



डा० ए० पी० जे० अब्दुल कलाम प्राविधिक
विश्वविद्यालय, उ० प्र०
सेक्टर-11, जानकीपुरम विस्तार, लखनऊ (226031)

पत्रांक : ए०के०टी०यू० / सी०टी०पी०सी० / 2024 / 1179

दिनांक : 21 दिसम्बर, 2024

सेवा,

विश्वविद्यालय से सम्बद्ध
समस्त संस्थाओं के निदेशक/प्रचार्य

विषय : विश्वविद्यालय से सम्बद्ध समस्त संस्थाओं में साइबर सुरक्षा जागरूता अभियान के आयोजन के सम्बन्ध में।

महोदय,

कृपया संलग्न प्राविधिक शिक्षा अनुभाग के पत्र दिनांक 17 दिसम्बर, 2024 का अवलोकन करना चाहे। उक्त के सम्बन्ध में अवगत कराना है कि जनवरी 2024 से अभी तक उपरोक्त से सम्बंधित जो भी कार्यक्रम आपके द्वारा अपने संस्थान में आयोजित कराया गया है उससे सम्बन्धित फोटो एवं कार्यक्रम की गतिविधियों की रिपोर्ट नीचे दिए गए गूगल फार्म के लिंक के माध्यम से दिनांक 26 दिसम्बर, 2024 तक सांय 4:00 बजे तक आवश्यक रूप से उपलब्ध कराने का कष्ट करें जिससे कि उपरोक्त सूचना से शासन को ससमय अवगत कराया जा सके।

<https://forms.gle/vBTZhTU5F8THsRxM9>

संलग्नक : यथोक्त

भवदीय

(प्र० नीलम श्रीवास्तव)
अधिष्ठाता

प्रतिलिपि सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित :

1. कुलसचिव, ए०के०टी०यू०, लखनऊ।
2. स्टाफ आफिसर, मा० कुलपति महोदय के अवलोकनार्थ हेतु प्रेषित।

(प्र० नीलम श्रीवास्तव)
अधिष्ठाता

प्रेषक,

मानिक चन्द्र,
अनु सचिव
उत्तर प्रदेश शासन।

सेवा में,

- 1-कुलसचिव,
ए०के०टी०यू० लखनऊ/एम०एम०एम०यू०टी०, गोरखपुर/
एच०बी०टी०यू०, कानपुर।
- 2-निदेशक
समस्त राजकीय अभियंत्रण संस्थान, उ०प्र०।

प्राविधिक शिक्षा अनुभाग-1

लखनऊ: दिनांक 17 दिसम्बर, 2024

विषय: राज्य के समस्त जिले के कार्यालयों, विद्यालयों तथा जल सेवा केन्द्रों पर साइबर सुरक्षा जागरूकता अभियान आयोजित किये जाने के सम्बन्ध में।

महोदय,

उपर्युक्त विषयक प्रमुख सचिव आई.टी. एवं इलेक्ट्रॉनिक्स अनुभाग-1 के पत्र दिनांक 19.10.2024 (प्रति संलग्न) का कृपया संदर्भ ग्रहण करने का कष्ट करें।

2- उक्त के सम्बन्ध में मुझे यह कहने का निदेश हुआ है कि संदर्भित पत्र दिनांक 19.10.2024 द्वारा की गयी अपेक्षा के क्रम में उक्त वांछित आवश्यक कार्यवाही कराते हुए जागरूकता कार्यक्रम आरम्भ किये जाने तथा गतिविधियों की प्रगति रिपोर्ट नियमित रूप से सेन्टर फार ई-गवर्नेंस यू०पी० (ई-मेल आई०डी०-ceglko.up@gmail.com) तथा कृत कार्यवाही से शासन को अवगत कराने का कष्ट करें।

संलग्नक: यथोक्त।

Signed by भवदीय,
Manik Chandra

Date: 16-12-2024 18:49:17

(मानिक चन्द्र)

अनु सचिव

संख्या व दिनांक तदैव।

प्रतिलिपि प्राविधिक शिक्षा अनुभाग-3, उत्तर प्रदेश शासन को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

4459
18/12/24

आज्ञा से,

(मानिक चन्द्र)

अनु सचिव

DR(D)/Sri V.V. Singh | Dear T&P | Dear
Sum N. Chandra | General

Reg
17/12/24

संख्या 3178 सोलह-प्रा०-सि०-1-2020/8

संख्या:-1692/78-1-2024-1099/619/2020

प्रेषक,

अनिल कुमार सागर,
प्रमुख सचिव,
30प्र० शासन।

सेवा में,

1. समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव, 30प्र० शासन।
2. समस्त मण्डलायुक्त, उत्तर प्रदेश।
3. समस्त जिलाधिकारी, उत्तर प्रदेश।

आई.टी. एवं इलेक्ट्रॉनिक्स अनुभाग-1

तखतः दिनांक 1 अक्टूबर, 2024

विषय: राज्य के समस्त जिले के कार्यालयों, विद्यालयों तथा जन सेवा केन्द्रों पर साइबर सुरक्षा जागरूकता अभियान आयोजित किये जाने के संबंध में।

महोदय,

VS(A-A)

उपर्युक्त विषय के संबंध में अवगत कराना है कि वर्तमान परिदृश्य के अन्तर्गत डिजिटल युग में साइबर अपराधों की बढ़ती घटनाओं के दृष्टिगत यह नितान्त आवश्यक हो गया है कि नागरिकों, छात्र-छात्राओं तथा सरकारी अधिकारियों को साइबर हमलों/खतरों से खुद को सुरक्षित

रखने के उपायों के बारे में पर्याप्त जानकारी हो। उल्लेखनीय है कि माह-अक्टूबर को राष्ट्रीय एवं अन्तरराष्ट्रीय स्तर पर राष्ट्रीय साइबर सुरक्षा जागरूकता माह (एन०सी०एस०ए०एम०) के रूप में (प्रवीणमन्त्रालय शिक्षा) है, जिसका उद्देश्य सार्वजनिक एवं निजी क्षेत्र के साथ-साथ आम नागरिकों को भी

साइबर सुरक्षा हेतु जागरूक करना है।

संयुक्त शिष्टाचार प्रणाली में भारत सरकार द्वारा इस वर्ष के अभियान का विषय 'साइबर सुरक्षित भारत' (SatarK Nagrik) रखा गया है, जिसके माध्यम से साइबर सुरक्षा हेतु सम्पूर्ण देश को

सम्मिलित करते हुए एक दृष्टिकोण अपनाया गया है। इस अक्टूबर माह में सार्वजनिक, निजी क्षेत्र एवं आम नागरिकों को जागरूक / सतर्क करते हुए देश को साइबर सुरक्षित बनाने पर विशेष बल दिया जा रहा है। इस क्रम में मुख्य बिन्दुओं को समाहित करते हुए हैण्डबुक भी तैयार कर उपलब्ध करायी जा रही है। इस हेतु आम नागरिकों, छात्र-छात्राओं को हैण्डबुक उपलब्ध कराते हुए साइबर सुरक्षा हेतु जागरूकता को बढ़ाया जा रहा है।

