



डॉ० ए०पी०जे० अब्दुल कलाम प्राविधिक विश्वविद्यालय उत्तर प्रदेश
सेक्टर-11, जानकीपुरम विस्तार योजना, लखनऊ-226031

पत्रांक: ए०के०टी०य० / कुस०का० / स्था० / २०२४ / ४८५
सेवा में,

दिनांक: ३० नवम्बर, २०२४

निदेशक / प्राचार्य,

विश्वविद्यालय से सम्बद्ध समस्त संस्थान।

विषय: 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 संख्या: १/७९६३४४/२०२४/१६-३०९९/२९२/२०२४ दिनांक १४.११.२०२४ (प्रति संलग्न) का संदर्भ ग्रहण करने का कष्ट करें।

उक्त के संदर्भ में अवगत कराना है कि शासन के पत्र में उल्लिखित आई०टी० एवं इलेक्ट्रानिक्स अनुभाग-1 के पत्र संख्या-१६९२/७८-१-२०२४-१०९९/६१९/२०२० दिनांक १९.१०.२०२४ (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, य०पी० (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 १४.११.२०२४ के साथ संलग्न इलेक्ट्रानिक्स अनुभाग-1 के पत्र दिनांक १९.१०.२०२४ में की गयी अपेक्षानुसार साइबर सुरक्षा जागरूकता अभियान/कार्यक्रम आयोजित करते हुए गतिविधियों की प्रगति रिपोर्ट नियमित रूप से सेंटर फार ई-गवर्नेंस, य०पी० (ई-मेल ceglko@gmail.com) तथा शासन को उपलब्ध कराने का कष्ट करें।

संलग्नक: यथोक्त।

भवदीय
(रीना सिंह)
कुलसचिव

प्रतिलिपि: निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

- अधिष्ठाता, ट्रेनिंग एण्ड प्लेसमेंट, ए०के०टी०य०, 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 आई०ई०टी० एवं इलेक्ट्रानिक्स अनुभाग-1 के पत्र दिनांक १९.१०.२०२४ में की गयी अपेक्षानुसार साइबर सुरक्षा जागरूकता अभियान/कार्यक्रम आयोजित करते हुए गतिविधियों की प्रगति रिपोर्ट नियमित रूप से सेंटर फार ई-गवर्नेंस, य०पी०(ई-मेल ceglko@gmail.com) पर उपलब्ध कराने का कष्ट करें।
- श्री वीर विक्रम सिंह, रिसर्च इंजीनियर, ए०के०टी०य०, लखनऊ।
- स्टाफ ऑफिसर, ए०के०टी०य०, लखनऊ को मा० कुलपति महोदय के अवलोकनार्थ।

(रीना सिंह)
कुलसचिव

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, ए०के०टी०य००, उ०प्र० लखनऊ।
3. कुलसचिव, ए८०बी०टी०य००, उ०प्र० कानपुर।
4. कुलसचिव, एम०एम०एम०य००टी०, उ०प्र० गोरखपुर।
5. निदेशक, प्राविधिक शिक्षा, उ०प्र०, कानपुर।
6. सचिव, प्राविधिक शिक्षा परिषद, उत्तर प्रदेश, लखनऊ।
7. सचिव, संयुक्त प्रवेश परीक्षा परिषद, उ०प्र०, लखनऊ।
8. निदेशक, बुंदेलखण्ड अभियांत्रिकी एवं प्रौद्योगिकी संस्थान, झांसी।
9. निदेशक, कमला नेहरू 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

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 १८६७-लुद्दीपुर राज्य/अधिकारी प्रक्रिया २२५

संख्या:-1692/78-1-2024-1099/619/2020

प्रेषक,

अनिल कुमार सागर,
प्रमुख सचिव,
उत्तर प्रदेश।

सेवा में,

VS(AA/D)

- समस्त अपर मुख्य सचिव/प्रमुख सचिव/सचिव, उत्तर प्रदेश।
- समस्त भण्डलायुक्त, उत्तर प्रदेश।
- समस्त जिलाधिकारी, उत्तर प्रदेश।

25/10/24 आईटी. एवं इलेक्ट्रोनिक्स अनुभाग-1

लखनऊ: दिवांक | १ अक्टूबर, 2024

विषय: राज्य के समस्त जिले के कार्यालयों, विद्यालयों तथा जन सेवा केन्द्रों पर साइबर सुरक्षा
 (आलोक कुमार)
 प्रमुख सचिव जागरूकता अभियान आयोजित किये जाने के संबंध में।
 प्राविधिक शिक्षकों
 उत्तर प्रदेश, शासन;

उपर्युक्त विषय के संबंध में अवगत कराना है कि वर्तमान परिवर्ष 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 मनाया जाता है, जिसका उद्देश्य सार्वजनिक एवं निजी क्षेत्र के साथ-साथ आम नागरिकों को भी (अजीज साइबर सुरक्षा हेतु जागरूक करना है।

विशेष उपर्युक्त विषय: इसी क्रम में भारत सरकार द्वारा इस वर्ष के अभियान का विषय 'साइबर सुरक्षित भारत' प्राविधिक शिक्षकों (#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 हैंडबुक भी तैयार कर उपलब्ध करायी जा रही है। इस हेतु आम नागरिकों, छात्र-छात्राओं को हैंडबुक 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/सार्वजनिकों निम्नवत् हैं:-

(1) नागरिकों हेतु साइबर सुरक्षा जागरूकता:-

यितीय तेत-देन करने वाले विभागों द्वारा आम नागरिकों में साइबर सुरक्षा के प्रति जागरूकता फैलाने पर ध्योन 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-

(1) UPI घोटाले

(2) नेट बैंकिंग धोखाधड़ी

मिलानी १०/१०/२०२४

- (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, कर्यशालाओं 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 देते 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 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, ३०प्र० शासन साइबर सुरक्षा धोखाधड़ी रोकथाम तथा सुरक्षा के मुख्य उपायों की एक हैण्डबुक नागरिकों एवं विद्यार्थियों हेतु संलग्न (संलग्नक-१) की गयी है, जिससे वे साइबर सुरक्षा संदर्शों 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-२) भी तैयार किया गया है, जिसको समस्त विलेज लेवल इन्टरप्रिन्टर (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 करते तथा जागरूकता कार्यक्रम आरम्भ किए जाने तथा गतिविधियों की प्रगति रिपोर्ट नियमित रूप से सेन्टर फॉर ई-गवर्नेंस, यू०षी० (ई-मेल आई०डी०-ceglko.up@gmail.com) तथा शासन को उपलब्ध कराने का कष्ट करें।

संलग्नक: यथोक्त।

भवदीय,

Signed by
Anil Kumar Sagar (अनिल कुमार सागर)
Date: 18-10-2024 19:49:32 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, 30प्र० शासन।
2. राज्य समन्वयक, सेन्टर फॉर ई-गवर्नेंस, ३०प्र०, अपट्रान बिल्डिंग, गोमती नगर, लखनऊ।
3. राज्य सूचना विज्ञान अधिकारी, एन० आई०सी०, लखनऊ।
4. हेड, एस०ई०एम०टी०, ३०प्र०।
5. गार्ड फाइल।

