डॉ0 ए0पी0जे0 अब्दुल कलाम प्राविधिक विश्वविद्यालय उत्तर प्रदेश
सेक्टर-11, जानकीपुरम विस्तार योजना, लखनऊ-226031

पत्रांकः ए0के0टी0यू0/कुस0का0/स्था0/2024/4845 दिनांकः 30 नवम्बर, 2024

सेवा में,

निदेशक/प्राचार्य,

विश्वविद्यालय से सम्बद्ध समस्त संस्थान।

विषयः साइबर सुरक्षा जागरूकता अभियान आयोजित किये जाने के संबंध में।

महोदय,

कृपया उपर्युक्त विषय के संबंध में प्राविधिक शिक्षा अनुभाग–3, उत्तर प्रदेश शासन, लखनऊ के पत्र संख्याः I/796344/2024/16–3099/292/2024 दिनांक 14.11.2024 (प्रति संलग्न) का संदर्भ ग्रहण करने का कष्ट करें।

उक्त के संदर्भ में अवगत कराना है कि शासन के पत्र में उल्लिखित आई0टी0 एवं इलेक्ट्रानिक्स अनुभाग–1 के पत्र संख्या–1692/78–1–2024–1099/619/2020 दिनांक 19.10.2024 (छायाप्रति संलग्न) के माध्यम से नागरिकों, छात्र/छात्राओं तथा सरकारी अधिकारियों को साइबर खतरों/हमलों से खुद को सुरक्षित रखने हेतु उपाय/सावधानियों संबंधी हैण्डबुक उपलब्ध कराते हुए इस संबंध में आवश्यक कार्यवाही सुनिश्चित किये जाने हेतु संबंधित अधिकारियों/संस्थाओं को निर्देशित करने तथा जागरूकता कार्यक्रम आरम्भ किये जाने एवं गतिविधियों की प्रगति रिपोर्ट नियमित रूप से सेंटर फार ई–गवर्नेंस, यू0पी0 (ई–मेल ceglko@gmail.com) तथा शासन को उपलब्ध कराये जाने की अपेक्षा की गयी है।

अतः मुझे यह कहने का निदेश हुआ है कि शासन के पत्र दिनांक 14.11.2024 के साथ संलग्न इलेक्ट्रानिक्स अनुभाग–1 के पत्र दिनांक 19.10.2024 में की गयी अपेक्षानुसार साइबर सुरक्षा जागरूकता अभियान/कार्यक्रम आयोजित करते हुए गतिविधियों की प्रगति रिपोर्ट नियमित रूप से सेंटर फार ई–गवर्नेंस, यू0पी0 (ई–मेल ceglko@gmail.com) तथा शासन को उपलब्ध कराने का कष्ट करें।

संलग्नकः यथोक्त।

भवदीय

(रीना सिंह)
कुलसचिव

प्रतिलिपिः निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

1. अधिष्ठाता, ट्रेनिंग एण्ड प्लेसमेंट, ए0के0टी0यू0, लखनऊ को इस आशय से प्रेषित है कि सक्षम स्तर द्वारा उक्त कार्य हेतु आप को नोडल अधिकारी नामित किया गया है। अतः नोडल अधिकारी से अपेक्षा है कि शासनादेश में दिये गये निर्देश के क्रम में आई0ई0टी0 एवं इलेक्ट्रानिक्स अनुभाग–1 के पत्र दिनांक 19.10.2024 में की गयी अपेक्षानुसार साइबर सुरक्षा जागरूकता अभियान/कार्यक्रम आयोजित करते हुए गतिविधियों की प्रगति रिपोर्ट नियमित रूप से सेन्टर फार ई–गवर्नेंस, यू0पी0(ई–मेल ceglko@gmail.com) पर उपलब्ध कराने का कष्ट करें।
2. श्री वीर विक्रम सिंह, रिसर्च इंजीनियर, ए0के0टी0यू0, लखनऊ।
3. स्टाफ आफिसर, ए0के0टी0यू0, लखनऊ को मा0 कुलपति महोदय के अवलोकनार्थ।

(रीना सिंह)
कुलसचिव

355

संख्या: I/796344/2024/16-3099/292/2024

प्रेषक,

प्रभाकर चन्द्र मिश्र,
संयुक्त सचिव,
उत्तर प्रदेश शासन।

सेवा में,

1. महानिदेशक, प्राविधिक शिक्षा, उ०प्र०।
2. कुलसचिव, ए0के0टी0यू0, उ०प्र० लखनऊ।
3. कुलसचिव, एच0बी0टी0यू0, उ०प्र० कानपुर।
4. कुलसचिव, एम0एम0एम0यू0टी0, उ०प्र० गोरखपुर।
5. निदेशक, प्राविधिक शिक्षा, उ0प्र0, कानपुर।
6. सचिव, प्राविधिक शिक्षा परिषद, उत्तर प्रदेश, लखनऊ।
7. सचिव, संयुक्त प्रवेश परीक्षा परिषद, उ0प्र0, लखनऊ।
8. निदेशक, बुंदेलखण्ड अभियांत्रिकी एवं प्रौद्योगिकी संस्थान, झांसी।
9. निदेशक, कमला नेहरु प्रौद्योगिकी संस्थान, सुल्तानपुर।
10. निदेशक, समस्त राजकीय इंजीनियरिंग कालेज, उ०प्र०।
11. सचिव, प्रवेश एवं फीस विनियम समिति, लखनऊ।
12. निदेशक, उत्तर प्रदेश वस्त्र प्रौद्योगिकी संस्थान, कानपुर।
13. निदेशक, आई०आर०डी०टी०, उ०प्र० कानपुर।

प्राविधिक शिक्षा अनुभाग-3 **लखनऊ: दिनांक:14-11-2024**

विषय- साइबर सुरक्षा जागरूकता अभियान आयोजित किये जाने के संबंध में।

महोदय,

उपर्युक्त विषयक आई.टी. एवं इलेक्ट्रानिक्स अनुभाग-1 के पत्र संख्या-1692/78-1-2024-1099/619/2020, दिनांक 19.10.2024 (छायाप्रति मय संलग्नक संलग्न) का कृपया सन्दर्भ ग्रहण करने का कष्ट करें, जिसके माध्यम से नागरिकों, छात्र/छात्राओं तथा सरकारी अधिकारियों को साइबर खतरों/हमलों से खुद को सुरक्षित रखने हेतु उपाय/सावधानियों संबंधी हैण्डबुक उपलब्ध कराते हुए इस संबंध में आवश्यक कार्यवाही सुनिश्चित किये जाने हेतु संबंधित अधिकारियों/संस्थाओं को निर्देशित करने तथा जागरूकता कार्यक्रम आरम्भ किये जाने एवं गतिविधियों की प्रगति

354

रिपोर्ट नियमित रूप से सेंटर फार ई-गवर्नेंस, यू0पी0 (ई-मेल ceglko@gmail.com) तथा शासन को उपलब्ध कराये जाने की अपेक्षा की गयी है।

2. उक्त के सम्बन्ध में मुझे यह कहने का निदेश हुआ है कि आई.टी. एवं इलेक्ट्रानिक्स अनुभाग-1 के पत्र दिनांक 19.10.2024 में की गयी अपेक्षानुसार साइबर सुरक्षा जागरूकता अभियान/कार्यक्रम आयोजित करते हुए गतिविधियों की प्रगति रिपोर्ट नियमित रूप से सेंटर फार ई-गवर्नेंस, यू0पी0 (ई-मेल ceglko@gmail.com) तथा शासन को उपलब्ध कराने का कष्ट करें।