4- नागरिकों, छात्र-छात्राओं तथा सरकारी अधिकारियों को साइबर हमलों/खतरों से खुद को सुरक्षित रखने हेतु उपाय/सावधानियों निम्नवत् है:-

(1) नागरिकों हेतु साइबर सुरक्षा जागरूकता:-

वितीय लेन-देन करने वाले विभागों द्वारा आम नागरिकों में साइबर सुरक्षा के प्रति जागरूकता फैलाने पर ध्यान केंद्रित किया जाना है, जिसमें प्रमुख रूप से वितीय धोखाधड़ी से जुड़े नवीनतम साइबर अपराधों के रुझानों के बारे में जानकारी देना सम्मिलित है जैसे-

- (1) UPI धोखाधड़ी
- (2) नेट बैंकिंग धोखाधड़ी

So-1

92

10/12/24

श्री न.प.प. 10/12/24

- (3) क्रेडिट कार्ड धोखाधड़ी
- (4) निवेश या लांटेरी घोटाले
- (5) नौकरी घोटाले
- (6) ई-कॉमर्स धोखाधड़ी
- (7) सोशल मीडिया घोटाले
- (8) डिजिटल गिरफ्तारी वसूली घोटाले
- (9) फिशिंग घोटाले
- (10) साइबर अपसर्धों की रिपोर्टिंग

उपरोक्त गतिविधियों को सार्वजनिक अभियानों, कार्यशालाओं तथा जागरूकता कार्यक्रमों के माध्यम से संचालित किया जाना चाहिए, जिससे उत्तर प्रदेश राज्य के प्रत्येक नागरिक को उचित जानकारी प्राप्त हो सके।

(2) छत्रों हेतु साइबर सुरक्षा जागरूकता:-

छत्रों पर विशेष ध्यान देने की आवश्यकता है, जो निम्नलिखित साइबर खतरों के प्रति अत्यधिक संवेदनशील होते हैं:-

- (1) पहचान की चोरी (Identity Theft)
- (2) फिशिंग घोटाला (Phishing Scams)
- (3) सोशल मीडिया घोटाला (Social Media Scams)
- (4) गेमिंग ऐप घोटाला (Gaming App Scams)
- (5) ऑनलाइन डेटिंग ऐप घोटाला (Online Dating App Scams)
- (6) ई-कॉमर्स घोटाला (E-Commerce Scams)
- (7) नौकरी के घोटाला (Job Scams)
- (8) डिजिटल गिरफ्तारी/जबरन वसूली घोटाला (Digital Arrest/Extortion Scams)
- (9) रैनसमवेयर हमला (Ransomware Attacks)

इस हेतु स्कूलों तथा कॉलेजों से यह अनुरोध किया जाता है कि वे नियमित रूप से जागरूकता कार्यक्रम आयोजित करें, ताकि छत्रों को अपनी डिजिटल Identity की सुरक्षा के महत्व तथा सुरक्षित ऑनलाइन उपायों के बारे में शिक्षित किया जा सके।

(3) सरकारी अधिकारियों हेतु:-

जिला स्तर के अधिकारियों को साइबर सशक्त बनाने के लिए आई०टी० एवं इलेक्ट्रॉनिक्स विभाग, उपरो शासन साइबर सुरक्षा धोखाधड़ी रोकथाम तथा सुरक्षा के मुख्य उपायों की एक हैंडबुक नागरिकों एवं विद्यार्थियों हेतु संलग्न (संलग्नक-1) की गयी है, जिससे वे साइबर सुरक्षा संदेशों को नियमित सार्वजनिक बातचीत तथा बैठकों में सम्मिलित कर अधिक से अधिक साइबर सुरक्षा को प्राप्त कर सकते हैं।

जन सेवा केन्द्रों पर साइबर जागरूकता को बढ़ाये जाने हेतु एक बैनर (संलग्नक-2) भी तैयार किया गया है, जिसको समस्त विलेज लेवल इन्टरप्रिन्योर (वी०एल०ई०) द्वारा अपने जन सेवा केन्द्रों पर लगाया जाना है।

5- अतएव इस संबंध में मुझे यह कहने का निदेश हुआ है कि कृपया इस संबंध में आवश्यक कार्यवाही सुनिश्चित किये जाने हेतु संबंधित अधिकारियों/संस्थाओं को निर्देशित करने तथा जागरूकता कार्यक्रम आरम्भ किए जाने तथा गतिविधियों की प्रगति रिपोर्ट नियमित रूप से सेन्टर फॉर ई-गवर्नेन्स, यू0पी0 (ई-मेल आई0डी0-ceglko.up@gmail.com) तथा शासन को उपलब्ध कराने का कष्ट करें।

संलग्नक: यथोक्त।

भवदीय,

Signed by

Anil Kumar Sagar

Date: 18-10-2024 19:49:32

(अनिल कुमार सागर)

प्रमुख सचिव।

संख्या-1692(1)/78-1-2014 तददिनांक

उपर्युक्त की प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित:-

1. निजी सचिव, मुख्य सचिव, 30प्र0 शासन।
2. राज्य समन्वयक, सेन्टर फॉर ई-गवर्नेन्स, 30प्र0, अपट्रान बिल्डिंग, गोमती नगर, लखनऊ।
3. राज्य सूचना विज्ञान अधिकारी, एन० आई०सी०, लखनऊ।
4. हेड, एस०ई०एम०टी०, 3०प्र०।
5. गार्ड फाइल।

आज्ञा से,

(नेहा जैन)

विशेष सचिव।



1. भूमिका

वर्तमान परिदृश्य की डिजिटल दुनिया में युवा छात्र इंटरनेट का उपयोग जैसे- अध्ययन, सामाजिकता (सोशलइजिंग), खेल तथा अन्य गतिविधियों के लिए अधिकाधिक कर रहे हैं। सामान्यता इंटरनेट के अनेकानेक लाभ हैं, परन्तु इसके साथ जोखिम भी जुड़े होते हैं। साइबर अपराधी (साइबर यह पुस्तिका नागरिकों को साइबर अपराध के बढ़ते खतरों के प्रति जागरूक करने और उन्हें अपने आप को सुरक्षित करने के मुख्य तरीकों के बारे में जानकारी देने के लिए तैयार की गई है। इसमें साइबर वर्ल्ड में होने वाले धोखाधड़ी के तरीकों, उनके चेतावनी संकेतों और खुद को सुरक्षित रखने के उपायों के बारे में बताया गया है।) अक्सर छात्रों को विभिन्न प्रकार की ऑनलाइन धोखाधड़ी के माध्यम से निशाना (टारगेट) बनाते हैं। इस पुस्तिका का उद्देश्य स्कूल और कॉलेज के छात्र/छात्राओं को नवीनतम साइबर सुरक्षा धोखाधड़ी के सम्बन्ध में जागरूक करना तथा ऑनलाइन सुरक्षित रहने के लिए आवश्यक कदम उठाने में उनकी सहायता करना है।

