सांगून, नोंदणी, प्रशिक्षण किंवा पडताळणीच्या नावाखाली विविध आगाऊ शुल्काची मागणी केली जाते, जे परत मिळेल असे खोटे सांगतात.

शुल्क घेण्यासोबतच, खोट्या पेमेंट गेटवेद्वारे बँक तपशील चोरतात. आधार/पॅनसारखी वैयक्तिक माहिती घेऊन ओळख चोरी आणि मालवेअर इन्स्टॉल करतात.

पैसे आणि गोपनीय माहिती मिळाल्यावर, गुन्हेगार संपर्क तोडून गायब होतात. पीडित नोकरीविना, पैसे गमावून, आणि चोरी झालेल्या डेटासह एकटा राहतो.

सूचना:

- नोकरीसाठी कोणतीही कंपनी किंवा रिक्रूटर कधीही पैसे मागत नाही. पैशाची मागणी झाल्यास, तो घोटाळा आहे.
- ऑफर देणाऱ्या कंपनीची अधिकृत वेबसाइट तपासा आणि लिंक्डइनसारख्या ठिकाणी तिचे अस्तित्व पडताळा.
- भरपूर पगार किंवा कमी कामाची हमी देणाऱ्या ऑफर्सबद्दल संशय बाळगा; त्या फसव्या असू शकतात.
- नोकरी मिळण्यापूर्वी बँक खाते, आधार, पॅन यांसारखी संवेदनशील माहिती कोणासोबतही शेअर करू नका.
- आलेल्या ऑफरमधील नंबरऐवजी, कंपनीच्या अधिकृत वेबसाइटवरील नंबरवर संपर्क साधून ऑफरची सत्यता पडताळा.
- मुलाखती किंवा चाचण्यांसाठी सांगितले जाणारे अनोळखी ॲप्स डाउनलोड करू नका, ते मालवेअर असू शकतात.

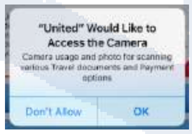
Bhandara Cyber Police

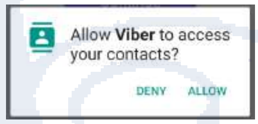
मोबाईल ॲप्सचे धोके: असुरक्षित डाउनलोडमुळे तुमचा फोन धोक्यात!

मोबाईल ॲप्स सायबर हल्ल्यांचे, गोपनीय डेटा चोरीचे, किंवा तुमच्या फोनवर नियंत्रण मिळवण्याचे माध्यम बनू शकतात. अनेकदा लोक सुरक्षा इशाऱ्यांकडे दुर्लक्ष करून अनोळखी स्रोतांकडून ॲप्स डाउनलोड करतात.या ॲप्समध्ये व्हायरस असू शकतात, जे तुमची संवेदनशील माहिती बाहेर पाठवतात किंवा तुमच्या फोनचा ताबा सायबर गुन्हेगारांना देतात. यामुळे तुमचे संपर्क, पासवर्ड, आर्थिक माहिती त्यांच्या हाती लागते.अनोळखी ॲप्स अनेकदा अनावश्यक परवानग्या मागतात, ज्या वापरकर्ते तपासणी न करता देतात. यामुळे ही ॲप्स तुमच्या वैयक्तिक माहिती, फोटो यांसारख्या मोठ्या प्रमाणात डेटा ॲक्सेस करू शकतात, किंवा आर्थिक फसवणूक करू शकतात ज्यामुळे तुम्ही धोक्यात येता.

फसवणूकदार लोकप्रिय ॲप्सची हुबेहूब नक्कल करतात आणि त्यात दूषित कोड घालतात (उदा. स्पायवेअर, रॅन्समवेअर) डेटा चोरण्यासाठी किंवा डिव्हाइस नियंत्रित करण्यासाठी. यासाठी अनेकदा एआय टूल्सचा वापर केला जातो.