संलग्नक: यथोक्त।

भवदीय,

Signed by
Prabhakar Chandra Mishra (प्रभाकर चन्द्र मिश्र)
Date: 14-11-2024 10:56:28 संयुक्त सचिव।

संख्या व दिनांक तदैव।

प्रतिलिपि मय संलग्नक प्राविधिक शिक्षा अनुभाग-1/2 को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

संलग्नक: यथोक्त।

आज्ञा से,

(प्रभाकर चन्द्र मिश्र)
संयुक्त सचिव।

संख्या-2400/ माह-3-2024

संख्या 1367/मु. सचिव/.../2024

संख्या:-1692/78-1-2024-1099/619/2020

प्रेषक,

अनिल कुमार सागर,
प्रमुख सचिव,
उ0प्र0 शासन।

सेवा में,

1. समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव, उ0प्र0 शासन।
2. समस्त मण्डलायुक्त, उत्तर प्रदेश।
3. समस्त जिलाधिकारी, उत्तर प्रदेश।

VS(AA/D)

25/10/24

(आलोक कुमार)
प्रमुख सचिव
प्राविधिक शिक्षा विभाग,
उत्तर प्रदेश, शासन

आई.टी. एवं इलेक्ट्रानिक्स अनुभाग-1 लखनऊ:दिनांक 19 अक्टूबर, 2024

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

महोदय,

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 अर्न्तराष्ट्रीय स्तर पर राष्ट्रीय साइबर सुरक्षा जागरूकता माह (एन०सी०एस०ए०एम०) के रूप में मनाया जाता है, जिसका उद्देश्य सार्वजनिक एवं निजी क्षेत्र के साथ-साथ आम नागरिकों को भी साइबर सुरक्षा हेतु जागरूक करना है।

720/VS(T) 17/24

25/10/24

(अजीज ...)
विशेष स...
प्राविधिक शि...
उ०प्र० श...

3- इसी क्रम में भारत सरकार द्वारा इस वर्ष के अभियान का विषय 'साइबर सुरक्षित भारत" (#SatarkNagrik) 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/सावधानियाँ निम्नवत् हैः-

SO-3

(1) नागरिकों हेतु साइबर सुरक्षा जागरूकता:-

वित्तीय 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 वित्तीय धोखाधड़ी से जुड़े नवीनतम साइबर अपराधों के रुझानों के बारे में जानकारी देना सम्मिलित है जैसे-

25/10/24

(1) UPI घोटाले

(2) नेट बैंकिंग धोखाधड़ी

28/10/2024

(3)क्रेडिट कार्ड धोखाधड़ी

(4) निवेश या लॉटरी घोटाले

(5) नौकरी घोटाले

(6) ई-कॉमर्स धोखाधड़ी

(7) सोशल मीडिया घोटाले

(8) डिजिटल गिरफ्तारी वसूली घोटाले

(9) फ़िशिंग घोटाले

(10) साइबर अपराधों 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) छात्रों हेतु साइबर सुरक्षा जागरूकता:-

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

(1) पहचान की चोरी (Identity Theft)

(2) फ़िशिंग घोटाले (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 छात्रों 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, उ0प्र0 शासन साइबर सुरक्षा धोखाधड़ी रोकथाम तथा सुरक्षा के मुख्य उपायों की एक हैण्डबुक 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 जागरुकता 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-गर्वेन्स, यू0पी0 (ई-मेल आई0डी0-cegiko.up@gmail.com) तथा शासन को उपलब्ध कराने का कष्ट करें।

संलग्नकः 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 तद्दिनांक

उपर्युक्त की प्रतिलिपि निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषितः-

1. निजी सचिव, मुख्य सचिव, उ0प्र0 शासन।
2. राज्य समन्वयक, सेन्टर फॉर ई-गवर्नेन्स, उ0प्र0, अपट्रान बिल्डिंग, गोमती नगर, लखनऊ।
3. राज्य सूचना विज्ञान अधिकारी, एनं० आई०सी०, लखनऊ।
4. हेड, एस०ई०एम०टी०, उ०प्र०।
5. गार्ड फाइल।

आज्ञा से,

(नेहा जैन)
विशेष सचिव।

350

1. भूमिका

वर्तमान परिदृश्य की डिजिटल दुनिया में युवा छात्र इंटरनेट का उपयोग जैसे- अध्ययन, सामाजिकता (सोशलाइजिंग), 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) फ़िशिंग 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

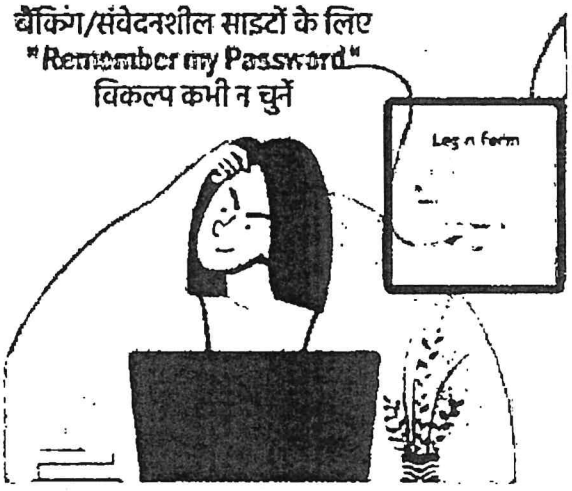
नेट बैंकिंग धोखाधड़ी तब होती है जब साइबर अपराधी फ़िशिंग अटैक, मैलवेयर या नकली वेबसाइटों के माध्यम से आपके बैंकिंग क्रेडेंशियल्स चुराते हैं, जिससे अनधिकृत लेनदेन होता है।

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 अनाधिकृत साफ्टवेयर का इस्तेमाल करना।

रोकथाम के सुझाव:

- अंजान 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 (पी0ओ0एस0) मशीनों पर स्किमिंग डिवाइस लगे होना।
- आपका कार्ड सेवा प्रदाता होने का दावा करने वाले फ़िशिंग 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