2. साइबर धोखाधड़ी के तरीकों की सूची

- | | |
|-----------------------------|-------------------------------------|
| i) UPI घोटाले | ii) नेट बैंकिंग धोखाधड़ी |
| iii) क्रेडिट कार्ड धोखाधड़ी | iv) निवेश या लॉटरी घोटाले |
| v) नौकरी घोटाले | vi) ई-कॉमर्स धोखाधड़ी |
| vii) सोशल मीडिया घोटाले | viii) डिजिटल गिरफ्तारी/वसूली घोटाले |
| ix) फिशिंग घोटाले | x) साइबर अपराधों की रिपोर्टिंग |

2.1 UPI घोटाले

यूनिफाइड पेमेंट इंटरफेस (UPI) घोटाले तब होते हैं जब धोखेबाज नकली भुगतान अनुरोधों या नकली QR कोड स्कैन करके उपयोगकर्ताओं को पैसे ट्रान्सफर/भेजने के लिए बाध्य करते हैं।

आम परिदृश्य:

- नकली भुगतान अनुरोध प्राप्त करना।
- नकली QR कोड स्कैन करना।
- फर्जी कस्टमर केयर प्रतिनिधियों द्वारा UPI क्रेडेंशियल्स पूछना।

रोकथाम के सुझाव:

- कभी भी अपना UPI पिन किसी के साथ साझा न करें।
- भुगतान करने से पहले हमेशा भेजने वाले या प्राप्तकर्ता की पहचान सत्यापित करें।
- अनजान QR कोड स्कैन करने से बचें।
- मल्टी-फैक्टर ऑथेंटिकेशन का उपयोग करें और UPI ऐप्स को अपडेट रखें।





2.2 नेट बैंकिंग धोखाधड़ी

नेट बैंकिंग धोखाधड़ी तब होती है जब साइबर अपराधी फिशिंग अटैक, मेलवेयर या नकली वेबसाइटों के माध्यम से आपके बैंकिंग क्रेडेंशियल्स चुराते हैं, जिससे अनधिकृत लेनदेन होता है।

आम परिदृश्य:

- एसएमएस या ईमेल के माध्यम से नकली (फेक) बैंक लिंक पर क्लिक करना।
- सार्वजनिक वाई-फाई के माध्यम से आनलाइन बैंकिंग का उपयोग करना।
- अनजाने में अनधिकृत साफ्टवेयर का इस्तेमाल करना।

रोकथाम के सुझाव:

- अज्ञान लिंक्स पर क्लिक न करें। अपने बैंक की वेबसाइट तक पहुंचने के लिए यूआरएल टाइप करें।
- किसी भी बैंकिंग लेनदेन के लिए सार्वजनिक वाई-फाई का उपयोग न करें।
- अतिरिक्त सुरक्षा के लिए मल्टी-फैक्टर ऑथेंटिकेशन का उपयोग करें।
- अपने खाते की नियमित रूप से निगरानी करें और किसी भी संदिग्ध गतिविधि की तुरंत रिपोर्ट करें।



2.3 क्रेडिट कार्ड धोखाधड़ी

जब कोई व्यक्ति आपके कार्ड विवरणों को चुरा लेता है और ऑनलाइन शॉपिंग या कार्ड की नकल (क्लोनिंग) करके अनधिकृत लेनदेन करता है।

आम परिदृश्य:

- सुरक्षित वेबसाइटों पर शॉपिंग करना।
- एटीएम या Point of Sale (पीओएस) मशीनों पर स्किमिंग डिवाइस लगे होना।
- आपका कार्ड सेवा प्रदाता होने का दावा करने वाले फिशिंग ईमेल।

रोकथाम के सुझाव:

- कार्ड विवरण किसी भी ब्राउज़र या वेबसाइट पर स्टोर न करें।
- क्रेडिट कार्ड स्टेटमेंट की नियमित रूप से निगरानी करें और खोए हुए कार्ड की तुरंत सम्बन्धित बैंक को रिपोर्ट करें।
- ऑनलाइन खरीदारी के लिए सुरक्षित भुगतान गेटवे का उपयोग करें।



2.4 निवेश या लॉटरी घोटाला

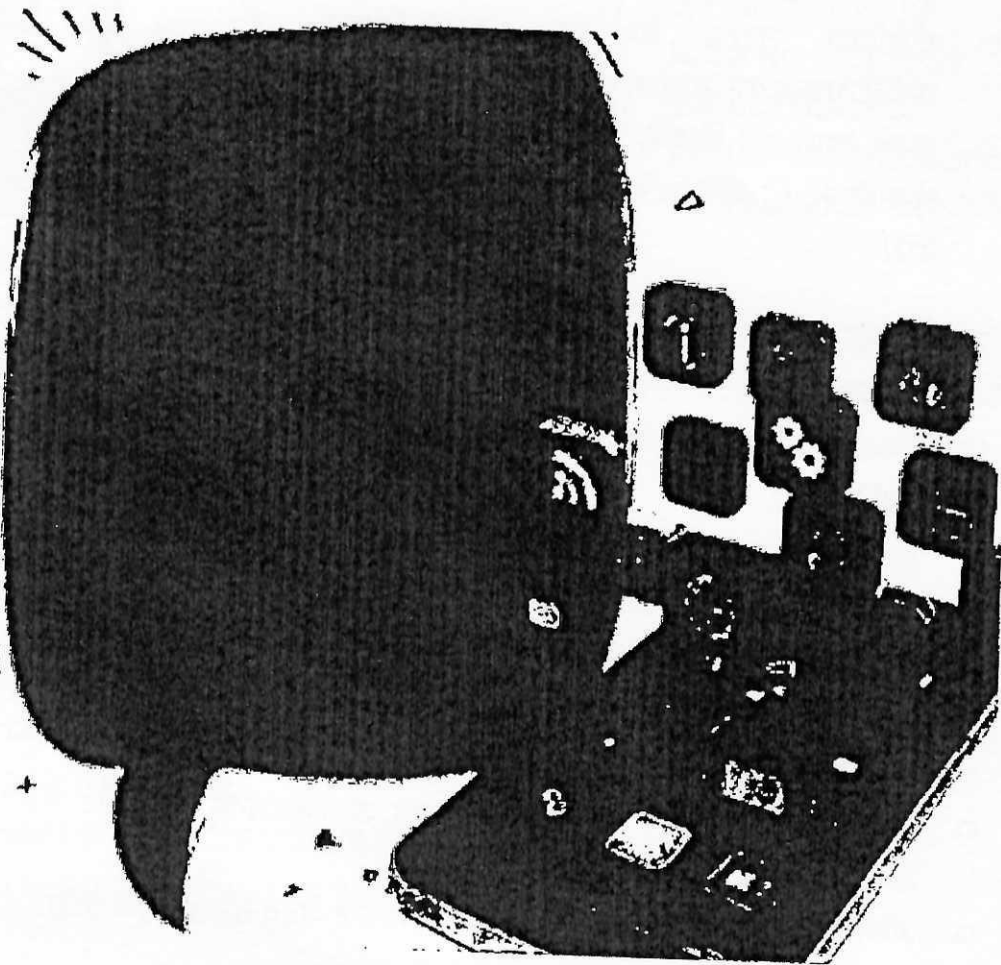
धोखेबाज पीड़ितों को नकली एवं लुभावनी योजनाओं में निवेश करने के लिए प्रोत्साहित करते हैं एवं बड़े रिटर्न का वादा करते हैं, या यह दावा करते हैं कि आपने लॉटरी जीती है और पुरस्कार एकत्र करने के लिए कर या शुल्क का भुगतान करना होगा।

