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 है। सामान्यता इंटरनेट के अनेकानेक लाभ है, परन्तु इसके साथ जोखिम भी जुड़े होते है। 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 है। 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 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 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 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 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 है या फिशिंग ई-मेल इस प्रकार से तैयार किये जाते है 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।

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।