साइबर सुरक्षा

–जागरूकता पुस्तिका

प्रस्तावना

सूचना और संचार टेक्नोलॉजी आज हमारे दैनिक जीवन का एक अभिन्न अंग बन गया है। इसने हमारे जीवन में दोस्तों के साथ जुड़ने, नौकरी खोजने, शादी करने हेतु जीवनसाथी खोजने, व्यवसाय चलाने, खेल खेलने, शॉपिंग करने इत्यादि के तरीके को बदल दिया है। ब्रॉडबैंड और स्मार्टफोन की सस्ती उपलब्धता के बाद लगभग हर किसी की पहुंच साइबर स्पेस तक हो गयी है, जो दुनिया भर में लगभग करोड़ों ऑनलाइन उपयोगकर्ताओं को जोड़ता है। साइबर स्पेस के बढ़ते उपयोग ने हमें साइबर क्राइम के खतरों के प्रति सुभेद्य बना दिया है। हमारे द्वारा डिजिटल जीवन के प्रबंधन में मामूली चूक व लापरवाही साइबर अपराधियों के लिए दरवाजे खोल सकती है और इससे हमें वित्तीय नुकसान, प्रतिष्ठा का नुकसान, मानसिक उत्पीड़न इत्यादि हो सकता है। अतः यह आवश्यक है कि हम बाहरी डिजिटल दुनिया से वित्तीय लेन–देन, सोशल नेटवर्किंग, गेम खेलने या इंटरनेट पर चीजें खोजने इत्यादि हेतु जुड़ते समय सतर्कता और सावधानी बरतें।

इस पुस्तिका में दी गई जानकारी का उद्देश्य नागरिकों में विभिन्न प्रकार के साइबर अपराध, जो उन्हें प्रभावित कर सकते हैं, के खतरों के बारे में जागरूकता फैलाना तथा खुद को उससे सुरक्षित रखने के लिए कुछ उपायों के बारे में जानकारी देना है।

पुस्तिका का प्रारंभिक भाग इन दिनों प्रचलित विभिन्न प्रकार के साइबर अपराधों का उल्लेख करता है, जिनका वर्गीकरण उनकी अपराध शैली (Modus Operandi) के अनुसार किया गया है। साइबर अपराध की प्रत्येक अपराध शैली के संबंध में सर्वप्रथम उसकी संक्षिप्त जानकारी शीर्ष पर बने बॉक्स में दी गई है। उसके नीचे एक चित्रात्मक विवरणी दी गई है, जिसमें यह प्रदर्शित किया गया है कि कैसे साइबर अपराधियों ने पीड़ित को उस विशेष साइबर अपराध शैली के माध्यम से घटना का शिकार बनाया। हमने इसे सरल रखने की कोशिश की है ताकि आम आदमी भी इसे आसानी से समझ सके। पृष्ठ के निचले बॉक्स में वैसे सुझाव/संभव तरीके दिये गये हैं जिन्हें अपनाकर कोई भी व्यक्ति उस विशिष्ट साइबर अपराध/फ्रॉड से बच सकता है।

पुस्तिका में बताए गए विभिन्न प्रकार के साइबर अपराधों के तौर–तरीकों में कुछ परस्पर समानताएं पाई जा सकती है। फिर भी उन पर अलग से चर्चा की गई है क्योंकि साइबर अपराधी बहुत ही सूक्ष्म अंतर के साथ उन तौर–तरीकों का अक्सर उपयोग करते हैं, जिसके कारण कई लोग इनका शिकार बन जाते हैं। इस छोटी सी पुस्तिका में सभी अलग–अलग तौर–तरीकों को शामिल करना संभव नहीं है। अतः पुस्तिका के अंत में साइबर स्पेस में स्वयं को सुरक्षित रखने हेतु कुछ महत्वपूर्ण सामान्य सुझाव दिए गये हैं। जिन व्यक्तियों के पास सभी अपराध शैलियों के बारे में विस्तृत रूप से पढ़ने का समय नहीं है, वे कम–से–कम इन सामान्य सुझावों को अवश्य पढें व अपनायें ताकि वे साइबर अपराध का शिकार होने से बच सकें।

अक्तूबर, 2021

भारत में साइबर अपराध

साइबर धोखाधड़ी में हर गुजरते साल में भारी वृद्धि देखी गई है, क्योंकि बैंकिंग प्रणाली और भुगतान तंत्र ऑनलाइन तरीके में स्थानांतरित हो गए हैं, जागरूकता की कमी के कारण मामलों में तेजी आई है।

स्टेटिस्टा की नवीनतम रिपोर्ट के अनुसार, भारत में इंटरनेट का इस्तेमाल दर 2021 में लगभग 45 प्रतिशत तक पहुंच गई, जो 2007 में केवल चार प्रतिशत थी। हालांकि ये आंकड़े अपेक्षाकृत कम लगते हैं। सक्रिय इंटरनेट उपयोगकर्ताओं के मामले में भारत दुनिया में दूसरा स्थान रखता है।

भारतीय दूरसंचार विनियामक प्राधिकरण (TRAI) के अनुसार भारत में लगभग 800 मिलियन से अधिक सक्रिय मोबाइल इंटरनेट उपयोगकर्ता हैं और प्रति उपयोगकर्ता औसत मासिक डेटा खपत लगभग 13 जीबी है। भारत में दुनिया में सबसे सस्ती इंटरनेट डेटा सेवाएं भी हैं। 1 जीबी डेटा की कीमत भारत में लगभग ₹ 6.75 है, जबकि यूएस में औसत $8 और यूके में $1.4 है।

कुछ सर्वेक्षण कंपनियों ने 10 देशों – ऑस्ट्रेलिया, फ्रांस, जर्मनी, भारत, इटली, जापान, नीदरलैंड, न्यूजीलैंड, यूनाइटेड किंगडम (यूके) और संयुक्त राज्य अमेरिका (यूएस) में 10,000 से अधिक वयस्कों का सर्वेक्षण किया। इनमें से 1,000 वयस्क भारत के थे। रिपोर्ट के अनुसार, पिछले 12 महीनों में 27 मिलियन भारतीय वयस्क पहचान की चोरी (Identity theft) के शिकार हुए हैं और देश में 52% वयस्क नहीं जानते कि साइबर अपराध से खुद को कैसे बचाया जाए।

विषय–सूची

साइबर सुरक्षा का महत्व

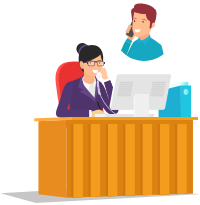
उन्नत तकनीकों ने आधुनिक जीवन शैली को बदल दिया है। इंटरनेट हमें कई लाभ प्रदान करता है। चाहे वह दोस्तों के साथ संवाद करना हो, सूचनाओं की खोज करना हो, ऑनलाइन सेवाओं का लाभ उठाते हुए बैंकिंग लेनदेन करना हो, नौकरी ढूंढना हो, जीवनसाथी की तलाश करना हो या यहां तक कि पूरे व्यवसाय को चलाना हो। इंटरनेट हमारे जीवन के लगभग सभी पहलुओं को छूता है। हालाँकि, यह हमें कई तरह के खतरों के प्रति संवेदनशील भी बनाता है। इंटरनेट पर नियमित रूप से नए और शक्तिशाली साइबर हमले हो रहे हैं। हमारे डिजिटल जीवन को प्रबंधित करने में एक छोटी सी चूक साइबर अपराधियों के लिए द्वार खोल सकती है। साइबर अपराधी हमारा पैसा चुरा सकते हैं या हमारी प्रतिष्ठा को नुकसान पहुंचा सकते हैं। एक प्रमुख उद्योग अनुसंधान संगठन के एक अध्ययन के अनुसार, सभी साइबर हमलों में से 90% मानवीय लापरवाही के कारण होते हैं। इसलिए साइबर सुरक्षा के प्रति जागरूकता आज सभी के लिए जरूरी है।

साइबर खतरों के जोखिम को कम करने के लिए टेक्नोलॉजी का उपयोग करते समय हमें सतर्क रहना चाहिए।

सोशल इन्जिनियरिंग फर्जीवाड़ा

सी.वी.वी./ओ.टी.पी. शेयरिंग फर्जीवाड़ा

साइबर अपराधी बैंक व भारतीय रिजर्व बैंक अधिकारी बन कर लोगों को फोन करते हैं और उनसे कहते हैं कि उनका ए.टी.एम. कार्ड ब्लॉक हो गया है या उनका के.वाई.सी. अपडेट नहीं है या उनका आधार बैंक खाते से जुड़ा नहीं है और इसलिए उनका खाता ब्लॉक किया जाएगा । फिर आधार को बैंक खाते से जोड़ने, के.वाई.सी. अपडेट कराने, या नया ए.टी.एम. कार्ड शुरू करने के बहाने उनसे उनके खाते से जुड़े गोपनीय जानकारी जैसे ए.टी.एम. नंबर, सी.वी.वी. नंबर, ओ.टी.पी. इत्यादि जानकारी प्राप्त कर लेते हैं। जैसे ही ये जानकारी साइबर अपराधियों को मिलती है वे संबंधित व्यक्ति के खाते से पैसे निकाल लेते हैं।



साइबर अपराधी बैंक व आर.बी.आई. अधिकारी का प्रतिरूपण कर फोन करते हैं। के.वाई.सी. व आधार अपडेट या नए ए.टी.एम. कार्ड की सक्रियता को बनाये रखने के बहाने,साइबर अपराधी ए.टी.एम. कार्ड नंबर और ओ.टी.पी. की मांग करते हैं।

पीड़ित

पीड़ित ए.टी.एम. कार्ड एवं गोपनीय जानकारी साझा कर देता है।

पीड़ित सी.वी.वी. नंबर भी साझा कर देता है।

पीड़ित अपने मोबाइल पर प्राप्त ओ.टी.पी. को साइबर अपराधी के साथ साझा कर देता है।

पीडित का बैंक खाता

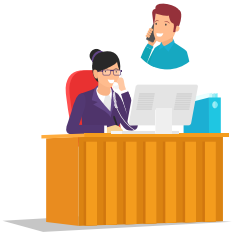
साइबर अपराधी पीड़ित के पैसों को अन्य ई–वॉलेट, यू.पी.आई. अकाउंट में हस्तांतरित कर लेता है या इससे खरीददारी कर लेता है।

सुझाव

- ध्यान रखें कि बैंक कभी भी ए.टी.एम. नंबर, सी.वी.वी. नंबर, ओ.टी.पी. इत्यादी गोपनीय जानकारी की मांग नहीं करता है।
- व्हाट्सएप मैसेज, फोन या अन्य सोशल मीडिया के माध्यम से कभी भी किसी को ए.टी.एम. नंबर, सी.वी.वी. नंबर, ओ.टी.पी. इत्यादी गोपनीय जानकारी साझा न करें।
- ई–मेल आई.डी. को साझा नहीं किया जाना चाहिए क्योंकि इसका उपयोग कर साइबर अपराधी इंटरनेट बैंकिग को एक्टिवेट कर खाते में उपलब्ध राशि को हस्तांतरित कर सकते हैं।

यू.पी.आई. फिशिंग फर्जीवाड़ा

साइबर अपराधी बैंकिंग या अन्य ई–कॉमर्स की समस्या को सुलझाने के बहाने पीड़ित के बैंक के साथ पंजीकृत मोबाइल नंबर से अल्फान्यूमेरिक लिंक को किसी खास नंबर (अलग–अलग बैंक पर निर्भर) पर फॉरवर्ड करवा लेते हैं और एक बार लिंक फॉरवर्ड होने के पश्चात् सिम बाईन्डिग को दरकिनार कर पीड़ित के खाते से संबंधित यू.पी.आई. वॉलेट अपने मोबाइल में इंस्टॉल कर लेते हैं। इस प्रकार पीड़ित के मोबाइल नंबर से जुड़े खातों तक पहुंच बना पैसे की अवैध निकासी कर लेते हैं।



साइबर अपराधी पीड़ित को कॉल कर के.वाई.सी. अपडेट करने या आधार को खाते से जोड़ने के बहाने अल्फान्यूमेरिक लिंक या ओ.टी.पी. को किसी खास नंबर पर फॉरवर्ड करने के लिए कहता है।

पीड़ित ओ.टी.पी. व पिन को साझा कर देते हैं।

साइबर अपराधी अब अपनी पहुंच पीड़ित के बैंक से जुड़े यू.पी.आई. वॉलेट तक बना लेता है एवं अपने अनुसार एम.पिन बना लेता है।

साइबर अपराधी पीड़ित के खाते को अब अपने अनुसार उपयोग करते हैं।

पीड़ित के खाते से पैसों की अवैध निकासी शुरू हो जाती है एवं तब तक नहीं रूकती जब तक वह अपने अकाउंट को ब्लॉक नहीं करा लेता है या यू.पी.आई. से डिलिंक नहीं करा लेता है।

