ੴ ਸ੍ਰੀ ਵਾਹਿਗੁਰੂ ਜੀ ਕੀ ਫ਼ਤਹਿ

पंजाब एण्ड सिंध बैंक
(भारत सरकार का उपक्रम)

Punjab & Sind Bank
(A Govt. of India Undertaking)

Where service is a way of life

साइबर सुरक्षा डाइजेस्ट

"अपने डिजिटल जीवन को सुरक्षित रखें: स्मार्ट रहें, सुरक्षित रहें"

#CyberSurakshitBharat#SatarkNagrik

प्रस्तुतकर्ता –
प्र.का. सीसो सेल

प्रिय साथियों,

मैं साइबर सुरक्षा डाइजेस्ट बनाने की सक्रिय पहल के लिए हमारे सीसो सेल के प्रयासों की सराहना करना चाहता हूँ। आज के तेजी से विकसित हो रहे डिजिटल परिदृश्य में, साइबर सुरक्षा के महत्व को कम करके नहीं आंका जा सकता। यह पुस्तिका एक महत्वपूर्ण संसाधन है जिसका उद्देश्य बैंक की महत्वपूर्ण जानकारी और प्रणालियों की सुरक्षा के बारे में हम सभी को शिक्षित और सशक्त बनाना है। साइबर सुरक्षा डाइजेस्ट विभिन्न प्रकार के साइबर हमलों, साइबर स्वच्छता के महत्व और व्यावहारिक साइबर सुरक्षा प्रथाओं पर बहुमूल्य ज्ञान प्रदान करता है। मैं प्रत्येक स्टाफ सदस्य को न केवल इस दस्तावेज़ को पढ़ने के लिए प्रोत्साहित करता हूँ बल्कि अपने दैनिक कार्यों में उल्लिखित प्रथाओं को एकीकृत करने के लिए भी प्रोत्साहित करता हूँ। ऐसा करके, आप संभावित साइबर खतरों के खिलाफ हमारी रक्षा को मजबूत करने में महत्वपूर्ण भूमिका निभाएँगे।

आइए हम सभी इस संसाधन का अधिकतम उपयोग करें और बैंक की डिजिटल संपत्तियों की सुरक्षा के लिए अपनी साझा जिम्मेदारी के प्रति सतर्क रहें। साथ मिलकर, हम अपने संस्थान और अपने ग्राहकों के लिए अधिक सुरक्षित और सुरक्षित वातावरण सुनिश्चित कर सकते हैं।

साभार,

राजीवा
कार्यकारी निदेशक
पंजाब एंड सिंध बैंक

साइबर सुरक्षा का महत्व

•इंटरनेट किसी भी हमलावर को दुनिया में कहीं से भी काम करने की अनुमति देता है।

•साइबर सुरक्षा, कंप्यूटर प्रणालियों और नेटवर्कों को डेटा लीक, चोरी, या उनके हार्डवेयर, सॉफ्टवेयर या इलेक्ट्रॉनिक डेटा को होने वाली क्षति, साथ ही सेवाओं में व्यवधान या गलत दिशा-निर्देशन से सुरक्षा प्रदान करना है।

•इंटरनेट पर नियमित रूप से नए और शक्तिशाली साइबर हमले हो रहे हैं। हमारे डिजिटल जीवन को प्रबंधित करने में एक छोटी सी चूक साइबर अपराधियों के लिए दरवाज़ा खोल सकती है। साइबर अपराधी हमारे पैसे चुरा सकते हैं या हमारी प्रतिष्ठा को नुकसान पहुंचा सकते हैं।

•एक प्रमुख अनुसंधान संगठन के अध्ययन के अनुसार, सभी साइबर हमलों में से 90% मानवीय लापरवाही के कारण होते हैं। इसलिए, आज हर किसी के लिए साइबर सुरक्षा जागरूकता महत्वपूर्ण है।

#CyberSurakshitBharat#SatarkNagrik

साइबर हमलों के सामान्य कारण

- कमज़ोर या चोरी हुए उपयोगकर्ता नाम और पासवर्ड का उपयोग करना
- सॉफ़्टवेयर एप्लिकेशन की कमज़ोरियाँ
- एंटीवायरस और नवीनतम पैच की अनुपस्थिति
- पायरेटेड ऑपरेटिंग सिस्टम का उपयोग
- सिस्टम और नेटवर्क फ़ायरवॉल अक्षम
- सोशल इंजीनियरिंग (लोगों को सुरक्षा प्रोटोकॉल तोड़ने के लिए धोखा देना)
- खराब एक्सेस कंट्रोल (अनधिकृत उपयोगकर्ताओं के पास एक्सेस है)
- अंदरूनी खतरे (सिस्टम पासवर्ड सेट नहीं किया गया है)
- वाईफ़ाई डिवाइस और हॉटस्पॉट का अनुचित कॉन्फ़िगरेशन
- बैकडोर एंट्री के लिए नेटवर्क पर अनावश्यक पोर्ट खोले जाना

#CyberSurakshitBharat#SatarkNagrik

रैंसमवेयर

रैनसमवेयर संक्रमण कैसे होता है?