ते अनधिकृत स्टोअर्स, बनावट वेबसाइट्स किंवा सोशल मीडिया द्वारे ॲप्स पसरवतात (उदा. फिशिंग लिंक्स, बनावट जाहिराती) ज्यामुळे वापरकर्ते फसून दुर्भावनापूर्ण सॉफ्टवेअर डाउनलोड करतात.





एकदा इन्स्टॉल झाल्यावर, बनावट ॲप जास्त परवानग्या मागते ज्यामुळे संवेदनशील डेटा गोळा होतो, ओटीपी रोखले जातात किंवा अनधिकृत आर्थिक व्यवहार करून वापरकर्त्यांचे शोषण होते.

तुम्ही परवानग्या दिल्या नंतर फसवणूकदार तुमचे मोबाइलला चे ॲक्सेस घेतो किंवा sms/call forwarding सेवा सुरू करतो व त्याचा गैरवापर करतो किंवा आर्थिक फसवणूक करतो

सूचना:

- फक्त Google Play (Android) किंवा App Store (Apple) मधूनच ॲप्स मिळवा. Play Protect shield असल्याची खात्री करा.
- ॲपचे रिव्ह्यू आणि विकसकाची माहिती काळजीपूर्वक वाचा, सुरक्षा समस्या किंवा संशयास्पद तपशील शोधा.
- महत्वाचे सुरक्षा पॅचेस मिळवण्यासाठी तुमचे सॉफ्टवेअर आणि सर्व ॲप्स नियमितपणे अपडेट करा.
- ॲप्सना फक्त आवश्यक परवानग्या द्या; अनावश्यक परवानग्या मालवेअरसाठी धोका वाढवतात.
- फसव्या ॲप्स डाउनलोड करण्यासाठी वापरल्या जाणाऱ्या संशयास्पद लिंक्स किंवा ऑफर्सपासून दूर रहा.

Bhandara Cyber Police

मुलांसाठी सायबर सुरक्षेच्या टिप्स

काय करावे

- ऑनलाइन वैयक्तिक माहिती शेअर करू नका उदा. नाव, पत्ता, शाळेचं नाव, मोबाईल नंबर, पासवर्ड इ.
- इंटरनेटवर अनोळखी व्यक्तींशी बोलू नका, कधीही अज्ञात व्यक्तीकडून आलेले मेसेज किंवा कॉल्स स्वीकारू नका.
- सोशल मीडियावर गोपनीयता जपा
- खाते "Private" ठेवा, फक्त ओळखीच्या लोकांनाच add करा.
- अनोळखी लिंक किंवा जाहिरातींवर क्लिक करू नका ते व्हायरस किंवा फसवणुकीचे दुवे असू शकतात.
- मजबूत पासवर्ड वापरा आणि कुणालाही सांगू नका पासवर्डमध्ये अंक, अक्षरं आणि चिन्हे असू द्या.
- काहीही डाउनलोड करताना पालकांची परवानगी घ्या फसवणूक करणारे गेम्स, ॲप्स किंवा व्हिडीओ डाउनलोड होऊ शकतात.
- सायबर धमकी किंवा त्रास दिल्यास लगेच सांगावे पालक, शिक्षक किंवा सायबर तक्रार विभागाकडे तक्रार करा.
- मर्यादित वेळ इंटरनेट वापरा आणि सुरक्षित गेम खेळा, ऑनलाइन गेमिंगमध्येही अनोळखी लोक टाळा.