सुझाव

- कभी भी कोई लिंक या ओ.टी.पी. को किसी नंबर पर फॉरवर्ड न करें।
- लोग विभिन्न ई–कॉमर्स कंपनी इत्यादि के कस्टमर केयर नंबर गूगल सर्च के माध्यम से प्राप्त नंबर पर बात करने के पश्चात इस प्रकार की ठगी का शिकार हुये हैं। अतः कभी भी कस्टमर केयर अधिकारी का नंबर गूगल सर्च पर न प्राप्त करें। इस कार्य हेतु एयरलाइंस/ई–कॉमर्स कंपनी की आधिकारिक वेबसाइट का ही इस्तेमाल करें।

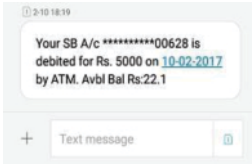
रिक्वेस्ट मनी क्यूआर कोड/लिंक के माध्यम से गुगल पे/फोन पे/पे.टी.एम. पर फर्जीवाड़ा

साइबर अपराधी द्वारा व्यक्ति को पैसा प्राप्त करने हेतु लिंक क्लिक कर या क्यूआर कोड स्कैन कर पैसा अपने खाते में लेने की बात करते हैं परंतु जैसे ही व्यक्ति के द्वारा इसे स्कैन या क्लिक किया जाता है, व्यक्ति के खाते से पैसे की निकासी हो जाती है, क्योंकि यह पैसा प्राप्ति का क्यूआर कोड/लिंक होता है।

जालसाज किसी दुकानदार/व्यापारी को कॉल कर पैसों के भुगतान के लिए गूगल पे या फोनपे के साथ पंजीकृत मोबाइल नंबर की मांग करता है।

पीड़ित पंजीकृत मोबाइल नंबर साझा कर देता है एवं जालसाज द्वारा दिये गये लिंक या क्यूआर कोड प्राप्त कर लेता है।

क्यूआर कोड को साइबर अपराधी द्वारा पैसा रिफंड या कैशबैक इत्यादि लिख इस प्रकार संपादित कर दिया जाता है कि पीड़ित उनके बातों पर भरोसा कर लें, जबकि वास्तव में यह निकासी लिंक/क्यूआर कोड होता है।



पीडित बैंक खाते के साथ पंजीकृत फोन नंबर पर आये मैसेज पर ध्यान नहीं देता है।

निकासी लिंक या क्यूआर कोड को स्कैन कर पीड़ित पैसा प्राप्त करने के बजाए खुद पैसा अपने खाते से स्थानान्तरित कर देता है।

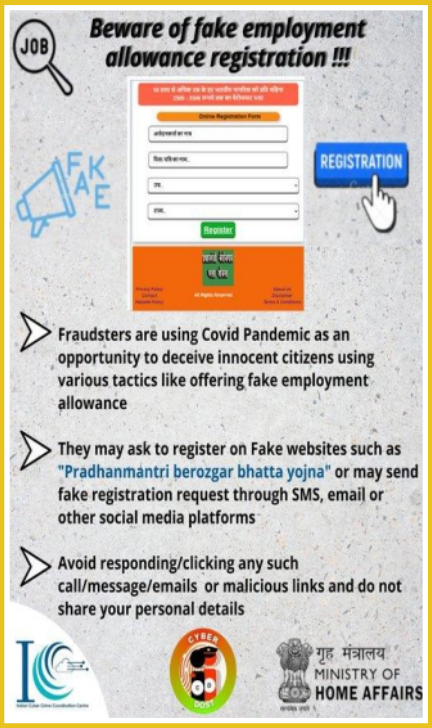
सुझाव

- किसी भी अज्ञात स्त्रोत से प्राप्त किसी भी प्रकार के लिंक या क्यूआर कोड पर क्लिक/स्कैन न करें।
- पैसे की प्राप्ति करने हेतु कभी भी एम.पिन या यू.पी.आई. पिन दर्ज करने की आवश्यकता नहीं होती है।

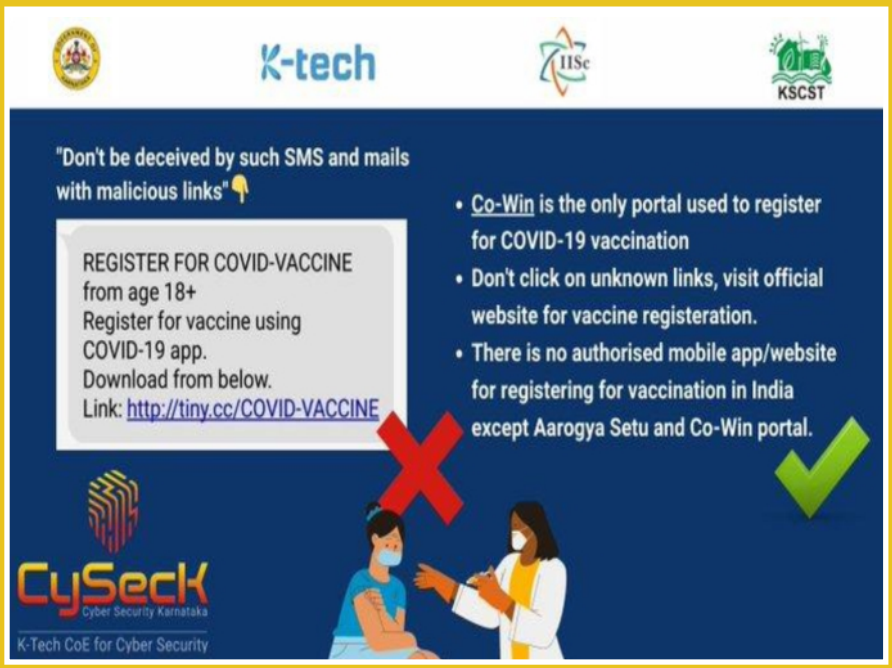

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
"ऑन लाइन Earning App" धोखाधड़ी
वर्तमान महामारी के दौरान, साइबर अपराधी, आकर्षक ऑफर का वादा करके ऑनलाइन कमाई करने वाले ऐप द्वारा मासूम/अनभिज्ञ लोगों को ठग रहे हैं।
साइबर अपराधी, लोगों को अपनी गाढ़ी कमाई को ऑनलाइन ऐप में निवेश करने के लिए समझा लेते हैं, उच्च रिटर्न का वादा करते हैं किन्तु निवेश वापसी संदेहास्पद होती हैं।
हमेशा आरबीआई / सेबी द्वारा विनियमित कंपनियों में निवेश करें और त्वरित लाभ की उम्मीद में संदेहास्पद ऐप्स में निवेश करने से बचें ।
CASH BACK
www.cybercrime.gov.in


गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
1 Covid-19 vaccination certificate contains your name and other personal details.
2 Avoid sharing your vaccination certificate on social media platforms as it may be misused by cyber fraudsters to defraud you.
"Be aware and be cybersafe"
www.cybercrime.gov.in
@Cyberdost


THIS CALL IS FRAUD.
BEWARE OF FRAUDSTERS!
Forwarded
Just now my friend received a call from 912250041117 asking him to press 1 if he had vaccinated. He pressed 1. Immediately the phone was blocked and his phone had been hacked. So be careful when you get similar calls. (Rec'd from a colleague). Msg rec'd in other grp. But be alert. Also inform all senior citizens. and friends
FAKE
#PIBFactCheck
Send us your queries here
Follow us on social media!

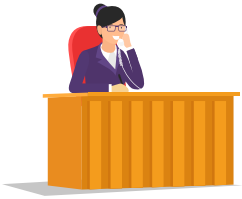

JOB
Beware of fake employment allowance registration !!!
FAKE
REGISTRATION
Register
Fraudsters are using Covid Pandemic as an opportunity to deceive innocent citizens using various tactics like offering fake employment allowance
They may ask to register on Fake websites such as "Pradhanmantri berozgar bhatta yojna" or may send fake registration request through SMS, email or other social media platforms
Avoid responding/clicking any such call/message/emails or malicious links and do not share your personal details
CYBER DOST
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

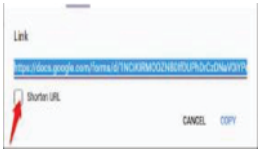

JOB
बेरोजगारी भत्ता योजना" धोखाधड़ी
FAKE
REGISTRATION
Register
साइबर अपराधी इस महामारी का इस्तेमाल, मासूम/अनभिज्ञ लोगों को फर्जी रोजगार भत्ता की पेशकश कर, ठगने के अवसर के रूप में कर रहे है।
वे लोगों को "प्रधानमंत्री बेरोजगारी भत्ता योजना" जैसी नकली वेबसाइटों में पंजीकरण करने के लिए कह सकते हैं या एसएमएस, ईमेल या अन्य सोशल मीडिया प्लेटफॉर्म के माध्यम से फर्जी पंजीकरण अनुरोध भेज सकते हैं।
इन नकली वेबसाइटों से सतर्क रहें और किसी भी कारण से संदिग्ध होने पर अनजान कॉल/संदेश/ईमेल आदि का जवाब न दें और अपनी व्यक्तिगत जानकारी साझा न करें।
CYBER DOST
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS


K-tech
IISc
KSCST
"Don't be deceived by such SMS and mails with malicious links"
REGISTER FOR COVID-VACCINE
from age 18+
Register for vaccine using COVID-19 app.
Download from below.
Link: http://tiny.cc/COVID-VACCINE
Co-Win is the only portal used to register for COVID-19 vaccination
Don't click on unknown links, visit official website for vaccine registeration.
There is no authorised mobile app/website for registering for vaccination in India except Aarogya Setu and Co-Win portal.
CySecK
Cyber Security Karnataka
K-Tech CoE for Cyber Security

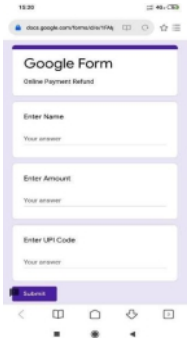
गुगल डॉक्स ऐप के जरिए फर्जीवाड़ा

किसी से जानकारी प्राप्त करने हेतु ऑनलाइन फॉर्म गूगल डॉक्स इत्यादि का व्यापक रूप से उपयोग किया जाता है। साइबर अपराधी द्वारा इन एप्लीकेशन का दुरूपयोग कर पीड़ित से बैंकिग लेन–देन से संबंधित गोपनीय जानकारी जैसेः ए.टी.एम. नंबर, यू.पी.आई. पिन, पासवर्ड इत्यादि दर्ज करवा लिया जाता है। जैसे ही पीड़ित फॉर्म में बैंक से सम्बंधित गोपनीय जानकारी भरता है, यह गोपनीय जानकारी साइबर जालसाज द्वारा प्राप्त कर लिया जाता है और इसके माध्यम से पीड़ित के खाते से पैसों की अवैध निकासी कर ली जाती है।





साइबर अपराधी गुगल डॉक्स फॉर्म के लिए लिंक भेजता है। वह आपको यह लिखकर गुमराह करते हैं कि पैसा रिफंड करने के लिए यह फॉर्म भरना आवश्यक है।



साइबर अपराधी पीड़ित व्यक्ति को उसके गोपनीय बैंक संबंधित जानकारी जैसे ए.टी.एम. नंबर, यू.पी.आई. पिन और पासवर्ड आदि भरने या जमा करने के लिए गुमराह करता है।

जैसे ही पीडित फॉर्म में बैंक से संबंधित गोपनीय जानकारी भरता है यह गोपनीय जानकारी साइबर जालसाज द्वारा प्राप्त कर लिया जाता है

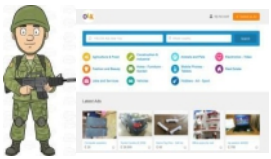
साइबर अपराधी अब पीड़ित के खाते से पैसों की अवैध निकासी कर लेता है।

सुझाव

- आपको सलाह दी जाती है कि गुगल डॉक्स जैसे ऑनलाइन फॉर्म में गोपनीय बैंकिंग विवरणी कभी भी साझा न करें।
- बैंक कभी भी ऐसे ऑनलाइन फॉर्म भरने को नहीं कहता है।

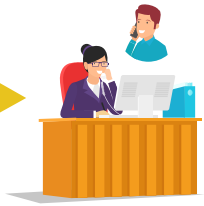
ओ.एल.एक्स./ई-कॉमर्स प्लेटफॉर्म्स के जरिए फर्जीवाड़ा