संदिग्ध वेबसाइट पर जाना / फ़िशिंग ईमेल खोलना

सिस्टम संक्रमित / फ़ाइलें एन्क्रिप्टेड और फिरौती की मांग

संक्रमित होने पर क्या करें?

सिस्टम को इंटरनेट से डिस्कनेक्ट करें

संबंधित प्राधिकारी को घटना की सूचना दें

बैकअप से क्लीन डिवाइस पर डेटा पुनर्स्थापित करें

एंटीवायरस और विंडोज को अपडेट रखें

संदेहास्पद ईमेल न खोलें

वेबसाइटो पर संदिग्ध लिंक पर क्लिक न करें

नियमित रूप से डेटा का बैकअप लें

फ़ायरवॉल सुरक्षा सक्षम करें

रैनसमवेयर से खुद को सुरक्षित रखें !!!

#CyberSurakshitBharat
#SatarkNagrik

विशिंग/सोशल इंजीनियरिंग

काम करने का ढंग

- धोखेबाज अपने लक्षित लोगों की पृष्ठभूमि की जांच करते हैं और अभियान चलाकर हमला करते हैं।
- अधिकतर यह कॉल पर होता है जिसमें आपसे लिंक पर क्लिक करने, धन दान करने, खाता विवरण अपडेट करने आदि के लिए कहा जाता है।
- वे पीड़ितों की स्वाभाविक प्रतिक्रियाओं का लाभ उठाकर मनोवैज्ञानिक रूप से उनका शोषण करते हैं।

कैसे सुरक्षित रहें?

- सुनहरा नियम यह है कि इनबाउंड ग्राहक सेवा/तकनीकी सेवा कॉल या ईमेल समर्थन अनुरोधों से बचें।
- बैंक प्रतिनिधि बनकर आने वाले लोगों की कॉल कभी न सुनें। बैंक कभी भी कॉल करके CVV/PIN/OTP नहीं मांगते।
- यदि कोई दूरस्थ सहकर्मी फोन करके आपके खाते के क्रेडेंशियल या आधिकारिक जानकारी मांगता है, तो आईटी सुरक्षा टीम को सूचित रखें और निर्देशानुसार कार्य करें।

#CyberSurakshitBharat
#SatarkNagrik

सोशल मीडिया धोखाधड़ी

काम करने का ढंग

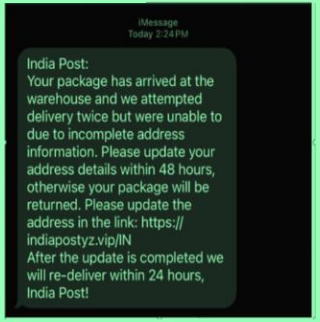
- जालसाज सोशल मीडिया प्लेटफॉर्म पर बैंकों और यूपीआई प्लेटफॉर्म के फर्जी ग्राहक सेवा नंबर डालते/फैलाते हैं।
- समान डिज़ाइन वाली फर्जी बैंक वेबसाइटें और फर्जी यूपीआई ऐप अपलोड किए गए हैं।
- उपयोगकर्ता इन नंबरों पर कॉल करते हैं, धोखेबाज खुद को आधिकारिक प्रतिनिधि बताते हैं।
- धोखेबाज संवेदनशील जानकारी निकाल लेता है और उपयोगकर्ता के खाते से पैसे काट लेता है।

कैसे सुरक्षित रहें?

