सायबर सुरक्षित पालघर

पालघर जिल्हा पोलीस दल महाराष्ट्रात प्रथम

सत्यमेव जयते

देवेंद्र फडणवीस
मुख्यमंत्री महाराष्ट्र

मंत्रालय
मुंबई ४०० ०३२

२७ फेब्रु. २०२५

अभिनंदन पत्र

राज्यस्तरीय, विभागस्तरीय व जिल्हास्तरीय प्रशासन हे लोकाभिमुख, गतिमान व पारदर्शक पध्दतीने चालावे याकरिता दिनांक ७ जानेवारी, २०२५ ते १६ एप्रिल, २०२५ या कालावधीत राज्यात १०० दिवसांची 'कार्यालयीन सुधारणांची' विशेष मोहीम हाती घेण्यात आली आहे.

या मोहिमेच्या अंतरिम प्रगतीचा आज दिनांक २७ फेब्रुवारी, २०२५ रोजी आढावा घेण्यात आला. राज्यातील सर्व मंत्रालयीन विभागांचे अपर मुख्य सचिव/प्रधान सचिव/सचिव,

आयुक्त/संचालक, पोलीस आयुक्त, विभागीय आयुक्त, पोलीस परिक्षेत्र महानिरीक्षक / उप महानिरीक्षक, जिल्हाधिकारी महानगरपालिका आयुक्त, पोलीस अधीक्षक व मुख्य कार्यकारी अधिकारी यांच्या कामगिरीचे – कार्यालयांची संकेतस्थळे, सुकर जीवनमान, स्वच्छता, तक्रार निवारण, अधिकारी कर्मचारी प्रशिक्षण, सेवा विषयक बाबी, कृत्रीम बुद्धिमत्ता तंत्रज्ञानाचा वापर (AI) नाविन्यपूर्ण उपक्रम, इत्यादी निकषांच्या आधारे मूल्यमापन करण्यात आले.

या अंतरिम प्रगतीच्या मूल्यमापनामध्ये राज्यातील सर्व पोलीस अधीक्षक कार्यालयांमधून पालघर पोलीस अधीक्षक कार्यालयास राज्यात प्रथम क्रमांक प्राप्त झाला आहे. आपल्या नेतृत्वाखाली पालघर पोलीस अधीक्षक कार्यालयाने केलेल्या उत्कृष्ट कामगिरीबद्दल आपले व आपल्या चमूचे मन:पूर्वक अभिनंदन !

दिनांक १६ एप्रिल, २०२५ रोजी ही १०० दिवसांची विशेष मोहीम पूर्ण होणार आहे. ही मोहीम यापुढे अधिक व्यापक व प्रभावीपणे राबवून, आपल्या हातून अशीच नेत्रदीपक कामगिरी होत राहावी याकरिता शुभेच्छा !

श्री. बाळासाहेब पाटील,
पोलीस अधीक्षक, पालघर

देवेंद्र फडणवीस

मनोगत - श्री बाळासाहेब पाटील पोलीस अधीक्षक पालघर यांचे

श्री बाळासाहेब पाटील

मा. पोलीस अधीक्षक सो पालघर

सध्याच्या डिजीटल युगात प्रत्येक व्यक्ती मोबाईल फोन, इंटरनेटचा वापर करत आहे. आपण आपल्या अनेक दैनंदिन कामासाठी इंटरनेटवर अधिक अवलंबून झाले आहेत. सायबर गुन्हेगार नागरीकांना वेगवेगळे आमिष दाखवणारे फोन कॉल करत असतात. काही नागरीक सायबर गुन्हेगारांच्या जाळ्यात अडकत आहेत. त्यामुळे सायबर गुन्ह्याचे प्रमाण दिवसेंदिवस वाढत चाललेले आहे. पालघर जिल्ह्यामध्ये सन २०२४ मध्ये सायबर गुन्हेगाराकडून १८.०४ कोटी रुपयांची फसवणुक झालेली असून हे प्रमाण प्रत्यक्ष घडलेल्या घटनांच्या प्रमाणात कमी आहे. सायबर फसवणुक हा एक प्रकारचा आर्थिक दहशतवाद आहे. सध्या शासनाच्या लोकप्रिय योजना लाडकी बहिण, पीएम किसान इ. योजनांचे पैसे थेट लाभार्थींच्या बँक खात्यात जमा होत आहेत. त्यांचीही फसवणूक होवु नये व पालघर जिल्ह्यातील नागरीक सायबर गुन्ह्यांना बळी पडु नये व त्याच्यामध्ये सायबर साक्षरता निर्माण करण्यासाठी पालघर जिल्हा पोलीस दलाच्या वतीने सायबर सुरक्षित पालघर ही मोहिम राबविण्यात येत आहे.

तसेच सायबर गुन्हे संदर्भात नागरीकांमध्ये जनजागृती करण्यासाठी व सायबर गुन्हे संदर्भात तक्रार नोंदविण्यासाठी मदत व मार्गदर्शन करण्यासाठी आयटी क्षेत्रातील विद्यार्थी, सायबर कॅफे, महा ई-सेवा केंद्र, सीएससी केंद्र, पोलीस पाटील, महिला दक्षता सदस्य यांना सायबर संदर्भात प्रशिक्षण देवुन त्यांना गाव निहाय सायबर योध्दा म्हणुन तयार करण्यात आलेले आहे. त्यांची मदत ही नागरीक घेवु शकतात.

सध्या सायबर गुन्हेगारी खुप वेगाने वाढत आहे. याचे मुख्य कारण लोकांमध्ये सायबर सुरक्षेच्या बाबतीत आवश्यक असणा-या माहितीचा अभाव असल्याचे दिसुन येत आहे. सायबर गुन्ह्यापासुन बचाव करण्यासाठी व सायबर सुरक्षित राहण्यासाठी जागरुकता निर्माण व्हावी. सायबर सुरक्षेची माहिती सर्वश्रुत व्हावी

हा मुख्य हेतु हे पुस्तक प्रकाशित करण्यामागे आहे. यामध्ये सध्या सायबर गुन्हेगार कश्या प्रकारे गुन्हे करतात याबाबत पध्दत, माहिती व त्यावर काय सावधगिरी बाळगता येईल तसेच सायबर गुन्ह्यामुळे आपले होणारे व्यक्तिगत, आर्थिक, सामाजिक नुकसान कसे टळेल व गुन्हा घडण्यापासुन अटकाव करण्यासाठी या पुस्तकातील सुचना व मार्गदर्शनाचा आपणास निश्चित फायदा होईल. त्याचबरोबर सायबर गुन्हेसंदर्भात नागरीक बळी पडल्यास त्यांनी पुढे GOLDEN HOUR मध्ये काय करावे, कुठे तक्रार नोंदवावी याबाबतही या पुस्तकात सुचना व मार्गदर्शन करण्यात आलेले आहे.

सायबर गुन्ह्यांचा वाढता आवाका पाहता सदर पुस्तकातील मार्गदर्शनामुळे व दिलेल्या टिप्स मुळे पालघर जिल्ह्यातील नागरीक सायबर साक्षर होतील अशी मला खात्री आहे. या पुस्तकाचा फायदा पोलीस अधिकारी, अंमलदार, विद्यार्थी, पालक, शिक्षक, महिला, व्यावसायीक व सर्व नागरीकांनी घ्यावा ही सदिच्छा.

प्रस्तावना

आजच्या तंत्रज्ञान प्रधान युगात इंटरनेट आणि डिजिटल माध्यमांचा वापर सर्व स्तरांवर वाढत आहे. शिक्षण, व्यवसाय, बँकिंग, सोशल मीडिया आणि दैनंदिन व्यवहार यामध्ये इंटरनेट महत्त्वाची भूमिका बजावत आहे. मात्र, या सोयी सुविधांसोबतच सायबर गुन्ह्यांचाही मोठा धोका निर्माण झाला आहे.