आज्ञा से,

(नेहा जैन)
विशेष सचिव।



1. भूमिका

वर्तमान परिवर्ष की डिजिटल दुनिया में युवा छात्र इंटरनेट का उपयोग जैसे- अध्ययन, सामाजिकता (सोशलाइजिंग), स्कैल तथा अन्य गतिविधियों के लिए आधिकारिक 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 सुन्दर 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 इंटरफ्रेस (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 परिणाम:

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

शोकथाम 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 फ्रिशिंग अटैक, मैलवेयर या नकली वेबसाइटों के माध्यम से आपके बैंकिंग क्रेडेंशियल्स चुगते हैं, जिससे अनधिकृत लेनदेन होता है।

आम परिदृश्य:

- एसएमएस या ईमेल के माध्यम से नकली (फ़ेक) बैंक लिंक पर विलक करना।
- सार्वजनिक वाई-फाई के माध्यम से ऑनलाइन बैंकिंग का उपयोग करना।
- अनज्ञान में अनधिकृत साप्टवेयर का इस्तेमाल करना।

शोकथाम के सुझाव:

- अंजान लिंक्स पर विलक न करें। आपने 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।
- आपने खाते की नियमित रूप से निगरानी करें और किसी भी संदिग्ध गतिविधि की तुरंत रिपोर्ट करें।

बैंकिंग/संवेदनशील साइटों के लिए
"Remember my Password"
विकल्प कभी न छुटें



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 स्ट्रिकमिंग डिवाइस लगे होना।
- आपका कार्ड सेवा प्रदाता होने का दावा करने वाले फ्रिशिंग ईमेल।

शोकथाम 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।



३८६



नागरिकों के लिए साइबर अपराध से बचने हेतु पुस्तिका

Department of
IT & Electronics

2.4 निवेश या लॉटरी घोटाला

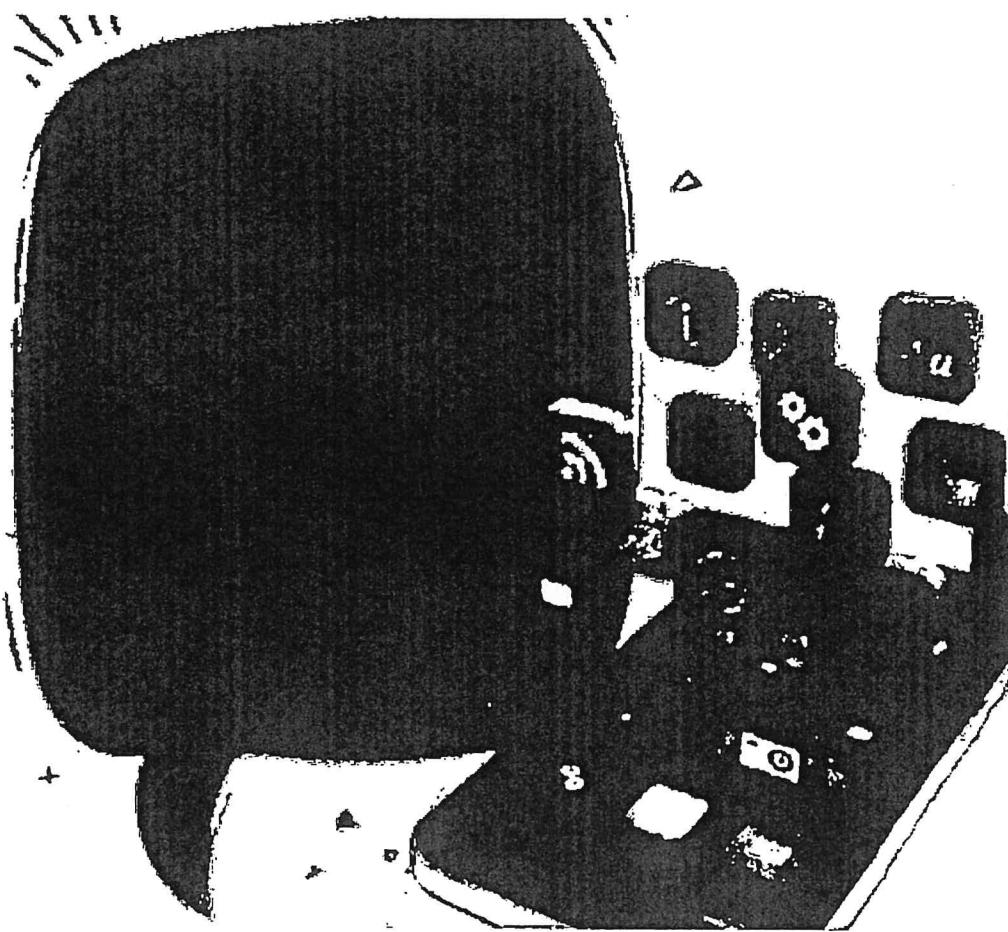
घोषणेबाज पीडितों को नकली एवं लुभावनी योजनाओं में निवेश करने के लिए प्रोत्साहित करते हैं एवं बड़े रिटर्न का वादा करते हैं, या यह दावा करते हैं कि आपने लॉटरी जीती हैं और पुरस्कार एकत्र करने के लिए कर या शुल्क का भुगतान करना होगा।

आम परिणय:

- 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 वेबसाइटों

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।



Cyber Surakshit Bharat

P200-2

State e-Mission Team



जागरिकों के लिए साइबर अपराध से बचने हेतु पुस्तिका

Department of
IT & Electronics

347

2.5 नौकरी का घोटाला (Job Scams)

घोषेबाज, 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 परिणय:

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



रोकथाम के सुझाव:

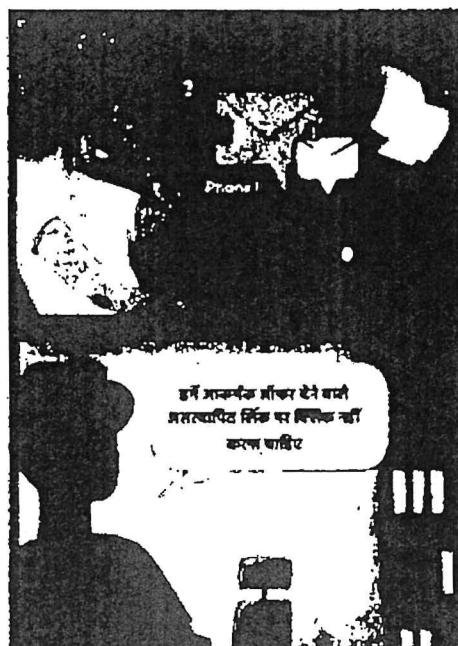
- जिस कंपनी द्वारा नौकरी या इंटर्नशिप की पेशकश की गई है, उसकी जांच करें।
- उन नौकरी प्रस्तावों से बचें जो व्यक्तिगत जानकारी या अधिक भुगतान मांगते हैं।
- नौकरी के प्रस्ताव को सीधे कंपनी से सत्यापित करें।

2.6 ई-कॉर्मर्स धोखाधड़ी

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

आम परिणय:

- नकली वेबसाइटों 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-कॉर्मर्स 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।





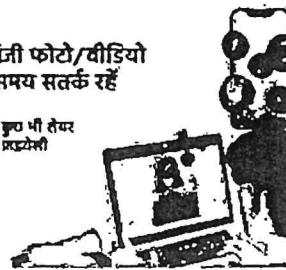
2.7 सोशल मीडिया घोटाला

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

आम परिणय:

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

इंटरनेट पर निजी फोटो/वीडियो
साझा करते समय सतर्क रहें
सोशल मीडिया पर ज़्यादा भी तेज़
हस्ते से बचते सही प्रक्रिया
संवित्त करें



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। घोखेबाज मुद्दे को "भुलझाने" के लिए पैसे की मांग करते हैं।

आम परिणय:

- आपकी जांच या कानूनी कार्रवाई का दावा करने वाले धमकी भरे ईमेल या कॉल।
- कानून प्रवर्तन या कर अधिकारी बनकर धनराशि की माँग करने वाले घोखेबाज।
- 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 परिटृप्त:

- आपके बैंक से आये प्रतीत होने वाले नकली ईमेल, जो आपको अपना आता 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 विलक करने से आपके डिवाइस में मैलवेयर इंस्टॉल हो जाता है।

शोकथाम के सुझाव:

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

प्रलोभन से बचें



बैंक खाते
फ़िशिंग आपके रदारथ्य
के लिए अच्छा नहीं है



344



नागरिकों के लिए साइबर अपराध से बचने हेतु पुस्तिका

Department of
IT & Electronics

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 यिलक करने या जवाब देने से पहले सत्यापित करें।
- नियमित अपडेट: आपने सॉफ्टवेयर और उपकरणों को नवीनतम सुरक्षा अपडेट के साथ अपडेट रखें।
- ग्रोपनीयता 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 रकूल 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 आपने बैंक से भी संपर्क कर सकते हैं और आपने खातों/कार्डों को ब्लॉक करा सकते हैं ताकि आगे नुकसान से बचा जा सके।

सतर्क रहें, सुरक्षित रहें।

1



Cyber Surakshit Bharat

Page-7

State e-Mission Team



छात्रों के लिए साइबर अपराध से बचने हेतु पुस्तका

Department of
IT & Electronics

2.3 सोशल मीडिया घोटाला

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

आम परिणयः

- नकली प्रोफाइल द्वारा मित्रता या धन मांगने की पेशकशा
- व्यक्तिगत डेटा चुराने वाले Malicious लिंक वाले संदेशों
- आपातकालीन वित्तीय सहायता मांगने वाले थोर्डोबाज़ों

रोकथाम के सुझावः

- 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 प्राइवेसी 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 घोखा देते हैं, जिनके लिए लॉगिन विवरण या भुगतान की आवश्यकता होती है।

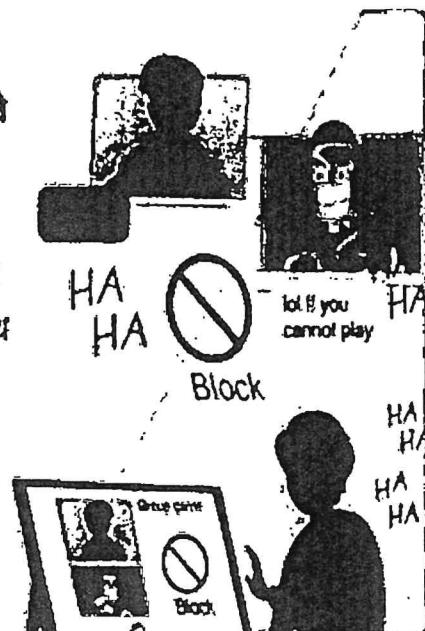
आम परिणय:

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

ऑनलाइन गेम
अनोटेशन के लिए हैं, वे
आपको परिभाषित
नहीं करते हैं।
सुरक्षित टैंप्स और किसी
बदमाश को अपने साथ
प्रिलगाइन 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।



योकथाम 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 घोखेबाज भावनाओं का लाभ उठाकर धनराशि या व्यक्तिगत जानकारी चुराने का प्रयास करते हैं।

आम परिणय:

- 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 क्रेडेशियल्स 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 पंता, पासवर्ड या निजी तस्वीरें) साझा करने से बचें।

2.6 ई-कॉमर्स धोखाधड़ी

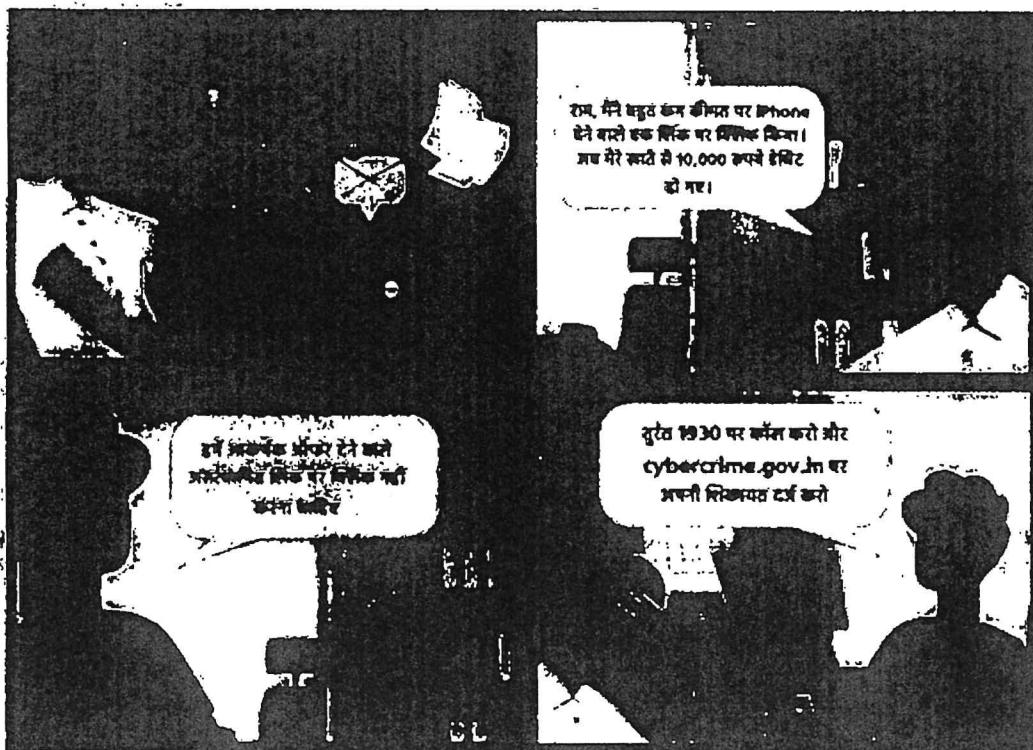
धोखेबाज नकली (फेक) ई-कॉमर्स वेबसाइट या प्लेटफॉर्म पर प्रोफाइल बनाकर उपभोगताओं को लुभावने डील के माध्यम से घटिया उत्पाद बेचने का प्रयास करते हैं।

आम परिणय:

- 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)

घोखेबाज, 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 बैंकग्राउंड 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 अधिक 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 दायें में हैं या उनके खिलाफ गिरफ्तारी वारंट लंबित है। घोखेबाज 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 घोखेबाज।
- 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 क्रिप्टोकरेसी में) की मांग करता है।

आम परिणय:

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

शोकथाम के सुझाव:

- अपनी फ़ाइलों का नियमित रूप से किसी अन्य जंगह (ऑनलाइन/ऑफलाइन) बाहरी स्रोत पर बैकअप लें।
- एंटीवायरस सॉफ्टवेयर इनस्टॉल 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 विलक्षण 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 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 रखें!"