साइबर अपराधी ई–कॉमर्स वेबसाइट जैसे–ओ.एल.एक्स., क्विकर, फेसबुक इत्यादि का प्रयोग वस्तुओं का आकर्षक मूल्य रख फर्जी विज्ञापन के माध्यम से साइबर ठगी का कार्य करते हैं। जब भी कोई व्यक्ति इनकी खरीददारी हेतु उनसे संपर्क करता है तो वे पैकेजिंग चार्ज, रजिस्ट्रेशन चार्ज, ट्रांसपोटेशन चार्ज, टैक्स इत्यादि के बहाने अग्रिम राशि की मांग करते हैं। व्यक्ति इसे वास्तविक विज्ञापन समझ अग्रिम पैसों की भुगतान कर देते हैं और साइबर ठगी का शिकार हो जाते हैं। साइबर अपराधी कभी खुद ग्राहक बनकर वस्तुओं को इन ई–कॉमर्स वेबसाइट बेचने वाले से भी पैसा ठग लेते हैं। इस अपराध शैली में वे मालिक को अग्रिम राशि का भुगतान करने हेतु क्रेडिट लिंक/क्यूआर कोड भेजने के बजाय डेबिट लिंक/क्यूआर कोड भेजते हैं एवं इसे स्कैन या क्लिक करने के पश्चात् पीड़ित के खाते से पैसे की निकासी हो जाती है।



सेना/अर्ध–सैनिक बल के जवान वस्तुओं (वाहन, मोबाइल इत्यादि) को बेचने के लिए ओ.एल.एक्स., क्विकर, फेसबुक इत्यादि में विज्ञापन डालते हैं।

साइबर अपराधी विज्ञापन में प्रदर्शित वस्तु को खरीदने के बहाने उनसे संपर्क करते हैं एवं उनके पहचान पत्र, कैंटीन कार्ड एवं अन्य दस्तावेज प्राप्त कर लेते हैं।



साइबर अपराधी फिर उनके पहचान पत्र एवं अन्य दस्तावेज का प्रयोग कर खुद फर्जी विज्ञापन ओ.एल.एक्स. या फेसबुक में डाल देते हैं।

आकर्षक कीमत देख खरीददार साइबर अपराधी को सेना/अर्ध–सैनिक बल का सदस्य समझ संपर्क करता है।

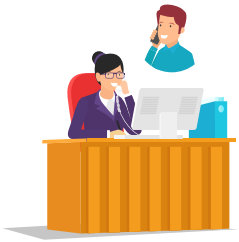
जीएसटी/ट्रांर्पोटेशन चार्ज/पैकेजिंग चार्ज/रजिस्ट्रेशन चार्ज इत्यादि के बहाने साइबर अपराधी खरीददार से अग्रिम राशि प्राप्त कर लेते है।

सुझाव

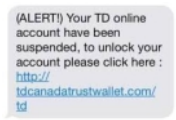
- इन वेबसाइट के माध्यम से खरीददारी करते वक्त कभी भी किसी प्रकार का अग्रिम भुगतान न करें एवं खरीददारी या बेचने से पूर्व सम्बंधित व्यक्ति से मिलकर वस्तु की जाँच अवश्य करें।
- क्यूआर कोड या लिंक के माध्यम से किसी भी तरह के पैसों की प्रप्ति के लिए एम.पिन या यू.पी.आई. पिन की आवश्यकता नहीं होती है।
- हमेशा ध्यान रहे कि एम.पिन. या यू.पी.आई. पिन की जरूरत सिर्फ पैसों के भुगतान के लिए होती है, न कि प्राप्ति के लिए।

फर्जी कैशबैक ऑफर्स के जरिए फर्जीवाड़ा

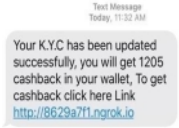
साइबर अपराधी पीड़ित को फोनपे/गूगल पे इत्यादि पर कैशबैक का झूठा लालच देते हैं एवं कैशबैक की प्राप्ति हेतु लिंक को क्लिक कर/क्यूआर कोड को स्कैन कर राशि को अपने खाते में जमा करने के लिए कहते हैं। जैसे ही पीड़ित लिंक को क्लिक करने के पश्चात् यू.पी.आई. या एम. पिन अंकित करता है उनके खाते में पैसा जमा होने के बजाए उसके खाते से पैसे की निकासी हो जाती है। ये लिंक इस प्रकार के हो सकते हैं **http://8629a7f1.ngrok.io or SMS 1533c608933b85f448a7428b4365a042ae6**



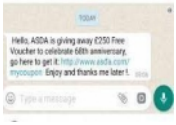
जालसाज पीड़ित को झूठा कैशबैक का लालच देते हैं।



या



या



यहां लिखी बातों से भ्रमित न हो।

जालसाज क्यूआर कोड पर पेमेंट रिफंड या कैशबैक इत्यादि लिख पीड़ित को भ्रमित करने का काम करता है।

पैसा प्राप्त करने के बजाए पीड़ित क्यूआर कोड व डेबिट लिंक के माध्यम से यू.पी.आई. पिन व एम.पिन अंकित कर खुद पैसा साइबर अपराधी के खाते में हस्तांतरित कर देता है।

पीड़ित यहाँ लिखे बातों पर ध्यान नहीं देते हैं

सुझाव

- कभी भी असत्यापित स्त्रोत से प्राप्त लिंक को क्लिक या अग्रसर न करें।
- ध्यान रखे एम.पिन या यू.पी.आई. पिन अंकित करने की आवश्यकता केवल पैसों को दूसरे के खातों में हस्तांतरित करने के लिए होती है न कि प्राप्ति के लिए।

स्क्रीन शेयरिंग ऐप्स के जरिए फर्जीवाड़ा

साइबर अपराधी पीड़ित को बैंकिंग कार्यो में मदद करने या कंपनी की पॉलिसी का बहाना बना पीड़ित को मोबाइल में स्क्रीन शेयरिंग ऐपलिकेशन जैसे एनीडेस्क/क्विकसपोर्ट इत्यादि डाउनलोड व इंस्टॉल करवाकर पीड़ित के मोबाइल तक अपनी पहुंच बना पीड़ित के बैंक से सम्बंधित गोपनीय जानकारी जैसे सी.वी.वी. नंबर, ओ.टी.पी. इत्यादि प्राप्त कर लेते हैं तथा उसके पश्चात् पीड़ित के खाते से पैसों की अवैध निकासी शुरू कर देते हैं। जब तक पीड़ित को इस अवैध निकासी का एहसास होता है तब तक पीड़ित के खाते से काफी पैसे की निकासी हो चुकी होती है।

एनीडेस्क

या

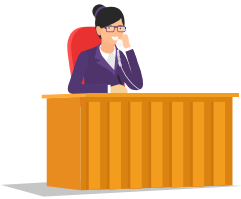
व्यक्ति गुगल सर्च के माध्यम से बैंक या ई – कॉमर्स सेवाओं के कस्टमर केयर अधिकारी का नंबर खोज उन्हें कॉल करते हैं।

या

क्विकसपोर्ट

साइबर अपराधी स्वयं को ऑपरेटर बताते हुये पीड़ित को उपरोक्त में से किसी भी स्क्रीन साझा करने वाले ऐप को इंस्टॉल कर एवं सम्बंधित कोड को साझा करने के लिए कहते हैं जिससे पीड़ित के फोन के स्क्रीन तक पहुँच बनाई जाती है।

पीड़ित कोड को साइबर अपराधी से साझा कर देते हैं।



साइबर अपराधी पीड़ित के फोन तक अपनी पहुचं बना बंकै से संबंधित गोपनीय जानकारी चुरा लेता है।

अब वह पीड़ित के खाते से पैसों को अपने अकाउंट में ट्रांसफर कर लेता है। इसके लिए किसी भी प्रकार की ओ.टी.पी. की आवश्यकता नहीं होती है।

सुझाव

- फोन के माध्यम से किसी कम्पनी के अधिकारी के कहे जाने पर कभी भी किसी प्रकार का स्क्रीन शेयरिंग ऐप डाउनलोड न करें।
- ध्यान रहे बैंक/ई–कॉमर्स कंपनी इत्यादि कभी भी किसी तृतीय पक्ष का स्क्रीन शेयरिंग ऐप इत्यादि डाउनलोड करने के लिए नहीं कहता है।

सिम कार्ड स्वैपिंग फर्जीवाड़ा

यह एक प्रकार से व्यक्ति की पहचान की चोरी (Identity theft) है जहां साइबर अपराधी टेलीकॉम सेवा प्रदाता के माध्यम से आपके पंजीकृत मोबाइल नंबर के लिए जारी किए गए पुराने सिम कार्ड के जगह नए सिम कार्ड को प्राप्त कर लेते हैं। नए सिम कार्ड की मदद से साइबर अपराधी पीड़ित के बैंक खाते से वित्तीय लेनदेन के लिए आवश्यक ओ.टी.पी. और अन्य गोपनीय जानकारी प्राप्त कर लेते हैं।

साइबर अपराधी किसी खुदरा विक्रेता से एक खाली सिम कार्ड प्राप्त कर लेता है। (जो उसी गिरोह के सदस्य भी होते हैं)

साइबर अपराधी अब कस्टमर केयर अधिकारी बनकर पीड़ित को कॉल करते हैं तथा अपने सिम को 4जी में बदलने हेतु कहते हैं अन्यथा सिम बंद हो जाने की बात बताते हैं।

सिम स्वैप करने हेतू वे एक सिम नंबर पीड़ित को देते हैं और उन्हें यह नंबर कस्टमर केयर अधिकारी को अग्रेषित/फॉरवर्ड करने के लिए कहते हैं।

पीड़ित उसे वास्तविक समझ अपने मोबाइल से सिम नंबर को कस्टमर केयर अधिकारी को अग्रेषित/फॉरवर्ड कर देता है।

मोबाइल सेवा प्रदाता कंपनी पीड़ित के पुराने सिम को बंद कर उसी नंबर से नया सिम साइबर अपराधी को जारी कर देता है।

अब साइबर अपराधी पीड़ित के मोबाइल नंबर से पंजीकृत सभी बकैं खातो ं तक अपनी पहुचं बना लेता ह ै तथा पैसों की अवैध निकासी कर लेता है।

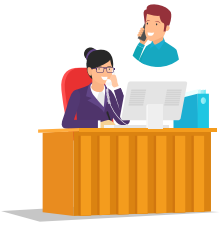
सुझाव

- फोन कॉल पर कभी भी अपने खाते और सिम से सम्बंधित कोई भी जानकारी साझा न करें। सिम के पीछे वर्णित सिम संख्या बहुत महत्वपूर्ण गोपनीय जानकारी होती है।
- यदि आपका मोबाइल नंबर कुछ घंटों के लिए निष्क्रिय व नेटवर्क क्षेत्र से बाहर हो जाता है, तो तुरंत इस संदर्भ में अपने मोबाइल ऑपरेटर से पूछताछ करें।
- अपने बैंकिंग लेनदेन के लिए नियमित एस.एम.एस. के साथ–साथ ई–मेल अलर्ट के लिए रजिस्टर करें। इस तरह, सिम स्वैप होने के पश्चात् बैंक से अवैध निकासी होने पर आपको इसकी जानकारी ई–मेल के माध्यम से मिल सकती है और आप इसे रोक सकते हैं।

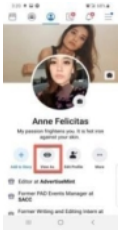
सोशल मीडिया प्लेटफार्म्स का उपयोग कर किये जाने वाले वित्तीय फर्जीवाड़ा

फर्जी सोशल मीडिया अकाउंट के द्वारा फर्जीवाड़ा

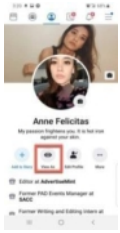
साइबर अपराधी प्रचलित सोशल मीडिया जैसे फेसबुक/इंस्टाग्राम अकाउंट को लक्षित करते हैं। वे किसी अकाउंट से मिलता–जुलता फेक अकाउंट बना उनके दोस्तों या रिश्तेदारों से किसी मेडिकल इमरजेंसी इत्यादि का बहाना बनाकर पीड़ित के दोस्तों से पैसे की मांग करते है। पीड़ित का दोस्त उसे अपना वास्तविक दोस्त समझ कर पैसा ट्रांसफर कर देता है। जब तक पीड़ित को इसका एहसास होता है तब तक कई लोग पैसा ट्रांसफर कर फर्जीवाड़ा का शिकार बन चुके होते हैं। किसी व्यक्ति का फेसबुक अकाउंट हैक कर भी इसी तरह का साइबर अपराध किया जाता है।



साइबर अपराधी द्वारा पीड़ित के अकाउंट से मिलता–जुलता फर्जी प्रोफाइल बनाया जाता है।



वास्तविक फेसबुक प्रोफाइल



वास्तविक प्रोफाइल से मिलता–जुलता फर्जी प्रोफाइल

इसके पश्चात् उनलोगों को फ्रेंड रिक्वेस्ट भेजा जाता है जो पीड़ित के वास्तविक अकाउंट में पहले से ही फ्रेंड सचूी में जुड़े होते हैं।

वास्तविक प्रोफाइल के मित्रों को जोड़ने के पश्चात् मेसेंजर के माध्यम से किसी आपातकालीन स्थिति का बहाना बनाकर तत्काल पैसों की मांग की जाती हैं एवं पे.टी.एम. या अन्य किसी अकाउंट में पैसा ट्रांसफर करने के लिए कहा जाता है।