काय करू नये

- सायबरबुलिंगमध्ये (ऑनलाइन त्रास देणे) सहभागी होऊ नका किंवा इतरांना दुखवणारे मेसेज पाठवू नका.
- ऑनलाइन बँकिंग किंवा वैयक्तिक माहिती शेअर करण्यासारख्या संवेदनशील कामांसाठी सार्वजनिक वाय-फाय वापरू नका, कारण ही नेटवर्क सहसा असुरक्षित असतात.
- आवश्यक असल्यासच आणि पालकांच्या परवानगीनेच ॲप्स किंवा डिव्हाइससाठी लोकेशन सेवा चालू करण्याची परवानगी द्या.
- पालकांनी सेट केलेले पॅरेंटल कंट्रोल्स किंवा निर्बंधांना बगल देऊ नका.
- आपल्या ऑनलाइन क्रियाकलाप पालकांपासून लपवण्याचा प्रयत्न करू नका. सुरक्षित राहण्यासाठी मोकळा संवाद खूप महत्त्वाचा आहे.
- अनोळखी व्यक्तींसोबत वेबकॅम चॅट्स किंवा व्हिडिओ कॉल्स सुरू करू नका.
- फक्त ऑनलाइन भेटलेल्या कोणालाही, मोठ्या व्यक्तीच्या माहिती आणि देखरेखीशिवाय प्रत्यक्षात भेटू नका.
- अनोळखी व्यक्तींच्या फ्रेंड रिक्वेस्ट किंवा फॉलो रिक्वेस्ट स्वीकारू नका.

पालकांसाठी सायबर सुरक्षा टिप्स

काय करावे

- तुमच्या मुलांशी त्यांच्या ऑनलाइन जीवनाबद्दल नेहमी मोकळेपणाने बोला, जेणेकरून ते कोणतीही भीती न बाळगता काहीही शेअर करण्यास सुरक्षित वाटतील.
- इंटरनेट वापरासाठी, स्क्रीन टाइमसाठी आणि स्वीकारार्ह ऑनलाइन वर्तनासाठी, तुमच्या मुलांच्या सहभागाने, स्पष्ट कौटुंबिक नियम स्थापित करा आणि त्यांचे नियमितपणे पुनरावलोकन करा.
- तुमच्या मुलांना गंभीर विचार, ऑनलाइन अनोळखी व्यक्तींचे धोके, सायबरबुलिंग कसे हाताळायचे आणि पोस्ट करण्यापूर्वी ऑनलाइन गोपनीयतेचे महत्त्व शिकवा.
- पॅरेंटल कंट्रोल्स वापरा, सर्व सॉफ्टवेअर अपडेटेड ठेवा, मजबूत आणि अद्वितीय पासवर्ड तयार करण्यास मदत करा, ॲप परवानग्या तपासा आणि तुमचा घरगुती वाय-फाय सुरक्षित करा.
- तुमच्या मुलांसमोर जबाबदार ऑनलाइन वर्तन आणि निरोगी स्क्रीन टाइम सवयींचे उदाहरण ठेवा, कारण ते तुम्हाला पाहून शिकतात.
- सायबर गुन्हे कसे नोंदवायचे यासाठी संसाधने जाणून घ्या आणि तुमच्या मुलाच्या ऑनलाइन ॲक्टिव्हिटीमुळे त्यांच्या वर्तनात लक्षणीय बदल झाल्यास व्यावसायिक मदत घ्या.

काय करू नये

- तुमच्या मुलांच्या ऑनलाइन क्रियाकलापांना कमी लेखू नका किंवा त्यांच्या सुरक्षिततेची जबाबदारी केवळ तंत्रज्ञानावर सोडू नका, कारण डिजिटल जग त्यांच्यासाठी महत्त्वाचे आहे.
- ऑनलाइन समस्यांवर त्वरित डिव्हाइस जप्त करून किंवा इंटरनेट बंदी घालून जास्त कठोर होऊ नका, कारण यामुळे मुले भविष्यात तुमच्यापासून गोष्टी लपवू शकतात.
- फक्त काय करू नये हे सांगू नका, तर नियमांमागील 'का' हे स्पष्ट करा आणि तंत्रज्ञानावर पूर्णपणे अवलंबून न राहता त्यांच्याशी सतत संवाद साधा.
- सर्व खात्यांसाठी मजबूत पासवर्ड सेट करा, सॉफ्टवेअर अपडेट्सकडे लक्ष द्या, तुमच्या परवानगीशिवाय ॲप्स डाउनलोड करू देऊ नका आणि प्रायव्हसी सेटिंग्ज नेहमी 'प्रायव्हेट' ठेवा.
- तुमच्या मुलांची डिजिटल गोपनीयता जपून आणि तुम्ही स्वतः जबाबदार ऑनलाइन वर्तन करून त्यांच्यासाठी एक चांगला आदर्श बना.
- गुंतागुंतीच्या सायबर सुरक्षा समस्या एकट्याने हाताळण्याचा प्रयत्न करू नका; त्याऐवजी शाळा अधिकारी, कायदेशीर यंत्रणा किंवा विशेष संस्थांकडून मदत घ्या.