- अपने ऐप या बैंक के कस्टमर केयर नंबर को सर्च इंजन या सोशल मीडिया पर न खोजें।
- हमेशा आधिकारिक वेबसाइट पर जाएं, यूआरएल जांचें और वास्तविक नंबरों पर संपर्क करें।
- स्थान, अक्सर जाने वाले स्थान, वित्तीय खरीदारी आदि जैसी व्यक्तिगत
जानकारी साझा न करें।

#CyberSurakshitBharat
#SatarkNagrik

कूरियर घोटाला



काम करने का ढंग

- घोटालेबाज धोखाधड़ी वाले ईमेल, एसएमएस या कॉल भेजकर दावा करते हैं कि पार्सल की डिलीवरी के लिए भुगतान या जानकारी की आवश्यकता है।
- संदेश में एक नकली वेबसाइट का लिंक शामिल है जो एक वैध कूरियर सेवा की नकल करता है, तथा व्यक्तिगत या भुगतान विवरण मांगता है।
- इस घोटाले में अक्सर दबाव शामिल होता है, जैसे कि “तत्काल भुगतान आवश्यक है” या “डिलीवरी रद्द कर दी जाएगी”।
- पीड़ितों को धोखे से भुगतान संबंधी जानकारी या व्यक्तिगत विवरण दर्ज करवा लिया जाता है, जिसके परिणामस्वरूप वित्तीय चोरी या पहचान संबंधी धोखाधड़ी हो जाती है।

कैसे सुरक्षित रहें?

- कूरियर नोटिफिकेशन की पुष्टि हमेशा आधिकारिक चैनल या ऐप के माध्यम से करें।
- अनचाहे संदेशों में दिए गए लिंक पर क्लिक न करें। ईमेल पते और फ़ोन नंबरों के असामान्य फ़ॉर्मेट की जाँच करें।
- वर्तनी संबंधी त्रुटि वाले संदेशों से सावधान रहें।
- पार्सल को केवल कूरियर की आधिकारिक वेबसाइट या ऐप के माध्यम से ही ट्रैक करें।

#CyberSurakshitBharat
#SatarkNagrik

डिजिटल गिरफ्तारी घोटाला

काम करने का ढंग

- धोखेबाज़ कानून प्रवर्तन अधिकारी का रूप धारण कर दावा करते हैं कि आप जांच के दायरे में हैं या आपने कोई अपराध किया है।
- वे गिरफ्तारी या कानूनी परेशानी से बचने के लिए भुगतान की मांग करते हैं (आमतौर पर वायर ट्रांसफर या क्रिप्टोकरेंसी के माध्यम से)।
- इन घोटालों में अक्सर धमकियाँ, झूठी तात्कालिकता और नकली कानूनी दस्तावेज़ शामिल होते हैं

कैसे सुरक्षित रहें?

- कानून प्रवर्तन अधिकारी कभी भी गिरफ्तारी से बचने के लिए फोन पर पैसे की मांग नहीं करेंगे।
- किसी भी दावे की पुष्टि स्थानीय प्राधिकारियों से सीधे संपर्क करके करें।
- अज्ञात खातों या दबाव में आए व्यक्तियों को भुगतान करने से बचें ।

#CyberSurakshitBharat
#SatarkNagrik

काम करने का ढंग

- साइबर अपराधी आपका प्रतिरूपण करने के लिए आपकी व्यक्तिगत जानकारी (जैसे, नाम, ईमेल, मोबाइल नंबर, बैंक खाता विवरण) चुरा लेते हैं।
- वे आपके नाम पर नए क्रेडिट खाते खोल सकते हैं, पैसे निकाल सकते हैं या ऋण के लिए आवेदन कर सकते हैं।
- वे सोशल मीडिया पर आपकी पहचान ग्रहण कर लेते हैं।
- पहचान की चोरी डेटा उल्लंघन, फ़िशिंग या भौतिक दस्तावेज़ों की चोरी के माध्यम से हो सकती है।

कैसे सुरक्षित रहें?

- अपने वित्तीय खातों और क्रेडिट रिपोर्ट की नियमित निगरानी करें।
- ऑनलाइन खातों के लिए मजबूत एवं अद्वितीय पासवर्ड का उपयोग करें।
- असुरक्षित संचार चैनलों पर व्यक्तिगत जानकारी साझा करने से बचें।

#CyberSurakshitBharat
#SatarkNagrik

डीपफेक घोटाला

काम करने का ढंग

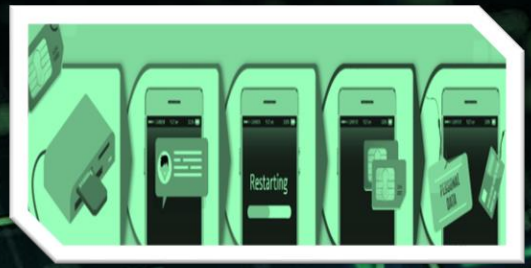
- धोखेबाज व्यक्ति, लक्षित व्यक्ति के बारे में पर्याप्त डेटा, जैसे चित्र, वीडियो, सोशल मीडिया पोस्ट या ऑडियो रिकॉर्डिंग एकत्रित कर लेता है, ताकि एक वास्तविक डिजिटल प्रतिकृति तैयार की जा सके।
- जालसाज एआई एल्गोरिदम, विशेष रूप से डीप लर्निंग तकनीकों का उपयोग करके ऐसे मॉडलों को प्रशिक्षित करता है, जो जालसाज द्वारा एकत्र किए गए पीड़ित के डेटा का उपयोग करके अत्यधिक विश्वसनीय डीपफेक सामग्री उत्पन्न कर सकते हैं।
- धोखेबाज लोग धोखा देने के लिए फर्जी वीडियो या ऑडियो के माध्यम से विश्वसनीय व्यक्तियों का रूप धारण कर लेते हैं।

कैसे सुरक्षित रहें?