युवीआई वीएसपीसी बैटरी ने दिये साइबर सुरक्षा टिप्पणी काउंसिल योगाचार्य

- सेनेटर मी. परमेश देवाना प्रभारी ने आठ साइबर सुरक्षा टिप्पणी के लिए साइबर सुरक्षा जागरूकता और अधिकारी विभाग के लिए सहज और उपयोग का उपरोक्त दर्शाया।
- परमेश देवाना ने आठ साइबर सुरक्षा टिप्पणी के लिए साइबर सुरक्षा जागरूकता और उपरोक्त दर्शाया।

नियमों या नाटकीय धाराघास्ति

- नियमों या नाटकीय धाराघास्ति के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।
- नियमों या नाटकीय धाराघास्ति के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।

डू-कॉर्सर्स धोखाघास्ति

- डू-कॉर्सर्स धोखाघास्ति के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।
- डू-कॉर्सर्स धोखाघास्ति के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।

सोशल श्री-ईया धोखाघास्ति/ऑनलाइन ड्रेटिंग धोखाघास्ति

- सोशल श्री-ईया धोखाघास्ति के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।
- सोशल श्री-ईया धोखाघास्ति के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।

लोकार्थी धोखाघास्ति

- लोकार्थी धोखाघास्ति के कार्यकारी की विवेक की विवेक के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।
- लोकार्थी धोखाघास्ति के कार्यकारी की विवेक की विवेक के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।

फिलिंग धोखाघास्ति/पहचान की धोखाघास्ति

- फिलिंग धोखाघास्ति के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।
- फिलिंग धोखाघास्ति के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।

गोमिंग धोखाघास्ति

- गोमिंग धोखाघास्ति के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।
- गोमिंग धोखाघास्ति के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।

ट्रैकर धोखाघास्ति

- ट्रैकर धोखाघास्ति के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।
- ट्रैकर धोखाघास्ति के साथपाइन कर्त्तव्य या नामांकन कर्त्तव्य के लिये साइबर सुरक्षा टिप्पणी में विवेक की पहले पुस्ती नक्शे दी गई हैं।

Stay Informed, Stay Safe – Report Cyber Crimes Immediately!

सचेत रहें, सुरक्षित रहें – साइबर अपराधों की तुरंत रिपोर्ट करें!

साइबर हेल्पलाइन: 1930

खुद को औट अपके पटिवार को साइबर खतरों से बचाओं।



1. भूमिका

वर्तमान परिवेश की डिजिटल दुनिया में युवा छात्र इंटरनेट का उपयोग जैसे- आध्ययन, 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 क्रिमिनल्स) 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 गिरफतारी/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 आईडी, पासवर्ड इत्यादि का दुरुपयोग करके धोखाधड़ी करता है।

आम परिवेश:

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

कभी भी अपना
पासवर्ड कहीं भी न लियें

मासकर कंप्यूटर
पर दोस्त मिला के रूप में

रोकथाम के सुझाव:

- प्रत्येक खाते के लिए जटिल और यूनिक पासवर्ड का उपयोग करें।
- ऑनलाइन या अजनकियों के साथ अपनी व्यक्तिगत जानकारी साझा न करें।
- जहां भी संभव हो, टू-फैक्टर ॲथेंटिकेशन (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 घोष्या 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 परिणय:

- 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 फ़ेक नकली वेबसाइटों पर ले जाते हैं।
- ऐसे ईमेल में अटैचमेंट जिन पर विलक करने से आपके डिवाइस में मैलवेयर इंस्टॉल हो जाता है।

रोकथाम के सुझाव:

- अवांछित ईमेल या एसएमएस में प्राप्त लिंक पर विलक 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 विलक करने से बचें।
- एंटी-फ़िशिंग सॉफ्टवेयर इंस्टॉल करें और यह सुनिश्चित करें कि आपका डिवाइस सुरक्षित है।



संख्या-1692/78-1-2024-1099/619/2020

प्रेषक,

आनंदल, कुमार सागर,

प्रमुख सचिव

उम्प्र० शासन।

सेवा मं.

1063/VSTB/24
T.S.150-3

251024

(महेश चन्द्र)

निजी सचिव, ब्रेणी-2

विशेष सचिव

प्राविधिक शिक्षा विभाग

उम्प्र० शासन।

VS(AA/10)

1. समस्त अपरा. मुख्य सचिव/प्रमुख सचिव/सचिव, उम्प्र० शासन।

2. समस्त मण्डलायुक्त, उत्तर प्रदेश।

3. समस्त जिलाधिकारी, उत्तर प्रदेश।

विषय: राज्य के समस्त निलं के कार्यालयों तथा जन सेवा केन्द्रों पर साइबर सुरक्षा (आलोक कुमार) नागरुकता अभियान आयोजित किये जाने के सबध में।

प्रमुख सचिव प्राविधिक शिक्षा विभाग, संघर्ष एवं उत्तर प्रदेश शासन उपर्युक्त विषय के सबध में अवगत कराना है कि वर्तमान परिदृश्य के अन्तर्गत डिजिटल

युग में साइबर अपराधों की बढ़ती घटनाओं के दृष्टिगत यह वितान्त 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 का राष्ट्रीय एवं अन्तर्राष्ट्रीय स्तर पर, राष्ट्रीय साइबर सुरक्षा नागरुकता माह (एन०सी०एस०एम०) के रूप में मनाया जाता है, जिसका उद्देश्य सार्वजनिक एवं निजी क्षेत्र के साथ सम्बद्ध आम नागरिकों का भी साइबर सुरक्षा हेतु जागरूक करना है।

3. इसी क्रम में भारत सरकार द्वारा इस वर्ष के अभियान का विषय साइबर सुरक्षित भारत (#SafeAIKNagrik) रखा गया है, जिसके माध्यम से साइबर सुरक्षा हेतु सम्पूर्ण देश को समिलित करते हुए एक दृष्टिकोण अपनाया गया है। इस अवृद्धि भाव में सार्वजनिक, निजी क्षेत्र एवं आम नागरिकों का जागरूक सतर्क करते हुए देश को साइबर सुरक्षित बनाने पर, विशेष बल दिया जा रहा है। इस क्रम में मुख्य विन्दुओं को समाहित करते हुए हेण्डबुक भी तैयार कर लपलध करणी जा रही है। इस हेतु आम नागरिकों छात्र-छात्राओं को हेण्डबुक उपलब्ध कराते हुए साइबर सुरक्षा हेतु जागरूकता की बढ़ाया जा रहा है।

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

(1) नागरिकों हेतु साइबर सुरक्षा जागरूकता लेने देने करने याने याने आम नागरिकों में साइबर सुरक्षा के प्रति जागरूकता फैलाने पर आनंद करते किया जाना है, जिसमें प्रमुख रूप से वित्तीय औद्योगिक संस्कृतीय व्यापारों के लिए जागरूकता अपराधों के खानों के बारे में जानकारी देना समिलित है। जैसे-

(1) UPI धूटाल

(2) बैट बॉक्स, धूषणपटी

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 संतुलित गिरफ्तारी की जाए और जिससे उत्तर प्रदेश राज्य के प्रत्येक नागरिक को उन्मत्त जानकारी प्राप्त हो सके।