महिलांसाठी सायबर सुरक्षा टिप्स

काय करावे

- मजबूत आणि वेगळे पासवर्ड वापरा, पासवर्ड कमीतकमी 8–12 अक्षरांचा असावा आणि त्यात मोठी अक्षरे, लहान अक्षरे, संख्या व विशेष चिन्हे असावीत; प्रत्येक खात्यासाठी वेगळा पासवर्ड ठेवा.
- सोशल मिडियाचे गोपनीयता सेटिंग्ज योग्यरित्या ठेवा, तुमचा प्रोफाइल “Private” ठेवा आणि तुमचे पोस्ट, फोटो, लोकेशन, आणि फ्रेंड लिस्ट फक्त विश्वासू लोकांनाच दिसतील अशा सेटिंग्ज करा.
- खाजगी माहिती आणि फोटो शेअर करताना काळजी घ्या, आधार क्रमांक, बँक माहिती, घराचा पत्ता, प्रवासाची योजना अशा गोष्टी शेअर करू नका, कारण त्या तुमच्यावर हेरगिरी किंवा फसवणुकीस कारण ठरू शकतात.
- ऑनलाईन ओळखी करताना वैयक्तिक माहिती शेअर करू नका, नव्या व्यक्तीवर लगेच विश्वास ठेवू नका; व्हिडीओ कॉल, वैयक्तिक फोटो किंवा इतर खाजगी माहिती शेअर करण्याआधी योग्य खात्री करा.
- संशयास्पद गोष्टी वाटल्यास त्वरित सावध व्हा, एखादा अज्ञात मेसेज, लिंक किंवा कॉल संशयास्पद वाटल्यास त्यावर क्लिक करू नका; सुरक्षिततेसाठी लगेच कनेक्शन बंद करा.

काय करू नये

- फेसबुक, इंस्टाग्रामवर लोकेशन शेअर करू नका, तुम्ही कुठे आहात हे लगेच शेअर करू नका; त्यामुळे कोणीही तुमचा मागोवा घेऊ शकतो किंवा गैरफायदा घेऊ शकतो.
- बिनधास्तपणे कोणत्याही ॲपला सर्व परवानग्या (permissions) देऊ नका, ॲप इंस्टॉल करताना 'कॅमेरा', 'मायक्रोफोन', 'लोकेशन' यासारख्या परवानग्या देताना नीट विचार करा; गरज नसलेल्या परवानग्या नकारा.
- ऑनलाईन ट्रोलिंग किंवा छेडछाड सहन करू नका – प्रतिक्रिया द्या, कोणी ऑनलाईन अपमान करत असेल, अश्लील कमेंट करत असेल तर गप्प बसू नका – स्क्रीनशॉट घ्या आणि त्याविरुद्ध तक्रार करा.
- कोणालाही खाजगी फोटो, OTP, बँक डिटेल्स पाठवू नका, अगदी ओळखीच्या व्यक्तींनाही OTP, क्रेडिट कार्ड नंबर, ATM पिन किंवा वैयक्तिक फोटो पाठवू नका, कारण त्यांचा गैरवापर होऊ शकतो.
- अनोळखी व्यक्तींशी खाजगी माहिती शेअर करू नका, सोशल मीडियावर किंवा मेसेजिंग ॲप्सवर ओळख नसलेल्या व्यक्तींशी तुमचे नाव, पत्ता, मोबाईल नंबर, नोकरीचे तपशील यांसारखी माहिती देणे टाळा.