आम परिदृश्य:

- निवेश के उच्च रिटर्न वाले अवसरों के बारे में ईमेल प्राप्त करना।
- पुरस्कार जारी करने के लिए प्रोसेसिंग शुल्क मांगने वाले लॉटरी ईमेल।
- नकली निवेश ऐप्स और वेबसाइटें।

रोकथाम के सुझाव:

- ऐसी योजनाओं में निवेश न करें जो असामान्य रूप से उच्च रिटर्न का वादा करती हों।
- निवेश कंपनी की वैधता की हमेशा सत्यापन करें।
- जब आपने किसी लॉटरी में भाग नहीं लिया है तो लॉटरी ईमेल को नज़रअंदाज़ करें।
- बड़े निवेश करने से पहले वित्तीय विशेषज्ञों से सलाह लें।





2.5 नौकरी का घोटाला (Job Scams)

धोखेबाज, छात्रों को विशेष रूप से पार्ट-टाइम कार्य या इंटरनशिप के लिए नकली नौकरी के प्रस्ताव देकर निशाना बनाते हैं ताकि वे उनकी व्यक्तिगत जानकारी या पैसे चुरा सकें।

आम परिदृश्य:

- नकली (फेक) नौकरी के प्रस्ताव जो आपको प्रशिक्षण या बैकग्राउंड चेक के लिए पैसे जमा करने की मांग करते हैं।
- आपके बैंक खाते के विवरण जैसी व्यक्तिगत जानकारी मांगना।
- ऐसी इंटरनशिप जो वास्तविक रोजगार की ओर कभी नहीं ले जाती।

रोकथाम के सुझाव:

- जिस कंपनी द्वारा नौकरी या इंटरनशिप की पेशकश की गई है, उसकी जांच करें।
- उन नौकरी प्रस्तावों से बचें जो व्यक्तिगत जानकारी या अग्रिम भुगतान मांगते हैं।
- नौकरी के प्रस्ताव को सीधे कंपनी से सत्यापित करें।



2.6 ई-कॉमर्स धोखाधड़ी

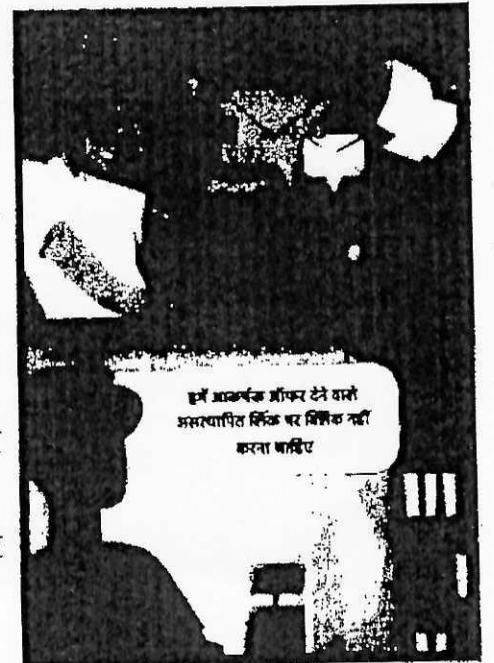
धोखेबाज नकली (फेक) ई-कॉमर्स वेबसाइट या प्लेटफॉर्म पर प्रोफाइल बनाकर उपभोगताओं को लुभावने डील के माध्यम से घटिया उत्पाद बेचने का प्रयास करते हैं।

आम परिदृश्य:

- नकली वेबसाइटें या विक्रेता जो बहुत ही कम कीमत पर उत्पाद बेच रहे हों।
- भुगतान करने के बाद उत्पाद की डिलीवरी नहीं होती।
- असली वस्तुओं के भुगतान के बाद नकली उत्पाद मिलना।

रोकथाम के सुझाव:

- विश्वसनीय ई-कॉमर्स वेबसाइटों से ही खरीदारी करें।
- खरीदारी करने से पहले विक्रेता की प्रमाणिकता तथा रेटिंग की जांच करें।
- सुरक्षित भुगतान गेटवे का उपयोग करें और अज्ञात खातों में सीधे हस्तांतरण से बचें।
- बहुत कम कीमत वाले ऑफर से सावधान रहें।





2.7 सोशल मीडिया घोटाला

साइबर अपराधी सोशल मीडिया प्लेटफॉर्म का उपयोग लोगों की व्यक्तिगत जानकारी साझा करने, Malicious लिंक पर क्लिक करने या धनराशि ट्रांसफर करने के लिए कहते हैं।

आम परिदृश्य:

- नकली प्रोफाइल द्वारा मित्रता या धन मांगने की पेशकश
- व्यक्तिगत डेटा चुराने वाले Malicious लिंक वाले संदेश
- आपातकालीन वित्तीय सहायता मांगने वाले धोखेबाजा

इंटरनेट पर निजी फोटो/वीडियो साझा करते समय सतर्क रहें

सोशल मीडिया पर कुछ भी शेयर करने से पहले सही प्राइवैसी सेटिंग्स चुनें



रोकथाम के सुझाव:

- अज्ञात व्यक्तियों की मित्रता अनुरोधों को स्वीकार करते समय सतर्क रहें।
- अपना फ़ोन नंबर, पता, या बैंकिंग जानकारी सार्वजनिक रूप से शेयर न करें।
- संदिग्ध खातों को रिपोर्ट और ब्लॉक करें और सोशल मीडिया पर गोपनीयता सेटिंग्स का उपयोग करें।

2.8 डिजिटल गिरफ्तारी/वसूली घोटाला

इन घोटालों में, पीड़ितों को धमकी भरे कॉल या संदेश प्राप्त होते हैं जिनमें कहा जाता है कि वे जांच के दायरे में हैं या उनके खिलाफ गिरफ्तारी वारंट लंबित है। धोखेबाज मुद्दे को "सुलझाने" के लिए पैसे की मांग करते हैं।

आम परिदृश्य:

- आपकी जांच या कानूनी कार्रवाई का दावा करने वाले धमकी भरे ईमेल या कॉल
- कानून प्रवर्तन या कर अधिकारी बनकर धनराशि की मांग करने वाले धोखेबाजा
- गिरफ्तारी या कानूनी जुर्माने के नकली नोटिस।

रोकथाम के सुझाव:

- धमकी भरे ईमेल या कॉल से घबरानें नहीं या प्रतिक्रिया न दें।
- कार्रवाई करने से पहले कानूनी अधिकारियों के साथ सत्यापन करें।
- वसूली के प्रयासों को साइबर अपराध सेल या स्थानीय पुलिस थानों को रिपोर्ट करें।





2.9 फिशिंग घोटाला

फिशिंग घोटाले नकली ईमेल या संदेश के माध्यम से नागरिकों को पासवर्ड या बैंक विवरण जैसे संवेदनशील निजी जानकारी प्राप्त कर धोखा देने का प्रयास करते हैं या फिशिंग ई-मेल इस प्रकार से तैयार किये जाते हैं कि वे वैध संगठनों से भेजे गये प्रतीत होते हैं।

आम परिदृश्य:

- आपके बैंक से आये प्रतीत होने वाले नकली ईमेल, जो आपको अपना खाता सत्यापित करने के लिए कहते हैं।
- ईमेल या एसएमएस के साथ Malicious लिंक, जो आपको वैध सेवाओं की फेक नकली वेबसाइटों पर ले जाते हैं।
- ऐसे ईमेल में अटैचमेंट जिन पर क्लिक करने से आपके डिवाइस में मैलवेयर इंस्टॉल हो जाता है।

रोकथाम के सुझाव:

- अवांछित ईमेल या एसएमएस में प्राप्त लिंक पर क्लिक करने से बचें।
- हमेशा प्रेषक (सेन्डर) का ईमेल पता जांच लें तथा यह सुनिश्चित कर लें कि यह ईमेल वैध (अथैटिक सोर्स) से आया है।
- अज्ञात स्रोतों से आने वाले लिंक और अटैचमेंट पर क्लिक करने से बचें।
- एंटी-फिशिंग सॉफ्टवेयर इंस्टॉल करें और यह सुनिश्चित करें कि आपका डिवाइस सुरक्षित है।





3 ऑनलाइन सुरक्षित रहने के लिए प्रमुख सुझाव

- जटिल पासवर्ड: प्रत्येक खाते के लिए जटिल और यूनिक पासवर्ड का उपयोग करें और टू-फैक्टर ऑथेंटिकेशन का प्रयोग करें।
- सतर्क रहें: लिंक, ईमेल या संदेशों को विलक करने या जवाब देने से पहले सत्यापित करें।
- नियमित अपडेट: अपने सॉफ्टवेयर और उपकरणों को नवीनतम सुरक्षा अपडेट के साथ अपडेट रखें।
- गोपनीयता महत्वपूर्ण है: ऑनलाइन साझा की जाने वाली व्यक्तिगत जानकारी को सीमित रखें।
- संदिग्ध गतिविधि की रिपोर्ट करें: यदि आप किसी संदिग्ध संदेश या ऑनलाइन गतिविधि का सामना करते हैं, तो अपनी स्कूल या कॉलेज की आईटी टीम को सूचित करें।

4 साइबर अपराधों की रिपोर्टिंग

अगर आपको संदेह है कि आप किसी साइबर अपराध का शिकार हुए हैं, तो आप निकटतम पुलिस स्टेशन पर रिपोर्ट कर सकते हैं या राष्ट्रीय साइबर अपराध रिपोर्टिंग सम्बन्धी पोर्टल (<https://cybercrime.gov.in>) से संपर्क कर सकते हैं। किसी भी वित्तीय धोखाधड़ी के लिए राष्ट्रीय साइबर अपराध हेल्पलाइन नम्बर 1930 पर सूचित करें अथवा अपने बैंक से भी संपर्क कर सकते हैं और अपने खातों/कार्डों को ब्लॉक करा सकते हैं ताकि आगे नुकसान से बचा जा सके।

सतर्क रहें, सुरक्षित रहें।





2.3 सोशल मीडिया घोटाला

साइबर अपराधी सोशल मीडिया प्लेटफॉर्म का उपयोग लोगों की व्यक्तिगत जानकारी साझा करने, Malicious लिंक पर क्लिक करने या धनराशि ट्रांसफर करने के लिए कहते हैं।

आम परिदृश्य:

- नकली प्रोफाइल द्वारा मित्रता या धन मांगने की पेशकश
- व्यक्तिगत डेटा चुराने वाले Malicious लिंक वाले संदेश
- आपातकालीन वित्तीय सहायता मांगने वाले धोखेबाजा

रोकथाम के सुझाव:

- अज्ञात व्यक्तियों की मित्रता अनुरोधों को स्वीकार करते समय सतर्क रहें।
- अपना फ़ोन नंबर, पता, या बैंकिंग जानकारी सार्वजनिक रूप से शेयर न करें।
- संदिग्ध खातों को रिपोर्ट और ब्लॉक करें और सोशल मीडिया पर गोपनीयता सेटिंग्स का उपयोग करें।

इंटरनेट पर निजी फोटो/वीडियो साझा करते समय सतर्क रहें

सोशल मीडिया पर कुछ भी शेयर
करने से पहले सही प्राइवैसी
सेटिंग्स चुनें





2.4 गेमिंग ऐप घोटाला (Gaming App Scams)

गेमिंग ऐप घोटाला खिलाड़ियों को मुफ्त इन-गेम करेंसी, दुर्लभ आइटम या चीट्स का वादा करके धोखा देते हैं, जिनके लिए लॉगिन विवरण या भुगतान की आवश्यकता होती है।

आम परिदृश्य:

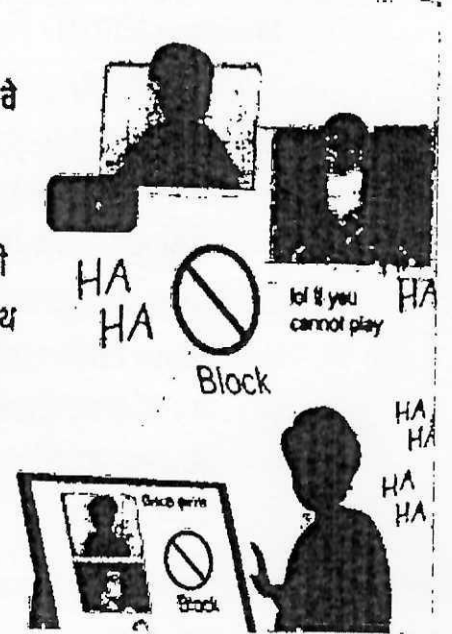
- नकली (फेक) वेबसाइट या ऐप्स जो मुफ्त गेम डाउनलोड या चीट्स की पेशकश करते हैं।
- खिलाड़ियों को ऐसे इन-गेम आइटम खरीदने के लिए धोखा देना जो असल में मौजूद नहीं होते।
- इन-गेम नोटिफिकेशन या संदेशों के रूप में छिपे हुए फिशिंग प्रयास।

ऑनलाइन गेम मनोरंजन के लिए हैं, वे आपको परिभाषित नहीं करते हैं।

सुरक्षित रहें और किसी वदमाश को अपने साथ खिलवाड़ न करने दें।

Online games are for fun, they do not define you. Play safe and don't let a bully mess with you.