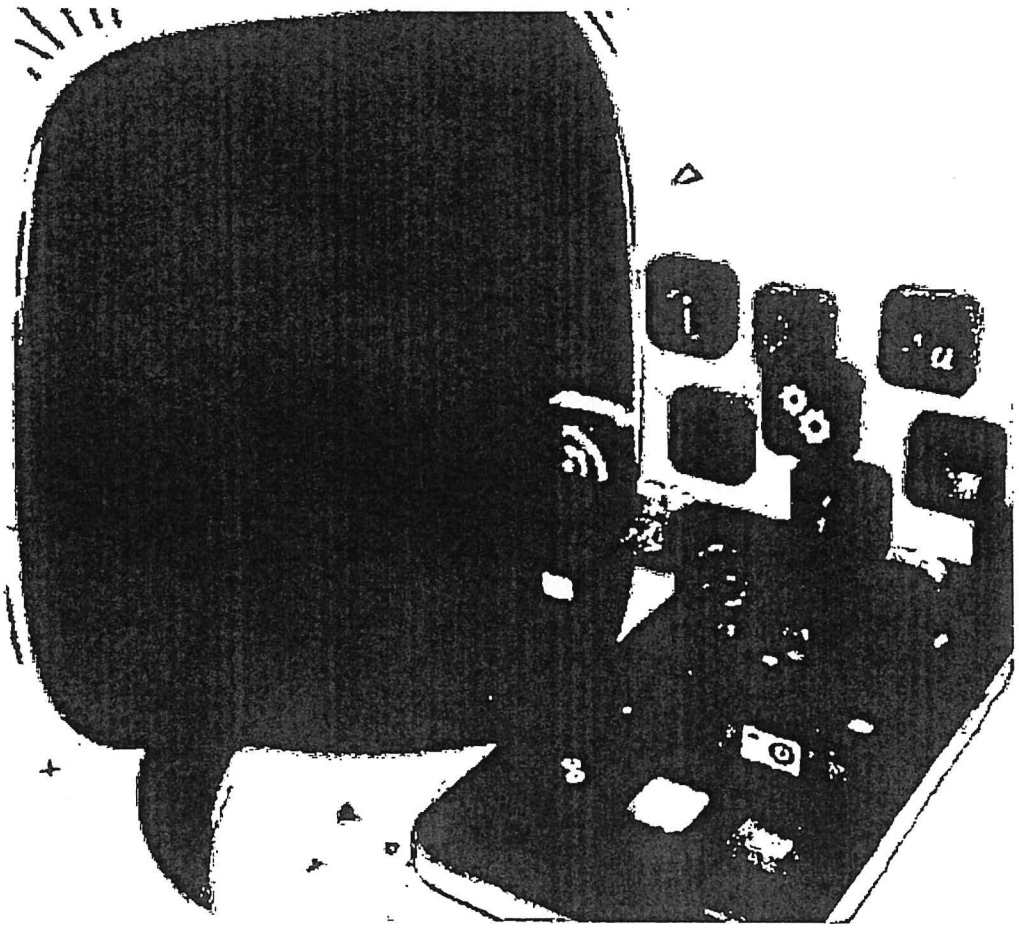
धोखेबाज पीड़ितों को नकली एवं लुभावनी योजनाओं में निवेश करने के लिए प्रोत्साहित करते हैं एवं बड़े रिटर्न का वादा करते हैं, या यह दावा करते हैं कि आपने लॉटरी जीती है और पुरस्कार एकत्र करने के लिए कर या शुल्क का भुगतान करना होगा।

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 इंटर्नशिप 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 इंटर्नशिप जो वास्तविक रोजगार की ओर कभी नहीं ले जाती।

रोकथाम के सुझाव:

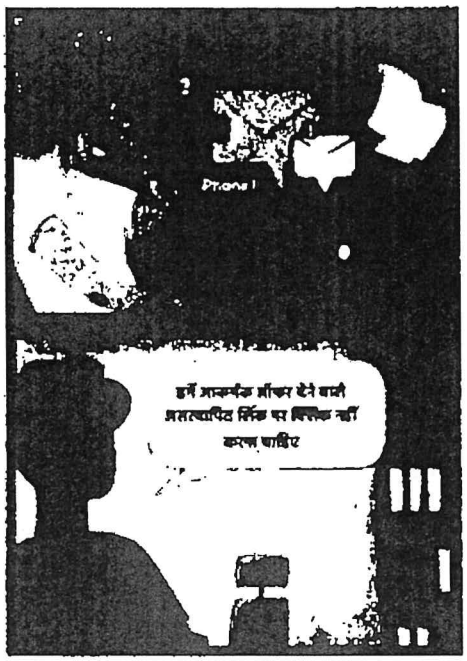
- जिस कंपनी द्वारा नौकरी या इंटर्नशिप की पेशकश की गई है, उसकी जांच करें।
- उन नौकरी प्रस्तावों से बचें जो व्यक्तिगत जानकारी या अग्रिम भुगतान मांगते हैं।
- नौकरी के प्रस्ताव को सीधे कंपनी से सत्यापित करें।

2.6 ई-कॉमर्स धोखाधड़ी

धोखेबाज नकली (फेक) ई-कॉमर्स वेबसाइट या प्लेटफ़ॉर्म 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:

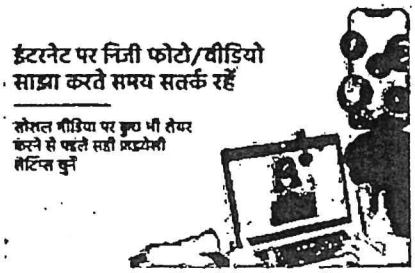
- विश्वसनीय ई-कॉमर्स वेबसाइटों से ही खरीदारी करें।
- खरीदारी करने से पहले विक्रेता की प्रमाणिकता तथा रेटिंग की जांच करें।
- सुरक्षित भुगतान गेटवे का उपयोग करें और अज्ञात खातों में सीधे हस्तांतरण से बचें।
- बहुत कम कीमत वाले ऑफ़र से सावधान रहें।

2.7 सोशल मीडिया घोटाला

साइबर अपराधी सोशल मीडिया प्लेटफ़ॉर्म का उपयोग लोगों की व्यक्तिगत जानकारी साझा करने, Malicious लिंक पर क्लिक करने या धनराशि ट्रान्सफर 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 धोखेबाज।



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 हैं। 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 मॉग करने वाले धोखेबाज।
- 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 फ़िशिंग घोटाला

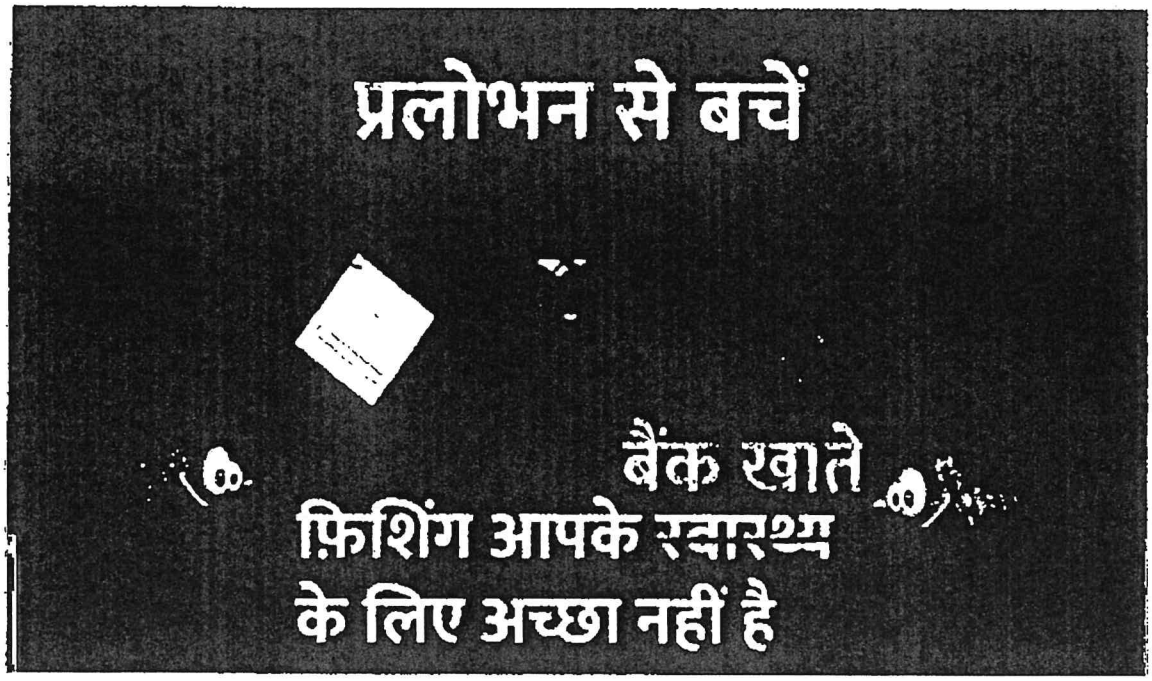
फ़िशिंग घोटाले नकली ईमेल या संदेश के माध्यम से नागरिकों को पासवर्ड या बैंक विवरण जैसे संवेदनशील निजी जानकारी प्राप्त कर धोखा देने का प्रयास करते हैं या फ़िशिंग ई-मेल इस प्रकार से तैयार किये जाते हैं कि वे वैध संगठनों से भेजे गये प्रतीत होते हैं।