(2) छात्रों हेतु साइबर सुरक्षा जागरूकता:-

छात्रों पर विशेष ध्यान देने की आवश्यकता है, जो निम्नलिखित साइबर खतरों के प्रति अंत्यंधिक 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 घोटाला (Job Scams)
- (8) डिजिटल गिरफ्तारी/जबरन वसूली घोटाला (Digital Arrest/Extortion Scams)
- (9) रैनसम्वेयर 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 कियां जा सके।

(3) सरकारी अधिकारियों हेतु:-

जिला स्तर के अधिकारियों को साइबर सशक्त बनाने के लिए आई०टी० एवं इलेक्ट्रॉनिक्स विभाग, ३०प्र० शासन साइबर सुरक्षा धोखाधड़ी रोकथाम तथा सुरक्षा के मुख्य उपायों की एक हैण्डबुक नागरिकों एवं विद्यार्थियों हेतु संलग्न (संलग्नक-१) की गयी है, जिससे वे साइबर सुरक्षा संदेशों को नियमित सार्वजनिक बातचीत तथा बैठकों में सम्मिलित कर अधिक से अधिक साइबर सुरक्षा की प्राप्ति सकते हैं।

जन सेवा केन्द्रों पर साइबर जागरूकता को बढ़ाये जाने हेतु एक बैनर (संलग्नक-२) भी तैयार किया गया है, जिसको समस्त विलेज लेवल इन्टरप्रिन्टर (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 कार्यगाही सुनिश्चित किये जाने हेतु संबंधित अधिकारियों/संस्थाओं को निर्देशित करने तथा जागरूकता कार्यक्रम आरम्भ किए जाने तथा गतिविधियों की प्रगति रिपोर्ट तियाम्बत रूप से सेन्टर फॉर इन्डिपेंडेंट एंड ऑफिशियल ऑफिस (इ-मेल: cegiko.up@gmail.com) तथा रासनको
उपलब्ध कराने का काम कर।

अलगैकं यथोक्तं

भवदीय,

Signed by

अम्बेज गृह दाम्भ

(अम्बेज गृह दाम्भ)

Date: 18-10-2024 19:49:32 प्रमुख सचिव।

संख्या-1692(1)/78-1-2014 जददिलाक्ष

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

1. निजा साधव, मुख्य सचिव, ३०प्र० रासन।
2. राज्य समन्वयक, सेन्टर फॉर इन्डिपेंडेंट एंड ऑफिशियल बिल्डिंग, गोमती नगर, लखनऊ।
3. राज्य सूचना विज्ञान अधिकारी, एन० आई०सी०, लखनऊ।
4. हेड, एस०इ०एम०टी०, उप्रा।
5. गार्ड फाइल।

आज्ञा से,

(नैहा जैन),
विशेष सचिव।



नागरिकों के लिए साइबर अपराध से बचने हेतु पुस्तका

Department of
IT & Electronics

1. भूमिका

वर्तमान परिवेश 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 पुस्तका 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 तौयार की गई है। इसमें साइबर वर्ल्ड में होने वाले धोखाधड़ी के तरीकों, उनके चेतावनी संकेतों और सूचना को सुरक्षित रखने के उपायों के बारे में बताये गया है।) अवसर छात्रों को विभिन्न प्रकार की ऑनलाइन धोखाधड़ी के माध्यम से निशाना (टारगेट) बनाते हैं। इस पुस्तका का उद्देश्य स्कूल और कॉलेज के छात्र/छात्राओं को नवीनतमें साइबर सुरक्षा धोखाधड़ी के सम्बन्ध में जागरूक करना तथा ऑनलाइन सुरक्षित रहने के लिए आवश्यक कंदम उठाने में उनकी सहायता करना है।

2. साइबर धोखाधड़ी के तरीकों की सूची

- | | |
|-----------------------------|-------------------------------------|
| i) UPI घोटाले | ii) ब्रेट बैंकिंग धोखाधड़ी |
| iii) क्रेडिट कार्ड धोखाधड़ी | iv) निवेश या लॉटरी घोटाले |
| v) नौकरी घोटाले | vi) ई-कॉर्मर्स 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 परिवेश:

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

योकथाम 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 आपराधिक फिलिंग, अटक, मलवयर या नफली वेबसाइटों के माध्यम से आपके बैंकिंग क्रेडेशियल्स चुयते हैं जिससे अनधिकृत लेनदेन होता है।

आम परिणय:

- एसएमएस या ईमेल के माध्यम से नफली (फ़र) लिंक पर विलक्षण होना।
- सार्वजनिक वाई-फ़ाई के माध्यम से ऑनलाइन बैंकिंग का उपयोग करना।
- अनजाक्ले भेजे अनधिकृत साप्टवेयर का इस्तेमाल करना।

शोकथाम के सुझाव:

○ अजान लिंक पर विलक्षण करने और अपने बैंक की वेबसाइट वर्कप्लेट तक पहुंचने के लिए सार्वजनिक साइटों के लिए "Remember my Password" विकल्प कभी न घुमा करें।

- किसी भी बैंकिंग लेनदेन के लिए सार्वजनिक वाई-फ़ाई का उपयोग न करें।
- अतिरिक्त सुरक्षा के लिए मर्टी-फैप्टर अंथेटिकेशन का उपयोग करें।
- अपने छाते की नियमित रूप से निगरानी करें और किसी भी स्टिन्ग गतिविधि की तुरत रिपोर्ट करें।



2.3. क्रेडिट कार्ड धोखाधड़ी

जब कोई व्यक्ति आपके कार्ड विवरणों को चुया लेता है और ऑनलाइन शॉपिंग या कार्ड की नफली (वलोगिंग) करके अनधिकृत लेनदेन करता है।

आम परिणय:

- सुरक्षित वेबसाइट पर शोपिंग करना।
- एटीएम या Point of Sale (पीओएस) मशीनों पर स्ट्रिकमिंग डिवाइस लेने होना।
- आपका कार्ड सेवा प्रदाता होने का दावा करने वाले फिलिंग ईमेल।

शोकथाम के सुझाव:

- कार्ड विवरण किसी भी बांज़र या वेबसाइट पर रखने से बचें।
- क्रेडिट कार्ड स्टेटमेंट की नियमित रूप से निगरानी करें और योद्धे हुए कार्ड की तुरत सम्बन्धित बैंक को रिपोर्ट करें।
- ऑनलाइन खरीदारी के लिए सुरक्षित भुगतान गेटवे का उपयोग करें।