सायबर फसवणुकीपासून दूर राहण्यासाठी आवश्यक सुरक्षा उपाय

१. तुमचे पासवर्ड आणि खाती सुरक्षित ठेवा

- मजबूत, अद्वितीय पासवर्ड वापरा: वेगवेगळ्या खात्यांसाठी कधीही एकच पासवर्ड पुन्हा वापरू नका. मोठे आणि लहान अक्षरे, संख्या आणि चिन्हे यांचा वापर करून जटिल पासवर्ड तयार करा. हे पासवर्ड सुरक्षितपणे साठवण्यासाठी आणि तयार करण्यासाठी प्रतिष्ठित पासवर्ड मॅनेजर वापरण्याचा विचार करा.
- टू-फॅक्टर ऑथेंटिकेशन (2FA) / मल्टी-फॅक्टर ऑथेंटिकेशन (MFA) सक्षम करा: तुमच्या सर्व ऑनलाइन खात्यांवर (ईमेल, बँकिंग, सोशल मीडिया, खरेदीच्या साइट्स) नेहमी 2FA किंवा MFA सक्रिय करा. यामुळे तुमच्या पासवर्ड व्यतिरिक्त तुमच्या फोनमधून कोडची आवश्यकता असल्याने सुरक्षेचा एक अतिरिक्त स्तर वाढतो.
- खात्याच्या हालचालींचे नियमितपणे पुनरावलोकन करा: तुमच्या बँक स्टेटमेंट, क्रेडिट कार्ड बिले आणि ऑनलाइन खात्याचे लॉग्स संशयास्पद किंवा अनधिकृत व्यवहारांसाठी वारंवार तपासा.

२. अनपेक्षित संपर्कांबद्दल संशय बाळगा

- पाठवणाऱ्याची पडताळणी करा: अनोळखी नंबरवरून आलेल्या ईमेल, टेक्स्ट मेसेज किंवा कॉल्सबद्दल किंवा कायदेशीर संस्थांकडून (बँका, सरकार, टेक सपोर्ट) असल्याचे दिसणाऱ्या अनपेक्षित मेसेज/ कॉल्सबद्दल अत्यंत सावधगिरी बाळगा.
- संशयास्पद लिंक्सवर क्लिक करू नका किंवा अटॅचमेंट्स डाउनलोड करू नका: फिशिंगचे प्रयत्न अनेकदा तातडीच्या विनंत्या किंवा आकर्षक ऑफर म्हणून येतात. क्लिक करण्यापूर्वी लिंक्सवर माऊस फिरवून वास्तविक URL पहा आणि सत्यापित न केलेल्या पाठवणाऱ्यांकडून आलेले अटॅचमेंट्स कधीही डाउनलोड करू नका.
- दबावाच्या डावपेचांपासून सावध रहा: फसवणूक करणारे अनेकदा तुम्हाला चुका करण्यास प्रवृत्त करण्यासाठी तातडीची भावना निर्माण करतात ("तुम्ही आता कृती न केल्यास तुमचे खाते निलंबित केले जाईल!"). एक क्षण थांबून पडताळणी करा.
- ओटीपी, पिन किंवा पूर्ण पासवर्ड कधीही शेअर करू नका: कायदेशीर संस्था कधीही फोन, ईमेल किंवा टेक्स्ट मेसेजद्वारे तुमचे वन-टाइम पासवर्ड (ओटीपी), पिन किंवा पूर्ण पासवर्ड मागणार नाहीत.