अगर कोई व्यक्ति तथ्यों को बिना जाँच किये हुये पैसा ट्रांसफर कर देता है तो वह साइबर ठगी का शिकार हो जाता है।

सुझाव

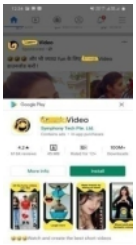
- अपने प्रोफाइल के प्राइवेसी के सेटिंग्स में **My friends only** का चयन करें।
- फेसबुक मेसेंजर इत्यादि से जब भी कोई पैसे की मांग करें तो इसकी सघन जांच सम्बंधित व्यक्ति से मिलकर या उनके निजी मोबाईल फोन पर कॉल करने के पश्चात् ही पैसों का हस्तांतरण करें।
- अपने फेसबुक एवं सभी सोशल मीडिया अकाउंट में 02 स्टेप सत्यापन को ऑन रखें।
- अपने अकाउंट से सम्बंधित आई.डी./पासवर्ड को मजबूत रखें (अपना मोबाईल नम्बर, नाम इत्यादि कमजोर पासवर्ड है) एवं इसकी गोपनीयता को बनाये रखें।

फेसबुक पर सेक्सटोर्शन

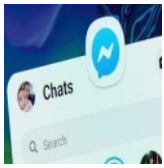
साइबर अपराधी द्वारा किसी महिला का फर्जी फेसबुक अकाउंट बना फेसबुक मेसेंजर के माध्यम से पीड़ित के साथ वीडियो चैट किया जाता है। साइबर अपराधी पीड़ित से वीडियो चैट पर अश्लील कार्य करने हेतु राजी कर लेता है। उसके पश्चात् इस वीडियो चैट का स्क्रिन शॉट रिकॉर्ड कर लेता है फिर पीड़ित को यह रिकॉड किया गया विडियो या स्क्रीन शॉट को विभिन्न सोशल मीडिया प्लेटफॉर्म पर वायरल करने की धमकी देकर पीड़ित से पैसे की मॉग करता है।

Or

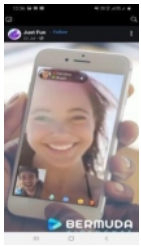
साइबर अपराधी पीड़ित के द्वारा लाइक किये गये पोस्ट एवं विडियो के आधार पर फ्रेंड रिक्वेस्ट भेजते हैं।



कई बार साइबर अपराधी पीड़ित को कई तरह के वीडियो चैट एप्लिकेशन डाउनलोड करने की सलाह देते हैं



कई चैट के बाद, साइबर अपराधी पीड़ितों को वीडियो कॉलिंग पर आने के लिए मना लेता है



साइबर अपराधी वीडियो कॉल पर पीड़ित को नग्न एवं अश्लील कार्य करने हेतु राजी कर लेता है एवं स्क्रीन रिकॉर्ड कर लेता है।

साइबर अपराधी पीड़ित को ब्लैकमेल करना शुरू कर देता है और पैसे मांगता है, अन्यथा पोर्न वेबसाइट, यूट्यूब इत्यादि पर नग्न तस्वीर अपलोड करने की धमकी देता है

पीड़ित बदनाम होने के डर से पैसा भेज देता है और ब्लैकमेलिंग और साइबर अपराध का शिकार हो जाता है।

सुझाव

- सोशल मीडिया प्लेटफॉर्म पर अनजान लोगों से दोस्ती करने से बचें।
- फेसबुक या किसी अन्य सोशल मीडिया प्लेटफॉर्म पर अनजान लोगों के साथ वीडियो कॉल न करें।

सोशल मीडिया प्लेटफार्मों का उपयोग कर किये जाने वाले अन्य साइबर अपराध

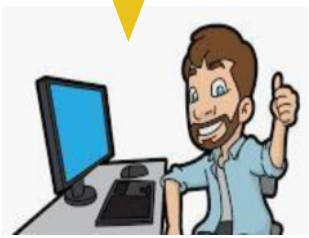
फर्जी सोशल मीडिया प्रोफाइल के जरिए उत्पीड़न

साइबर अपराधी सोशल मीडिया द्वारा पीड़ित का फोटो प्राप्त कर उसे रूपांतरित कर देते हैं तथा विभिन्न सोशल मीडिया प्लेटफॉर्म पर उसे अपलोड कर देते हैं। उसके पश्चात् वे रूपांतरित फोटो को विभिन्न सोशल मीडिया से हटाने हेतु पीड़ित से पैसों की मांग करते हैं। पीड़ित उनके जाल में फंस पैसा हस्तांतरित कर देता है।

पीड़िता सामान्यतः फर्जी व्यक्ति का रिक्वेस्ट स्वीकार कर लेती हैं जबकी वह उसे जानती भी नहीं।

OR

अपने अकाउंट के कमजोर प्राइवेसी सेंटिग्स के कारण कोई भी पीड़िता के पोस्ट, फोटोग्राफ्स इत्यादि तक अपनी पहुंच आसानी से बना लेता है, जिसका फायदा साइबर अपराधी भी उठाते हैं।



साइबर अपराधी पीड़िता के फोटोग्राफ्स को डाउनलोड कर पीड़िता के फोटो को रूपांतरित कर उससे मिलता–जुलता फर्जी अकाउंट बना लेता है और पीड़िता को बदनाम कर परेशान करने लगता है।

सुझाव

- सोशल मीडिया साइटस आपको अपनी प्रोफाइल की ''प्राइवेसी सेटिंग्स'' में यह चयन करने का विकल्प देती है कि कौन आपके पोस्ट व फोटो देख सकता है एवं फ्रेंड रिक्वेस्ट भेज सकता है। इन्हीं सेटिंग्स में **My Friends Only** सेटिंग का चयन कर अनजान लोगों को अपने प्रोफाइल तक पहुँचने से रोकें।
- यह सुनिश्चित करें कि आपकी निजी जानकारी, फोटो, विडियो इत्यादि तक केवल आपके मित्रों की ही पहुंच हो।
- सोशल मीडिया प्लेटफॉर्म्स पर अनजान लोगों से दोस्ती करने से बचें।

साइबर बुलिंग

डिजिटल तकनीक के माध्यम से सोशल मीडिया इत्यादि ऑनलाइन प्लेटफार्म्स पर धमकी देने को साइबर बुलिंग कहा जाता है। यह विभिन्न सोशल मीडिया प्लेटफार्म, गेमिंग प्लेटफार्म इत्यादि के माध्यम से किया जाता है। इसका उद्देश्य पीड़ित को डराना, धमकाना या बदनाम करना होता है, जैसे–किसी व्यक्ति के बारे में झूठी कहानी या रूपांतरित फोटो पोस्ट कर धमकी देना, किसी अन्य व्यक्ति की पहचान चोरी कर गलत मैसेज भेज उस व्यक्ति को बदनाम करना।

साइबर बुलिंग के अपराधी (आमतौर पर पीड़ित का परिचित) विभिन्न सोशल मीडिया साइटों से पीड़ित की व्यक्तिगत तस्वीरें और अन्य जानकारियाँ प्राप्त कर लेता है।

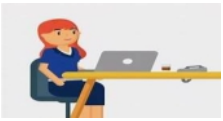
साइबर बुलिंग के अपराधी सोशल मीडिया पर पीड़ित या किसी काल्पनिक नाम से एक फर्जी अकाउंट बनाते हैं और पीडित व्यक्ति की तस्वीरें और वीडियो पोस्ट करता है जिसके वायरल होने के पश्चात हर कोई पीड़ित का मजाक बनाने लगता है और पीड़ित खुद को समाजिक/मानसिक रूप से प्रताडित महसुस करने लगते है।

सुझाव

- आपके द्वारा इस्तेमाल किये जा रहे सोशल मीडिया ऐप के निजी सेटिंग्स के बारे में जानकारी रखें।
- यह सुनिश्चित करें कि आपकी निजी जानकारी, फोटो, वीडियो इत्यादि तक केवल आपके भरोसेमंद लोगो की ही पहुँच हो।
- किसी भी जानकारी या फोटो इत्यादि को ऑनलाइन अपलोड करते समय अत्यंत सावधानी बरतें तथा यह ध्यान रखें कि यह हमेशा के लिए ऑनलाइन प्लेटफार्म पर उपल्बध रहेगा और भविष्य में इसका दुरूपयोग किया जा सकता है।
- अपने बच्चो को इस बात की जानकारी दें कि साइबर बुलिंग एक दण्डनीय अपराध है, ताकि ना ही वे साइबर बुलिंग करें और ना ही इसका शिकार बनें।
- संवेदनशील कमेंट्स, मैसेज और फोटो इत्यादि के बारे में अवश्य रिपोर्ट करें तथा संबंधित सोशल मीडिया प्लेटफॉर्म से उसे हटाने का अनुरोध करें। इसके अतिरिक्त किसी अनचाहे फ्रेडं को अनफ्रंडे करने के साथ–साथ हमेशा के लिए ब्लॉक करें ताकि वह पुनः आपकी प्रोफाइल तक पहुँच हासिल न कर सके।

साइबर स्टॉकिंग

साइबर स्टॉकिंग ऑनलाईन स्टॉकिंग है, जिसके अंतर्गत इंटरनेट व अन्य इलेक्ट्रानिक साधन का प्रयोग कर किसी व्यक्ति या ग्रुप को लगातार प्रताड़ित या डराया जाता है, गलत आरोप लगाना, आपत्तिजनक टिप्पणियां करना व किसी की ऑनलाइन गतिविधि पर लगातार नजर बनाए रखना साइबर स्टॉकिंग की शैली में आता है। साइबर अपराधी ई–मेल, मैसेज, फोन कॉल इत्यादि के माध्यम से पीड़ित का पीछा करते है। साइबर स्टॉकिंग यौन उत्पीडन, अनुचित संपर्क या आपकी व आपके परिवार की गतिविधियों की ओर अवांछित ध्यान/आकर्षण इत्यादि के रूप में हो सकता है।



पीड़ित, सोशल मीडिया के चेक–इन फीचर्स का उपयोग कर अपने सभी फॉलोअर्स व दोस्तो को अपने बारे में ज्यादातर जानकारी साझा कर देता है। वह अपनी भविष्य की योजनाओ को भी सोशल मीडिया प्लेटफार्म पर साझा कर देता है।

साइबर स्टॉकर पीड़ित के हर एक पोस्ट पर अपनी नजर बनाए रखता है।

साइबर अपराधी मौका देख पीड़ित के द्वारा किए गए पोस्ट, भविष्य की योजना की जानकारी, निजी जानकारी इत्यादि का दुरूपयोग कर उसे प्रताड़ित करता है।

सुझाव

- सोशल मीडिया प्लेटफार्म पर निजी जानकारी, फोटो, वीडियो इत्यादि साझा करते समय सावधान रहें। ध्यान रहे कि इन जानकारियों तक सिर्फ आपके विश्वसनीय लोगों की ही पहुँच हो।
- कभी भी अनजान लोगों को अपने फ्रेंड लिस्ट में ना जोड़े।
- सोशल मीडिया द्वारा प्रदत **Privacy and Security setting** का अवलोकन करें एवं इसे **My Friends Only** तक ही सीमित रखें।

अन्य साइबर अपराध/फर्जीवाड़ा

ए.टी.एम./डेबिट कार्ड क्लोनिंग फर्जीवाड़ा

प्रत्येक ए.टी.एम. व डेबिट कार्ड में एक मैगनेटिक स्ट्रीप होता है, जिसमें कार्ड से संबंधित महत्वपूर्ण गोपनीय जानकारी होती है। साइबर अपराधी द्वारा स्कीमिंग डिवाइस के माध्यम से इस गोपनीय जानकारी को कार्ड से संग्रह कर लिया जाता है तथा किसी खाली कार्ड पर कॉपी कर असली ए.टी.एम. कार्ड का क्लोन बना लिया जाता है। पीड़ित के द्वारा ए.टी.एम. पिन अंकित करते समय पिन होल, स्पाई कैमरा, ए.टी.एम. की–पैड के ऊपर ओवरले डिवाइस इत्यादि का प्रयोग कर साइबर अपराधी पीड़ित के ए.टी.एम. कार्ड का पिन प्राप्त कर खाते से अवैध निकासी करते हैं।

1

साइबर अपराधी द्वारा ए.टी.एम. कार्ड के जानकारी को ए.टी.एम. मशीन से पैसे निकालते वक्त स्कीमिंग डिवाइस के माध्यम से संग्रह कर लिया जाता है एवं पीछे से झांक कर कार्ड का पीन प्राप्त कर लिया जाता है।

2

साइबर अपराधी पीड़ित के ए.टी.एम. कार्ड की जानकारी को किसी खाली कार्ड में कॉपी कर पीड़ित के ए.टी.एम. का क्लोन तैयार करते हैं। आजकल साइबर अपराधी संबंधित कार्ड व पिन का अनुमान लगा कर भी ए.टी.एम. का क्लोन तैयार कर लेते हैं।

3

क्लोन किये गये ए.टी.एम. कार्ड एवं चुराये गये पिन के माध्यम से साइबर अपराधी पैसे की अवैध निकासी कर लेते हैं।