- वीडियो या ऑडियो अनुरोधों की हमेशा प्रत्यक्ष संचार के माध्यम से जांच करें।
- संदेहशील बनें, वास्तविक दिखने या सुनने वाली सामग्री पर तुरंत भरोसा न करें, डीपफेक भ्रामक हो सकता है।
- केवल विश्वसनीय समाचार आउटलेट और आधिकारिक चैनलों से प्राप्त जानकारी पर ही विश्वास करें।
- अनधिकृत पहुंच को रोकने के लिए सोशल मीडिया पर दो कारक प्रमाणीकरण (2FA) सक्षम करें।

#CyberSurakshitBharat
#SatarkNagrik

सिम क्लोनिंग



काम करने का ढंग

- धोखेबाज आपके फोन नंबर पर नियंत्रण पाने के लिए अक्सर फिशिंग या सोशल इंजीनियरिंग के माध्यम से आपके सिम कार्ड का क्लोन बना लेते हैं।
- इसके बाद जालसाज पीड़ित को एक एसएमएस भेजेगा जिसमें किसी बहाने से मोबाइल को फिर से चालू करने का अनुरोध किया जाएगा। एक बार जब पीड़ित अपना मोबाइल बंद कर देता है, तो जालसाज पीड़ित के मोबाइल को फिर से चालू करने से पहले, अपने नियंत्रण में एक डुप्लिकेट सिम के साथ फोन चालू कर देता है। यह कार्य क्लोन किए गए सिम कार्ड के साथ मोबाइल को सफलतापूर्वक चालू/सक्रिय कर देगा।
- एक बार क्लोन सिम सफलतापूर्वक चालू हो जाने पर हमलावर पीड़ित के मोबाइल नंबर, सिम और उसके खाते पर कब्जा कर लेगा।

कैसे सुरक्षित रहें?

- सार्वजनिक मंचों पर या अज्ञात व्यक्तियों के साथ अपनी संवेदनशील व्यक्तिगत जानकारी, जैसे कि अपना मोबाइल नंबर, साझा करने से बचें।
- अपने सिम कार्ड को सुरक्षित स्थान पर रखें और इसे दूसरों के साथ साझा करने से बचें। किसी भी खोए या चोरी हुए सिम कार्ड की सूचना तुरंत अपने सेवा प्रदाता को दें।
- सुरक्षा की एक अतिरिक्त परत जोड़ने के लिए अपने सिम कार्ड पर व्यक्तिगत पहचान संख्या (पिन) और व्यक्तिगत अनब्लॉकिंग कुंजी (पीयूके) कोड सक्षम करें।
- एसएमएस-आधारित सत्यापन के अलावा अन्य तरीकों का उपयोग करके 2FA को लागू करें, जैसे ईमेल प्रमाणीकरण, ऐप-आधारित प्रमाणक, या हार्डवेयर टोकन।

#CyberSurakshitBharat
#SatarkNagrik

टेलगेटिंग

काम करने का ढंग

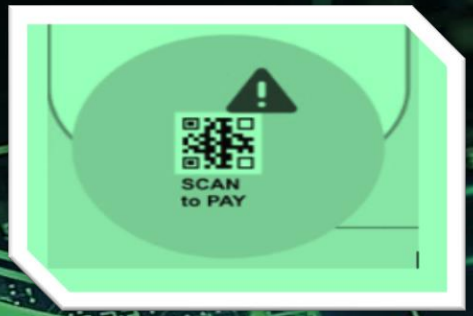
- वैध कार्ड धारक के साथ लाइन में घुसना।
- उपयोगकर्ता वैध आईडी कार्ड के साथ प्रवेश करता है और सॉफ्टवेयर-आधारित इलेक्ट्रॉनिक गेट पर प्रवेश चाहता है।
- वैध पहचान पत्र धारक को प्रवेश देने के लिए गेट खुलता है। इस बीच धोखेबाज़ उसी समय अनधिकृत रूप से अंदर घुसने का अवसर प्राप्त कर लेता है।
- जालसाज किसी अधिकृत कर्मचारी का पहचान पत्र भी चुरा सकता है ताकि वह प्रतिबंधित स्थान में प्रवेश कर सके।

कैसे सुरक्षित रहें?