३. तुमची डिव्हाइसेस आणि नेटवर्क सुरक्षित ठेवा

- सॉफ्टवेअर अद्ययावत ठेवा: तुमची ऑपरेटिंग सिस्टम, वेब ब्राउझर, अँटीव्हायरस सॉफ्टवेअर आणि सर्व ॲप्स नेहमी त्यांच्या नवीनतम आवृत्त्यांवर अद्ययावत असल्याची खात्री करा. अपडेट्समध्ये अनेकदा महत्त्वाचे सुरक्षा उपाय असतात.
- प्रतिष्ठित अँटीव्हायरस/अँटी-मालवेअर सॉफ्टवेअर वापरा: तुमच्या संगणकावर आणि स्मार्टफोनवर चांगले सुरक्षा सॉफ्टवेअर स्थापित करा आणि नियमितपणे स्कॅन करा.
- सार्वजनिक वाय-फाय वापरताना सावधगिरी बाळगा: असुरक्षित सार्वजनिक वाय-फाय नेटवर्कवर संवेदनशील व्यवहार (जसे की ऑनलाइन बँकिंग किंवा खरेदी) करणे टाळा.

- जर तुम्हाला ते वापरणे आवश्यक असेल, तर एन्क्रिप्टेड कनेक्शनसाठी व्हर्च्युअल प्रायव्हेट नेटवर्क (VPN) वापरण्याचा विचार करा.
- तुमचे घरगुती वाय-फाय सुरक्षित करा: तुमच्या वाय-फाय राउटरचा डीफॉल्ट पासवर्ड बदलून एक मजबूत, अद्वितीय पासवर्ड सेट करा.

४. तुमची ऑनलाइन उपस्थिती आणि डेटा व्यवस्थापित करा

- वैयक्तिक माहिती शेअर करणे मर्यादित करा: तुम्ही सोशल मीडिया आणि इतर सार्वजनिक प्लॅटफॉर्मवर किती वैयक्तिक माहिती शेअर करता याबद्दल जागरूक रहा. फसवणूक करणारे या डेटाचा वापर लक्ष्यित फसवणुकीसाठी करू शकतात.
- गोपनीयता सेटिंग्जचे पुनरावलोकन करा: तुमच्या सोशल मीडिया खात्यांवरील आणि इतर ॲप्सवरील गोपनीयता सेटिंग्ज (privacy settings) नियमितपणे तपासा आणि समायोजित करा जेणेकरून तुमची माहिती कोण पाहू शकेल यावर तुमचे नियंत्रण राहील.
- ऑनलाइन खरेदी करताना सावध रहा: केवळ प्रतिष्ठित वेबसाइट्सवरच खरेदी करा (URL मध्ये "https://" आणि कुलूपाचे चिन्ह (padlock symbol) शोधा). खूप चांगल्या वाटणाऱ्या डील्सबद्दल सावध रहा.

५. स्वतःला शिक्षित करा आणि माहिती ठेवा

- सामान्य फसवणुकीचे प्रकार जाणून घ्या: फिशिंग (Phishing), स्मिशिंग (Smishing - SMS द्वारे फिशिंग), विशिंग (Vishing - व्हॉइस फिशिंग), रोमान्स स्कॅम्स, जॉब स्कॅम्स आणि लॉटरी स्कॅम्स यांसारख्या सामान्य फसवणुकीच्या प्रकारांबद्दल स्वतःला परिचित करून घ्या.
- अधिकृत स्रोतांचे अनुसरण करा: तुमच्या बँक, सरकारी सायबर सुरक्षा एजन्सी (जसे की भारतातील CERT-In), आणि प्रतिष्ठित सायबर सुरक्षा बातम्यांच्या स्रोतांकडून नवीन फसवणुकीच्या प्रवृत्तींबद्दल माहिती ठेवा.
- जर काहीतरी चुकीचे वाटले, तर ते बहुधा चुकीचेच असते: तुमच्या अंतःप्रेरणेवर (instincts) विश्वास ठेवा. जर ऑनलाइन काहीतरी किंवा एखाद्या संवादात संशयास्पद वाटले किंवा खूप चांगले वाटले, तर ते बहुधा फसवणूकच असते.