4

5

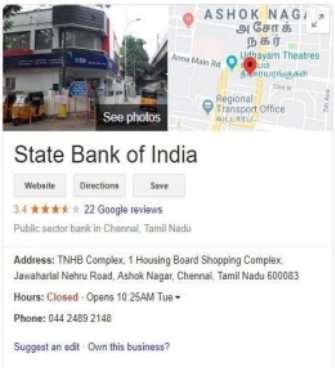
6

सुझाव

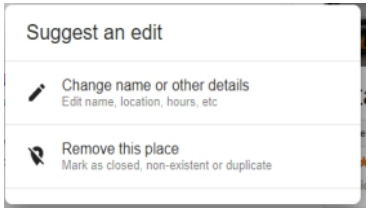
- ए.टी.एम. पिन हमेशा स्वंय अंकित करें एवं यह सुनिश्चित करें कि कोई इसे देख नहीं सके (जैसा कि चित्र 01 में प्रदर्शित किया गया है।)
- पैसे निकालने के पूर्व छुपे हुए कैमरे, स्कीमर डिवाइस इत्यादि की जांच कर लें। (जैसा कि चित्र **02** में प्रदर्शित किया गया है।)
- ए.टी.एम. की–पैड की जाँच कर यह आश्वस्त हो ले कि किसी भी प्रकार का ओवरले डिवाइस की–पैड में न लगा हो।
- ए.टी.एम. कार्ड इत्यादि से पैसे निकासी करते समय अपने अगल–बगल या पीछे किसी को खड़ा न होने दें।
- ए.टी.एम. पिन को हमेशा बदलते रहें एवं ऐसा पिन न रखें जो आसानी से अनुमान लगाया जा सके।
- यह सुनिश्चित कर लें कि बैंकिंग लेनदेन से संबंधित विवरणी आपको मैसेज के माध्यम से भी प्राप्त हो।
- यह सुनिश्चित कर लें कि ए.टी.एम. मशीन का कोई हिस्सा/पुर्जा खुला ना हो।

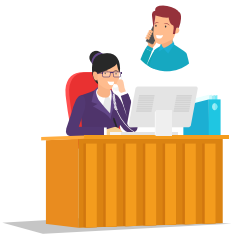
एडिटेड गुगल कस्टमर केयर नंबर फर्जीवाड़ा

साइबर अपराधी गूगल पेज पर बैंक/एयरलाइन इत्यादि के कस्टमर केयर नंबर को इस प्रकार से संपादित कर देते हैं कि जब भी कोई गूगल पर संबंधित बैंक/एयरलाइन इत्यादि के कस्टमर केयर नंबर को सर्च करें तो साइबर अपराधी द्वारा संपादित नंबर ही ऊपर में दिखे। पीड़ित वास्तविक कस्टमर केयर नंबर के स्थान पर साइबर अपराधी द्वारा संपादित नंबर पर कॉल कर देते है एवं उसके पश्चात् अपने निर्देशानुसार वह उनसे पैसे ठग लेते हैं।

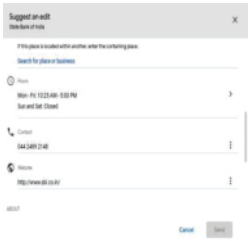


जालसाज गूगल पर मौजूद **Suggest an edit** विकल्प का लाभ उठाते हैं।





जालसाज अपना नबंर बैंक के हेल्पलाइन नंबर के रूप में अकिंत करते हैं। लोग संपादित नंबर को वास्तविक मान उस नंबर पर कॉल करते हैं और उनके निर्देशों का पालन करने के पश्चात् ठगी का शिकार बन जाते हैं।



सुझाव

- बैंक या एयरलाइन कस्टमर केयर का नंबर सम्बंधित बैंक या एयरलाइन के आधिकारिक वेबसाइट से ही प्राप्त करें न कि गूगल सर्च के माध्यम से ।
- किसी भी बैंक के कस्टमर केयर अधिकारी का नंबर ए.टी.एम./डेबिट/क्रेडिट कार्ड के पीछे दिया रहता है, उसी नंबर पर ही कॉल कर संपर्क करें।
- ध्यान रखें कि गूगल सर्च हमेशा सत्यापित जानकारी नहीं देता है।

रैन्समवेयर हमला

रैन्समवेयर एक प्रकार का हानिकारक सॉफ्टवेयर है, जिसको चलाने (RUN) पर कम्प्यूटर या डिवाइस की कार्यशैली बाधित हो जाती है एवं इसके पश्चात स्क्रीन पर एक मैसेज प्रकट होने लगता है, जिसके माध्यम से संबधित कम्प्यूटर या डिवाइस की कार्यशैली को वापस शुरू कराने हेतु पैसों का भुगतान करने के लिए कहा जाता है। अन्य शब्दों में यह एक प्रकार की ऑनलाइन फिरौती है। रैन्समवेयर मुख्यतः फिशिंग ई–मेल या अनजाने में किसी संक्रमित वेबसाईट के इस्तेमाल से फैलता है।

साइबर अपराधी पीड़ित को संदिग्ध फाईल या फिशिंग लिंक वाले ई–मेल भेजते हैं। पीड़ित फाईल को डाउनलोड कर खोलता है या फिशिंग लिंक को क्लिक कर देता है।

एक बार संक्रमित फाईल खोलने या लिंक को क्लिक करने के बाद, पीड़ित का कम्प्यूटर लॉक हो जाता है और सभी फाईलें एन्क्रिप्ट (ENCRYPT) हो जाती हैं। कंप्यूटर स्क्रीन पर अलर्ट संदेश प्रकट होने लगता है और एन्क्रिप्टेड जानकारी को अनलॉक (DECRYPT) करने के लिए फिरौती का भुगतान करने की मांग की जाती है।

सुझाव

- किसी भी अज्ञात स्त्रोत से प्राप्त ई–मेल, जिसमें संदिग्ध फाईल या लिंक हो, को ना खोलें।
- अपने कम्प्यूटर में हमेशा एंटी वायरस को अपडेट रखें एवं सुनिश्चित करें कि विंडोज फायरवॉल चालू (ON) हो व ठीक से कॉन्फिगर (Configure) किया गया हो।
- अपने अति महत्वपूर्ण दस्तावेजों का नियमित अंतराल पर किसी अन्य स्थान पर बैकअप बनाते रहे।
- अपने ई–मेल एकाउंट मे उचित स्पैम फिल्टर को सक्रिय रखें।

ज्यूस जैकिंग

ज्यूस जैकिंग एक तरह का साइबर फ्रॉड है जिसमें यू.एस.बी. चार्जिंग पोर्ट, जो पोर्ट वास्तव में डेटा कनेक्शन और चार्जिंग दोनों के लिए उपयोग किया जाता है, का उपयोग करके स्मार्ट फोन, टैबलेट या अन्य कंप्यूटर उपकरणों से डेटा कॉपी किया जाता है। पीड़ित यह सोचता है कि यह केवल चार्जिंग पोर्ट है।

पीड़ित (Victim)

हैकर (Hacker)

हैकर डेटा केबल का उपयोग करके यू.एस.बी. पोर्ट के माध्यम से डेटा चोरी करने के लिए उसी चार्जिंग पॉइंट का उपयोग करता है।

पीड़ित के द्वारा किसी सार्वजनिक स्थान पर अपने मोबाइल या डिवाइस को चार्जिंग पोर्ट में प्लग किया जाता है।

इस प्रकार पीड़ित के मोबाइल से डेटा चुराने की प्रकिया को जूस जैकिंग कहा जाता है।

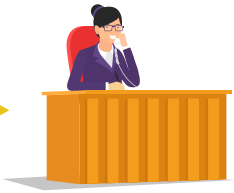
सुझाव

- चार्ज करते समय अपने फोन का डेटा ट्रांसफर को ऑफ (Disable) करके रखें।
- सार्वजनिक स्थानों पर चार्ज करने से पहले अपने डिवाइस को स्विच ऑफ कर दें।
- अपने साथ पोर्टेबल पावर पैक या पावर बैंक लेकर चलें।
- मोबाइल चार्ज करने हेतु डेटा डिसेबल्ड चार्जिंग केबल का प्रयोग कर सकते हैं।

लॉटरी फर्जीवाड़ा/नाइजेरियन फर्जीवाड़ा

इस प्रकार के अपराध मे साइबर अपराधी ई–मेल या मैसेज भेज पीड़ित को यह सूचित करते है कि उसने लॉटरी या लाखों रुपये जीते है एवं पीड़ित को सिर्फ यह चयन करना होता है कि वह पैसों को कैसे लेना पंसद करेगा। पीड़ित व्यक्ति से सकारात्मक जवाब प्राप्त होने पर पैसे या लॉटरी प्राप्त करने हेतु वह उन्हे रजिस्ट्रेशन, शिपमेंट चार्ज, जी.एस.टी. इत्यादि बारी–बारी से माँगते हैं तथा पीड़ित लगातार पैसे साइबर ठग को देते चला जाता है, जब तक कि उसे इस ठगी का एहसास नहीं हो जाता। शुरूआत में इस तरह के साइबर अपराध नाईजीरिया से होते थे, अतः इसे नाइजेरियन फर्जीवाड़ा भी कहते है।

साइबर ठग मैसैज/ई–मेल या कॉल कर पीड़ित को लॉटरी के माध्यम से जीती राशि के बारे मे जानकारी देता है।



यदि पीड़ित सकारात्मक जवाब देता है, तो धोखेबाज पूछते हैं कि वे पुरस्कार राशि कैसे प्राप्त करना चाहते हैं

प्राप्त करने के तरीके को बताने पर, फिर वे पुरस्कार राशि जारी करने के लिए पंजीकरण, शिपमेंट, सेवा शुल्क या जी.एस.टी. आदि मांगते हैं

व्यक्ति (पीड़ित) जाल में फँस जाता है और धोखेबाज द्वारा मांगी गई धनराशि को एक–एक करके भेजता जाता है जब तक कि उसे धोखाधड़ी का एहसास नहीं हो जाता

सुझाव

- वैसे कॉल/मैसज/ई–मेल इत्यादि का जवाब ना दे जो आपसे लॉटरी या पुरस्कार जीतने की बात कहते हो या निजी/वित्तीय जानकारी की माँग करते हों।
- अनचाहे या खतरनाक स्त्रोत से प्राप्त ई–मेल को रोकने के लिए अपने ई–मेल अकाउंट में उचित स्पैम फिल्टर रखें।
- एक बात का हमेशा ध्यान रखें कि उच्च रिटर्न व लॉटरी/पुरस्कार जीतने की प्रत्याशा में कभी भी अनजान व्यक्ति या संस्था को पैसो का अग्रिम भुगतान ना करें।

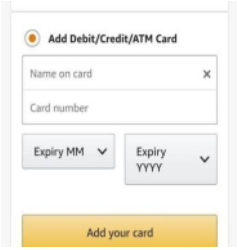
ऑनलाइन नौकरी फर्जीवाड़ा

साइबर अपराधी फर्जी वेबसाइटों, समाचार पत्रों जैसे विभिन्न प्लेटफार्मों का उपयोग करके फर्जी नौकरी का विज्ञापन देते हैं। पीड़ित नौकरी की तलाश में इन फर्जी जॉब ऑफर्स को देखता है और साइबर अपराधी से संपर्क करता है। साइबर अपराधियों से संपर्क करने पर, पीड़ित को नौकरी पाने के लिए पंजीकरण शुल्क या अग्रिम भुगतान (जो वे वापसी योग्य होने का दावा करते हैं) करने के लिए कहा जाता है। पीड़ित पैसा हस्तांतरित करता है और नौकरी पाने के लिए जालसाज के दिशा–निर्देशों का पालन करता है और साइबर अपराध का शिकार हो जाता है। कुछ मामलों में, फर्जी वेबसाइट के माध्यम से नकली भुगतान चैनल का प्रयोग कर गोपनीय वित्तीय जानकारी प्राप्त की जाती है।

लोग नौकरी की तलाश में विभिन्न वेबसाइटों या सोशल मीडिया प्लेटफॉर्म पर अपना जानकारी साझा करते हैं।

साइबर अपराधी इस जानकारी का उपयोग कर पीड़ितों से संपर्क करते हैं और एक अच्छी नौकरी प्रदान करने के नाम पर, वे पंजीकरण शुल्क, सेवा शुल्क आदि के रूप में पैसे की मांग करते हैं परंतु वे कभी भी नौकरी प्रदान नहीं करते हैं।

OR



तकनीकी रुप से साइबर अपराधी फर्जी वेबसाइट बनाते हैं और फर्जी भुगतान चैनल के माध्यम से वित्तीय जानकारी प्राप्त कर लेते है।