सायबर गुन्हेगारीमध्ये डिजीटल अटक, बनावट सोशल मिडीया प्रोफाइलद्वारे छळ, ऑनलाईन नोकरी फसवणुक, वैवाहिक वेबसाईटद्वारे फसवणुक आर्थिक फसवणूक, ऑनलाईन धमक्या, ओळख चोरी, सोशल मीडिया गैरवापर, बनावट वेबसाईट्स, हॅकिंग, क्युआर कोड/लिंक द्वारे पैसे मागवुन फसवणूक, यांसारख्या घटना वाढत्या प्रमाणात घडत आहेत. अशा गुन्ह्यांपासून स्वत:ला आणि आपल्या परिवाराला सुरक्षित ठेवण्यासाठी प्रत्येकाला सायबर सुरक्षेची माहिती असणे गरजेचे आहे.

ही माहिती पुस्तिका सायबर गुन्हे आणि त्यावरील प्रतिबंधात्मक उपाय यांची सविस्तर माहिती देण्याच्या उद्देशाने तयार केली आहे. यात सायबर सुरक्षेच्या महत्त्वपूर्ण बाबी, सुरक्षित इंटरनेट वापर, पासवर्ड संरक्षण, सोशल मीडियावर सुरक्षितता, ऑनलाईन आर्थिक व्यवहारांतील सावधगिरी आणि पालक, महिला, मुले, यांच्यासाठी सायबर सुरक्षा टिप्स यांचा समावेश आहे.

सायबर गुन्ह्यांपासून स्वत:ला आणि आपल्या कुटुंबाला सुरक्षित ठेवण्यासाठी सावध राहणे, योग्य सुरक्षितता उपाय अवलंबणे आणि संशयास्पद गोष्टी त्वरित संबंधित यंत्रणेला कळवणे आवश्यक आहे. आपण सर्वांनी सायबर सुरक्षिततेची काळजी घेतली, तर डिजिटल विश्व अधिक सुरक्षित आणि विश्वासार्ह होईल. या पुस्तिकेद्वारे नागरिकांना जागरूक करणे आणि सायबर सुरक्षेसाठी सक्षम बनवणे हा आमचा उद्देश आहे. आशा आहे की, या पुस्तिकेद्वारे नागरिकांना जागरूक करणे आणि सायबर सुरक्षेसाठी सक्षम बनवणे हा आमचा उद्देश आहे. आशा आहे की, ही पुस्तिका सर्व वाचकांसाठी उपयुक्त ठरेल.

अनुक्रमणिका

विषय	पान क्र.
डिजिटल अटक	1
सेक्सटॉर्शन स्कॅम	2
फिशींग व हॅकिंग द्वारे केली जाणारी आर्थिक फसवणुक	3
UPI फिशिंग फ्रॉड	4
ऑनलाइन शॉपिंग घोटाळे	5
ऑनलाइन गेम फ्रॉड	6
फेक लोन संदर्भात सायबर फसवणुक	7
पार्टटाईम जॉब स्कॅम	8
सोशल मीडीया प्लॅटफॉर्मचा वापर करून आर्थिक फसवणूक	9
बनावट सोशल मीडिया प्रोफाइलद्वारे छळ	10
एटीएम / डेबीट कार्डसाठी सूचना	11
केवायसी/रिमोट ऍक्सेस अॅप फसवणूकीपासुन सावध रहा	12
लग्नाचे आमिष दाखवून होणारी फसवणूक टाळण्यासाठी घ्यावयाची खबरदारी	13
ऑनलाईन गेमिंग सायबर फसवणूक	14
बनावट APK फाईल सायबर फसवणूक	15
CYBER BULLYING पासुन आपल्या पाल्याचे रक्षण करा	16

अनुक्रमणिका

विषय	पान क्र.
मोबाईल हरवल्यास काय करावे	17
बनावट फेसबुक अकाउंट बनवल्यास काय कराल ?	18
बनावट इंस्टाग्राम अकाउंट बनवल्यास काय कराल ?	19
तुमचे व्हॉट्सॲप अकाउंट हॅक केल्यास किंवा व्हॉट्सॲप संबधीत इतर तक्रारी असल्यास काय कराल ?	20
बनावट / फसव्या लिंक पासून सावधान	21
मुलांसाठी सायबर सुरक्षितता टिप्स	22
पालकांसाठी सायबर सुरक्षितता टिप्स	23
महिलांसाठी सायबर सुरक्षितता टिप्स	24
महिलांसाठी सायबर सुरक्षितता टिप्स	25
महिलांसाठी सायबर सुरक्षितता टिप्स	26
सामान्य सायबर सुरक्षा टिप्स	27
सामान्य सायबर सुरक्षा टिप्स	28
सामान्य सायबर सुरक्षा टिप्स	29
वेबसाईट वरील नवीन टॅब	30
आवाहन	31

डिजिटल अटक

डिजिटल अटक घोटाळ्यात, गुन्हेगार स्वत:ला कायदा अंमलबजावणी अधिकारी म्हणून भासवतात आणि फोन कॉलद्वारे पीडितांशी संपर्क साधतात, त्यानंतर, ते व्हॉट्सॲप किंवा स्काईप सारख्या प्लॅटफॉर्मवर व्हिडिओ कॉलसाठी पीडितांना आवाहन करतात. फसवणूक करणारे पीडितांना विविध कायदेशीर उल्लंघनांसाठी डिजिटल अटक वॉरंटची धमकी देतात आणि त्यांना मोठ्या प्रमाणावर पैसे विशिष्ठ बँक खात्यांमध्ये किंवा यु.पी.आय. आयडींमध्ये हस्तांतरित करण्यास भाग पाडतात. एकदा पैसे दिले की, स्कॅमर गायब होतात, ज्यामुळे पीडितांना आर्थिक नुकसान आणि ओळख चोरीला सामोरे जावे लागते.

डिजिटल अटक घोटाळ्याचे बळी होण्यापासून कसे वाचावे ?

- बनावट अधिकाऱ्यांच्या कॉलवर लक्ष ठेवा. अधिकारी कधीही पैसे मागत नाहीत.
- सायबर गुन्हेगारांच्या दबावाखाली त्वरित कारवाई करु नका.
- शंका असल्यास, संबंधित एजन्सीशी थेट संपर्क साधा.
- अज्ञात नंबरवर संवेदनशील माहिती शेअर करु नका.
- सरकारी संस्था व्हॉट्सॲप/स्काईप वापरत नाहीत.
- फसवणूकीचा संशय असल्यास, पोलीसांना तक्रार करा.
- डिजिटल अटक असा कोणताही कायदेशीर प्रकार नाही.

सेक्सटॉर्शन स्कॅम

सेक्सटॉर्शन पासून सावधान राहा !

- सायबर गुन्हेगार आकर्षक महिलांचे फोटो वापरून फेक अकाऊंट बनवतात.
- तुम्हाला ऑनलाईन चॅट व व्हिडिओ कॉल करण्यासाठी आग्रह करतात.
- तुम्हाला आक्षेपार्ह स्थितीत ओढण्याचा प्रयत्न करतात.
- तुम्हाला आक्षेपार्ह स्थितीत रेकॉर्ड करतात.
- ऑडिओ किंवा व्हिडिओ समस्या असल्याचे कारण देत तुम्हाला ती समस्या दूर करण्यासाठी एक अँप इन्स्टॉल करायला सांगतात.
- ह्या अँपमध्ये लपलेल्या मॅलवेअर तुमचे कॉन्टॅक्टस आणि इतर माहिती सायबर गुन्हगारांना पाठवतो.
- सायबर गुन्हेगार तुमच्याकडे रकमेची मागणी करतात व नाही दिल्यास तुमचे व्हिडिओ किंवा फोटो लीक करण्याची धमकी देतात.

