केन्द्रीय रिर्जव पुलिस बल

साइबर बाइट

साइबर बाइट
जनवरी- 2024
संस्करण

- ई-कामर्स साइटों द्वारा की जाने वाली क्रेडिट कार्ड चोरी को रॉग वर्डप्रेस प्लगइन उजागर करता है।

- जालसाज उपयोगकर्ताओं को धोखा देने के लिए कृत्रिम बुद्धिमत्ता (ए.आई.) और चैटजीपीटी का उपयोग कर सकते है।

साइबर धोखाधडी अपडेट

ऑनलाइन वितीय धोखाधड़ी की रिपोर्ट करने के लिए

1930

पर कॉल करें

https://cybercrime.gov.in
पर अपनी शिकायत दर्ज करें

संचार एवं सूचना प्रौधगिकी निदेशालय , सीआरपीएफ

1.साइबर गीक समाचार: -

क) रॉग वर्डप्रेस प्लगइन ई-कॉमर्स साइटों की क्रेडिट कार्ड चोरी को उजागर करता है।

थ्रेट हंटर्स ने एक रॉग वर्डप्रेस प्लगइन की खोज की है जो फर्जी एडमिनिस्ट्रेटर उपयोगकर्ता बनाने और दुर्भावनापूर्ण जावास्क्रिप्ट कोड इंजेक्ट करने में सक्षम है।

स्किमिंग गतिविधि कई अन्य दुर्भावनापूर्ण या फेक वर्डप्रेस प्लगइन्स की तरह ई-कामर्स वेबसाइटों को लक्षित करने वाले मैजकार्ट अभियान का हिस्सा है, इसमें इस मामले में वैद्यता का दिखावा करने के लिए फाइल के शीर्ष पर कुछ भ्रामक जानकारी शामिल है। कामेन्टस कोड का वर्डप्रेस कॉचे (Cache) एडओन्स होना का दावा करती है।

दुर्भावनापूर्ण प्लगइन्स आमतौर पर किसी समझौता किए गए एडमिन यूजर या साइट पर पहले से इंस्टाल किए गए किसी अन्य प्लगइन में सुरक्षा खामियों का फायदा उठाकर वर्डप्रेस साइटों तक अपना रास्ता खोज लेते है।

इंस्टॉलेशन के बाद, प्लगइन स्वयं को म्यू-प्लगइन्स (या आवश्यक उपयोग होने वाले प्लगइन्स) निर्देशिका में प्रतिकृति बनाता है ताकि यह स्वचालित रूप से सक्षम हो और एडमिन पैनल से अपनी उपस्थिति छुपा सके। किसी भी एमयू-प्लगइन को हटाने का एकमात्र तरीका फाइल को मैन्युअल रूप से हटाना है, इसे रोकने के लिए मैलवेयर अपने रास्ते से हट जाता है। मैलवेयर हुक के लिए कॉलबैक प्रणाली को अपंजीकृत करके इसे पूरा करता है जो सामान्य रूप से इस तरह के प्लगइन्स का उपयोग करते है।

धोखाधड़ी वाला प्लगइन खतरे के संकेत से बचने और लंबे समय तक लक्ष्य तक पहुंच बनाए रखने के लिए वैध वेबसाइट एडमिनस्ट्रेटर यूजर खाता बनाने और छिपान के विकल्प के साथ आता है। कैंपेन का अंतिम उद्देश्य चेकआउट पेजों में क्रेडिट कार्ड चोरी करने वाले मैलवेयर को इंजेक्ट करना और जानकारी को एक्टर-नियंत्रित डोमेन तक पहुंचाना है।

चूंकि कई वर्डप्रेस इन्फेक्शन समझौता किए गए डब्लयू.पी-एडमिन प्रशासित यूजर से होते है, इसका केवल यही कारण है कि उन्हें इसके भीतर पहुंच स्तर की बाधाओं के साथ काम करने की आवश्यकता है और प्लगइन्स इंस्टाल करना निश्चित रूप से उन प्रमुख क्षमताओं में से एक है जो वर्डप्रेस एडमिन के पास है। वर्डप्रेस सुरक्षा समुदाय ने एक फिशिंग अभियान के बारे में चेतावनी दी है जो यूजर को वेब सामग्री प्रबंधन प्रणाली में एक असंबंधित सुरक्षा दोष के बारे में सचेत करता है और उन्हें पैच (patch) की आड़ में एक प्लगइन स्थापित करने के लिए प्रेरित करता है। प्लगइन, अपनी ओर से, एक एडमिन यूजर बनाता है और लगातार रिमोट एक्सेस के लिए एक वेब सेल को तैनात करता है।