पीड़ित ऐसी नौकरी के लिए पैसा खो बैठता है, जो वास्तव में है ही नहीं।

सुझाव

- इस तरह के फर्जीवाड़े से बचने हेतु यह आवश्यक है कि हमेशा आधिकारिक रूप से पंजीकृत वेबसाईट पर ही अपना आवेदन समर्पित करे।
- नौकरी प्राप्त करने हेतु किसी भी प्रकार का अग्रिम भुगतान ना करें।

कंप्यूटर अथवा डिवाइस हैकिंग

हैकिंग किसी कंप्यूटर/डिवाईस तक अवैध तरीके से पहुँच बनाने की प्रक्रिया है। साइबर अपराधी विभिन्न तरीको जैसे–फिशिंग लिंक, मालवेयर इत्यादि के माध्यम से पीड़ित के कंप्यूटर/डिवाईस तक पहुँच बनाने के लिए हैकिंग का उपयोग करते है। हैकिंग के माध्यम से किसी व्यक्ति के कंप्यूटर/डिवाइस में उपस्थित महत्वपूर्ण दस्तावेज, फोटो इत्यादि चुराया जा सकता है या इनसे छेड़छाड़ की जा सकती है।

साइबर अपराधी पीड़ित को आकर्षक फाईल या लिंक के रूप में हानिकारक दस्तावेज भेजता है।

पीडित दस्तावेज डाउनलोड कर लेता है या किसी अनजाने वेबसाईट से कोई संदिग्ध एप्प डाउनलोड करता है जिससे उसका कम्प्यूटर/डिवाइस वायरस से संक्रमित हो जाता है।

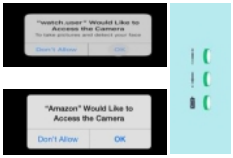
यहाँ पीड़ित सामान्य सुरक्षात्मक नियमों का अनुपालन नहीं करते हुए अपने कम्प्यूटर में किसी भी प्रकार का एंटी वायरस नहीं रखता है। धीरे–धीरे पीड़ित का कंप्यूटर धीमा काम करने लगता है उसके पश्चात पीड़ित अपने सिस्टम में उपस्थित सभी फोटो, महत्वपूर्ण दस्तावेज खो देता है।

सुझाव

- अपने कंप्यूटर/लेपटॉप में हमेशा/फायरवाल एवं एंटी वायरस इन्स्टॉल रखें एवं इसे Update रखें। कभी भी किसी कॉपी किए ऍप या साफ्टवेयर को अपने कंप्युटर/लेपटॉप या मोबाईल में डाउनलोड ना करें।
- अपने कंप्यूटर/डिवाइस पर किसी भी प्रकार का पाइरेटेड सॉफ्टवेयर/एप्लीकेशन डाउनलोड या इन्सटॉल न करें।
- अपने कंप्यूटर में किसी बाहरी डिवाइस को जोड़ते समय उसे स्कैन अवश्य करें ताकि वायरस के संक्रमण से बचा जा सके।
- सार्वजनिक स्थल पर उपस्थित वाई–फाई का प्रयोग करते वक्त सावधान रहें व निजी तथा वित्तीय जानकारी अंकित करने वाले वेबसाईट मे लॉग–इन करने से बचें।

मोबाइल एप्लीकेशन फर्जीवाड़ा

मोबाईल एप्लीकेशन निजी जानकारी चुराने, मोबाईल कंट्रोल को साइबर अपराधी तक पहुँचाने व अन्य साइबर अटैक कराने में महत्वपूर्ण भूमिका निभाते हैं। लोग सामान्यतः सुरक्षात्मक चेतावनी को अनदेखा करते हुए विभिन्न अज्ञात स्त्रोतों से मोबाईल एप्लीकेशन डाउनलोड करते हैं। ये एप्लीकेशन वायरस से संक्रमित हो सकते हैं एवं आपकी गोपनीय जानकारी को किसी अन्य बाहरी स्त्रोतों में ट्रांसफर कर सकते हैं जिसके माध्यम से कोई अन्य व्यक्ति आपके पासवर्ड वित्तीय जानकारी इत्यादि को नियंत्रित कर सकता है। ज्यादातर मोबाईल एप्लीकेशन इंस्टाल करते समय ऐसी अनावश्यक चीजों की अनुमति माँगी जाती है, जिसकी आवश्यकता भी नहीं होती और लोग उसे बिना सोचे समझें अनुमति प्रदान कर देते हैं। जिसके पश्चात् उनकी निजी एवं अन्य गोपनीय जानकारी सम्बंधित एप तक पहुँच जाती है।



पीड़ित सामान्य सुरक्षात्मक नियमों का पालन न करते हुए अक्सर अज्ञात स्त्रोतों से बहुत से एप डाउनलोड करते हैं एंव उसे अनावश्यक अनुमति भी प्रदान कर देते हैं जिसका उस ऍप की कार्यशैली से कोई लेना–देना नहीं होता है।

साइबर अपराधी इसका फायदा उठातें है और पीड़ित के मोबाईल में इन संदिग्ध ऍप के माध्यम से आक्रमण करते हैं। वे इन एप्लीकेशन को हानिकारक सॉफ्टवेयर से संक्रमित कर पीड़ित के मेसेज, कैमरा, फोटो इत्यादि तक अपनी पहुँच बना इसका दुरूपयोग करते हैं।

सुझाव

- हमेशा विश्वसनीय स्त्रोत जैसे एंड्रायड हेतु गुगल प्ले स्टोर तथा एप्पल डिवाइस हेतु एप स्टोर इत्यादि के माध्यम से ही एप्लीकेशन को डाउनलोड करें। यह सुनिश्चित करें कि एप में प्ले प्रोटेक्ट शील्ड है अथवा नहीं।
- यह भी आवश्यक है कि किसी एप को डाउनलोड करने से पूर्व उससे सम्बंधित रिव्यू प्राप्त कर लें। अगर किसी एप के बारे में नकारात्मक रिव्यू है तो उस एप के बारे में और पढ़कर उसके और किसी सुरक्षा सम्बंधी जानकारी को प्राप्त करें।
- अपने साफ्टवेयर एवं मोबाईल एप्लीकेशन को निरंतर समय पर अपडेट करते रहें ताकि किसी भी प्रकार की सुरक्षात्मक कमियां छूट न जाएँ।
- एप इन्स्टाल करते समय उसके द्वारा माँगी गई अनुमति को स्वीकार करते समय सावधान रहें, जैसे – एक सामान्य दस्तावेज स्कैन करने वाले एप को अपना कार्य करने हेतु आपकी लोकेशन अथवा कॉल लॉग की आवश्यकता नहीं पड़ती। कभी–कभी ऐसे ऍप्स स्पाईवेयर व अन्य हानिकारक सॉफ्टवेयर से भरे होते हैं।

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

Indian Cyber Crime Coordination Center

के.वाई.सी./रिमोट एक्सेस ऐप धोखाधड़ी से सावधान रहें।

- के.वाई.सी. सत्यापन से संबंधित धोखाधड़ी वाले एस.एम.एस. या कॉल से सावधान रहें।

- एस.एम.एस./फोन पर व्यक्तिगत जानकारी साझा न करें।
- यदि आपको यह बताते हुए कोई एसएमएस प्राप्त होता है कि आपका खाता अवरुद्ध या निलंबित हो जाएगा, यदि केवाईसी पूरा नहीं हुआ, तो बैंक/ई–वॉलेट/सेवा प्रदाता के प्रामाणिक ग्राहक सेवा से संपर्क करें।

- के.वाई.सी. केवल अधिकृत के.वाई.सी. बिंदुओं पर या अधिकृत प्रतिनिधि द्वारा किया जा सकता है।

- के.वाई.सी. पूरा करने के लिए कभी भी कोई ऐप जैसे क्विक सपोर्ट, एनीडेस्क या टीमव्यूअर आदि डाउनलोड न करें।
  ऐसे ऐप्स आपके उपकरणों को रिमोट एक्सेस देते हैं, जिससे धोखेबाज आपके पिन, ओ.टी.पी. बैंक खाते के विवरण आदि को धोखाधड़ी करने के लिए जान सकते हैं।

www.cybercrime.gov.in

@Cyberdost

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

1. Matrimonial sites पर फर्जी प्रोफाइल से सावधान रहें, याद रखें साइबर अपराधियों द्वारा गिफ्ट भेजने के नाम पर/कोई समस्या बताकर पैसे की मांग की जाती है, सत्यापित किये बिना किसी भी व्यक्ति के खाते में पैसे न डालें।

2. Matrimonial sites पर साइबर अपराधियों द्वारा दोस्ती कर कुछ रूपये की जरूरत है बताकर पैसे खाते में डलवाकर साईबर ठगी की जा सकती है।

3. पर साइबर अपराधियों द्वारा आपके पास डॉलर या पाउंड में पैसे भिझवाने का झांसा देकर, किसी खाते में आपसे पैसे जमा करवाकर आपके साथ ठगी की जा सकती है।

4. पर साइबर अपराधियों द्वारा आपको विदेश से पार्सल में मंहगा गिफ्ट भेजने व एयरपोर्ट पर कस्टम ड्यूटी द्वारा पार्सल पकड़े जानें/ पार्सल पर विभिन्न ज।ग्मै लगने का झांसा देकर साइबर ठगी की जा सकती है।

5. Matrimonial sites पर सत्यापित किये बिना किसी भी व्यक्ति को अपनी निजी जानकारी और फोटो/वीडियो शेयर न करें।

क्या करें

जब आप किसी भी सोशल मीडिया पोस्ट/मेल/चैटिंग इत्यादि से असहज महसूस करते हैं, तो तुरंत अपने माता–पिता या किसी भरोसेमंद व्यक्ति के साथ अपनी चिंता को साझा करें।

पासवर्ड हमेशा अल्फान्युमेरिक व विशेष चिन्ह (Special Character) के संयोजन से मिला हुआ मजबूत होना चाहिए।

वास्तविक जीवन के शिष्टाचार व संस्कार साइबर दुनिया में भी समान रूप से लागू होते हैं।

हमेशा उन्हीं लोगों को जोड़ें जिन्हें आप वास्तविक जीवन में जानते हो तथा अपने माता–पिता की अनुमति अवश्य लें।

बच्चों हेतु साइबर सुरक्षा संबंधी सुझाव

क्या न करें

कभी भी अपनी निजी जानकारी जैसे मोबाइल नंबर, पता, जन्मतिथि इत्यादि किसी ऑनलाइन प्लेटफार्म यानि फेसबुक, इंस्टाग्राम, ब्लॉग, ट्विटर इत्यादि पर साझा न करें।

उस साईट के लिए साईन अप न करें जिसमें पंजीकरण हेतु एक विशेष उम्र की सीमा तय की गई हो।

अश्लील/आपत्तिजनक परेशान करने वाले ई–मेल, चैट या पोस्ट का जवाब न दें।

बिना अपने माता–पिता के साथ चर्चा किये कोई भी सामान ऑनलाइन न खरीदें।

अपने अकाउंट से सम्बंधित पासवर्ड को कभी भी किसी के साथ साझा न करें।

किसी व्यक्ति को तब तक अपने ऑनलाइन फ्रेंड लिस्ट में शामिल न करें जब तक आप उसे अपनी वास्तविक जिंदगी में न जानते हो या पहले कभी न मिलें हों।

कभी भी किसी ऑनलाइन फ्रेंड से मिलने को राजी ना हो जब तक की अपने माता–पिता की निगरानी या जानकारी में ऐसा न हो रहा हो।

सोशल मीडिया पर अश्लील/आपत्तिजनक ई–मेल, चैट या पोस्ट को साझा/पोस्ट न करें।

माता–पिता हेतु साइबर सुरक्षा संबंधी सुझाव

क्या करें

सुरक्षित ब्राउजिंग और कम्प्यूटर उपयोग के बारे में अपने बच्चों के साथ खुली बातचीत करें।

यह सुनिश्चित करें कि आपके बच्चे अगर आपको अपनी किसी समस्या के बारे में बताये तो उन्हें किसी भी प्रकार की परेशानी न हों।

अपने बच्चों के फेसबुक, व्हाट्सएप एवं अन्य सोशल मीडिया पर ऑनलाइन गतिविधियों पर ध्यान दें एवं अचानक बदले व्यवहार इत्यादि पर नजर रखें।

अपने बच्चों को यह समझाये कि सारे सोशल नेटवर्किंग प्रोफाइल निजी (Private) हो।

खुद भी सोशल मीडिया सुरक्षा के बारे में जानकारी प्राप्त करें एवं बच्चों के साथ खुली चर्चा करें।

कंप्यूटर को हमेशा खुले स्थान में रखें एवं यह नियम बनाये कि जब भी बच्चे ऑनलाइन हो तो दरवाजा हमेशा खुला हों।

अपने बच्चों को उन साइट से तुरंत बाहर निकलने की सलाह दें जिसमें वे अपने आप को असहज या चिंतित महसूस करते हों।

यदि आपको अपने बच्चे में किसी भी प्रकार का अनुचित बदलाव प्रतीत होता है तो जल्द से जल्द पुलिस से संपर्क करें।