लक्षात ठेवा, सतर्कता आणि सक्रिय दृष्टीकोन हे सायबर फसवणुकीविरुद्ध तुमचे सर्वोत्तम संरक्षण आहेत. तुम्ही भारतात सायबर फसवणुकीचे बळी ठरल्याचा संशय आल्यास, त्वरित राष्ट्रीय सायबर क्राईम हेल्पलाइन १९३० वर संपर्क साधा किंवा घटनेची तक्रार करण्यासाठी www.cybercrime.gov.in ला भेट द्या.

सायबर फसवणूक झाल्यास काय करावे

आर्थिक फसवणूक झाल्यास

आर्थिक फसवणुकीच्या प्रकरणांमध्ये पैसे परत मिळवण्याची गुरुकिल्ली गती आहे. तुम्ही जितक्या लवकर कारवाई कराल, तितकी फसवणुकीचा व्यवहार थांबवण्याची शक्यता जास्त असते.

- राष्ट्रीय सायबर क्राईम हेल्पलाइनला कॉल करा: 1930/1945
  - हा सर्वात महत्त्वाचा पहिला टप्पा आहे, विशेषतः जर पैसे नुकतेच ट्रान्सफर झाले असतील. 1930 वर ताबडतोब कॉल करा. ही हेल्पलाइन 24/7 उपलब्ध असते.
  - या हेल्पलाइनशी जोडलेली नागरिक आर्थिक सायबर फसवणूक अहवाल आणि व्यवस्थापन प्रणाली फसवणुकीचे व्यवहार पैसे अजूनही प्रवासात असतानाच गोठवण्याचे उद्दिष्ट ठेवते.
  - व्यवहाराची रक्कम, तारीख, वेळ, तुमच्या बँकेच्या खात्याचे तपशील आणि फसवणुकीच्या व्यवहाराचे तपशील (उदा. प्राप्तकर्त्याचा खाते क्रमांक/UPI आयडी, जर तुमच्याकडे असेल तर) यांसारखी माहिती देण्यासाठी तयार रहा.
- तुमच्या बँक/आर्थिक संस्थेला कळवा:
  - 1930/1945 वर कॉल करण्यासोबतच किंवा लगेच नंतर, तुमच्या बँक, क्रेडिट कार्ड कंपनी किंवा ई-वॉलेट प्रदात्याशी संपर्क साधा.
  - तुम्ही फसवणुकीला बळी पडला आहात हे त्यांना सांगा.
  - पुढील अनधिकृत व्यवहार रोखण्यासाठी ज्या कार्ड/खात्यातून पैसे काढले गेले आहेत ते ब्लॉक करण्याची विनंती करा.
  - फसवणुकीचा व्यवहार उलटवण्याची (reverse) त्यांना विनंती करा. RBI च्या मार्गदर्शक तत्त्वांनुसार, फसवणुकीच्या प्रकारानुसार, ३ कामकाजाच्या दिवसांच्या आत तक्रार केल्यास तुमची आर्थिक जबाबदारी शून्य असू शकते.