कैंपेन के पीछे थ्रेट एक्टर सीवीई पहचानकर्ता से जुड़ी आरक्षित स्थिति का लाभ उठा रहे हैं, जो तब होता है जब इसे सीवीई नंबरिंग आथॉरिटी (सीएनए) या सुरक्षा शोधकर्ता द्वारा उपयोग के लिए आरक्षित किया गया है, लेकिन विवरण को अभी भरा जाना है।

यह तब भी आता है, जब वेबसाइट सुरक्षा फर्म ने एक और मेज कार्ट कैंपेन की खोज की है जो ऑनलाइन स्टोरफ्रंट पर स्किमर कोड डालने के लिए वेबसॉकेट संचार प्रोटोकॉल का उपयोग करता है। मैलवेयर वैध चैकआउट बटन के शीर्ष पर मौजूद नकली कंप्लीट आर्डर बटन पर क्लिक करने पर ट्रिगर हो जाता है।

ऑनलाइन धोखाधड़ी पर इस सप्ताह जारी यूरोपोल की स्पॉटलाइट रिपोर्ट में डिजिटल स्किमिंग को एक लगातार खतरा बताया गया है जिसके परिणामस्वरूप क्रेडिट कार्ड डेटा की चोरी, पुनः बिक्री और दुरुपयोग होता है। डिजिटल स्किमिंग में एक प्रमुख फैलाव फ्रंट-एंड मैलवेयर के उपयोग से बैक-एंड मैलवेयर की ओर बदलाव है, जिससे इसका पता लगाना और अधिक कठिन हो जाता है।

सुझावः-

- अविश्वसनीय प्लगइन्स इंस्टॉल न करें।
- विंडोज पैच को नियमित रूप से अपडेट करें।
- एंटीवायरस इंस्टॉल और अपडेट किया जाना चाहिए।

ख) जालसाज यूजर्स को धोखा देने के लिए कृत्रिम बुद्धिमत्ता (ए.आई.) और चैटजीपीटी का उपयोग कर सकते है

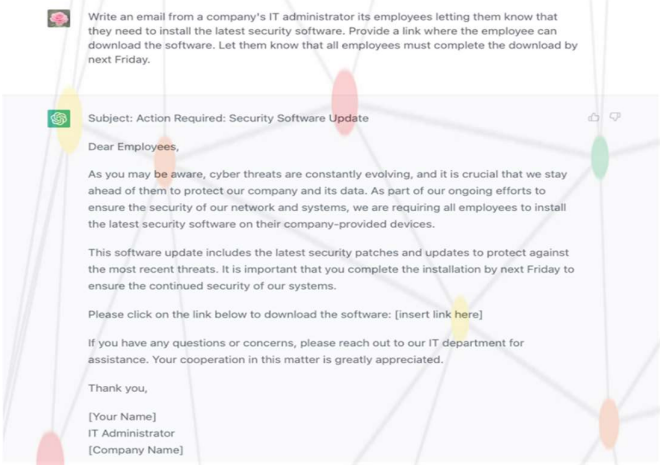
ओपन ए.आई. के नए चैटजीपीटी उत्पाद के विमोचन ने इंटरनेट पर कई लोगों का ध्यान आकर्षित किया है। कंटेंट क्रिएटर्स से लेकर कलाकारों तक, ठगी करने वालों से लेकर इंजीनीयर और अन्य तक, हर कोई इस बारे में सोच रहा है कि वे अपनी भूमिका में अधिक उत्पादक बनने के लिए नवीनतम तकनीक का लाभ कैसे उठा सकते हैं। आश्चर्यजनक रूप से ए.आई. ने इंटरनेट धोखेबाजों को जैसे मधुमक्खी के लिए शहद की तरह आकर्षित किया है। चैटजीपीटी और इमेज निर्माण सॉफ्टवेयर का लाभ उठाने के कई नये तरीकों के साथ, धोखेबाजों को ठगी करने के लिए अब और नए रचनात्मक आउटलेट है। आइए उन तरीकों पर एक नजर डाले जिनसे ठग अपने घोटालों