क्या न करें

अपने बच्चों को उन सोशल मीडिया में अकाउंट बनाने न दें जिसमें उम्र सीमा निर्धारित की गई हो एवं जिसके लिए वे योग्य न हो।

छोटे बच्चों को अनावश्यक रूप से बिना अपनी निगरानी के गूगल ब्राउज करने की अनुमति न दें।

अपने बच्चे को स्नैपचैट जैसे ऍप्स जो तुरंत पोस्ट हटा देते है, का उपयोग करने की अनुमति न दें।

बच्चों द्वारा घर पर उपयोग किए जाने वाले कम्प्यूटर पर व्यक्तिगत निगरानी सुनिश्चित करें तथा केवल किसी भी सुरक्षित सर्च इंजन या अन्य ऐसे उपकरण के हवाले न छोड़ें।

महिलाओं हेतु साइबर सुरक्षा संबंधी सुझाव

क्या करें

अपनी किसी जानकारी को सार्वजनिक करना है तो इसका चुनाव करते समय चयनात्मक बनें। जानकारी यानि वास्तविक नाम, जन्मतिथि, लिंग, शहर, ई–मेल, स्कूल का नाम, कार्य करने की जगह, निजी फोटो इत्यादि संवेदनशील जानकारी हैं।

निरंतर अंतराल पर अपने इंटरनेट संपर्कों एवं ऑनलाइन गतिविधि की समीक्षा करें।

उन लोगों को ब्लॉक करें जिनके साथ आप बातचीत नहीं करना चाहते हैं।

सोशल मीडिया अकाउंट में अपनी प्राइवेसी सेटिंग्स को कठिन व उच्च स्तर का रखें। अपने बारे में केवल मामूली पहचान के लिए आवश्यक जानकारी ही साझा करें।

व्हाट्सएप एवं अन्य मेसेजिंग ऍप में यह सुनिश्चित करें कि मीडिया ऑटो डाउनलोड की सेंटिग्स निष्क्रिय रहे खासकर वैसे लोगों के लिए जो आपके संपर्क सूची में नहीं है।

अपने फोटो पोस्ट करते समय सचेत रहे एवं ये सुनिश्चित करें कि कौन इसे देख सकता हैं।

यदि आपको ऐसा महसूस होता है कि आपकी ऑनलाईन निजता/सुरक्षा खतरे में है तो तुरंत अपने नजदीकी थाने से संपर्क करें। आप अपनी शिकायत **https://cybercrime.gov.in** या फोन नम्बर **155260** पर भी दर्ज करा सकते हैं।

विभिन्न अकाउंट के लिए अलग–अलग एवं मजबूत पासवर्ड का चयन करें।

क्या न करें

बिना किसी अन्य व्यक्ति को साथ लिए कभी भी वैसे व्यक्ति से न मिलें जिससे आप सिर्फ ऑनलाइन बातचीत किये हो एवं सुनिश्चित करें कि ऐसी मुलाकात केवल सार्वजनिक स्थल पर ही हों।

अपने पासवर्ड को किसी के साथ साझा न करें और न ही अपने अकाउंट को किसी अन्य व्यक्ति को हैंडल करने दें।

व्यक्तिगत जानकारी व्यर्थ में साझा न करें।

वैसे लोगों के फ्रेंड रिक्वेस्ट को स्वीकार न करें जो आपके लिए बिल्कुल ही अनजान हो और वार्तालाप नहीं करना चाहते हों।

अपनी निजी जानकारी जैसे मोबाइल नंबर, ई–मेल आईडी इत्यादि सोशल नेटवर्किंग साईट पर पोस्ट न करें।

किसी भी प्रकार के ओ.टी.पी. या पासवर्ड को किसी के भी साथ साझा न करें, चाहे वह आपका मित्र ही क्यों न हो।

किसी फ्रेंड रिक्वेस्ट को केवल इस आधार पर स्वीकार न करें कि यह आपके किसी अन्य मित्र का मित्र है।

फेसबुक मेसेंजर या अन्य मेसेजिंग एप इत्यादि के माध्यम से भेजे गए अनचाहे लिंक को क्लिक न करें चाहे यह आपके मित्र के द्वारा ही क्यों न भेजे गए हों।

साइबर सुरक्षा हेतु सामान्य सुझाव
डिवाइस/कम्प्यूटर सुरक्षा हेतु

- एंटीवायरस और ऑपरेटिंग सिस्टम को हमेशा अप–टू–डेट रखें।
- नियमित अंतराल पर अपने संवेदनशील / महत्वपूर्ण जानकारी का बैकअप बना लें।
- संदिग्ध वेब लिंक / यूआरएल खोलते समय सावधान रहें।
- बाहरी उपकरणों को अपने कम्प्यूटर से जोड़ते समय स्कैन अवश्य करें।
- अपने कम्प्यूटर / डिवाइस तक अनाधिकृत पहुंच से रोकने के लिए अपने वायरलेस राउटर के मैक एड्रेस फिल्टर को केवल अपने कम्प्यूटर / डिवाइस की अनुमति देते हुए सक्रिय करना सुनिश्चित करें।
- वायरलेस राउटर अपने से जुड़े सभी कम्प्यूटर / डिवाइस के मैक एड्रेस को स्क्रीन कर सकता है और उपयोगकर्ता अपने वायरलेस नेटवर्क को राउटर द्वारा पहचाने गये मैक एड्रेस से जुड़ने को स्वीकार करने के लिए सेट कर सकते हैं।
- एक मजबूत पासवर्ड के साथ अपने सभी वायरलेस एक्सेस प्वाइंटस को सुरक्षित रखें। हैकर्स आमतौर पर ओपन एक्सेस प्वाइंटस के लिए सर्च करते हैं और इसका गलत उपयोग अवांछित गतिविधियों को अंजाम देने के लिए कर सकते हैं और लॉग रिकार्ड के अनुसार आप इस दुरूपयोग के लिए उत्तरदायी बन सकते हैं।
- केवल संवेदनशील सामग्री को डिलीट करना पर्याप्त नहीं होता है, क्योंकि यह वास्तव में आपके उपकरण से डाटा को हटाता नहीं हैं। संवेदनशील फाइल को कम्प्यूटर से डिलीट करने के लिए **File Shredder Software** का प्रयोग करना चाहिए।
- अपने कम्प्यूटर उपकरणों से अवांछित फाइलों या डाटा को डिलीट कर दें। यह डाटा को किसी अनाधिकृत पहुंच से बचाता है।
- कम्प्यूटर में प्रवेश करने के लिए गैर प्रशासक **(Non-Administrator Account)** खाते का प्रयोग करें और दिन–प्रतिदिन उपयोग के लिए प्रशासक **(Administrator)** खाते का प्रयोग करने से बचें।
- अपने मोबाइल को प्रचलित साइबर खतरों से बचाने के लिए प्रतिष्ठित मोबाइल एंटीवायरस इन्स्टॉल करना सुनिश्चित करें और इसे अपडेट भी रखें।
- आपके मोबाइल उपकरण के नुकसान या चोरी होने की स्थिति में तुरंत अपने सिम को बंद करायें एवं सभी खातों के पासवर्ड बदल दें जो कि उस मोबाइल में कॅनफिगर किये गए थे।
- अपने फोन को सार्वजनिक स्थानों पर न रखें और किसी से भी अपना फोन पासवर्ड / पैटर्न लॉक साझा करने से बचें।
- अपने मोबाइल फोन पर अनाधिकृत पहुंच से रोकने के लिए हमेशा होम स्क्रीन पर पासवर्ड लगा कर रखें। एक निश्चित अवधि के बाद उपकरण के स्वचालित रूप से लॉक होने की व्यवस्था रखें।
- कम्प्यूटर को अनाधिकृत पहुंच से रोकने के लिए कार्यस्थल छोड़ने से पहले हमेशा अपने कम्प्यूटर को लॉक करें। उपयोगकर्ता **Ctrl+Alt+Del** दबाकर और **Lock this computer** को चुनें अथवा **Windows + L** बटन चुनकर कंप्यूटर लॉक कर सकते हैं।

- कम्प्यूटर से अनावश्यक प्रोग्राम्स या सेवाओं को हटा दें जो दिन–प्रतिदिन संचालन के लिए आवश्यक नहीं हैं।

सुरक्षित इंटरनेट ब्राउजिंग हेतु

- ब्राउज करते समय दिखने वाले विभिन्न धोखाधड़ी विज्ञापनों जैसे डिस्काउंट कूपन, कैशबैक और त्योहार कूपन जो यू.पी.आई. एप के माध्यम से पेमेंट पेशकश कर रहे हों, उनसे सावधान रहें।
- इंटरनेट पर कुछ यू.आर.एल. लिंक आपके ऑक्सीजन स्तर की जांच करने के लिए नकली मोबाइल ऑक्सीमिटर एप प्रदान करने के लिए विज्ञापन कर रहे हैं। अपने मोबाइल पर इस तरह के फर्जी ऑक्सीमिटर एप डाउनलोड न करें क्योंकि ये एप आपके मोबाइल फोन से आपके निजी या बायोमिट्रीक डाटा को चुरा सकते हैं।
- अपने वेब ब्राउजर के लिए तृतीय पक्ष एक्सटेंशन, प्लग इन या ऍड–ऑन का उपयोग करने से बचें क्योंकि यह आपकी गतिविधि को ट्रेक कर सकता है और आपकी व्यक्तिगत जानकारी चोरी कर सकता है।
- शॉपिंग के लिए हमेशा वास्तविक वेबसाइट का इस्तेमाल करें।
- हमेशा ऑनलाइन फॉर्म में जानकारी खुद टाइप करें और ऑनलाइन फॉर्म भरने के लिए वेब ब्राउजर पर ऑटो–फिल विकल्प का प्रयोग न करें क्योंकि ये फॉर्म आपकी व्यक्तिगत जानकारी जैसे कार्ड नंबर, बैंक खाता संख्या, सी.वी.वी. नंबर आदि स्टोर कर सकते हैं।
- वेबसाइट के नाम के बारे में सावधान रहें। एक अवैध वेबसाइट एक वैध साइट के समान दिख सकती है, किंतु नाम वर्तनी या किसी भिन्न डोमेन जैसे **[dot]com, [dot]net etc.** का उपयोग किया हो सकता है।
- सामान्य तौर पर सभी सरकारी वेबसाइटों के अंत में **[dot]gov** या **[dot]nic** होते हैं।
- वेबसाइटों पर और सार्वजनिक कंप्यूटर पर ''मुझे याद रखें **(Remember me)** या मुझे लॉग इन रखें **(Keep me logged in)** विकल्प पर क्लिक करने से बचें।
- सरकारी चैरिटी फंड के समान नाम वाले चैरिटेबल संगठन जो पीड़ितों के लिए धन का अनुरोध करते हैं उनसे सतर्क रहें। दान देने से पहले संगठनों की साख की जांच कर लें।
- कभी भी ब्राउजर को अपना उपयोगकर्ता नाम/पासवर्ड स्टोर करने की अनुमति न दें, खासकर यदि आप कम्प्यूटर उपकरण को किसी के साथ साझा करते हों। अपनी गोपनीयता की रक्षा के लिए प्रत्येक सत्र के बाद ब्राउजर से इतिहास को मिटा देने की आदत बनायें।
- **Tiny** यूआरएल से सतर्क रहें। यह **(http://tiny.cc/ba1j5y)** की तरह प्रतीत होता है। इस पर क्लिक न करें क्योंकि यह आपको संक्रमित वेबसाइट पर ले जा सकता है।
- जॉब सर्च पोर्टल पर पंजीकरण करने से पहले उपयोगकर्ता से एकत्र की गई जानकारी के प्रकार और इसे वेबसाइट द्वारा कैसे संशोधित किया जाएगा, यह जानने के लिए वेबसाइट की प्राइवेसी पॉलिसी की जांच करें।

- कई सामाजिक नेटवर्किंग साइटें एक तृतीय पक्ष एप्लीकेशन डाउनलोड करने का संकेत देती हैं जो आपको किसी अन्य संक्रमित पेज तक पहुंचा सकते हैं। इसकी सुरक्षा का पता लगाए बिना असत्यापित तृतीय पक्ष एप्लीकेशन डाउनलोड न करें।
- वैसे ई–कॉमर्स वेबसाईट या विज्ञापन से सावधान रहें जो सामानों को भारी छूट देने का दावा करते हैं। नेट बैंकिंग सुविधा का उपयोग करने हेतु हमेशा वर्चुअल की–बोर्ड का उपयोग करें और ऑनलाइन लेन–देन पूरा होने के बाद बैंकिंग पोर्टल/वेबसाइट से लॉग ऑफ करें। ऑनलाइन बैंकिंग गतिविधि समाप्त होने के बाद वेबब्राउजर से ब्राउजिंग हिस्ट्री को डिलिट करना भी सुनिश्चित करें।
- अपने बैंक खाता में लॉगइन करने के लिए विभिन्न चरणों के ऑथेन्टिकेशन का उपयोग करें।