सोशल मीडिया फसवणूक

- संबंधित प्लॅटफॉर्मला तक्रार करा
  - सोशल मीडिया प्लॅटफॉर्मला कळवा: ज्या सोशल मीडिया प्लॅटफॉर्मवर फसवणूक झाली आहे (उदा. फेसबुक, इंस्टाग्राम, ट्विटर/X, व्हॉट्सॲप), त्यांच्या 'रिपोर्टिंग' सुविधेचा वापर करून फसवणुकीची किंवा हॅक झालेल्या खात्याची तक्रार करा. बहुतेक प्लॅटफॉर्मवर हॅक केलेले खाते परत मिळवण्यासाठी किंवा बनावट प्रोफाइल हटवण्यासाठी विशिष्ट प्रक्रिया असते.
  - बनावट/इम्परसोनेटिंग खात्याची तक्रार: जर कोणी तुमच्या नावाने बनावट खाते तयार केले असेल, तर प्लॅटफॉर्मवर त्याची 'इम्परसोनेशन' (impersonation) म्हणून तक्रार करा.
- राष्ट्रीय सायबर क्राईम रिपोर्टिंग पोर्टलवर ऑनलाइन तक्रार:
  - भारत सरकारच्या अधिकृत पोर्टल www.cybercrime.gov.in ला भेट द्या.
  - 'Report Cyber Crime' वर क्लिक करा, नंतर 'File a Complaint' निवडा.
  - नवीन वापरकर्ता असल्यास नोंदणी करा, त्यानंतर लॉगिन करा.
  - 'घटनेचे तपशील' (Incident Details) मध्ये फसवणुकीचा प्रकार 'सोशल मीडिया संबंधित गुन्हा' (Social Media Related Crime) निवडा आणि आवश्यक ती सर्व माहिती सविस्तर भरा.
  - तुम्ही गोळा केलेले सर्व पुरावे अपलोड करा. (उदा. स्क्रीनशॉट्स, संभाषणाचे रेकॉर्डिंग, URLs, इ.)
  - तक्रार सबमिट केल्यानंतर, तुम्हाला एक पोचपावती क्रमांक (Acknowledgement Number) मिळेल—तो सुरक्षित ठेवा.

भंडारा पोलीस चे सर्व सोशल मीडिया हॅन्डल्स

भंडारा पोलीस चे वेबसाईट :- https://www.bhandarapolice.gov.in/

भंडारा पोलीस चे व्हाट्सअँप चॅनेल :- https://whatsapp.com/channel/0029VbBRpak3GJP30VHKDN0U

भंडारा पोलीस चे व्हाट्सअँप चॅट बोट (सायबर बोट) :- https://wa.me/+917447470100

भंडारा पोलीस चे फेसबुक पेज :- https://www.facebook.com/Bhandarapolice

भंडारा पोलीस चे इंस्टाग्राम अकाउंट :- https://www.instagram.com/bhandarapolice

भंडारा पोलीस चे ट्विटर/X अकाउंट :- https://x.com/BhandaraPolice

नागरिकांसाठी आपत्कालीन मदत क्रमांक

पोलीस (Police) :- 112

ऍम्ब्युलन्स (Ambulance) :- 108

महिला हेल्पलाइन (Women's Helpline) :- 1091

बाल हेल्पलाइन (Child Helpline) :- 1098

नागरिक कॉल सेंटर (Citizen Call Center) :- 155300

महावितरण (MSEDCL) :- 1912

कामगार कल्याण (Labour Welfare) :- 07184-252479 (भंडारा)

"सायबर गुन्ह्यांबाबत सर्वांना सतर्क बनवणारे" हे पुस्तक आधुनिक तंत्रज्ञानाच्या मोहक मुखवट्याआडचा भेसूर चेहरा दाखवते. यात, चेहरा नसलेल्या व्यक्तींनी फेकलेल्या जाळ्यांचे आणि आमिषांचे वर्णन आहे, ज्यात लोन फ्रॉड, एटीएम क्लोन, ऑनलाइन गेमिंग, घसघशीत उत्पन्नाची लालूच दाखवणारे प्रीपेड टास्क, कार्ड फ्रॉड, फिशिंग, आणि इन्व्हॉईस फ्रॉड अशा अनेक प्रकारांचा समावेश आहे. अशिक्षितांपासून उच्चशिक्षितांपर्यंत अनेकजण या फसवणुकीचे बळी ठरतात, जिथे एका क्षणात त्यांचे बँक खाते रिकामे होते. या ठकसेनांपासून स्वतःचा बचाव करण्याचा एकमेव मार्ग म्हणजे सतर्क राहणे, आणि हेच पुस्तक वाचून योग्य धडे घेऊन, संभाव्य धोके आधीच ओळखायला शिकणे महत्त्वाचे आहे.

भंडारा पोलीस
सायबर बॉट
7447470100

आपात्कालीन
क्रमांक 112
नियंत्रण कक्ष
07184-252400

नियंत्रण कक्ष
07184-256646
व्हॉटसअॅप नं.
9405841100