फिशींग व हॅकिंग द्वारे केली जाणारी आर्थिक फसवणुक

फिशिंग म्हणजे सायबर अपराधी बँक खातेदारांना त्यांच्या खात्याची आणि वैयक्तिक माहिती मागणारे ई-मेल, एसएमएस, किंवा फोन कॉल्स करतात. ते वित्तीय संस्थेचे प्रतिनिधी असल्याचा भास निर्माण करुन माहिती घेतात. एकदा माहिती मिळाल्यानंतर, ते बँक खात्यात अनाधिकृत प्रवेश करुन पैसे हस्तांतरित करतात. हॅकिंग म्हणजे संगणक प्रणाली किंवा नेटवर्कमध्ये अनाधिकृतपणे प्रवेश मिळवणे, जसे कि पासवर्ड क्रॅकिंग .

फिशिंग व हॅकिंगच्या घोटाळ्याचे बळी होण्यापासून कसे वाचावे ?

- अपडेटेड ब्राऊझर वापरा.
- संवेदनशील माहिती शेअर करु नका, जसे की क्रेडिट कार्ड, एटीएम पिन, पासवर्ड.
- स्ट्राँग पासवर्ड वापरा – पासवर्डमध्ये अक्षरे, अंक आणि विशेष चिन्हे असावीत.
- मल्टी – फॅक्टर ऑथेंटिकेशन वापरा.
- पब्लिक वाय-फाय वापरणे टाळा.
- पब्लिक कॉम्प्युटरवर बँकिंग टाळा – कॅफे किंवा लायब्ररीमध्ये सार्वजनिक कॉम्प्युटरवर आर्थिक व्यवहार करु नका.
- वैयक्तिक माहिती जसे की पत्ता, फोन नंबर किंवा बँक तपशिल अनोळखी वेबसाईट्सवर शेअर करु नका.
- हॅकर्सपासून सुरक्षित राहण्यासाठी तुमचे वायरलेस आणि लोकेशन सेवा बंद ठेवा.

UPI फिशिंग फ्रॉड

बँकिंग समस्यांमध्ये मदत देण्याच्या बहाण्याने, फसवणूक करणारे पिडीतांना लिंक फॉरवर्ड करण्यास सांगतात आणि त्यांच्या बँक खात्यात प्रवेश मिळवतात.

UPI युपीआय फसवणूक कशी होते :-

- फसवणूक करणारे केवायसी/आधार अपडेच्या बहाण्याने कॉल करतात.
- पिडीत व्यक्तीला युपीआयशी खाते लिंक करण्यासाटी अल्फान्युमेरिक लिंक आणि ओटीपी शेअर करण्यास सांगितले जाते.
- पिडीत व्यक्ती लिंक आणि ओटीपी शेअर करतो.
- फसवणूक करणारे युपीआय वॉलेटमध्ये प्रवेश मिळवतात आणि एमपीआयएन सेट करतात
- ते पिडीत व्यक्तीच्या खात्याचा गैरवापर करतात.
- खाते ब्लॉक होईपर्यंत पैसे फसवले जातात.

टिप्स :

- बँक/आरबीआय अधिकारी म्हणून ओळखणाऱ्या व्यक्तीला ओटीपी किंवा लिंक कधीही शेअर करु नका .
- एअरलाइन्स/ई-कॉमर्स कंपन्यांच्या कस्टमर केअर नंबरवर कॉल करणाऱ्या व्यक्तींच्या सूचनांचे पालन करून फसवणूकीपासून बचाव करा.

ऑनलाइन शॉपिंग घोटाळे

नुकत्याच झालेल्या एक ऑनलाईन सर्वेक्षणात असे उघड झाले आहे कि, प्रत्येक पाच शहरी भारतीयांपैकी एकाला ऑनलाईन शॉपिंग घोटाळ्यांमुळे आर्थिक नुकसान झाले आहे. YOUGOV द्वारे आयोजित केलेल्या सर्वेक्षणात ऑनलाइन शॉपिंग घोटाळे हे देशातील सर्वात व्यापक फसवणुकीच्या प्रकारांपैकी एक म्हणून हायलाइट केले गेले.

फसवणुकीची लक्षणे :-

- अत्यंत कमी किंमतीत आकर्षक ऑफर्स देऊन लोकांना फसवणे.
- बनावट किंवा अनोळखी वेबसाइट्स वरून उत्पादने विकणे.
- पेमेंट केल्यानंतर ऑर्डर न मिळणे किंवा खोटे/निकृष्ट दर्जाचे उत्पादन मिळणे.
- केवळ प्री-पेमेंटची मागणी आणि कॅश-ऑन-डिलिव्हरी पर्याय नसणे.
- वेबसाईटवर ग्राहक सेवा संपर्काची स्पष्ट माहिती नसणे.

सुरक्षित राहण्यासाठी उपाय :-

- फक्त नामांकित आणि विश्वसनीय वेबसाइट्सवरुन खरेदी करा.
- वेबसाइटचे युआरएल 'https://' आहे का तपासा.
- पेमेंटसाठी सुरक्षित पर्याय जसे की COD किंवा विश्वसनीय पेमेंट गेटवे वापरा.
- फसव्या ऑफर्स आणि अतिशय मोठ्या सवलतींपासून सावध राहा.
- ऑनलाइन खरेदी करताना ग्राहकांचे पुनरावलोकन आणि रेटिंग तपासा.
- संशयास्पद वेबसाइट्स आणि घोटाळ्यांची माहिती सायबर सेलला द्या.

टिप्स :-

- खरेदी प्रसिद्ध किरकोळ विक्रेत्यांकडून करा.
- ईमेल/सोशल मीडियाच्या लिंकवर क्लिक करताना काळजी घ्या.
- वेबसाइटचा URL तपासा. त्यात "https" आणि योग्य डोमेन असावा.
- विश्वास नसलेल्या वेबसाइटवर वैयक्तिक माहिती देऊ नका.
- ऑनलाइन खरेदी साठी क्रेडिट कार्ड वापरा.
- क्रेडिट कार्ड फसवणुकी पासून चांगले संरक्षण देते.
- क्रेडीट कार्ड वर पैसे देण्याची मर्यादा असल्याने अधिक सुरक्षित आहे.

ऑनलाइन गेम फ्रॉड

ऑनलाइन गेम फ्रॉड म्हणजे एक फसवी कृती ज्यात फसव्या युक्तांद्वारे खेळाडूंना वैयक्तिक माहिती, किंवा पैसे देण्यास भाग पाडले जाते. यात बक्षिसे, दुर्मिळ वस्तू किंवा गेममधील फायद्यांचे खोटे आश्वासन दिले जातात. लहान मुले आणि युवा वर्ग ऑनलाइन गेम खेळत असल्याने युजर्सची संख्या वाढत आहे, आणि सायबर गुन्हेगार त्यांना शिकार करण्यासाठी नवीन मार्ग शोधत आहेत.

टिप्स :-

- लॉगिन तपशील शेअर करु नका.
- संवेदनशील माहिती ऑनलाइन देण्याबाबत सावधगिरी बाळगा, जरी ते गेम कंपनीचे असले तरी.
- अविश्वसनीय प्रलोभनांना बळी पडू नका,
- संशयास्पद लिंक्सपासून सावध रहा. अज्ञात लिंक्सवर क्लिक करु नका, URL तपासा.
- संभाव्य घोटाळ्यांची माहिती गेम सपोर्ट टीमला द्या.
- FACTOR AUTHENTICATION सक्षम करा. अतिरिक्त सुरक्षा स्तरासाठी हॅकर्ससाठी प्रवेश कठीण करा.
- फक्त विश्वसनीय स्त्रोतांकडून खरेदी करा. जसे कि GOOGLE PLAY STORE, APPLE STORE.