- प्रबंधन को बायोमेट्रिक स्कैनर और टर्नस्टाइल लगाने होंगे, ताकि कोई भी पीछे से आकर इमारत में घुस न सके।
- बायोमेट्रिक स्कैनर और इलेक्ट्रिक प्रवेश द्वार, पीछे से आने वाले व्यक्ति को भवन के अंदर उपयोगकर्ता के साथ चलने से रोकते हैं।
- जब किसी कार्यालय में कोई अज्ञात व्यक्ति दिखाई दे तो जांच लें कि उसके पास आगंतुक बैज है या नहीं।

#CyberSurakshitBharat
#SatarkNagrik

क्यूआर कोड भुगतान



काम करने का ढंग

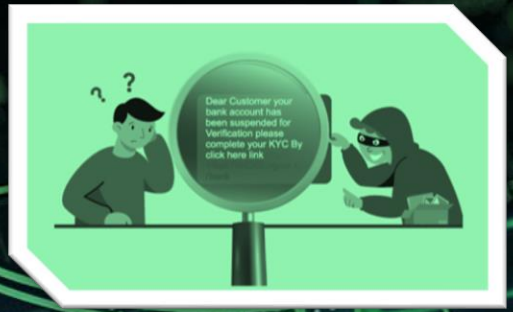
- व्यापारी अपनी भुगतान प्रणालियों से जुड़े अद्वितीय क्यूआर कोड बनाते हैं।
- कोड बिक्री स्थल पर दिखाए जाते हैं या डिजिटल रूप में भेजे जाते हैं।
- ग्राहक अपने स्मार्टफोन भुगतान ऐप से कोड को स्कैन करते हैं।
- ग्राहक राशि की पुष्टि करते हैं और भुगतान को अधिकृत करते हैं।
- लेन-देन संसाधित हो जाता है और दोनों पक्षों को पुष्टि प्राप्त हो जाती है।

कैसे सुरक्षित रहें?

- केवल प्रतिष्ठित भुगतान ऐप्स से कोड स्कैन करें।
- पुष्टि करें कि QR कोड वैध व्यवसाय से हैं.
- लेन-देन के लिए सुरक्षित नेटवर्क का उपयोग करें।
- छेड़छाड़ के संकेतों की जांच करें।

#CyberSurakshitBharat
#SatarkNagrik

केवाईसी धोखाधड़ी



काम करने का ढंग

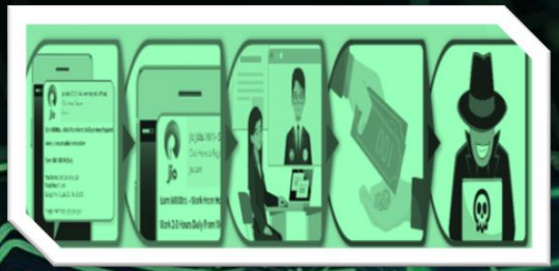
- जालसाज पीड़ित को फर्जी कॉल करके बैंक का प्रतिनिधि होने का नाटक करते हैं और उनसे तुरंत केवाईसी अपडेट करने का अनुरोध करते हैं तथा खाता ब्लॉक/निलंबित करने की चेतावनी देते हैं।
- कॉल करने वाला व्यक्ति कहता है कि खाते को सक्रिय रखने के लिए सत्यापन/केवाईसी ऑनलाइन किया जा सकता है, तथा वह ग्राहक से अपने डिजिटल डिवाइस पर एक ऐप डाउनलोड करने के लिए कहता है।
- एक बार ऐप डाउनलोड हो जाने पर, धोखेबाज आपसे कोड साझा करने और कुछ अनुमतियां देने के लिए कहेंगे, जिससे वे आपके डिजिटल डिवाइस तक पहुंच प्राप्त कर सकेंगे।
- धोखेबाज इन विवरणों का उपयोग पीड़ित के बैंक खाते तक अनधिकृत पहुंच प्राप्त करने के लिए धोखाधड़ी करने के लिए करता है।

कैसे सुरक्षित रहें?