#सुरक्षित रहें।



शेकथाम के सुझाव:

- केवल आधिकारिक ऐप स्टोर्स से गेम और ऐप्स डाउनलोड करें।
- कभी भी अपने गेम खाते का विवरण किसी के साथ साझा न करें।
- गेम के लिए थर्ड-पार्टी चीट्स या मॉड्स का उपयोग करने से बचें।

2.5 ऑनलाइन डेटिंग ऐप घोटाला (Online Dating App Scams)

डेटिंग ऐप्स पर धोखेबाज भावनाओं का लाभ उठाकर धनराशि या व्यक्तिगत जानकारी चुराने का प्रयास करते हैं।

आम परिदृश्य:

- नकली प्रोफाइल बनाकर आपसे मित्रता करने का प्रयास करते हैं।
- धनराशि भेजने की मांग करना, आपात स्थिति या तत्काल आवश्यकता का दावा करना।
- व्यक्तिगत जानकारी, तस्वीरें या लॉगिन क्रेडेंशियल्स मांगना।





शेकथाम के सुझाव:

- जब आप किसी से ऑनलाइन मिलें तो सतर्क रहें।
- किसी ऐसे व्यक्ति को कभी धनराशि न भेजें जिसे आप व्यक्तिगत रूप से नहीं मिले हैं।
- डेटिंग ऐप्स पर संवेदनशील जानकारी (जैसे पता, पासवर्ड या निजी तस्वीरें) साझा करने से बचें।

2.6 ई-कॉमर्स धोखाधड़ी

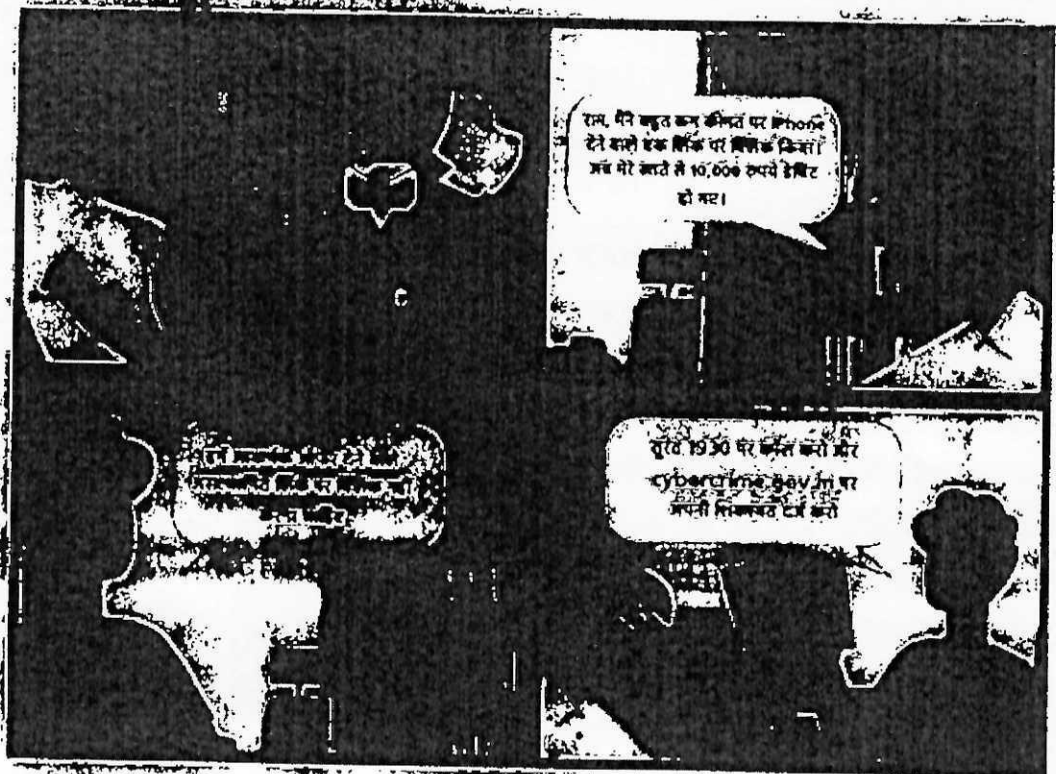
धोखेबाज नकली (फेक) ई-कॉमर्स वेबसाइट या प्लेटफॉर्म पर प्रोफाइल बनाकर उपभोक्ताओं को लुभावने डील के माध्यम से घटिया उत्पाद बेचने का प्रयास करते हैं।

आम परिदृश्य:

- नकली वेबसाइटें या विक्रेता जो बहुत ही कम कीमत पर उत्पाद बेच रहे हों।
- भुगतान करने के बाद उत्पाद की डिलीवरी नहीं होती।
- असली वस्तुओं के भुगतान के बाद नकली उत्पाद मिलना।

शेकथाम के सुझाव:

- विश्वसनीय ई-कॉमर्स वेबसाइटों से ही खरीदारी करें।
- खरीदारी करने से पहले विक्रेता की प्रमाणिकता तथा रेटिंग की जांच करें।
- सुरक्षित भुगतान गेटवे का उपयोग करें और अज्ञात खातों में सीधे हस्तांतरण से बचें।
- बहुत कम कीमत वाले ऑफर से सावधान रहें।





2.7 नौकरी का घोटाला (Job Scams)

धोखेबाज, छात्रों को विशेष रूप से पार्ट-टाइम कार्य या इंटरनशिप के लिए नकली नौकरी के प्रस्ताव देकर निशाना बनाते हैं ताकि वे उनकी व्यक्तिगत जानकारी या पैसे चुरा सकें।

आम परिदृश्य:

- नकली (फेक) नौकरी के प्रस्ताव जो आपको प्रशिक्षण या बैंकग्राउंड चेक के लिए पैसे जमा करने की मांग करते हैं।
- आपके बैंक खाते के विवरण जैसी व्यक्तिगत जानकारी मांगना।
- ऐसी इंटरनशिप जो वास्तविक रोजगार की ओर कभी नहीं ले जाती।

रोकथाम के सुझाव:

- जिस कंपनी द्वारा नौकरी या इंटरनशिप की पेशकश की गई है, उसकी जांच करें।
- उन नौकरी प्रस्तावों से बचें जो व्यक्तिगत जानकारी या अग्रिम भुगतान मांगते हैं।
- नौकरी के प्रस्ताव को सीधे कंपनी से सत्यापित करें।