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 (अथेंटिक सोर्स) से आया है।
- अज्ञात स्रोतों से आने वाले लिंक और अटैचमेंट पर क्लिक करने से बचें।
- एंटी-फ़िशिंग सॉफ़्टवेयर इंस्टॉल करें और यह सुनिश्चित करें कि आपका डिवाइस सुरक्षित है।



3 ऑनलाइन सुरक्षित रहने के लिए प्रमुख सुझाव

- जटिल पासवर्ड: प्रत्येक खातें 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 सॉफ़्टवेयर 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 हेल्पलाईन 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

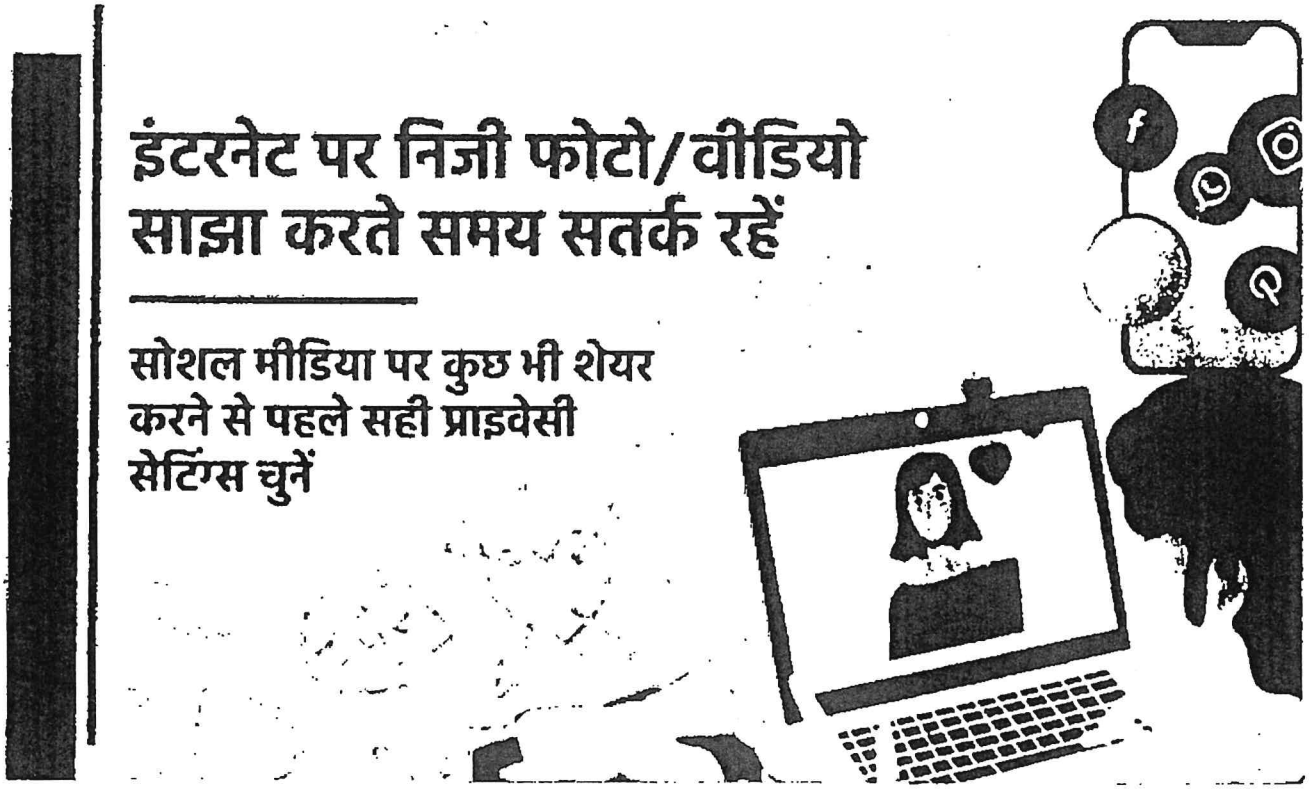
साइबर अपराधी सोशल मीडिया प्लेटफ़ॉर्म का उपयोग लोगों की व्यक्तिगत जानकारी साझा करने, Malicious लिंक पर क्लिक करने या धनराशि ट्रान्सफर करने के लिए कहते हैं।

आम परिदृश्य:

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

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।

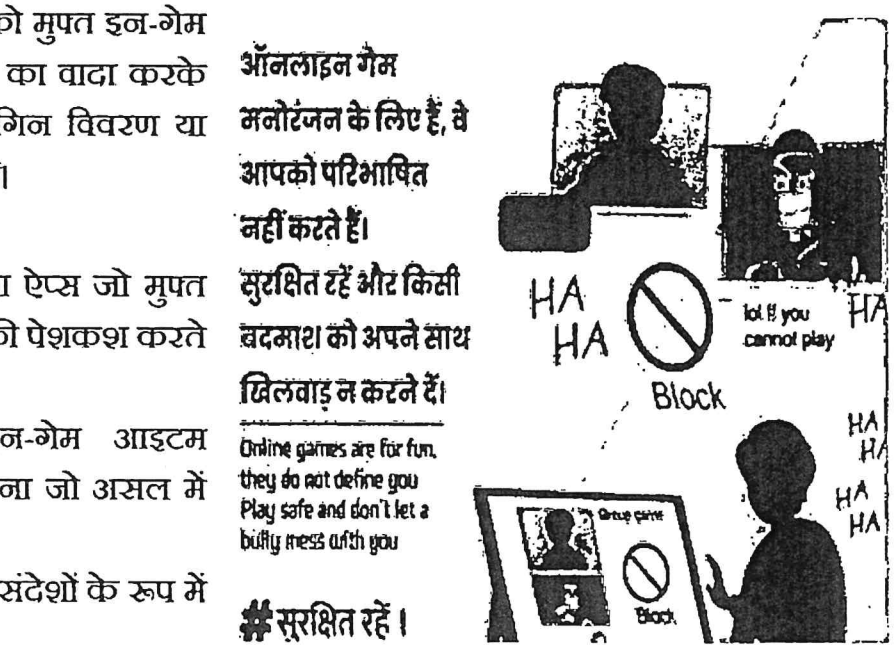


2.4 गेमिंग ऐप घोटाला (Gaming App Scams)

