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

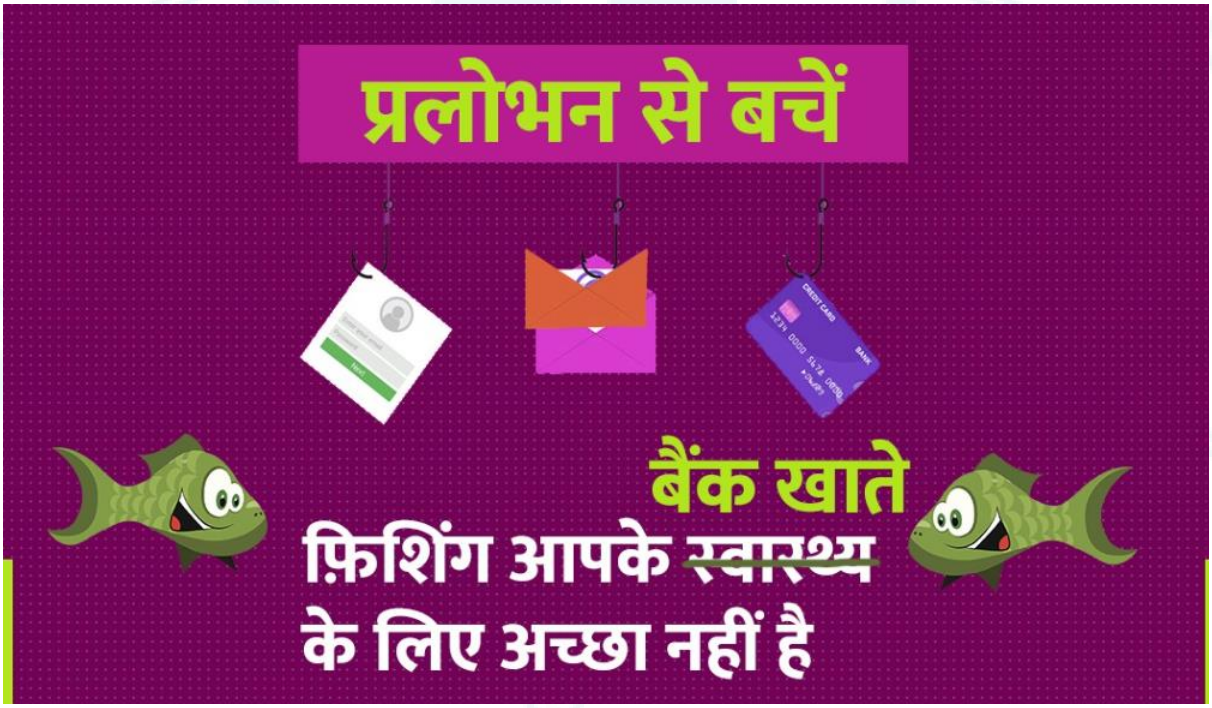
फ़िशिंग घोटाले नकली ईमेल या संदेश के माध्यम से नागरिकों को पासवर्ड या बैंक विवरण जैसे संवेदनशील निजी जानकारी प्राप्त कर धोखा देने का प्रयास करते हैं या फिशिंग ई-मेल इस प्रकार से तैयार किये जाते हैं कि वे वैध संगठनों से भेजे गये प्रतीत होते है।

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।



2.3 सोशल मीडिया घोटाला

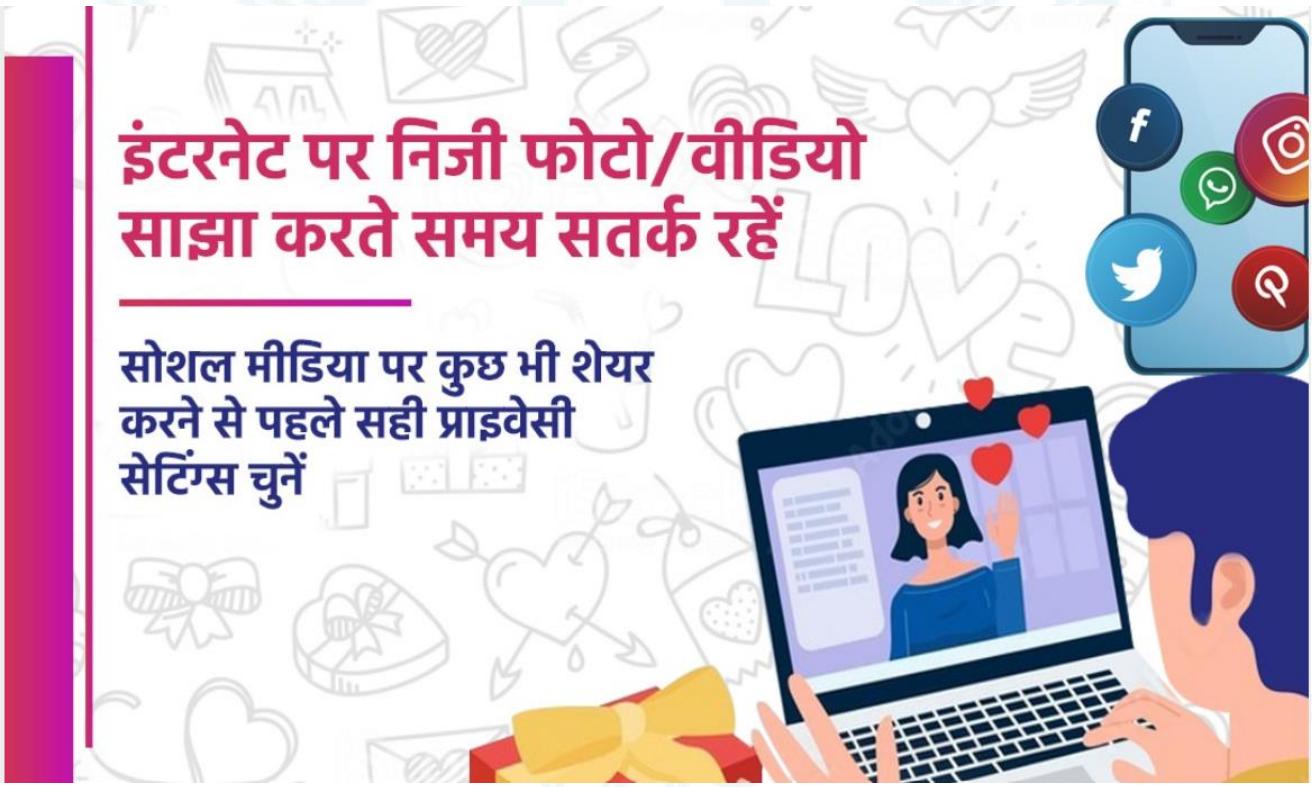
साइबर अपराधी सोशल मीडिया प्लेटफ़ॉर्म का उपयोग लोगों की व्यक्तिगत जानकारी साझा करने, Malicious लिंक पर क्लिक करने या धनराशि ट्रान्सफर करने के लिए कहते हैं।

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 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 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।