- कभी भी अज्ञात लिंक या असत्यापित स्रोतों से प्राप्त लिंक पर क्लिक न करें।
- हमेशा याद रखें कि कोई भी बैंक या अन्य अधिकृत संस्थाएं कभी भी कॉल पर केवाईसी नहीं करती हैं या केवाईसी अपडेट करने के लिए अपने ग्राहकों को कोई लिंक नहीं भेजती हैं।
- अपना मोबाइल नंबर, खाता संख्या, पासवर्ड, ओटीपी, पिन या कोई अन्य गोपनीय जानकारी कभी किसी के साथ साझा न करें। बैंक कभी भी अपने ग्राहकों से कोई गोपनीय जानकारी साझा करने के लिए नहीं कहता है।
- रिमोट एक्सेस के एप्लिकेशन (एनीडेस्क, क्विकसपोर्ट, टीम व्यूअर आदि) इंस्टॉल करके किसी को भी अपने डिवाइस तक पहुंच न दें।

#CyberSurakshitBharat
#SatarkNagrik

रोजगार घोटाले



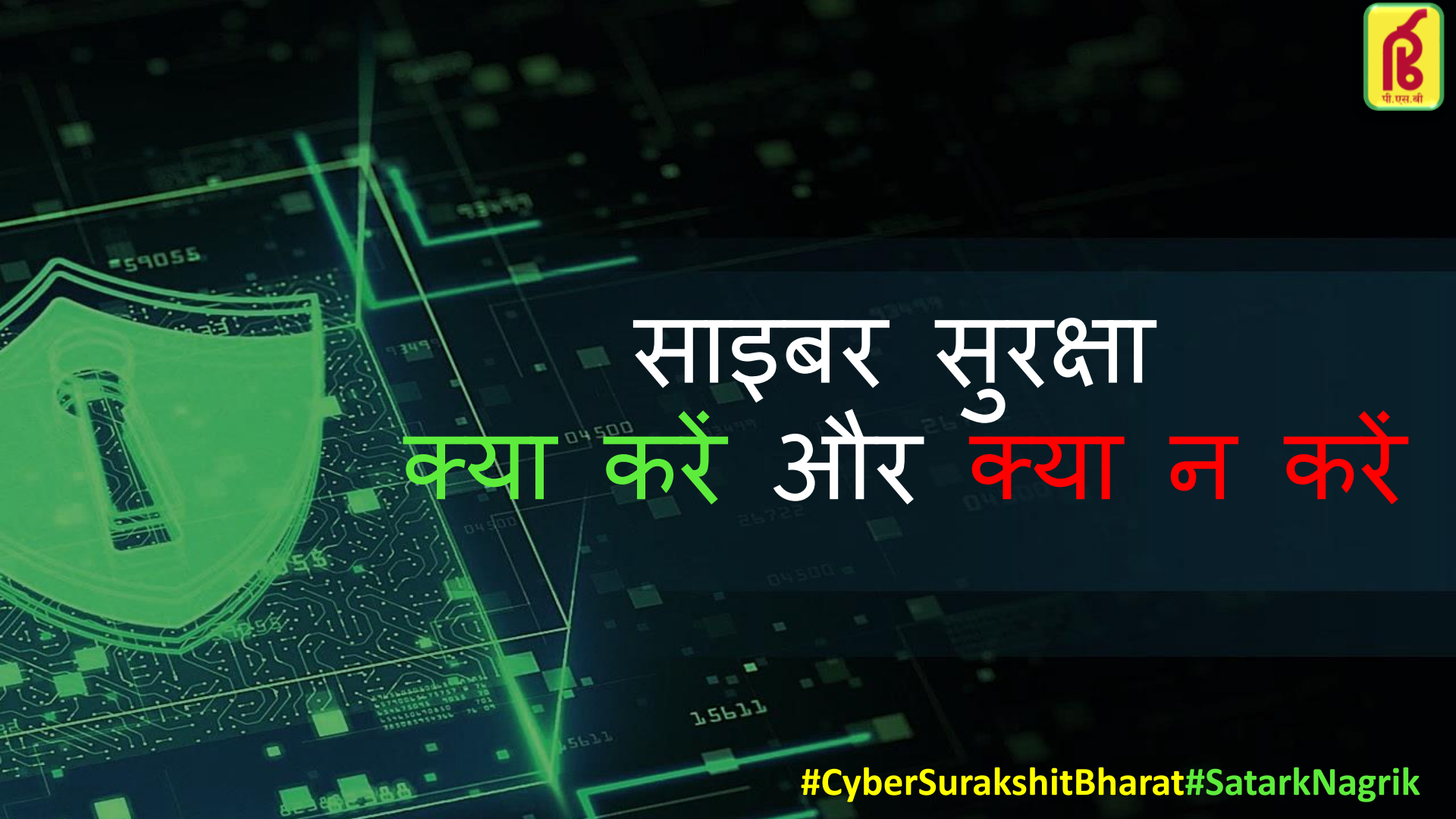
काम करने का ढंग

- उपयोगकर्ता को धोखेबाजों द्वारा बनाई गई आकर्षक नौकरी लिस्टिंग के संबंध में संदेश/ईमेल/कॉल प्राप्त होते हैं, जिनमें नौकरी चाहने वालों को आकर्षित करने के लिए उच्च वेतन वाले पद, लचीले कार्य घंटे और आशाजनक लाभ देने का दावा किया जाता है।
- घोटालेबाज, वास्तविक दिखने के लिए तथा संभावित पीड़ितों का विश्वास जीतने के लिए, परिचित नामों, लोगो का प्रयोग करते हुए, वैध कंपनियों का रूप धारण कर लेते हैं।
- एक बार जब कोई उपयोगकर्ता उनसे संपर्क करता है तो घोटालेबाज फोन कॉल या मैसेजिंग ऐप के जरिए फर्जी साक्षात्कार आयोजित कर सकते हैं।
- घोटालेबाज विभिन्न कारणों से अग्रिम भुगतान या शुल्क मांगते हैं जो अक्सर वापस नहीं किए जाते। एक बार जब वे भुगतान कर देते हैं तो धोखेबाज़ या तो जवाब देना बंद कर देता है या किसी बहाने से उनके कॉल/संदेश/ईमेल से बचता है या पूरी तरह से गायब हो सकता है।

कैसे सुरक्षित रहें?

- नौकरी के लिए आवेदन करने या कोई भी व्यक्तिगत जानकारी देने से पहले कंपनी या नियोक्ता के बारे में अच्छी तरह से शोध कर लें।
- नौकरी के अवसरों की खोज करते समय प्रतिष्ठित और सुप्रसिद्ध जॉब पोर्टलों से जुड़ें।