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 फ़िशिंग प्रयास।



रोकथाम 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।

रोकथाम 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

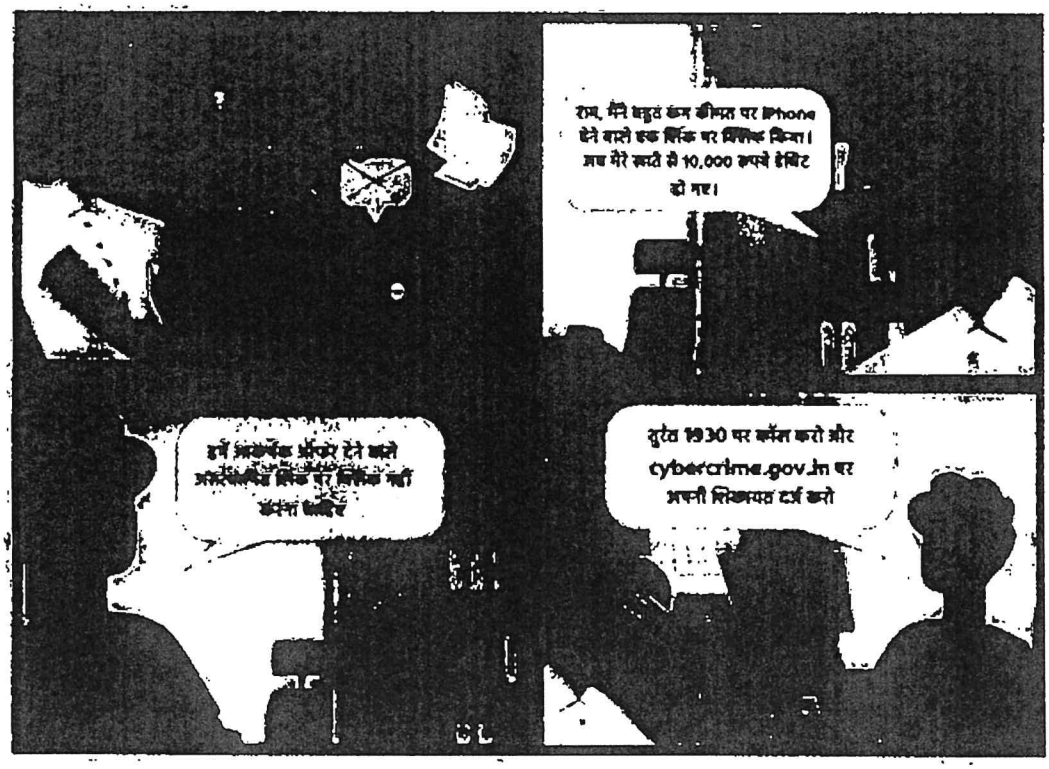
धोखेबाज नकली (फेक) ई-कॉमर्स वेबसाइट या प्लेटफ़ॉर्म पर प्रोफाइल बनाकर उपभोगताओं को लुभावने डील के माध्यम से घटिया उत्पाद बेचने का प्रयास करते हैं।

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 ऑफ़र से सावधान रहें।



2.7 नौकरी का घोटाला (Job Scams)

धोखेबाज, छात्रों को विशेष रूप से पार्ट-टाइम कार्य या इंटर्नशिप 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 इंटर्नशिप जो वास्तविक रोजगार की ओर कभी नहीं ले जाती।

रोकथाम के सुझाव:

- जिस कंपनी द्वारा नौकरी या इंटर्नशिप 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 मॉग करने वाले धोखेबाज।
- 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 मैलवेयर है जो आपकी फ़ाइलों को एन्क्रिप्ट कर देता है और उन्हें अनलॉक करने के लिए भुगतान (अक्सर क्रिप्टोकरेंसी 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 सॉफ़्टवेयर डाउनलोड करना।

रोकथाम के सुझाव:

- अपनी फ़ाइलों का नियमित रूप से किसी अन्य जगह (ऑनलाइन/ऑफलाइन) बाहरी स्रोत पर बैकअप लें।
- एंटीवायरस सॉफ़्टवेयर 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 खातें 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 सॉफ़्टवेयर 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 हेल्पलाईन 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।

330

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 रखो"

यूपीआई धोखाधड़ी/नेट बैंकिंग धोखाधड़ी/क्रेडिट कार्ड धोखाधड़ी

- ✓ [illegible]
- ✗ [illegible]

निवेश या लॉटरी धोखाधड़ी

- ✓ [illegible]
- ✗ [illegible]

ई-कॉमर्स धोखाधड़ी

- ✓ [illegible]
- ✗ [illegible]

सोशल मीडिया धोखाधड़ी/ऑनलाइन डेटिंग ऐप धोखाधड़ी

- ✓ [illegible]
- ✗ [illegible]

नौकरी धोखाधड़ी

- ✓ [illegible]
- ✗ [illegible]

फिशिंग धोखाधड़ी/पहचान की चोरी

- ✓ [illegible]
- ✗ [illegible]

गेमिंग ऐप धोखाधड़ी

- ✓ [illegible]
- ✗ [illegible]

रैंसमवेयर हमला

- ✓ [illegible]
- ✗ [illegible]

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

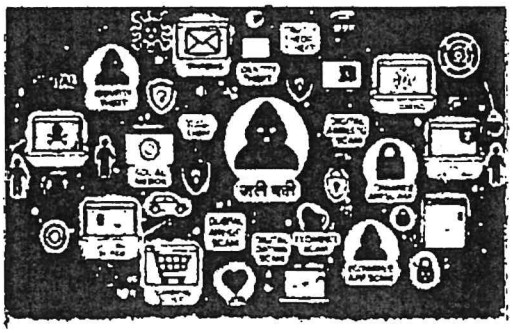
Department of
IT & Electronics

1. भूमिका

वर्तमान परिदृश्य की डिजिटल दुनिया में युवा छात्र इंटरनेट का उपयोग जैसे- अध्ययन, सामाजिकता (सोशलाइजिंग), 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 क्रिमिनल्स्) 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) पहचान की चोरी (Identity Theft)
ii) फ़िशिंग घोटाला (Phishing Scams)
iii) सोशल मीडिया घोटाला (Social Media Scams)
iv) गेमिंग ऐप घोटाला (Gaming App Scams)
v) ऑनलाइन डेटिंग ऐप घोटाला (Online Dating App Scams)
vi) ई-कॉमर्स घोटाला (E-Commerce Scams)
vii) नौकरी के घोटाला (Job Scams)
viii) डिजिटल गिरफ्तारी/जबरन वसूली घोटाला (Digital Arrest/Extortion Scams)
ix) रैनसमवेयर हमला (Ransom ware Attacks)

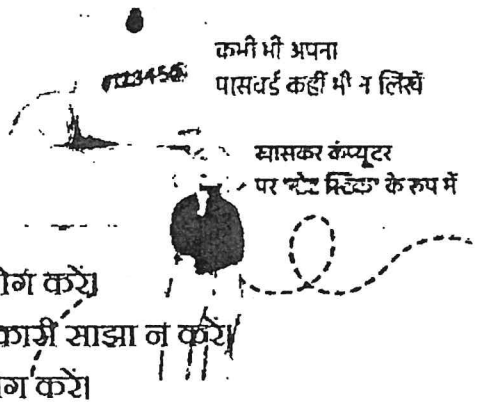


2.1 पहचान की चोरी (Identity Theft)

पहचान की चोरी तब होती है जब कोई व्यक्ति आपकी व्यक्तिगत जानकारी जैसे नाम, ई-मेल आई0डी0, 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 खातें 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 एकाउन्ट की गोपनीयता सेटिंग्स को चेक करें।

2.2 फ़िशिंग घोटाला

फ़िशिंग 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 हैं।

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 (अथेंटिक सोर्स) से आया है।
- अज्ञात स्रोतों से आने वाले लिंक और अटैचमेंट पर क्लिक करने से बचें।
- एंटी-फ़िशिंग सॉफ़्टवेयर इंस्टॉल करें और यह सुनिश्चित करें कि आपका डिवाइस सुरक्षित है।