फेक लोन संदर्भात सायबर फसवणुक

DO NOT TRUST EASY LOAN APPS

- सध्या भारतात अनेक फसवणुक करणारे कर्ज ॲप्स सक्रिय आहेत. जे लोकांना आकर्षक कर्जाच्या ऑफर देऊन फसवतात.

- या फसवणुक करणाऱ्या कर्ज ॲप्सची काही लक्षणे खालीलप्रमाणे आहे.

१. अतंत्य कमी व्याजदर आणि जलद मंजुरीचे आश्वासन देणे.

२. अधिकृत परवाना किंवा नोंदणी नसणे.

३. वैयक्तिक माहिती जसे की आधार कार्ड , पॅन कार्ड, बँक खाते तपशील इत्यादी विनाकारण मागणी करणे.

- तरी अशा फसवणुकीपासुन वाचण्यासाठी खालील खबरदारी घ्यावी :

१. फक्त अधिकृत आणि रिझर्व्ह बँक ऑफ इंडीया (RBI) मान्यताप्राप्त कर्जदात्यांकडूनच कर्ज घ्यावे

२. ॲप इन्स्टॉल करण्यापुर्वी त्याचे परवाना आणि नोंदणी तपासा.

३. वैयक्तिक माहिती शेअर करण्यापुर्वी ॲपची गोपनीयता धोरण वाचा.

सायबर फसवणूक होत असल्याचे जाणवल्यास अथवा सायबर फसवणुक झाल्यास संपर्क:-

https://cybercrime.gov.in/

टोल फ्री नं: 1930 / 1945

पार्टटाईम जॉब स्कॅम

स्कॅमर बनावट मेसेज/ई-मेल पाठवतात. ज्यात ते स्वत:ला नामांकित कंपन्यांकडून पार्टटाइम जॉब देत असल्याचा दावा करतात. एकदा पिडीत व्यक्तीला खात्री पटली की, स्कॅमर प्रशिक्षण आणि नोंदणी शुल्क इत्यादींच्या बदल्यात पैसे मागतो.

सुरक्षितता टिप्स :-

- असत्यापित लिंक्स कितीही आकर्षक दिसत असल्या तरी त्यावर क्लिक करण्यापासून दूर रहा.
- अज्ञात व्यक्तीसोबत कोणताही व्यवहार करण्यापुर्वी सावधगिरी बाळगा.
- आलेल्या नंबर ची तक्रार करा आणि ब्लॉक करा.

सोशल मीडीया प्लॅटफॉर्मचा वापर करून आर्थिक फसवणूक

फसवणूक करणारे फेसबुक आणि इंस्टाग्रामवर बनावट खाते तयार करून टार्गेट प्रोफाइलचे मित्रांना त्वरित पैसे ट्रान्सफर करण्याची विनंती करतात, अनेकदा वैद्यकीय आणीबाणीचा हवाला देऊन त्याला / तिला त्यांचा मित्र समजून पैस पाठवतात. टार्गेट प्रोफाइलला याची माहिती होईपर्यंत, अनेक मित्र फसवणूकीचे बळी होतात. तसेच लक्ष्य खाते हॅक करुन देखील फसवणूक केली जाते.

सोशल मीडिया प्लॅटफॉर्मचा वापर करुन आर्थिक फसवणूक कशी होते :-

- फसवणूक करणारा मुळ सोशल मीडिया प्रोफाइलसारखी बनवट प्रोफाइल तयार करतो.
- त्याच डिस्प्ले पिक्चर आणि नावाचा वापर करुन फेसबुक अकाऊंट नक्कल करतो.
- नक्कल केलेल्या प्रोफाइलमधून मूळ अकाउंटच्या फ्रेंड लिस्टमधील लोकांना फ्रेंड रिक्वेस पाठवतो.
- मेसेंजरद्वारे संपर्क साधून वैद्यकीय आणीबाणीच्या बहाण्याने पैशांची मागणी करतो.
- पेमेंटसाठी Phonepe/Google Pay/ Paytm किंवा बँक खाते शेअर करतो.
- जर कोणी मित्रांकडून पडताळणी न करता पैसे पाठवले, तर तो फसवणूकीचा बळी ठरतो.

टिप्स :-

- गोपनीयत सेटिंग्स ठेवा.
- सोशल मीडीया मार्फत पैसे ट्रान्सफर करण्यापूर्वी संबंधित व्यक्तीला भेटून किंवा कॉल करून सत्यता पडताळा.
- सोशल मीडीया अकाउंटसाठी २- स्टेप व्हेरिफिकेशन चालू करा.
- पासवर्ड मजबुत ठेवा आणि गोपनीयता राखा.

बनावट सोशल मीडिया प्रोफाइलद्वारे छळ

सायबर गुन्हेगार सोशल मीडिया वरुन मिळालेल्या पिडीतेचे फोटो मॉर्फ करतात आणि सोशल मीडिया प्लॅटफॉर्मवर अपलोड करतात. त्यानंतर ते सोशल मीडिया वरुन मॉर्फ केलेले फोटो काढून टाकण्यासाठी पैसे मागतात. पिडीत या सापळयात अडकतो आणि पैसे ट्रान्सफर करतो.

बनावट सोशल मीडिया प्रोफाईलद्वारे छळ कसा होतो :-

- पिडीत व्यक्ती नकळत फसवणूक करणाऱ्याच्या फ्रेंड रिक्वेस्ट स्वीकारतो.
- खराब गोपनीयता सेटिंग्जमुळे सायबर गुन्हेगारांना पिडीतेच्या फोटो आणि पोस्ट्स सहज मिळतात.
- गुन्हेगार फोटो डाउनलोड करुन त्याचा वापर बनावट प्रोफाइल तयार करण्यासाठी करतात.
- मॉर्फ केलेली अश्लील छायाचित्रे अपलोड करुन पिडीतेला मानसिक त्रास देतात.

टिप्स :-

- सोशल मीडिया ॲप्सच्या गोपनीयता सेटिंग्ज जाणून घ्या.
- वैयक्तिक माहिती, फोटो, व्हिडिओ फक्त विश्वासू व्यक्तिंनाच उपलब्ध करा.
- ऑनलाइन पोस्ट किंवा शेअर करण्यापूर्वी दोनदा विचार करा.
- मुलांना सायबर बुलिंगच्या गुन्हयाची जाणीव करुन द्या.
- दुखावणाऱ्या टिप्पण्या आणि फोटो रिपोर्ट करा, आणि ब्लॉक करा.

एटीएम / डेबीट कार्डसाठी सूचना

- तुमचे ATM/Credit/Debi कार्ड रिॲक्टीवेट करण्यासाठी किंवा के. वाय. सी. करण्यासाठी आपली माहिती विचारल्यास कोणालाही आपले कार्ड किंवा डेबिट कार्डचा १६ अंकी नंबर, पिन नंबर, सी.व्ही.व्ही. नंबर किंवा व्यक्तीगत माहिती फोन किंवा ई-मेलवरून देऊ नका.
- तुमच्या ओ.टी.पी. नंबर कोणालाही सांगु नका. तो ऑनलाईन फसवणूकीसाठी वापरला जावू शकतो. तुमचा मोबाईल नंबर बँक खात्याशी जोडा ज्यामुळे तुमच्या व्यवहारांची माहिती त्वरीत मोबाईल एस एम एस द्वारे समजेल.
- ए.टी.एम मधुन पैसे काढतांना ए.टी.एम. स्टॉल मध्ये लाईट ब्लींक होत नसल्यास पैसे काढु नये.
- ए.टी.एम मशिन मध्ये स्वाईप करते वेळी आजुबाजुस छुपा कॅमेरा असू शकतो. पिन नंबर टाकताना हातावर पेपर किंवा कोणत्याही वस्तुचा आडोसा घ्या.
- ए.टी.एम मशीनद्वारे व्यवहार करताना अन्य कोणालाही आजूबाजुस उभे राहु देऊ नका.