2.8 डिजिटल गिरफ्तारी/वसूली घोटाला

इन घोटालों में, पीड़ितों को धमकी भरे कॉल या संदेश प्राप्त होते हैं जिनमें कहा जाता है कि वे जांच के दायरे में हैं या उनके खिलाफ गिरफ्तारी वारंट लंबित है। धोखेबाज मुद्दे को "सुलझाने" के लिए पैसे की मांग करते हैं।

आम परिदृश्य:

- आपकी जांच या कानूनी कार्रवाई का दावा करने वाले धमकी भरे ईमेल या कॉल।
- कानून प्रवर्तन या कर अधिकारी बनकर धनराशि की मांग करने वाले धोखेबाजा।
- गिरफ्तारी या कानूनी जुर्माने के नकली नोटिस।

रोकथाम के सुझाव:

- धमकी भरे ईमेल या कॉल से घबराएं नहीं या प्रतिक्रिया न दें।
- कार्रवाई करने से पहले कानूनी अधिकारियों के साथ सत्यापन करें।
- वसूली के प्रयासों को साइबर अपराध सेल या स्थानीय पुलिस थानों को रिपोर्ट करें।





2.9 रैनसमवेयर हमला (Ransomware Attacks)

रैनसमवेयर एक प्रकार का मेलवेयर है जो आपकी फ़ाइलों को एन्क्रिप्ट कर देता है और उन्हें अनलॉक करने के लिए भुगतान (अक्सर क्रिप्टोकॉरेंसी में) की मांग करता है।

आम परिदृश्य:

- अज्ञात ईमेल से संलग्नक डाउनलोड करना या लिंक पर क्लिक करना।
- Compromised की गई वेबसाइटों पर जाना या अविश्वसनीय स्रोतों से मुफ्त सॉफ्टवेयर डाउनलोड करना।

रोकथाम के सुझाव:

- अपनी फ़ाइलों का नियमित रूप से किसी अन्य जगह (ऑनलाइन/ऑफलाइन) बाहरी स्रोत पर बैकअप लें।
- एंटीवायरस सॉफ्टवेयर इन्स्टॉल करें और इसे अपडेट रखें।
- अज्ञात या संदिग्ध स्रोतों से संलग्नक डाउनलोड करने से बचें।

3 ऑनलाइन सुरक्षित रहने के लिए प्रमुख सुझाव

- जटिल पासवर्ड: प्रत्येक खाते के लिए जटिल और यूनिक पासवर्ड का उपयोग करें और टू-फैक्टर ऑथेंटिकेशन का प्रयोग करें।
- सतर्क रहें: लिंक, ईमेल या संदेशों को क्लिक करने या जवाब देने से पहले सत्यापित करें।
- नियमित अपडेट: अपने सॉफ्टवेयर और उपकरणों को नवीनतम सुरक्षा अपडेट के साथ अपडेट रखें।
- गोपनीयता महत्वपूर्ण है: ऑनलाइन साझा की जाने वाली व्यक्तिगत जानकारी को सीमित रखें।
- संदिग्ध गतिविधि की रिपोर्ट करें: यदि आप किसी संदिग्ध संदेश या ऑनलाइन गतिविधि का सामना करते हैं, तो अपनी स्कूल या कॉलेज की आईटी टीम को सूचित करें।

4 साइबर अपराधों की रिपोर्टिंग

अगर आपको संदेह है कि आप किसी साइबर अपराध का शिकार हुए हैं, तो आप निकटतम पुलिस स्टेशन पर रिपोर्ट कर सकते हैं या राष्ट्रीय साइबर अपराध रिपोर्टिंग सम्बन्धी पोर्टल (<https://cybercrime.gov.in>) से संपर्क कर सकते हैं। किसी भी वित्तीय धोखाधड़ी के लिए राष्ट्रीय साइबर अपराध हेल्पलाइन नम्बर 1930 पर सूचित करें अथवा अपने बैंक से भी संपर्क कर सकते हैं और अपने खातों/कार्डों को ब्लॉक करा सकते हैं ताकि आगे नुकसान से बचा जा सके।

सतर्क रहें, सुरक्षित रहें।





CYBER SECURITY AWARENESS

"STAY ALERT, STAY SECURE!"



"Cyber Security Awareness for Citizens – Protect Yourself from Online Threats!"
"नागरिकों के लिए साइबर सुरक्षा जागरूकता – खुद को ऑनलाइन खतरों से सुरक्षित रखें"

यूपीआई धोखाधड़ी/नेट बैंकिंग धोखाधड़ी/क्रेडिट कार्ड धोखाधड़ी

- सेंटर में पहले हमेशा UPI ID या अपना अकाउंट बनाने से पहले बैंक के लिए टी-एचडी (T-Code) का उपयोग करें और अपना बैंक खाते के लिए संपूर्ण जानकारी का उपयोग करें
- OTP या SMS सिर्फ ही साझा या उन्हें इंटरनेट ब्राउज़िंग पर लिंक करने से करें

मिसेज या लॉटरी धोखाधड़ी

- मिसेज या लॉटरी को आधिकारिक खतरों से आसानी से अलग करने के लिए टी-एचडी (T-Code) का उपयोग करें
- अपनी अनजाने बहाने वाली संकेतकों पर विश्वास न करें अनजाने फोन कॉल पर व्यक्तिगत या बैंकिंग जानकारी साझा न करें

ई-कॉमर्स धोखाधड़ी

- विश्वसनीय और प्रमाणित ई-कॉमर्स वेबसाइटों से खरीदारी करें और अपने खरीदारी से पहले खरीदार और डीलर चेक करें
- अति इतनी सस्ता या टी-एचडी के बजाय से न करें अत्यधिक इच्छाओं पर कार्य विचार साझा करने से बचें

सोशल मीडिया धोखाधड़ी/ऑनलाइन डेटिंग ऐप धोखाधड़ी

- फ्रेंड रिक्वेस्ट स्वीकार करने से पहले प्रोफाइल सत्यापित करें अपनी जानकारी को शेयर न करें
- ऑनलाइन डेटिंग के लिए सोशल मीडिया प्रोफाइल का उपयोग करें
- अज्ञानियों के साथ व्यक्तिगत तथ्यों या संवेदनशील जानकारी साझा न करें केवल प्रोफाइल प्रोफाइल को चेक करने से बचें

नौकरी धोखाधड़ी

- नौकरी प्रस्तावों को कंपनी की आधिकारिक वेबसाइट या HR विभाग से आसानी से सत्यापित करें नौकरी प्रस्तावों से सम्बंधित सभी व्यक्तिगत जानकारी का सावधान रहें
- अनजाने ईमेल या कॉल के जरूरत से व्यक्तिगत जानकारी न दें

फिशिंग धोखाधड़ी/पहचान की चोरी

- फिशिंग वेबसाइटों को पहचानने से पहले फेसबुक की ईमेल नोटिफिकेशन चेक करें और वेबसाइटों को सत्यापित करने से सतर्क रहें
- अपनी अनजाने बहाने वाली संकेतकों पर विश्वास न करें अनजाने फोन कॉल पर व्यक्तिगत या बैंकिंग जानकारी साझा न करें