2.4 निवेश या लॉटरी घोटाला

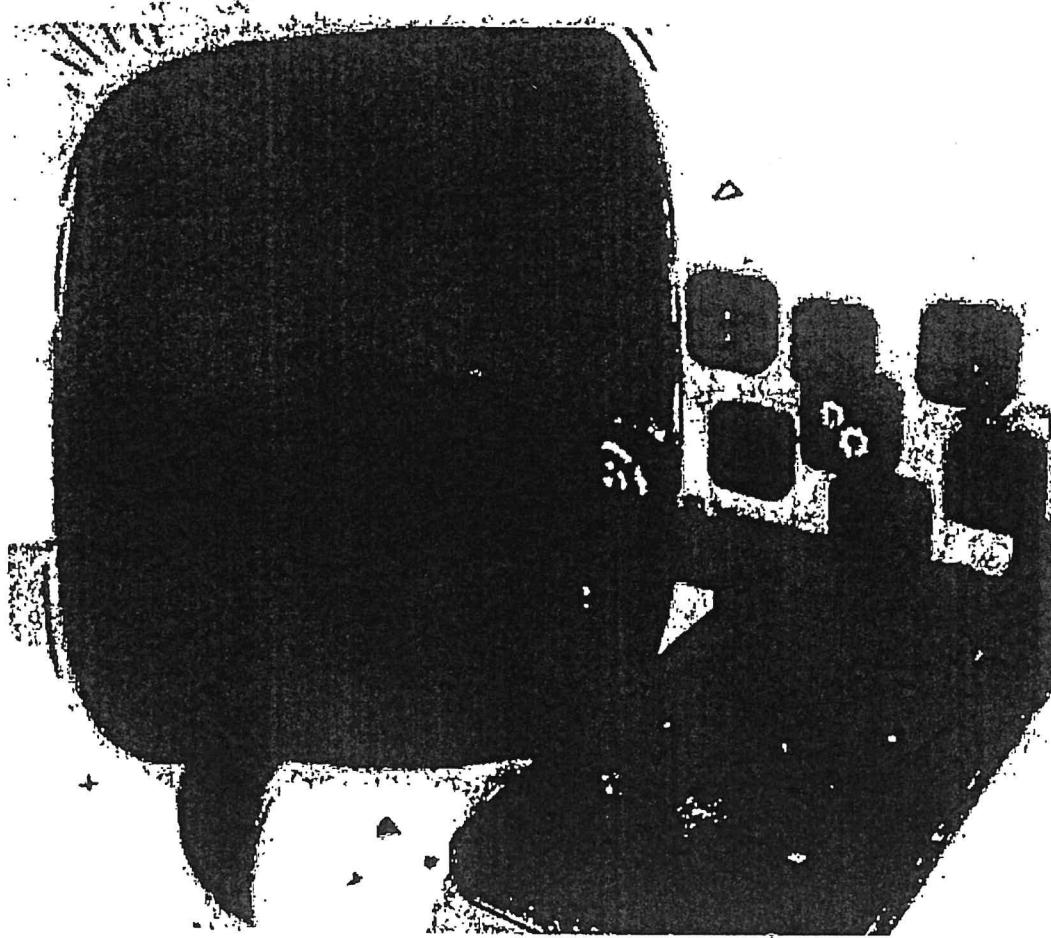
धोखेबाज पीड़ितों को नकली एवं लुआवनी योजनाओं में निवेश करने के लिए प्रोत्साहित करते हैं एवं बड़े रिटर्न का वादा करते हैं, या यह दावा करते हैं कि आपने लॉटरी जीती है और पुरस्कार एकत्र करने के लिए कर या शुल्क का भुगतान करना होगा।

आम परिणय:

- 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।

शोकथाम के सुझाव:

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





2.5. નૌકરી કા ઘોટાલા (Job Scams)

ધોરણોબાજ લાંબો કો વિશેષ રૂપ સે પાર્ટ-ટાઇમ કાર્ય યા ઇંટર્ન્ઝિપ કે લિએ નકલી નૌકરી કે પ્રસ્તાવ દેકર નિશાના બનાતે હૈનું તાકિ પેચે ઉનકી વ્યક્તિગત જાનકારી યા પૈસે ચુરા રાકે।

આમ પરિણય:

- નકલી (ફેફ) નૌકરી કે પ્રસ્તાવ જો આપનો પ્રશિક્ષણ યા બૈકગ્રાઉન્ડ ચેક કે લિએ પૈસે જમા કરને કી માંગ કરતો હૈનું
- આપને બૈંક ખાતે કે વિકરણ જીસી વ્યક્તિગત જાનકારી માંગના
- ને.ની નાઈન હો પણાંની રેસ્ટોરન્ટ દી હોલ્ડ કાઢી નાંની ને જાતીની



શેકથામ કે સુઝાવ:

- જિસ કંપની દ્વારા નૌકરી યા ઇંટર્ન્ઝિપ કી પેશકશ કી ગઈ હૈનું, તુસકી જાંચ કરોયું
- ઉન નૌકરી પ્રસ્તાવોને સે બચે જો વ્યક્તિગત જાનકારી યા આગ્રિમ મુંગતાન માંગતો હૈનું
- નૌકરી કે પ્રસ્તાવ કો સીધે કંપની સ્થે સત્યાપિત કરોયું

2.6. ઈ-કોર્મર્સ ધોરણાધડી

ધોરણોબાજ નકલી (ફેફ) ઈ-કોર્મર્સ વેબસાઇટ યા પ્લેટફોર્મ પર પ્રોફાઇલ બનાકર ઉપભોગતાઓનો કો લુભાવને ડીલ કે માદ્યમ સે ઘટિયા ઉત્પાદ બેચને કા પ્રયાસ કરતો હૈનું।

આમ પરિણય:

- નકલી વેબસાઇટો યા વિક્રેતા જો બહુત હી કમ કીમત પર ઉત્પાદ બેચ રહે હોયું
- મુંગતાન કરને કે બ્લુટ ઉત્પાદ કી ડિલીવરી નાંની હોતીની
- શરસ્તી યસ્તુઓને કે મુંગતાન કે બ્લુટ નકલી ઉત્પાદ મિલાની



શેકથામ કે સુઝાવ:

- વિન્યાસનીય ઈ-કોર્મર્સ વેબસાઇટોને સે હી ખરીદારી કરોયું
- ખરીદારી પ્રાણે સે પહુલે વિક્રેતા કી પ્રમાણિકતા તથા રેટિંગ કી જાંચ કરોયું
- સુરક્ષિત મુંગતાન ગેટવે કા ઉપયોગ કરોયું ઔર અજ્ઞાત સ્થળોને સીધે હસ્તાંતરણ સે બચોયું
- બહુત કમ કીમત વાતે ઑફર સે સાંવધાન રહોયું



2.7 सोशल मीडिया घोटाला

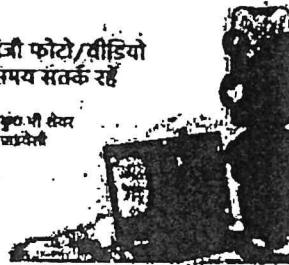
साइबर अपराधी सोशल मीडिया प्लेटफॉर्म का उपयोग लोगों की व्यक्तिगत जानकारी साझा करने, Malicious लिंक पर क्लिक करने या धनराशि ट्रान्सफर करने के लिए कहते हैं।

आम परिदृश्य:

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

इटरेट फर्निचर फोटो/वीडियो
साथी करते समय सतर्क रहें

लोकल वीडियो पर कूप भी करें
करने से बचते रही चाहेंगी
लैटर्न करें



शोकथाम के सुझाव:

- अज्ञात व्यक्तियों की मित्रता अनुयोधों को स्वीकार करते समय सतर्क रहें।
- अपना फोन नंबर, पता, या बैंकिंग जानकारी सार्वजनिक रूप से शेयर न करें।
- साइबर च्यातों 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। घोखेबाज 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 माँग करने वाले घोखेबाज।
- गिरफ्तारी या कानूनी जुर्माने के नकली नोटिस।