केवायसी/रिमोट ऍक्सेस ॲप फसवणूकीपासुन सावध रहा

केवायसी पडताळणीशी संबंधित फसव्या एसएमएस किंवा कॉलपासून सावध रहा.

एसएमएस/फोनवर वैयक्तिक माहिती शेअर करू नका. जरा तुम्हाला तुमचे खाते ब्लॉक किंवा निलंबित केले जाईल असा कोणताही एसएमएस मिळाला तर, केवायसी पूर्ण झाले असल्यास, बँकेच्या ई-वॉलेट/सेवा प्रदात्याच्या अधिकृत ग्राहक सेवेशी संपर्क साधा. केवायसी केवळ अधिकृत केवायसी पॉईंट्सवर किंवा प्रतिनिधीद्वारे केले जाऊ शकते.

केवायसी पूर्ण करण्यासाठी कधीही क्विक सपोर्ट, एनीडेस्क किंवा टीमव्ह्यूअर इत्यादी कोणतेही ॲप डाऊनलोड करु नका.

असे ॲप्स तुमच्या डिव्हाइसेस वर रिमोट ॲक्सेस देते, ज्यामुळे फसवणूक करणाऱ्यांना फसवणूक करण्यासाठी तुमचा पिन, ओटीपी, बँक खात्याचा तपशील इत्यादी माहिती मिळते.

लग्नाचे आमिष दाखवून होणारी फसवणूक टाळण्यासाठी घ्यावयाची खबरदारी

- विवाहविषयक संकेतस्थळावर फसवणूकीच्या उद्देशाने गुन्हेगार खोट्या आकर्षक प्रोफाइल बनवतात.
- लग्न करण्याचे आमिष दाखवुन त्या व्यक्तीशी जवळीक साधली जाते.
- पिडीत व्यक्तीला पैशांची मागणी किंवा एखादे गैरकृत्य करण्यास भाग पाडतात.
- सोशल मीडियावरून मैत्री करताना सावधानता बाळगा.
- आपली संवेदनशील वैयक्तिक माहिती अज्ञात व्यक्तीला सांगु नका.
- सोशल मीडियावरील समोरच्या व्यक्तीचे प्रोफाइल तपासुन बघावे.
- समोरच्या व्यक्तीचे प्रोफाइल तपासल्यावरच मैत्री करावी व खात्री केल्याशिवाय अशा माणसांना उधारी पैसे देऊ नका.
- अज्ञात व्यक्तींबरोबर वैयक्तिक फोटो शेअर करु नका.

ऑनलाईन गेमिंग सायबर फसवणूक

- या फसवणूकीच्या माध्यमातुन फसवणूक करणारे लोकांना पैसे गमवायला लावतात, वैयक्तिक माहिती चोरतात आणि ऑनलाईन गुन्हेगारीसाठी त्याचा वापर करतात.

- **ऑनलाईन गेमिंग फसवणूकीचे प्रकार:**
  १. फिशिंग घोटाळे : गेम खेळताना लिंक किंवा पॉपअपच्या माध्यमातुन युजर्सला त्यांची लॉगिन माहिती देण्यास भाग पाडले जाते आणि त्यानंतर माहिती चोरली जाते.
  २. फेक गेमिंग ॲप्स : अधिकृत ॲप्स सारखी दिसणारी फेक गेमिंग ॲप्स डाऊनलोड करण्यास प्रवृत्त केले जाते, त्यामुळे युजरच्या डिव्हाइसवर मालवेअर इन्स्टॉल केले जाते.
  ३. फ्रि गिफ्ट किंवा इन-गेम रिव्हार्ड्स: मोफत गिफ्ट्स, इन-गेम करन्सी किंवा रिव्हार्ड्स देण्याचे आश्वसन देऊन युजर्सकडुन वैयक्तिक माहिती किंवा पैसे मागितले जातात.
  ४. स्कॅम टुर्नामेंट्स : जिथे जिंकण्याचे मोठे इनामाचे प्रलोभन दाखवले जाते पण सहभागी होण्यासाठी नोंदणी शुल्क घेतले जाते, आणि नंतर कोणतेही इनाम दिले जात नाही.

- **ऑनलाईन गेमिंग फसवणूकीपासुन बचावाचे उपाय :**
  १. अधिकृत स्त्रोतांवरुन गेम डाऊनलोड करा. फक्त GOOGLE PLAY STORE किंवा APPLE APP STORE सारख्या अधिकृत प्लॅटफॉर्मवर आपली वैयक्तिक माहिती, बँकिंग तपशील किंवा पासवर्ड शेअर करु नका.
  २. खाजगी माहिती शेअर करु नका: कोणत्याही गेमिंग प्लॅटफॉर्मवर आपली वैयक्तिक माहिती, बँकिंग तपशील किंवा पासवर्ड शेअर करु नका.
  ३. सायबर सुरक्षेची साधने वापरा: अँटीव्हायरस सॉफ्टवेअर आणि फायरवॉलचा वापर करून आपल्या डिव्हाइसचे संरक्षण करा.

बनावट APK फाईल सायबर फसवणूक

तुमचे बँक लॉगिन तपशिल, एसएमएस आणि ओटीपी चोरण्यासाठी हे बनावट ॲप आहे. सुरक्षित राहण्यासाठी या तत्वांचे अनुसरण करा.

- APK फाईल ही पीएम किसान योजना, लाडकी बहीण योजना, गॅस कनेक्शन केवायसी अपडेट संदर्भात पाठवली जाते.
- यावर लगेच विश्वास ठेऊन अशा फाईल डाऊनलोड केल्या जातात. अशा फाईल डाऊनलोड झाल्यास तुमची वैयक्तीक माहिती सायबर गुन्हेगार प्राप्त करुन त्या माहिती वरुन आपली फसवणूक करत असतात.
- ईमेल संदेश किंवा WHATSAPP द्वारे प्राप्त झालेल्या अज्ञार्त इख फाईल्स कधीही डाऊनलोड करु नका .
- संदेश पाठवणाऱ्याची ओळख ओळखा पटवा आणि खाते संशयास्पद असल्यास ब्लॉक करा, आणि तक्रार करा.
- तुमच्या फोनवर install unknown apps/sources सेटिंग बंद करा.
- तुमची वैयक्तीक माहिती कोणालाही देऊ नका.

CYBER BULLYING पासुन आपल्या पाल्याचे रक्षण करा

password सुरक्षीततेचे महत्व समजवून सांगा.

त्यांच्याकडून खाजगी माहिती उघड केली जात नाही याची खात्री करावी.

त्यांचे सोशल मीडीया अकाऊंट प्रत्येक महिन्यात चेक करावे.

आपल्या पाल्याचे सोशल मीडीया अकाउंट Private करा.

CYBER BULLYING ची घटना आपल्या बाबतीत घडल्यास जवळच्या पोलीस स्टेशनशी संपर्क साधा.