- व्यक्तिगत जानकारी साझा करते समय सावधान रहें। वैध नियोक्ता आमतौर पर संवेदनशील विवरण नहीं मांगते हैं।
- संभावित नियोक्ताओं के साथ संवाद करते समय, सुरक्षित चैनलों का उपयोग करें ।

#CyberSurakshitBharat
#SatarkNagrik


साइबर सुरक्षा
क्या करें और क्या न करें
#CyberSurakshitBharat#SatarkNagrik

पासवर्ड सुरक्षा युक्तियाँ

- हमेशा अलग-अलग खातों के लिए अलग-अलग पासवर्ड का उपयोग करें। सुनिश्चित करें कि पासवर्ड मजबूत हो।
- मजबूत पासवर्ड में अपर केस, लोअर केस, संख्याएं, "विशेष" वर्णों का संयोजन होना चाहिए (उदाहरण के लिए, @#$%^&*()_+|~--=\'{}[]:";<>/,आदि)

- यदि कोई पासवर्ड गलती से साझा या प्रकट हो गया हो तो उसे तुरंत बदल दें।
- पासवर्ड सेट करते समय जन्मतिथि, नाम, पहचान प्रमाण और अन्य व्यक्तिगत जानकारी जैसे पता और फोन नंबर का उपयोग न करें।

#CyberSurakshitBharat#SatarkNagrik

इंटरनेट सुरक्षा सावधानियां

- किसी भी वेबसाइट को खोलते समय सुरक्षित कनेक्शन की जांच करें, यह जांच कर लें कि वेबसाइट “HTTPS” से शुरू होती है या नहीं।
- संदिग्ध लिंक/यूआरएल पर क्लिक/डाउनलोड करते समय सतर्क रहें।
- गोपनीय गतिविधियों/लेनदेन के बाद ब्राउज़र इतिहास साफ़ करने की आदत डालें।

- किसी भी पत्राचार में शामिल होने से पहले सोशल मीडिया प्रोफाइल की प्रामाणिकता और पहचान सत्यापित करें।
- ऑनलाइन शॉपिंग, इंटरनेट बैंकिंग, यूपीआई लेनदेन आदि जैसे वित्तीय लेनदेन के लिए किसी भी सार्वजनिक कंप्यूटर या वाई-फाई का उपयोग न करें।

#CyberSurakshitBharat#SatarkNagrik

यूपीआई और एटीएम लेनदेन संबंधी सावधानियां

- गोपनीय जानकारी किसी के साथ साझा न करें जैसे:-कार्ड नंबर, समाप्ति तिथि और सीवीवी नंबर आदि।
- याद रखें, भुगतान प्राप्त करते समय UPI पिन की आवश्यकता नहीं होती है।
- भुगतान के साथ आगे बढ़ने से पहले "भुगतानकर्ता" का नाम या क्यूआर कोड सत्यापित करें