335

संख्या 167 प्रमुख सचिव/व्या.शि.कौ.वि./प्रा.शि./2024

संख्या:-1692/78-1-2024-1099/619/2020

प्रेषक,

अनिल कुमार सागर,

1063/VSTE/24
T.S.|So-3

प्रमुख सचिव,
उ0प्र0 शासन।

सेवा में,

1. समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव, उ0प्र0 शासन।
2. समस्त मण्डलायुक्त, उत्तर प्रदेश।
3. समस्त जिलाधिकारी, उत्तर प्रदेश।

25/10/24
(महेश चन्द्र)
निजी सचिव, श्रेणी-2
विशेष सचिव
प्राविधिक शिक्षा विभाग
उ0 प्र0 शासन।

VS(AA|D)

[redacted]

25/10/24
(आलोक कुमार)
प्रमुख सचिव
प्राविधिक शिक्षा विभाग
उत्तर प्रदेश शासन

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

महोदय,

उपर्युक्त विषय के सबंध 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 अन्तर्राष्ट्रीय स्तर पर राष्ट्रीय साइबर सुरक्षा जागरूकता माह (एन०सी०एस०ए०एम०) के रूप में मनाया जाता है, जिसका उद्देश्य सार्वजनिक एवं निजी क्षेत्र के साथ-साथ आम नागरिकों को भी साइबर सुरक्षा हेतु जागरूक करना है।

3- इसी क्रम में भारत सरकार द्वारा इस वर्ष के अभियान का विषय "साइबर सुरक्षित भारत (#SatarkNagrik) 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।

So-3
25/X/24

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

(1) नागरिकों हेतु साइबर सुरक्षा जागरूकता [redacted]

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

(1) UPI घोटाले
(2) नेट बैंकिंग धोखाधड़ी

25/10/2024

(3)क्रेडिट कार्ड धोखाधड़ी

(4) निवेश या लॉटरी घोटाले

(5) नौकरी घोटाले

(6) ई-कॉमर्स धोखाधड़ी

(7) सोशल मीडिया घोटाले

(8) डिजिटल गिरफ्तारी वसूली घोटाले

(9) फ़िशिंग घोटाले

(10) साइबर अपराधों 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) छात्रों हेतु साइबर सुरक्षा जागरूकता:-

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

(1) पहचान की चोरी (Identity Theft)

(2) फ़िशिंग 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 घोटाले (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 छात्रों 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, उ0प्र0 शासन साइबर सुरक्षा धोखाधड़ी रोकथाम तथा सुरक्षा के मुख्य उपायों की एक हैण्डबुक 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 जागरुकता 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 फार ई-गवर्नेन्स, यू0पी0 (ई-मेल आई0डी0 cegiko.up@gmail.com) तथा शासन को उपलब्ध कराने का कष्ट करें।

संलग्नक: यथोक्त।

भवदीय,

Signed by
Anil Kumar Dayal
Date: 18-10-2024 19:49:32

(अनिल कुमार दयाल)
प्रमुख सचिव।

संख्या-1692(1)/78-1-2014 तद्दिनांक

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

1. निजी सचिव, मुख्य सचिव, उ0प्र0 शासन।
2. राज्य समन्वयक, सेन्टर फॉर ई-गवर्नेन्स, उ0प्र0, अपट्रान बिल्डिंग, गोमती नगर, लखनऊ।
3. राज्य सूचना विज्ञान अधिकारी, एन० आई०सी०, लखनऊ।
4. हेड, एस०ई०एम०टी०, उ०प्र०।
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 (सोशलाइजिंग), 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) फ़िशिंग 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

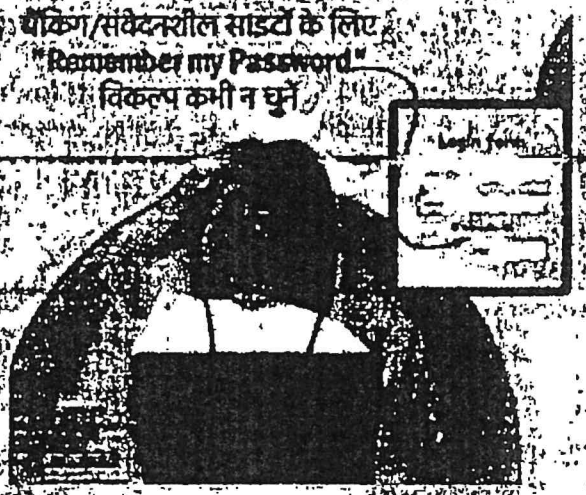
नेट बैंकिंग धोखाधड़ी तब होती है जब साइबर अपराधी फिशिंग अटैक, मैलवेयर या नकली वेबसाइटों के माध्यम से आपके बैंकिंग क्रेडेंशियल्स चुराते हैं, जिससे अनधिकृत लेनदेन होता है।

आम परिदृश्य:

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

रोकथाम के सुझाव:

- अज्ञात 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

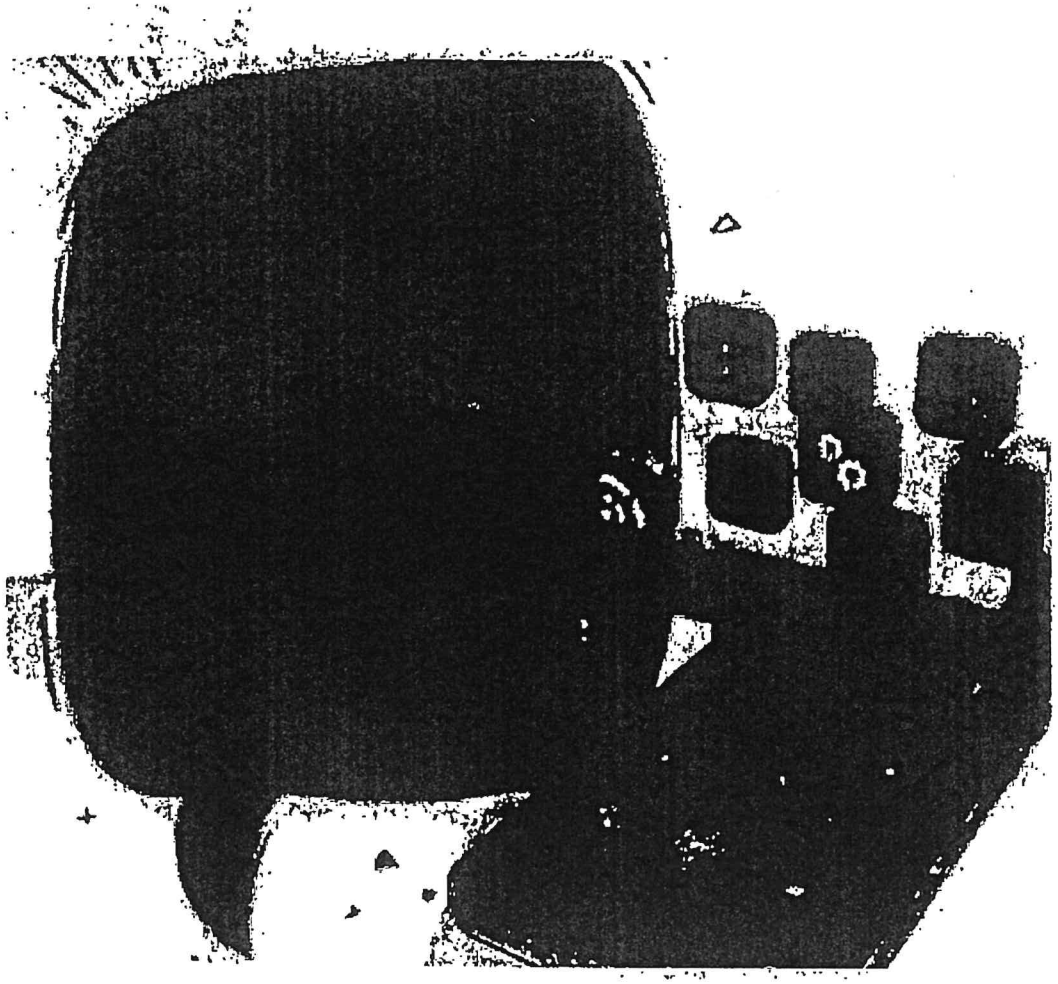
धोखेबाज़ पीड़ितों को नकली एवं लुभावनी योजनाओं में निवेश करने के लिए प्रोत्साहित करते हैं एवं बड़े रिटर्न का वादा करते हैं, या यह दावा करते हैं कि आपने लॉटरी जीती है और पुरस्कार एकत्र करने के लिए कर या शुल्क का भुगतान करना होगा।