मोबाईल हरवल्यास काय करावे

CENTRAL EQUIPMENT IDENTITY REGISTER (CEIR PORTAL)

- आपल्या हद्दीतील स्थानिक पोलीस स्टेशन येथे तक्रार नोंदवावी.
- हरविलेल्या मोबाईल फोनमधील सिमकार्ड ब्लॉक करावे व त्याच नंबरचे सिमकार्ड सुरु करून घ्यावे जेणे करून तोच मोबाईल नंबर CEIR वर रजिस्ट्रेशन करीता वापरता येईल.
- https://www.ceir.gov.in या वेबसाईट वर संपर्क साधावा.
- नमुद साईटवर BLOCK STOLEN / LOST MOBILE यावर क्लिक करुन आवश्यक ती माहिती भरून SUBMIT वर क्लिक करावे.
- खालील कागदपत्रे सोबत जोडावी (सॉफ्टकॉपी ५०० केबी पेक्षा कमी असावी.) पोलीस स्टेशनला केलेली तक्रारीची प्रत, मोबाईल खरेदीचे बिल, कोणतही शासकिय ओळखपत्र.
- ज्या नंतर आपल्याला CEIR वर तक्रार नोंदविल्याचा REQUEST NUMBER मिळेल.
- हरवलेला मोबाईल ACTIVE झाल्या नंतर त्या बाबतची माहिती पोर्टलद्वारे रजिस्टर मोबाईल क्रमांकावर एसएमएस द्वारे मिळते. त्या बाबतची माहिती आपण संबंधित पोलीस स्टेशनला द्यावी.

बनावट फेसबुक अकाउंट बनवल्यास काय कराल ?

नागरीकांसाठी सुचना :-

- सायबर गुन्हेगार तुमचे सोशल मीडियावरील फोटो वापरुन तुमचे बनावट फेसबुक अकाउंट तयार करतात.
- बनावट अकाउंटचा वापर करुन तुमचे मित्र, नातेवाईक व ओळखीच्या व्यक्तींना तुम्ही मेसेज केल्याचे भासवुन पैशांची मागणी केली जाते.
- तरी तुमचे बनावट फेसबुक अकाउंट बंद करण्यासाठी खालील लिंक वर जाऊन किंवा क्यु आर कोड स्कॅन करुन त्यामधील सुचनांप्रमाणे आपली तक्रार नोंदवावी.
- https://m.facebook.com/help/contact/278770247037228?wtsid=rdr_OZC3Q6veQiyVdmdsZ

बनावट इंस्टाग्राम अकाउंट बनवल्यास काय कराल ?

नागरीकांसाठी सुचना :-

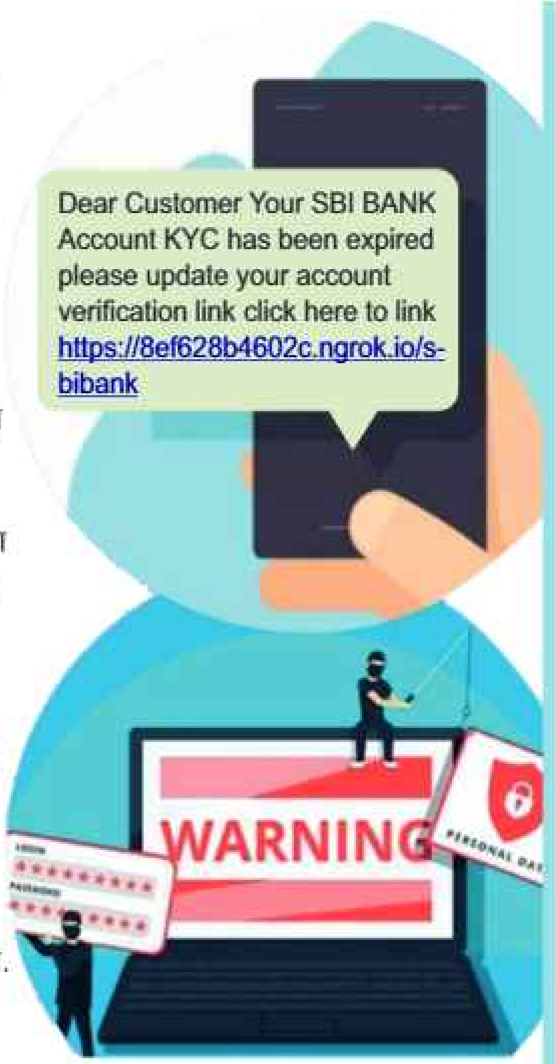
- सायबर गुन्हेगार तुमचे सोशल मीडियावरील फोटो वापरुन तुमचे बनावट इंस्टाग्राम अकाउंट तयार करतात.
- बनावट अकाउंटचा वापर करुन तुमचे मित्र, नातेवाईक व ओळखीच्या व्यक्तींना तुम्ही मेसेज केल्याचे भासवुन पैशांची मागणी केली जाते.
- तरी तुमचे बनावट इंस्टाग्राम अकाउंट बंद करण्यासाठी खालील लिंक वर जाऊन किंवा क्यु आर कोड स्कॅन करुन त्यामधील सुचनांप्रमाणे आपली तक्रार नोंदवावी.
- https://help.instagram.com/contact/779201836048501

तुमचे व्हॉट्सअ‍ॅप अकाउंट हॅक केल्यास किंवा व्हॉट्सअ‍ॅप संबधीत इतर तक्रारी असल्यास काय कराल ?

- सायबर गुन्हेगाराने तुमचे व्हॉट्सअ‍ॅप अकाउंट हॅक केले आहे.
- व्हॉट्सअ‍ॅप संदर्भात इतर काही तक्रारी असल्यास खालील लिंक वर जाऊन किंवा क्यु आर कोड स्कॅन करुन त्यामधील सुचनांप्रमाणे आपली तक्रार नोंदवावी.
- https://www.whatsapp.com/contact/forms/1534459096974129/

बनावट / फसव्या लिंक पासून सावधान

- तुमचा पासवर्ड, वैयक्तिक आणि संवेदनशील माहिती मिळवण्यासाठी, किंवा तुमच्या डिव्हाइसमध्ये मालवेअर/ व्हायरस इंस्टॉल करण्यासाठी अश्या लिंक चा वापर केला जातो.
- अशा माहितीचा वापर तुमच्या बँक खात्यातून पैसे चोरण्यासाठी किंवा तुमची आयडेंटिटी चोरण्यासाठी केला जातो.
- मालवेअर / व्हायरस चा वापर तुमचा डेटा चोरण्यासाठी, नष्ट करण्यासाठी किंवा एनक्रिप्ट करण्यासाठी केला जातो.
- अश्या लिंक ई-मेल, messaging ॲप्स, सोशल मीडिया किंवा जाहिरातिच्या माध्यमातून येतात.
- अज्ञात ई-मेल/नंबर वरुन आलेल्या कोणत्याही लिंकवर क्लिक करु नका.
- अशी लिंक आल्यास संबंधित बँक/कार्यालयाकडून संदेशाची पडताळणी करा.



मुलांसाठी सायबर सुरक्षितता टिप्स

DO'S :-

- जेव्हा तुम्हाला कोणत्याही सोशल मीडीया पोस्ट/मेल/चॅटिंगमध्ये अस्वस्थ वाटत असेल, तेव्हा लगेच तुमच्या पालकांशी किंववा कोणत्याही विश्वासर्ह व्यक्तीशी तुमची चिंता शेअर करा.
- वास्तविक जीवनातील शिष्टाचार आणि शिष्टाचार व्हर्च्युअल स्पेसलाही तितकेच लागू होतात.
- वास्तविक जीवनात आणि तुमच्या पालकांच्या परवानगीने तुम्हाला माहित असलेल्या व्यक्तींना नेहमी जोडा.
- पासवर्डमध्ये अल्फा- न्यूमेरिक चिन्हे आणि विशेष वर्णांचा समावेश असावा.