- अतिरिक्त सुरक्षा के लिए मोबाइल बैंकिंग ऐप्स का उपयोग करके अपनी कार्ड सीमा प्रबंधित करें।
- किसी भी लेनदेन/भुगतान करते समय सार्वजनिक वाईफाई/नेटवर्क का उपयोग न करें।

#CyberSurakshitBharat#SatarkNagrik

मोबाइल सुरक्षा सावधानियां

- किसी भी ऐप को डाउनलोड करने से पहले उसकी प्रतिष्ठा/प्रामाणिकता की जांच कर लेनी चाहिए।
- अपने डिवाइस को मजबूत पिन/पासवर्ड या बायोमेट्रिक्स से सुरक्षित रखें और मोबाइल फोन में ऑटो लॉक सेटिंग सक्षम करें।
- अजनबियों द्वारा एसएमएस, ई-मेल या चैट मैसेंजर के माध्यम से भेजे गए लिंक का जवाब न दें या उस पर क्लिक न करें।

- स्मार्टफोन, मोबाइल एप्लीकेशन और सोशल मीडिया अकाउंट की डिफ़ॉल्ट गोपनीयता सेटिंग की समीक्षा करें। सार्वजनिक दृश्यता के साथ सोशल मीडिया पर पोस्ट की गई व्यक्तिगत तस्वीरों का दुरुपयोग किया जा सकता है।
- मोबाइल डिवाइस में कोई भी वर्गीकृत/संवेदनशील डेटा (टेक्स्ट/वीडियो/फोटोग्राफ) संग्रहीत न करें।

#CyberSurakshitBharat#SatarkNagrik

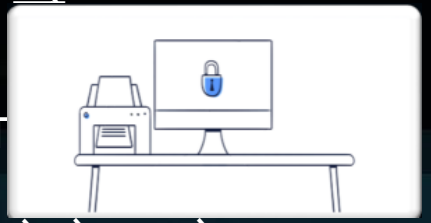
फ़िशिंग ईमेल

- ईमेल सामग्री में अनुचित वर्तनी या व्याकरण की जाँच करें।
- ईमेल की ऐसी सामग्री की जांच करें जो डेटा दर्ज करने या भुगतान करने या केवाईसी विवरण अपडेट करने आदि के लिए लिंक पर क्लिक करने की तत्काल आवश्यकता पैदा करती हो।

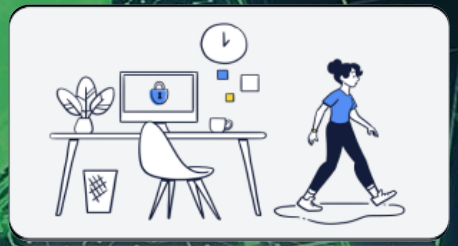
- ईमेल में संदिग्ध अनुलग्नकों की जांच करें।
- यूआरएल का सही पता जानने के लिए संदिग्ध ईमेल में उल्लिखित लिंक पर माउस घुमाएं।
- ऐसे ईमेल पर वित्तीय या व्यक्तिगत जानकारी साझा करने से बचें जो ज्ञात प्रेषक से नहीं हैं।

#CyberSurakshitBharat#SatarkNagrik

साफ़ डेस्क और साफ़ स्क्रीन नीति



- जब कार्यस्थल खाली हो तो कंप्यूटर/कार्यस्थान [illegible] लॉक कर देना चाहिए।
- प्रतिबंधित या संवेदनशील जानकारी वाले प्रिंटअ [illegible] को तुरंत प्रिंटर से हटा दिया जाना चाहिए।
- किसी भी प्रतिबंधित या संवेदनशील जानकारी को डेस्क से हटा दिया जाना चाहिए और जब डेस्क खाली हो और कार्य दिवस के अंत में एक दराज में बंद कर दिया जाना चाहिए।



- कार्य दिवस के अंत में कम्प्यूटर/वर्कस्टेशन को बंद कर देना चाहिए।
- प्रतिबंधित या संवेदनशील जानकारी वाली फाइल कैबिनेट को उपयोग में न होने पर या उपस्थित न होने पर बंद और ताला लगाकर रखना चाहिए।
- प्रतिबंधित या संवेदनशील जानकारी तक पहुंच के लिए उपयोग की जाने वाली चाबियों को किसी भी डेस्क पर अकेले नहीं छोड़ा जाना चाहिए।

#CyberSurakshitBharat#SatarkNagrik