सुरक्षित इंटरनेट ब्राउजिंग हेतु

- डिजिटल वॉलेट/बैंक खाता तक पहुंचने के लिए उपयोग किए जाने वाली जानकारी को मोबाइल में लिखने या स्टोर करने से बचें।
- सभी बैंकों के इंटरनेट बैंकिंग खातों के लिए एक ही पासवर्ड का इस्तेमाल नहीं किया जाना चाहिए।
- एक ही मोबाइल नंबर सभी बैंक खाते में पंजीकृत नहीं रखना चाहिए।
- एस.एम.एस. और ई–मेल के माध्यम से सूचना प्राप्त करना सुनिश्चित करें।
- नियमित रूप से लॉगइन कर अपने बैंक खाते की गतिविधि देखें और सुनिश्चित करें कि खाते से कोई अनाधिकृत लेन–देन न हुआ हो। यदि कोई त्रुटी हो तो अपने बैंक को तुरंत सूचित करें।
- हमेशा दो अलग–अलग ई–मेल खाते बनाए, एक उन लोगों से संवाद करने के लिए और दूसरा आपके वित्तीय लेनदेन के लिए।

ई–वॉलेट सुरक्षा हेतु

- अपने मोबाइल फोन, टैबलेट और अन्य उपकरणों में पासवर्ड/पिन लगा कर रखें।
- अपने ई–वालेट का उपयोग करते हुए लेन–देन करते समय आपको अपने डेबिट या क्रेडिट कार्ड के विवरणों को कभी भी Save नहीं करना चाहिए।
- अपने ई–वॉलेट में लॉगइन के लिए विभिन्न चरणों के ऑथेन्टिकेशन का उपयोग करें।
- मोबाइल फोन में डिजिटल वॉलेट तक पहुंचने के लिए उपयोग की जाने वाली जानकारी लिखने से बचें।
- उन स्त्रोतों से ई–वॉलेट खाते स्थापित करें जिन पर आप भरोसा करते हैं। ई–मेल, एस.एम.एस. या सोशल मीडिया पर साझा किए गए लिंक के माध्यम से ई–मेल एप इन्स्टॉल न करें। हमेशा अपने स्मार्ट फोन पर सीधे एप स्टोर (गूगल/आई.ओ.एस. स्टोर में) से ही प्राधिकृत ई–वॉलेट एप को सत्यापित कर इंस्टॉल करें। कृपया जांच लें कि एप में **Play Protect Shield** है या नहीं।

ई–मेल अकाउंट सुरक्षा हेतु

- अपने सभी ई–मेल खातों के लिए एक ही पासवर्ड कभी न रखें।
- सुरक्षित नेटवर्क कनेक्शन का उपयोग करें।
- सार्वजनिक वाई–फाई नेटवर्क के उपयोग से बचें। अधिक सुरक्षित वाई–फाई कनेक्शन के लिए पासवर्ड की आवश्यकता होती है और इसे आसानी से **WPA** या **WPA2** के रूप में पहचाना जाता है। अत्यधिक असुरक्षित वाई–फाई सभी के लिए उपयोग हेतु खुला होता है और **WEP (Wired Equivalent Privacy)** के रूप में केवल किया जा सकता है।
- संदिग्ध ई–मेल में दिए गए लिंक पर क्लिक न करें, भले ही वे वास्तविक दिखे, लेकिन यह आपको छद्म/दुर्भावनापूर्ण वेबसाइटों तक ले जा सकता है और यह आपकी मेहनत की कमाई को ठगने का एक प्रयास हो सकता है।

पहचान पत्र की सुरक्षा हेतु

- कभी भी अपने पहचान पत्र की खराब या अस्वीकृत प्रतिलिपि दुकान पर न छोड़ें।
- कभी भी दुकानदार को उनके कम्प्यूटर में अपने पहचान पत्र की एक प्रति रखने की अनुमति न दें।
- व्हाट्सएप सहित सोशल मीडिया प्लेटफॉर्म पर अज्ञात व्यक्तियों को अपना पहचान पत्र कभी साझा न करें।
- कभी भी अपने संपत्ति के कागजात या अन्य व्यक्तिगत जानकारी को सोशल मीडिया प्लेटफॉर्म पर साझा न करें।

पासवर्ड सुरक्षा हेतु

- अल्फान्युमेरिक, विशेष वर्ण, अपर केस और लोअर केस को शामिल करते हुए कम से कम 13 वर्णों का मजबूत पासवर्ड रखें।
- अपने सभी खातों के लिए **Two Factor Authentication** रखें।
- यदि आपको संदेह है कि आपका ऑनलाइन खाता हैक हो गया है, तो तुरंत पासवर्ड बदलें, जिसका अनुमान लगाना मुश्किल हो तथा तुरंत निकटतम पुलिस स्टेशन से संपर्क करें।

सरकार ऐसा कुछ नहीं कर रही है!

सभी कॉल रिकॉर्ड की जाती हैं।

सभी फ़ोन कॉल रिकॉर्डिंग सहेजी जाती हैं।

व्हाट्सएप पर नजर रखी जा रही है।

ट्विटर पर नजर रखी जा रही है।

फेसबुक पर नजर रखी जा रही है।

सभी सोशल मीडिया प्लेटफॉर्म्स पर नजर रखी जाती है।

ध्यान रखें कि अनावश्यक संदेश न भेजें।

राजनीति / वर्तमान स्थिति के बारे में सरकार / प्रधानमंत्री आदि के बारे में प्राप्त किसी भी पोस्ट या वीडियो आदि को फॉरवर्ड न करें।

पुलिस ने साइबर क्राइम नाम का नोटिफिकेशन जारी किया है और कार्रवाई की जाएगी बस डिलीट न करें।

To check if any Central Govt. related Policy/Schemes is a Fact or not.

Contact Us @PIBFactCheck 8799711259 /PIBFactCheck pibfactcheck@gmail.com

पुलिस में शिकायत कैसे करें

आप अपने नजदीकी पुलिस स्टेशन अथवा अगर आपके जिले में एक विशेष रूप से अधिसूचित साइबर थाना हो तो उसमें शिकायत दर्ज करा सकते हैं। साइबर अपराधों को **https://cybercrime.gov.in** पर भी ऑनलाइन पंजीकृत किया जा सकता है।

उचित जांच के लिए कृपया शिकायत करने के साथ–साथ या शिकायत के बाद जल्द से जल्द पुलिस अधिकारी को निम्न कागजात सौंप दें।

फेसबुक या अन्य सोशल मीडिया अकाउंट संबंधित शिकायतों हेतु

- अगर कोई फर्जी फेसबुक या इंस्टाग्राम अकाउंट बन गया है तो यू.आर.एल. के साथ फर्जी प्रोफाइल का स्क्रीनशॉट ले लें या आवेदन में प्रोफाइल के यू.आर.एल. का उल्लेख करें।
- शिकायत प्रति के साथ स्व–सत्यापित पहचान पत्र संलग्न करें।

वित्तीय फर्जीवाड़ा हेतु

- स्व–सत्यापित पासबुक/क्रेडिट कार्ड ट्रांजेक्शन स्टेटमेंट कॉपी जमा करना चाहिए, जिसमें बैंक अकाउंट नंबर, डेबिट कार्ड/क्रेडिट कार्ड नंबर और बैंक अकाउंट या क्रेडिट कार्ड से पंजीकृत मोबाइल नंबर का जिक्र किया गया हो।
- पंजीकृत मोबाइल नंबर पर प्राप्त धोखाधड़ी वाले लेन–देन के संदेशों का स्क्रीनशॉट संरक्षित किया जाना चाहिए तथा शिकायत पत्र के साथ संलग्न भी किया जाना चाहिए।
- धोखाधड़ी के लेन–देन हेतु प्राप्त किसी भी संदिग्ध लिंक या ओ.टी.पी. का स्क्रीनशॉट भी संरक्षित किया जाना चाहिए और शिकायत पत्र के साथ संलग्न किया जाना चाहिए।

फर्जी वेबसाइट संबंधी फर्जीवाड़ा हेतु

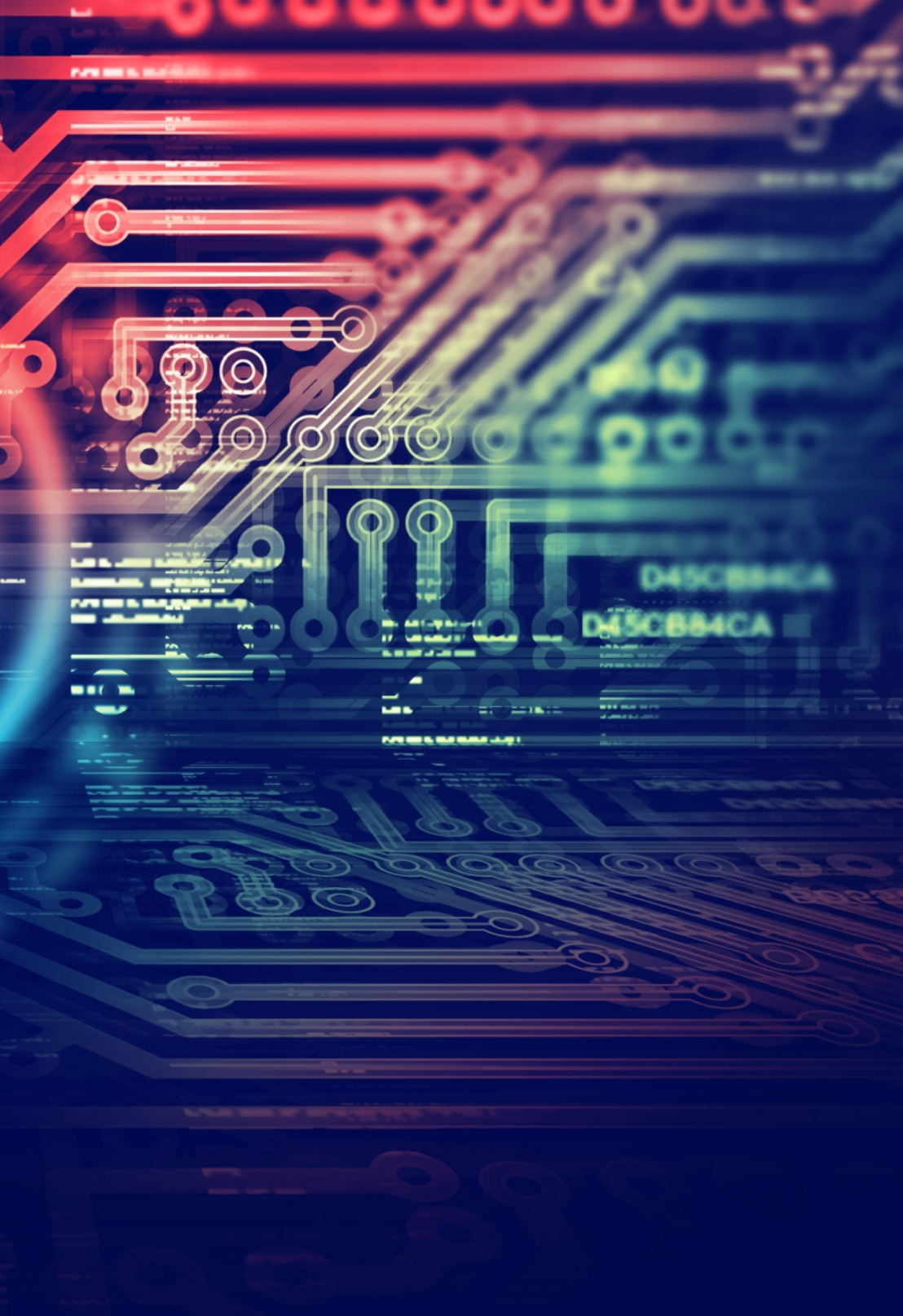
- वेबसाइट के यू.आर.एल. के साथ नकली वेबसाइट का स्क्रीनशॉट लिया जाना चाहिए और शिकायत कॉपी के साथ जमा किया जाना चाहिए।
- धोखाधड़ी वाले लेनदेन की स्व सत्यापित प्रति, यदि कोई हो तो शिकायत प्रति के साथ संलग्न किया जाना चाहिए।

APPEAL

एक जिम्मेदार नागरिक होने के नाते, जागरूक होकर तथा साइबर अपराधियों द्वारा बिछाये गये जाल में न फंसकर साइबर अपराध से लड़ने में हमारी मदद करें। इसके अलावा साइबर अपराधियों द्वारा अपराध कारित करने के सभी प्रयास के बारे में हमें सूचित करें। यह हमें साइबर अपराधियों को पकड़ने या किसी अन्य व्यक्ति को धोखा देने से पहले रोकने में मदद कर सकता है। इसे **https://cybercrime.gov.in** अथवा फोन नम्बर **155260** पर भी सूचित किया जा सकता है।

साइबर सुरक्षा

–जागरूकता पुस्तिका


D45CB84CA
D45CB84CA