DONT'S :-

- फेसबुक, इंस्टाग्राम, ब्लॉग, ट्विटर, चॅट-रुम इत्यादी कोणत्याही ऑनलाइन प्लॅटफॉर्मवर पत्ता, फोन नंबर नोंदणीसाठी विशिष्ठ वयाचे निकष आवश्यक असलेल्या साइट्ससाठी SIGN UP करु नका.
- तुमच्या पालकांशी चर्चा केल्याशिवाय ऑनलाइन काहीही खरेदी करू नका.
- जन्मतारीख इत्यादी तुमची वैयक्तिक माहिती कधीही शेअर करु नका. तुम्ही त्यांना प्रत्यक्ष जीवनात ओळखत नसल्यास किंवा त्यांना प्रत्यक्ष भेटल्याशिवाय लोकांना ऑनलाइन मित्र म्हणून जोडू नका.
- सोशल मीडीया प्लॅटफॉर्मवर अश्लील/आक्षेपार्ह /छळवणूक करणारे ईमेल/चॅट पोस्ट करु नका.
- तुमच्या पालकांच्या मार्गदर्शनाखाली आणि देखरेखीखाली असे केल्याशिवाय ऑनलाइन मित्राला कधीही भेटण्यास सहमती देऊ नका.
- तुमच्या खात्याचे पासवर्ड कधीही कोणाशीही शेअर करु नका.
- अश्लील/आक्षेपार्ह /छळवणूक करणारे इमेल/चॅट किंवा पोस्टला प्रतिसाद देऊ नका.

पालकांसाठी सायबर सुरक्षितता टिप्स

DO'S :-

- सुरक्षित ब्राऊझिंग आणि संगणक वापराबद्दल तुमच्या मुलांशी मोकळेपणाने चर्चा करा.
- तुमच्या मुलांना समजावून सांगा की सर्व सोशल नेटवर्किंग प्रोफाइल PRIVATE ठेवाव्यात.
- तुमच्या मुलांना हे समजेल की जर त्यांनी तुम्हाला त्याच्या समस्येबद्दल सांगितले तर ते अडचणीत येणार नाहीत याची खात्री करा.
- जर तुम्हाला तुमच्या मुलाबद्दल अनुचित सामग्री आढळली असेल, तर कृपया लवकरात लवकर जवळच्या पोलीस स्टेशनशी संपर्क साधावा.
- फेसबुक, व्हॉट्सअॅप इत्यादींवर तुमच्या मुलाच्या ONLINE ACTIVITY तपासा. विशेषत जर तुम्हाला वर्तनात अचानक बदल दिसला तर.
- सोशल मीडियाबद्दल स्वत:ला शिक्षित करा आणि किशोरवयीन मुलांशी खुलेपणाने चर्चा करा.
- संगणक उघड्या जागेत ठेवा. मुले ऑनलाइन असताना दरवाजे नेहमीच उघडे ठेवावेत अस नियम बनवा.
- तुमच्या मुलांना अशा कोणत्याही साईटवरुन त्वरित बाहेर पडण्यास सांगा ज्यामुळे त्यांना अस्वस्थ किंवा चिंता वाटेल.

DONT'S :-

- जर वयाची मर्यादा असेल तर तुमच्या मुलाला सोशल मीडिया अकाउंट उघडण्याची परवानगी देऊ नका.
- तुमच्या मुलाला स्नॅपचॅट सारखे अॅप्स वापरण्याची परवानगी देऊ नका जे पोस्ट लगेच डिलीट करतात.
- लहान मुलांना देखरेखीशिवाय अनावश्यकपणे गुगल किंवा इतर सर्च इंजिन ब्राऊझ करु देऊ नका.
- घरात सगंणक वापराच्या शारीरिक पालकांच्या देखरेखीऐवजी कोणत्याही सुरक्षित सर्च इंजिन किंवा इतर कोणत्याही साधनाने बदलू नका.

महिलांसाठी सायबर सुरक्षितता टिप्स

DO'S :-

- तुम्ही कोणती माहिती सार्वजनिक करता याबद्दल निवडक रहा. माहितीमध्ये खरे नाव जन्मतारीख, लिंग, शहर, ई-मेल, पत्ता, शाळेच नाव, कामाचे ठिकाण आणि वैयक्तिक फोटो समाविष्ठ आहेत.
- ज्या लोकांशी तुम्ही संवाद साधू इच्छित नाहीत त्यांना ब्लॉक करा.
- व्हॉट्सॲप आणि इतर मेसेजिंग ॲपवर मीडिया ऑटो-डाउनलोड निष्क्रिय केले आहे याची खात्री करा विशेषत: तुमच्या संपर्क यादीत नसलेल्या पाठवणाऱ्यांकडून.
- वेळोवेळी तुमच्या इंटरनेट संपर्कांचे आणि ऑनलाईन क्रियाकलापांचे पुनरावलोकन करा.
- जर तुम्हाला वाटत असेल की तुमची गोपनीयता/सुरक्षा ऑनलाइन धोक्यात आली आहे तर तावडतोब जवळच्या पोलीस स्टेशनशी संपर्क साधा. तुम्ही https :// cybercrime.gov.in / वर तुमच्या समस्या ऑनलाईन देखील नोंदवू शकता.
- मजबूत पासवर्ड वापरा आणि वेगवेगळ्या खात्यांसाठी वेगवेगळे पासवर्ड वापरा.
- सोशल मीडिया अकाउंटवर तुमच्या गोपनीयता सेटिंग्ज सर्वात कडक पातळीवर ठेवा. फक्त माहित असणे आवश्यक आहे या आधारावर स्वत: बद्दलची माहिती शेअर करा.
- छायाचित्रे पोस्ट करताना अत्यंत सावधगिरी बाळगा आणि ती कोण पाहू शकते यावर नियंत्रण ठेवा.

महिलांसाठी सायबर सुरक्षितता टिप्स

DON'T'S :-

- कधीही नाही ज्या व्यक्तीशी तुम्ही फक्त ऑनलाइन संवाद साधला आहे अशा व्यक्तीला दुसऱ्या कोणाला सोबत न घेता भेटण्याचा प्रयत्न करु नका.
- आणि अशा बैठका नेहमीच सार्वजनिक ठिकाणी असाव्यात.
- तुम्हाला पूर्णपणे अनोळखी लोकांकडून आणि ज्यांच्याशी तुम्ही संवाद साधू इच्छित नाहीत त्यांच्याकडून फ्रेंड रिक्वेस्ट स्वीकारु नका.
- मित्रांसोबतही कोणताही ओटीपी किंवा पासवर्ड शेअर करु नका.
- फेसबुक मेसेंजर किंवा इतर मेसेजिंग सेवांवरुन पाठवलेल्या अनपेक्षित लिंक्सवर क्लिक करु नका जरी त्या तुमच्या मित्राच्या खात्यावरून पाठवल्या गेल्या असल्या तरी.
- केवळ या आधारावर फ्रेंड रिक्वेस्ट स्वीकारु नका की ती व्यक्ती तुमच्या मित्राची परस्पर मित्र आहे.
- मोफत साठी वैयक्तिक माहितीची देवाण घेवाण करु नका.
- सोशल नेटवर्किंग साइट्सवर मोबाईल नंबर आणि वैयक्तिक इमेल आयडीसारखी वैयक्तिक माहिती पोस्ट करु नका.
- तुमचा पासवर्ड कोणाशीही शेअर करु नका किंवा तुमचे खाते दुसऱ्या कोणालाही हाताळू देऊ नका.

सामान्य सायबर सुरक्षा टिप्स

१. अँटीव्हायरस आणि ऑपरेटिंग सिस्टम अपडेट ठेवा.

२. महत्वाचा डेटा नियमितपणे बॅकअप करा.

३. संशयास्पद वेबलिंक्स आणि URL उघडणे टाळा.

४. बाह्य स्टोरेज डिव्हाइस स्कॅन करा.