गेलिंग ऐप धोखाधड़ी

- गेलिंग ऐप को आधिकारिक ऐप स्टोर से डाउनलोड करें और खरीदारी के लिए सर्विस प्रोवाइडर और वेबसाइटों से चेक करें
- अज्ञानियों के साथ व्यक्तिगत जानकारी साझा न करें

टैक्सोयड इमला

- अपनी महत्वपूर्ण डेटा का प्रोफाइल रूप में सुरक्षित रखें और केवल विश्वसनीय और प्रमाणित ऐप से डाउनलोड करें
- ऑनलाइन डेटिंग प्रोफाइल पर विश्वास न करें

Stay Informed, Stay Safe – Report Cyber Crimes Immediately!
सचेत रहें, सुरक्षित रहें – साइबर अपराधों की तुरंत रिपोर्ट करें!

साइबर हेल्पलाइन: 1930

खुद को और अपने परिवार को साइबर खतरों से बचाएं



छात्रों के लिए साइबर अपराध से बचने हेतु पुस्तिका

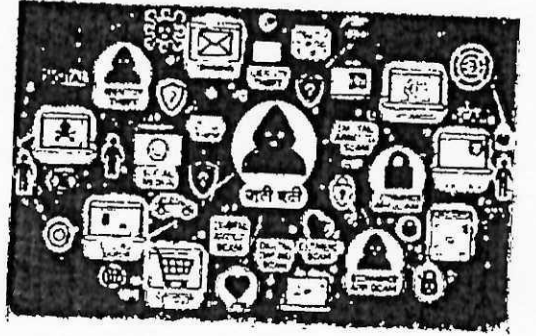
Department of
IT & Electronics

1. भूमिका

वर्तमान परिदृश्य की डिजिटल दुनिया में युवा छात्र इंटरनेट का उपयोग जैसे- अध्ययन, सामाजिकता (सोशल मीडिया), खेल तथा अन्य गतिविधियों के लिए अधिकाधिक कर रहे हैं। सामान्यता इंटरनेट के अनेकानेक लाभ हैं, परन्तु इसके साथ जोखिम भी जुड़े होते हैं। साइबर अपराधी (साइबर क्रिमिनल्स) अवसर छात्रों को विभिन्न प्रकार की ऑनलाइन धोखाधड़ी के माध्यम से निशाना (टारगेट) बनाते हैं। इस पुस्तिका का उद्देश्य स्कूल और कॉलेज के छात्र/छात्राओं को नवीनतम साइबर सुरक्षा धोखाधड़ी के सम्बन्ध में जागरूक करना तथा ऑनलाइन सुरक्षित रहने के लिए आवश्यक कदम उठाने में उनकी सहायता करना है।

2. साइबर धोखाधड़ी के तरीकों की सूची

- पहचान की चोरी (Identity Theft)
- फ़िशिंग घोटाला (Phishing Scams)
- सोशल मीडिया घोटाला (Social Media Scams)
- गेमिंग ऐप घोटाला (Gaming App Scams)
- ऑनलाइन डेटिंग ऐप घोटाला (Online Dating App Scams)
- ई-कॉमर्स घोटाला (E-Commerce Scams)
- नौकरी के घोटाला (Job Scams)
- डिजिटल गिरफ्तारी/जबरन वसूली घोटाला (Digital Arrest/Extortion Scams)
- रैनसमवेयर हमला (Ransom ware Attacks)



2.1 पहचान की चोरी (Identity Theft)

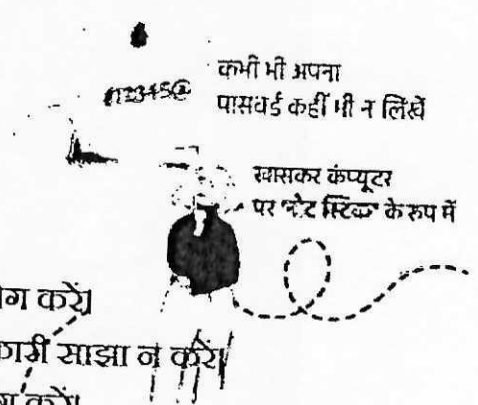
पहचान की चोरी तब होती है जब कोई व्यक्ति आपकी व्यक्तिगत जानकारी जैसे नाम, ई-मेल आईडी, पासवर्ड इत्यादि का दुरुपयोग करके धोखाधड़ी करता है।

आम परिदृश्य:

- सोशल मीडिया खातों को हैक करना
- फ़िशिंग ईमेल जो आपकी व्यक्तिगत जानकारी मांगते हैं।
- एक ही पासवर्ड का कई जगह उपयोग करना।

रोकथाम के सुझाव:

- प्रत्येक खाते के लिए जटिल और यूनिक पासवर्ड का उपयोग करें।
- ऑनलाइन या अजनबियों के साथ अपनी व्यक्तिगत जानकारी साझा न करें।
- जहां भी संभव हो, टू-फैक्टर ऑथेंटिकेशन (2FA) का उपयोग करें।
- नियमित रूप से अपने सोशल मीडिया एकाउंट की गोपनीयता सेटिंग्स को चेक करें।





2.2 फिशिंग घोटाला

फिशिंग घोटाले नकली ईमेल या संदेश के माध्यम से नागरिकों को पासवर्ड या बैंक विवरण जैसे संवेदनशील निजी जानकारी प्राप्त कर धोखा देने का प्रयास करते हैं या फिशिंग ई-मेल इस प्रकार से तैयार किये जाते हैं कि वे बैंक संगठनों से भेजे गये प्रतीत होते हैं।

आम परिदृश्य:

- आपके बैंक से आये प्रतीत होने वाले नकली ईमेल, जो आपको अपना खाता सत्यापित करने के लिए कहते हैं।
- ईमेल या एसएमएस के साथ Malicious लिंक, जो आपको बैंक सेवाओं की फेक नकली वेबसाइटों पर ले जाते हैं।
- ऐसे ईमेल में अटैचमेंट जिन पर क्लिक करने से आपके डिवाइस में मैलवेयर इंस्टॉल हो जाता है।

रोकथाम के सुझाव:

- अवांछित ईमेल या एसएमएस में प्राप्त लिंक पर क्लिक करने से बचें।
- हमेशा प्रेषक (सेन्डर) का ईमेल पता जांच लें तथा यह सुनिश्चित कर लें कि यह ईमेल बैंक (अथैटिक सोर्स) से आया है।
- अज्ञात स्रोतों से आने वाले लिंक और अटैचमेंट पर क्लिक करने से बचें।
- एंटी-फिशिंग सॉफ्टवेयर इंस्टॉल करें और यह सुनिश्चित करें कि आपका डिवाइस सुरक्षित है।