शोकथाम के सुझाव:

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





जानकियों के लिए साइबर आपाय से बचके हेतु पुस्तिका

Department of
IT & Electronics

2.9 फ़िशिंग घोटाला

फ़िशिंग घोटाल नकली ईमेल या संदेश के माध्यम से जानकियों को ग्राहक चौके विरोध जैसे संवेदनशील निजी जानकारी प्राप्त कर घोस्ता देने का प्रयास करते हैं या फ़िशिंग ईमेल इस प्रकार से तेजार किये जाते हैं कि वे वैध संगठनों से भेजे गये प्रतीत होते हैं।

आम परिणय:

- आपके बैंक से आये प्रतीत होने वाले नकली ईमेल, जो आपको अपना खाता सत्यापित करने के लिए कहते हैं।
- ईमेल या एसएमएस पर लिंक जो साप्तपो ऐप ऐप्प्स की फ़ॉर्म करानी चाहेंगी पर ले जाते हैं।
- ऐसे ईमेल में अटैचमेंट जिन पर विलक करने से आपके डिवाइस में मैलवेयर इस्टॉल हो जाता है।

खेल आगे बढ़ावा

- अवधित ईमेल या एसएमएस में प्राप्त लिंक पर विलक करने से बचो।
- छमशा प्रष्ठक (जेन्डर) का ईमेल पता जारी ले तथा यह सुनिश्चित कर लें कि यह ईमेल वैध (उर्योटिक साथ) से आया है।
- अज्ञात स्रोतों से आने वाले लिंक और अटैचमेंट पर विलक करने से बचो।
- एटी-फ़िशिंग रॉप्टवेयर इस्टॉल कर और यह सुनिश्चित करें कि आपका डिवाइस सुरक्षित है।



फ़िशिंग आपके रदारथ्य
के लिए भछा नहीं है



3 ऑनलाइन सुरक्षित रहने के लिए प्रमुख सुझाव

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

4 साइबर अपराधों की रिपोर्टिंग

अंगर 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 आपने बैंक से भी संपर्क कर सकते हैं और आपने खातों/कार्डों को ब्लॉक करा सकते हैं ताकि आगे गुक्सान से बचा जा सके।

सतर्क रहें, सुरक्षित रहें।





छात्रों के लिए साइबर अपर्याप्त से बचने के लिए पुस्तका

Department of
IT & Electronics

325

2.3 सोशल मीडिया प्रोटोकॉल

समझ अपर्याप्त सोशल मीडिया प्रोटोकॉल वा उपयोग लोगों की व्यक्तिगत जानकारी साझा करने

Malicious लिंक पर बिलकु करने या धनराशि ट्रान्सफर करने के लिए कहते हैं।

आम परिचय:

- जनकी प्राणी द्वारा भिन्नता या धन मानव की पेशकश।

- व्यक्तिगत डेटा दूर्योग वाले Malicious लिंक वाले अदेश।

- आपातकालीन वित्तीय सहायता मानव वाले धोखेबाज।

- अज्ञात व्यक्तियों की भिन्नता अनुरोधों को स्वीकार करते समय सतर्क रहें।

- अपना फोन नबर, पता, या बैंकिंग जानकारी सार्वजनिक रूप से शेयर न करें।

- स्थिन्य घाती 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 प्राइवेसी सेटिंग्स चुनें।



छात्रों के लिए साइबर आपराध से बचने हेतु पुस्तिका

Department of
IT & Electronics

2.4 गैमिंग ऐप घोटाला (Gaming App Scams)

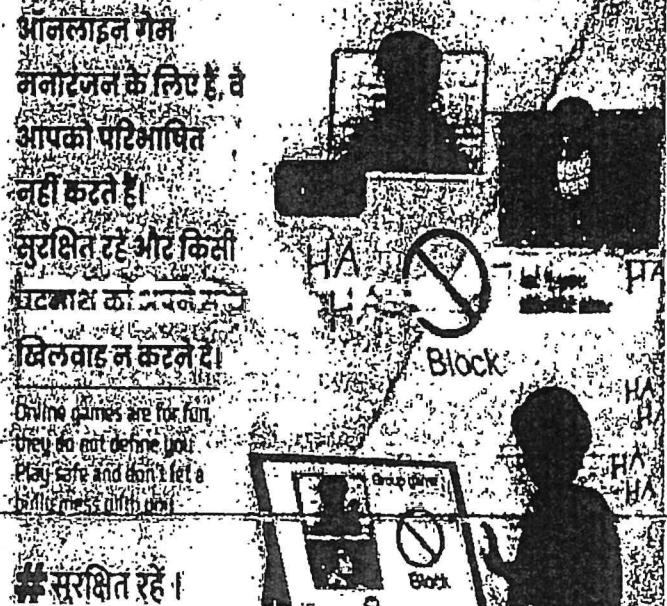
गैमिंग ऐप घोटाला खिलाड़ियों को मुफ्त इन-गेम करेसी, दुर्लभ आइटम या चीट्स का वादा करके धोखा देते हैं, जिनके लिए टॉगिन विवरण या भुगतान की आवश्यकता होती है।

आम परिणय:

- नकली (फेक) वेबसाइट या ऐप्स जो मुफ्त गेम डाउनलोड या चीट्स की पेशकाश करते हैं।
- खिलाड़ियों को ऐसे इन-गेम आइटम खरीदने के लिए धोखा देना जो असल में मोजूद नहीं होता।
- इन-गेम नोटिफिकेशन या संदेशों के रूप में छिपे हुए फिलिंग प्रयोग।

आनलाइन गेम
ननोटिफिकेशन के लिए है, वे
आपको परिभाषित
नहीं करते हैं।
सुरक्षित हो भारत किसी
प्रदाता का प्रबन्धन
निलंबन करते हैं।
Online games are for fun
not profit or define you.
Please don't let a
scammer trick you.

सुरक्षित रहें।



रोकथाम के सुझाव:

- केवल अधिकारिक ऐप स्टोर 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 चुयने का प्रयास करते हैं।

आम परिणय:

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





छान्तों के लिए साइबर अपराध से बचने के लिए पुस्तिका

Department of
IT & Electronics

रोकथाम के सुझाव:

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

2.6 ई-कॉमर्स धोखाधड़ी

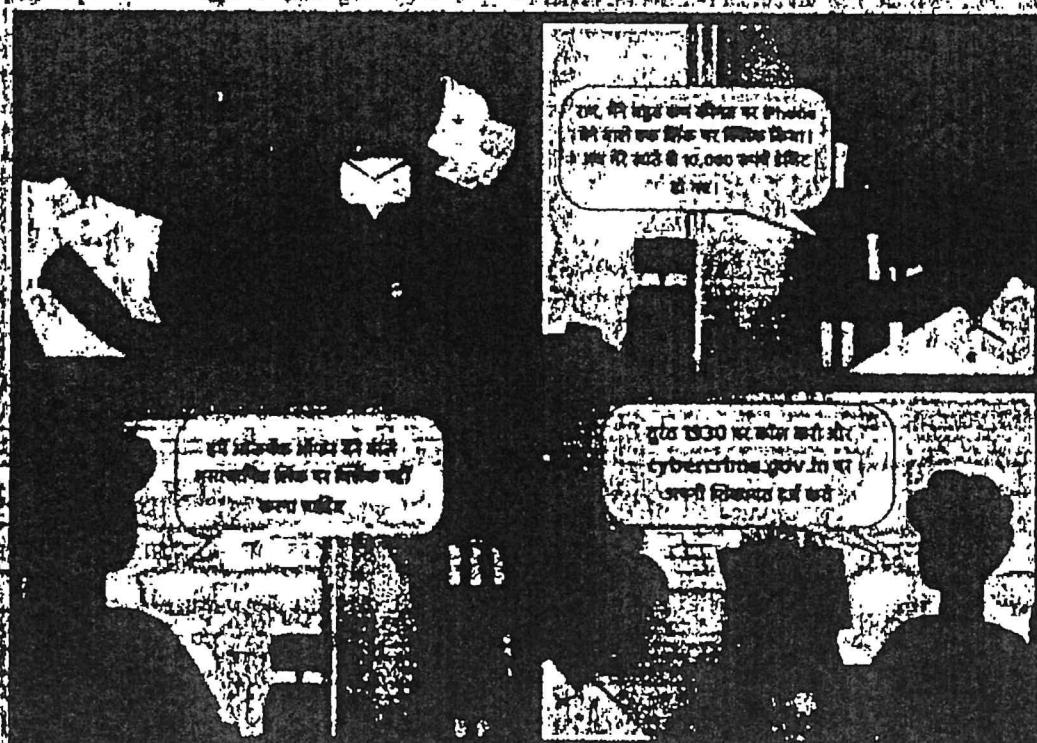
धोखाधड़ी, जकली, (फ्रैंक) ई-कॉमर्स वेबसाइट या प्लेटफॉर्म पर प्रोफाइल बनाकर उपभोग्ताओं को लूप्हाल दिए और मालयां से धृष्टिया उपयोग ऐप्स का प्रयोग करते हैं।

आम परिदृश्य:

- जकली वेबसाइट या विक्रेता जो बहुत ही कम कीमत पर उत्पाद बेच रहे हैं।
- भुगतान करने के बाद उत्पाद की डिलीवरी नहीं होती।
- दास्ती वस्तुओं के भुगतान के बाद बकली उत्पाद मिलता।

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 हस्तातरण से बचें।
- बहुत कम कीमत वाले ऑफर से सावधान रहें।





2.7 नौकरी का घोटाला (Job Scams)

घोखेबाज, 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 परिणय:

- 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 इंटर्नशिपें जो वास्तविक रोजगार की ओर कभी नहीं ले जाती।

योकथाम के सुझाव:

- जिस कंपनी द्वारा नौकरी या इंटर्नशिप की पेशकश की गई है, उसकी जांच करें।
- उन नौकरी प्राप्तावों से दूर रहें जो व्यक्तिगत जानकारी या अधिगम भुगतान मांगते हैं।
- नौकरी के प्रस्ताव को सीधे कंपनी से संत्यापित 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। घोखेबाज मुद्दे को "सुलझाने" के लिए पैसे की मांग करते हैं।

आम परिणय:

- आपको जांच या कानूनी कार्रवाई का दावा करने वाले धमकी भरे ईमेल या कॉल।
- कानून प्रवतन या कर अधिकारी बनकर धनराशि की मांग करने वाले घोखेबाज।
- गिरफ्तारी या कानूनी जुर्माने के नकली लॉटिस।

योकथाम के सुझाव:

- धमकी भरे ईमेल या कॉल से घबराएं नहीं या प्रतिक्रिया न दें।
- कार्रवाई करने से पहले कानूनी अधिकारियों के साथ संत्यापन करें।
- वसूली के प्रयोगों 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 फ़ोँटलीं को एन्क्रिप्ट कर देता है और उन्हें अनलैंक करने के लिए भुगतान (अक्सर क्रिप्टोकरेसी 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।

प्रदूषण के प्रदर्शन:

- अपनी फ़ोँटलों का नियामित रूप से किसी अन्य जगह (ऑनलाइन/ऑफलाइन) बाहरी स्रोत पर ढैक अप लें।
- एंटीवायरस सॉफ्टवेयर इनस्टॉल 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 चूनिक पासवर्ड का उपयोग करें और टूफ़ियर ऑथेंटिकेशन का प्रयोग करें।
- सतर्क रहें: लिंक, ईमेल या संदेशों को विलक्ष करने या जवाब देने से पहले सत्यापित करें।
- जियमित अपडेट: अपने सॉफ्टवेयर और उपकरणों को नवीनतम सुरक्षा अपडेट के साथ अपडेट रखें।
- शोपिंग वेबसाइट महत्वपूर्ण है: ऑनलाइन साझा की जाने वाली क्षक्तिगत जानकारी को जीमित रखें।
- संदिग्ध गतिविधि की रिपोर्ट करें: यदि आप किसी संदिग्ध स्टेशन या ऑनलाइन गतिविधि का संगमना करते हैं, तो अपनी स्कूल या कॉलेज की आईटी टीम लो सूचित करें।

4 साइबर अपराधों की रिपोर्टिंग

अगर आपको ऐदेह है कि आप किसी साइबर अपराध का शिकार हुए हैं, तो आप नियमित रूप से स्टेशन पर रिपोर्ट कर सकते हैं या राष्ट्रीय साइबर अपराध रिपोर्टिंग याम्बन्धी पोर्टल (<http://cybercrime.mca.gov.in>) से संपर्क कर सकते हैं। किसी भी वित्तीय धौखालियों के लिए राष्ट्रीय साइबर अपराध देवलाइन नंबर 1930 पर सूचित करें। आपके दैनिक संपर्क से भी संपर्क कर सकते हैं और अपने खातों/फ़ोँटों को ब्लॉक करा सकते हैं। ताकि आप 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 का आनलाइन खत्तों से सुरक्षित रखें"

ग्राम पंचायत व नगर पालिका काउंसिल द्वारा आयोजित

- सिस्टम में बहुत कमा और ID का बदला भवित्व पर बदला दें। यह अपने दोस्तों और जानीप्रियों द्वारा बड़ी अभियान है।
- डाटा के इस लिए जो जाता है तो उसे बदला देना चाहिए।

नियमों का लान्चरीज घोषणा

- नियमों के अधिकारियों को जाना चाहिए और जानार्थी के लिए नियमों के लिए जाना चाहिए।
- नियमों की विवरणों को जाना चाहिए और जानार्थी के लिए नियमों के लिए जाना चाहिए।

कानूनी घोषणाएँ

- नियमों के अधिकारियों को जाना चाहिए और जानार्थी के लिए नियमों के लिए जाना चाहिए।
- नियमों की विवरणों को जाना चाहिए और जानार्थी के लिए नियमों के लिए जाना चाहिए।

गोपनीयता गारंटी / गोपनीयता के लिए गोपनीयता

- नियमों के अधिकारियों को जाना चाहिए और जानार्थी के लिए नियमों के लिए जाना चाहिए।
- नियमों की विवरणों को जाना चाहिए और जानार्थी के लिए नियमों के लिए जाना चाहिए।

Stay Informed, Stay Safe - Report Cyber Crimes Immediately!

सचेत रहें, सुरक्षित रहें - साइबर अपदाधों की तुरंत रिपोर्ट करें।

साइबर हेल्पलाइन: 1930

खुद को और अपने परिवार को साइबर खत्तों से बचाएं।