५. वायरलेस राऊटरची सुरक्षा मजबूत करा (MAC अॅड्रेस फिल्टर आणि पासवर्ड वापरा)

६. संवदेनशील डेटा हटवण्यासाठी फाईल श्रेडर वापरा.

७. नॉन-ऍडमिनिस्ट्रेटर अकाऊंट वापरा.

८. मोबाइलसाठी अँटीव्हायरस इंस्टॉल करा.

९. सार्वजनिक ठिकाणी फोनचा वापर सावधतेने करा.

१०. अनावश्यक प्रोग्राम काढा.

११. फसव्या जाहिराती आणि डिस्काउंट कुपन्सपासून सावध रहा.

१२. बोगस अॅप्स डाउनलोड करु नका.

१३. थर्ड-पार्टी एक्सटेंशन्स टाळा.

१४. ऑटो-फिल टाळा आणि फॉर्म फक्त अधिकृत वेबसाईटवर भरा.

१५. सार्वजनिक संगणकांवर लॉगिन टाळा आणि पासवर्ड SAVE करु नका.

सामान्य सायबर सुरक्षा टिप्स

१६. व्हर्च्युअल कीबोर्ड वापरा आणि नेट बँकिंग सत्रानंतर लॉग ऑफ करा.

१७. ब्राउझिंग इतिहास मिटवा.

१८. MULTIPLE FACTOR AUTHENTICATION लागू करा.

१९. बँक खात्यातील क्रियाकलापांची तपासणी करा.

२०. संशयास्पद व्यवहारांची माहिती तात्काळ कळवा.

२१. सुरक्षित नेटवर्क कनेक्शन वापरा.

२२. संशयास्पद ई-मेल लिंक्सवर क्लिक करु नका.

२३. ओळखपत्रांची फोटो प्रत ठेवू नका.

२४. वैयक्तिक माहिती सोशल मीडियावर शेअर करू नका.

सामान्य सायबर सुरक्षा टिप्स

पोलीसांकडे तक्रार कशी करावी :

- सायबर पोलीस स्टेशन किंवा जवळच्या पोलीस स्टेशनमध्ये तक्रार करा.
- सायबर गुन्हाची नोंद : https://cybercrime.gov.in/ किंवा फोन नंबर 1930/1945 वर करा.
- तक्रारीसह आवश्यक माहिती पोलीस अधिकाऱ्यांना द्या.

फेसबुक किंवा इतर सोशल मीडिया अकाउंटशी संबंधित तक्रारींसाठी :

- बनावट फेसबुक / इंस्टाग्राम अकाउंटचा स्क्रीनशॉट आणि URL घ्या.
- तक्रारीसोबत प्रोफाइल URL नेमूद करा.
- स्व-प्रमाणित ओळखपत्र तक्रारीसोबत जोडा.

आर्थिक फसवणुकीसाठी :

- स्व-प्रमाणित पासबुक/क्रेडिट कार्ड व्यवहार स्टेटमेंट सबमिट करा, व्यवहारांसह बँक खाते नंबर, कार्ड नंबर आणि नोंदणीकृत मोबाईल नंबर समाविष्ट करा.
- नोंदणीकृत मोबाईलवर आलेल्या फसव्या व्यवहार मेसेजचा स्क्रीनशॉट तक्रारीसोबत जोडवा.
- फसव्या व्यवहारांसाठी मिळालेल्या संशयास्पद लिंक किंवा ओटीपीचा स्क्रीनशॉट जोडावा.
- बनावट वेबसाइटशी संबंधित फसवणूकीसाठी वेबसाईटचा स्क्रीनशॉट आणि URL तक्रारीसोबत जोडा.
- फसव्या व्यवहारांसाठी स्व:प्रमाणित प्रत तक्रारीसोबत जोडावी.

सामान्य सायबर सुरक्षा टिप्स

सायबर सुरक्षित राहण्यासाठी पालघर जिल्हा पोलीस दलाच्या सोशल मिडीया साईटला भेट द्या व सायबर क्राईम बाबत माहिती जाणुन घ्या.

- PALGHAR POLICE HELPLINE NUMBERS
- EMERGENCY NUMBER – 112
- COSTAL HELPLINE – 1093
- CYBER HELPLINE- 8806704075
- FINANCIAL/ONLINE FRAUD – 1930/1945
- WOMEN & CHILD HELPLINE – 8669609544
- CONTROL HELPLINE – 112
- CONTROL WHATSAPP NUMBER – 9730711119

सोशल मीडिया साईट्स –

- पालघर पोलीस वेबसाईट :-
  https://palgharpolice.gov.in/
- पालघर पोलीस सायबर ए. आय. चॅटबॉट :-
  https://strong-tartufo-be0d96.netlify.app/
- पालघर पोलीस व्हॉट्सॲप चॅटबॉट:-
  https://wa.me/918806704075
- पालघर पोलीस इंस्टाग्राम :
  https://www.instagram.com//palghar.police?igsh=a3Rod
- पालघर पोलीस ट्विटर :-
  https://twitter.com//palghar_police
- पालघर पोलीस फेसबुक पेज :-
  https://www.facebook.com/palghar District Police?mibextid=ZbWKWL
- पालघर पोलीस युट्युब चैनल :-
  https://youtube.com/@palgharpolice1335?si=KSDSeAGKynJJP5Yh

Palghar Police
वेबसाईट वरील नवीन टॅब
palgharpolice.gov.in

औद्योगिक संदर्भात तक्रार

उद्योजकांना औद्योगिक समस्यांसंबधी तक्रारींसाठी वेबसाईट वर नवीन टॅब देण्यात आलेला आहे.

हरवलेले / सापडलेली माहिती कळवा

नागरिकांच्या हरवलेल्या वस्तू, कागदपत्र व इतर ओळखपत्र हरवल्यास नागरिक सदर सुविधेचा वापर करुन पोलीसांना माहिती देऊ शकतात.

ई-चलन पेमेंट

नागरिकांनी वाहतूक नियमाचे उल्लंघन केल्यास इ-चलन प्रणालीद्वारे ऑनलाइन पेमेंट करता येते.

सिटीझन पोर्टल

या पोर्टलद्वारे नागरिक विविध तक्रारी नोंदवू शकतात, शासकीय सेवा ऑनलाईन मिळवू शकतात आणि महत्वाच्या दस्तऐवजांची पडताळणी करू शकतात.

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल

नागरिक सायबर गुन्ह्यांबाबत तक्रार करु शकता. विशेषत: महिला आणि मुलांविरुध्द सायबर गुन्हे, ऑनलाइन फसवणूक, सोशल मीडिया गैरवापार, फिशिंग, हॅकिंग, डेटा चोरी इत्यादी घटनांसाठी हे उपयुक्त आहे.

आवाहन

सायबर गुन्हेगारांनी रचलेल्या सापळ्यात न अडकता सायबर गुन्हांशी लढण्यात कृपया आम्हाला मदत करा. तसेचं, सर्व सायबर फसवणूकीच्या प्रयत्नांची तक्रार करा. यामुळे सायबर गुन्हेगारांना पकडण्यात आणि ते इतर कोणाचीही फसवणूक करण्यापूर्वी त्यांना न्याय मिळवून देण्यात मदत होईल.

धन्यवाद !

सायबर योध्दा प्रशिक्षण

श्री विनायक नरळे

अपर पोलीस अधीक्षक पालघर
सायबर योध्दांना मार्गदर्शक करतांना

श्रीमती संगीता शिंदे अल्फोन्सो

पोलीस उपअधीक्षक (गृह)
सायबर योध्दांना मार्गदर्शक करतांना

सायबर पोलीस स्टेशन पालघर, अधिकारी व अंमलदार