आम परिदृश्य:

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

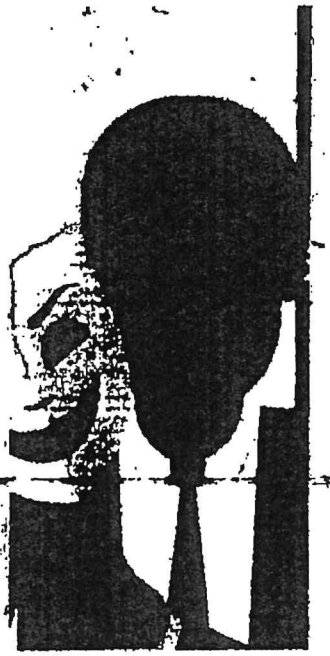
रोकथाम के सुझाव:

- 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 इंटर्नशिप 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।
- [illegible] से फर्जीवाड़ा रोजगार की ओर पहली कदम ले जाती।

रोकथाम के सुझाव:

- जिस कंपनी द्वारा नौकरी या इंटर्नशिप 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 (फ़ेक) ई-कॉमर्स वेबसाइट या प्लेटफ़ॉर्म 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:

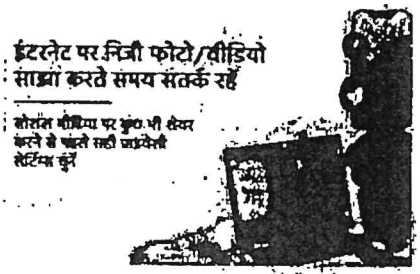
- विश्वसनीय ई-कॉमर्स वेबसाइटों से ही खरीदारी करें।
- खरीदारी करने से पहले विक्रेता की प्रमाणिकता तथा रेटिंग की जांच करें।
- सुरक्षित भुगतान गेटवे का उपयोग करें और अज्ञात खातों में सीधे हस्तांतरण से बचें।
- बहुत कम कीमत वाले ऑफ़र से सावधान रहें।

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 ट्रान्सफर 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 धोखेबाज।



बचाव के सुझाव:

- अज्ञात व्यक्तियों की मित्रता अनुरोधों को स्वीकार करते समय सतर्क रहें।
- अपना फोन 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 हैं। 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 मॉग करने वाले धोखेबाज।
- गिरफ्तारी या कानूनी जुर्माने के नकली नोटिस।

बचाव 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 फिशिंग घोटाला

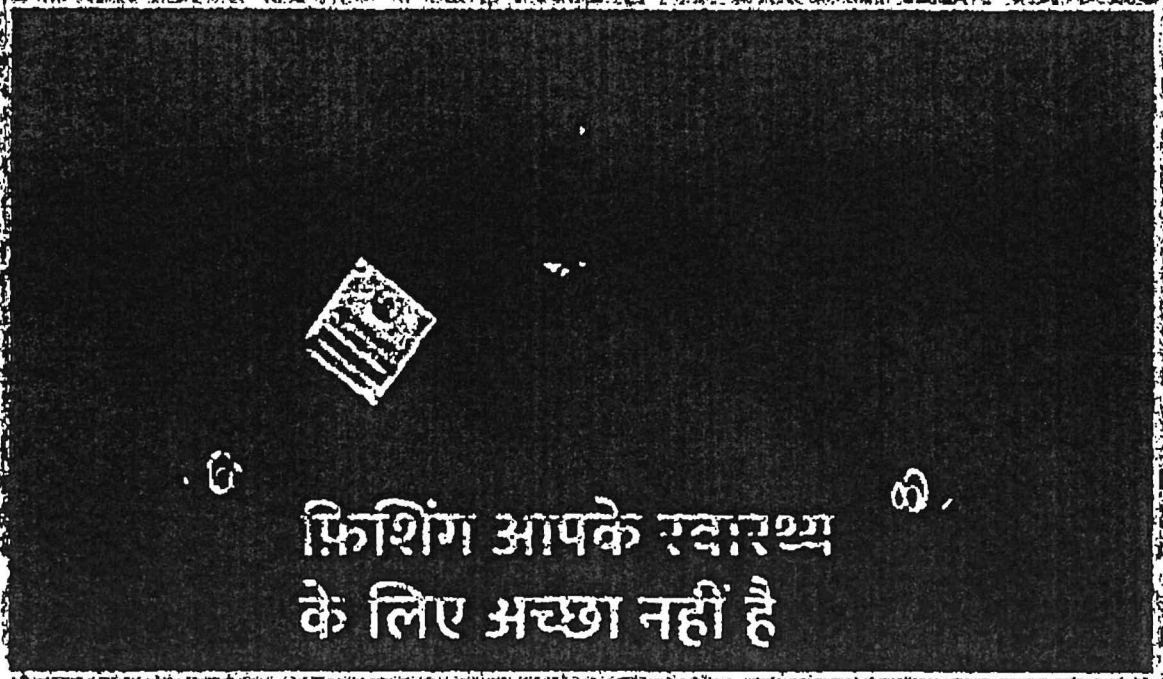
फिशिंग घोटाले नकली ईमेल या संदेश के माध्यम से नागरिकों का पासवर्ड या बैंक विवरण जैसे संवेदनशील निजी जानकारी प्राप्त कर धोखा देने का प्रयास करते हैं या फिशिंग ई-मेल इस प्रकार से तैयार किये जाते हैं कि वे वैध संगठनों से भेजे गये प्रतीत होते हैं।

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 लिंक, जो आपको पैसा 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 (अथेंटिक 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 क्लिक करने या जवाब देने से पहले सत्यापित करें।
- नियमित अपडेट: अपने सॉफ़्टवेयर 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 हेल्पलाईन 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 ट्रान्सफर करने के लिए कहते है।

आम परिदृश्य:

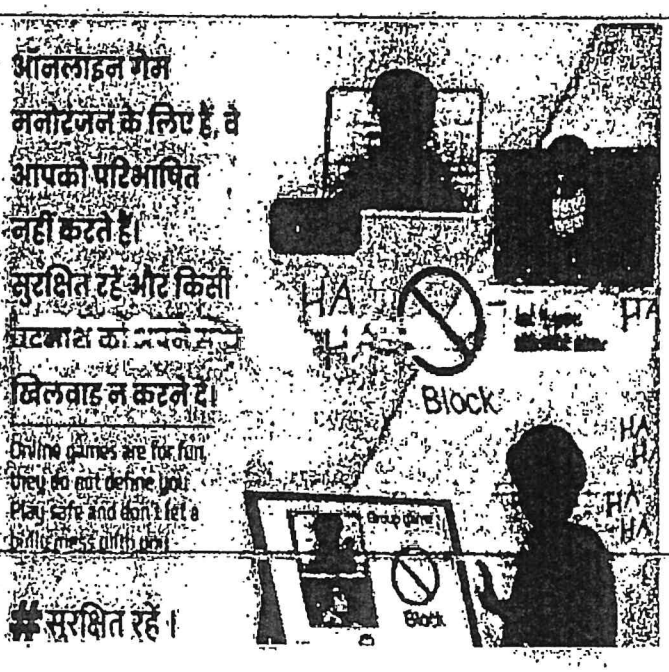
- नकली प्रोफाइल द्वारा मित्रता या धन मांगने की पेशकश।
- व्यक्तिगत डेटा चुराने वाले Malicious लिंक वाले संदेश।
- आपातकालीन वित्तीय सहायता मांगने वाले धोखेबाज।

बचाव:

- अज्ञात व्यक्तियों की मित्रता अनुरोधों को स्वीकार करते समय सतर्क रहें।
- अपना फोन 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।

2.4 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:

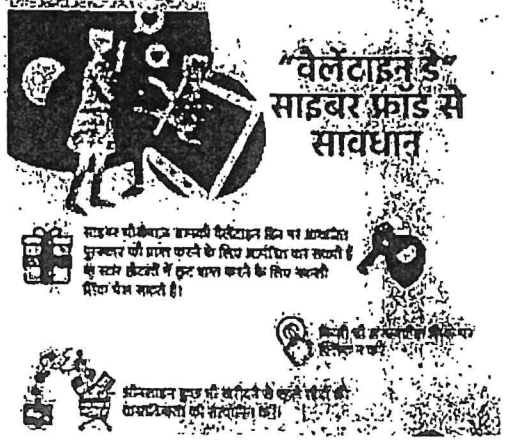
- नकली (फेक) वेबसाइट या ऐप्स जो मुफ्त गेम डाउनलोड या चीट्स की पेशकश करते हैं।
- खिलाड़ियों को ऐसे इन-गेम आइटम खरीदने के लिए धोखा देना जो असल में मौजूद नहीं होते।
- इन-गेम नोटिफिकेशन या संदेशों के रूप में छिपे हुए फ़िशिंग प्रयास।

रोकथाम 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।

रोकथाम 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

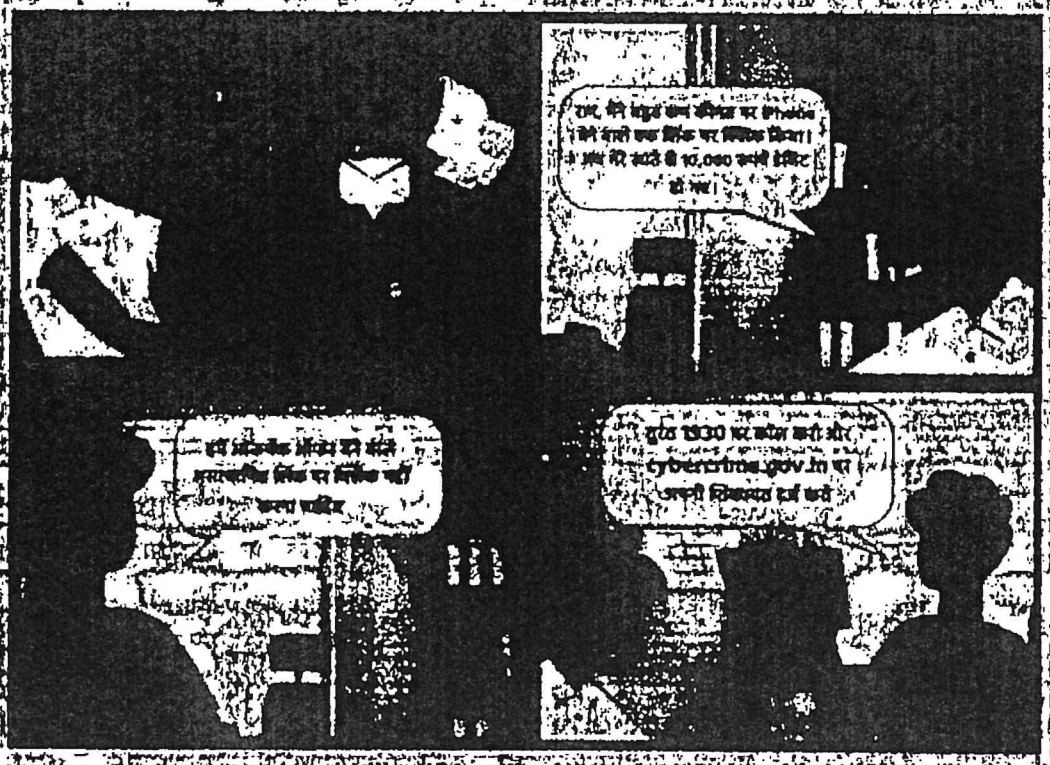
धोखेबाज नकली (फेक) ई-कॉमर्स वेबसाइट या प्लेटफॉर्म पर प्रोफाइल बनाकर उपभोगताओं को [illegible] के माध्यम से घटिया उत्पाद बेचने का प्रयास करते है।

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 नौकरी का घोटाला (Job Scams)

धोखेबाज, छात्रों को विशेष रूप से पार्ट-टाइम कार्य या इंटर्नशिप 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 इंटर्नशिप जो वास्तविक रोजगार की ओर कभी नहीं ले जाती।

रोकथाम के सुझाव:

- जिस कंपनी द्वारा नौकरी या इंटर्नशिप 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 धोखेबाज।
- 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 मैलवेयर है जो आपकी फ़ाइलों को एन्क्रिप्ट कर देता है और उन्हें अनलॉक करने के लिए भुगतान (अक्सर क्रिप्टोकरेंसी 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 सॉफ़्टवेयर डाउनलोड करना।

बचाव के सुझाव:

- अपनी फ़ाइलों का नियमित रूप से किसी अन्य जगह (ऑनलाइन/ऑफलाइन) बाहरी स्रोत पर बैकअप लें।
- एंटीवायरस सॉफ़्टवेयर 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 खातें 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 सॉफ़्टवेयर 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 साईबर अपराध रिपोर्टिंग सम्बन्धी पोर्टल (https://cybercrime.gov.in) से संपर्क कर सकते हैं। किसी भी वित्तीय धोखाधड़ी के लिए राष्ट्रीय साइबर अपराध हेल्पलाईन 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।

370

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 रखो"

[illegible]

- ✓ लेनदेन से पहले हमेशा UPI ID या खाता सत्यापित करें [illegible]
- ✗ OTP या पिन किसी के साथ न करें साझा [illegible]

निवेश या लॉटरी धोखाधड़ी

- ✓ [illegible]
- ✗ [illegible]

ई-कॉमर्स धोखाधड़ी

- ✓ [illegible]
- ✗ [illegible]

सोशल मीडिया धोखाधड़ी / ऑनलाइन डेटिंग ऐप धोखाधड़ी

- ✓ [illegible]
- ✗ [illegible]

[illegible]

- ✓ [illegible]
- ✗ [illegible]

फिशिंग धोखाधड़ी/पहचान की चोरी

- ✓ [illegible]
- ✗ [illegible]

गेमिंग ऐप धोखाधड़ी

- ✓ [illegible]
- ✗ [illegible]

रैंसमवेयर हमला

- ✓ [illegible]
- ✗ [illegible]

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