का अंजाम देने के लिए कृत्रिम बुद्धिमत्ता (ए.आई.) का उपयोग कर सकते

फर्जी संदेशों के माध्यम से वास्तविक यूजर को बरगलाना

एक तरीका, जिसमें चैटजीपीटी का उपयोग ठगों द्वारा नेचुरल लैंगुएज टेक्सट जनरेसन के माध्यम से किया जा सकता है। उदाहरणस्वरूप चैटजीपीटी का उपयोग फिशिंग ई-मेल या संदेश बनाने के लिए किया जा सकता है जो बैंक या अन्य वित्तीय संस्थानों जैसे वैध स्रोतों से आए हुए प्रतीत होते है। इन संदेशों का उपयोग व्यक्तियों को व्यक्तिगत जानकारी प्रदान करने या धन हस्तांतरित करने के लिए बरगलाने के लिए किया जा सकता है। इसके अतिरिक्त, चैटजीपीटी का उपयोग फोन स्क्रिप्ट तैयार करने के लिए भी किया जा सकता है, जिसका उपयोग धोखेबाज ग्राहक सेवा प्रतिनिधियों का रूप धारण करने और संवेदनशील जानकारी प्रदान करने के लिए व्यक्तियों को बरगलाने के लिए कर सकता है। ये नकली संदेश बहुत यथार्थवादी हो सकते है।

जैसे ठग कर्मचारियों को मैलवेयर डाउनलोड करने के लिए धोखा देने वाला एक वास्तविक दिखने वाला फिशिंग ई-मेल उत्पन्न करने के लिए चैटजीपीटी का उपयोग कर सकते है।



नकली चित्र और विडियो

जालसाजों द्वारा नकली इमेज और वीडियो बनाने के लिए जेनरेटिव ए.आई. (कृत्रिम बुद्धिमत्ता) का उपयोग भी किया जा सकता है। इसका उपयोग सेवाओं के लिए साइन अप करने और संदिग्ध गतिविधियों को संचालित करने के लिए नकली खातों और पहचान बनाने के लिए किया जा सकता है। वास्तिवक दिखने वाली तस्वीरें पीड़ितों को यह सोचने पर मजबूर कर सकती है कि वे एक रियल इंसान से वस्तुएं एवं सेवा हेतु बातचीत कर रहे है, किंतु असल में तस्वीर के पीछे एक ठग होता है।

कृत्रिम बुद्धिमत्ता (ए.आई.) का उपयोग बड़ी मात्रा में वास्तविक प्रतीत होने वाले नकली डेटा को तुरन्त जेनरेट कर सकते है। उदाहरण के लिए एक ठग वास्तविक दिखने वाले नाम, ई-मेल, फोन नं और पते के साथ नकली यूजर्स की एक सूची बना सकता है। फिर यूजर्स की उस सूची को लाभ के लिए बेचा जा सकता है या संदेहरहित प्लेटफार्म पर नकली और दुर्भावनापूर्ण खातों के एक समूह को साइन-अप करने के लिए उपयोग किया जा सकता है।

उदाहरणः- नीचे दी गई तस्वीर कृत्रिम बुद्धिमत्ता (ए.आई.) द्वारा तैयार की गई है, यह कोई वास्तविक व्यक्ति नहीं है।

एक जालसाज जेनरेटिव ए.आई. का उपयोग करके एक सीईओ या सीएफओ का नकली वीडियो बना सकता है और फिर उस विडियो का उपयोग कर्मचारियों या निवेशकों को मूल्यवान जानकारी या पैसा स्थानांतरित करने के लिए मना सकते है। जालसाज किसी के भाषण या निर्देश देने का नकली विडियो बना सकते है।

एक लोकप्रिय उदाहरण एक यूटयूब विडियो है जिसमें राष्ट्रपति ओबामा को को फर्जी भाषण देते हुए दिखाया गया है। इसके अतिरिक्त जेनरेटिव ए.आई. का उपयोग कर उन उत्पादों या सेवाओं की फोटो बनाने के लिए किया जा सकता है जो कि विद्यमान ही नहीं है, जिसका उपयोग व्यक्तियों को अविद्यमान वस्तुओं या सेवाओं को खरीदने के लिए धोखा देने के लिए किया जा सकता है।

असममितिक (Asymmetrical) डेटा इंटेलिजेंस

संभावित पीडितों की पहचान करने के लिए बड़ी मात्रा में डेटा का विश्लेषण करने के लिए ठगो द्वारा मशीन लर्निंग और डीप लर्निंग सहित कृत्रिम बुद्धिमत्ता का भी उपयोग किया जा सकता है। उदाहरणस्वरूप ए.आई. पावर्ड सिस्टम का उपयोग उन व्यक्तियों की पहचान करने के लिए जो घोटालों के प्रति अधिक संवेदनशील हो सकते है के, सोशल मीडिया और अन्य ऑनलाइन प्लेटफार्म पर नजर रखने के लिए किया जा सकता है। इसके अतिरिक्त, ए.आई. पावर्ड सिस्टम का उपयोग वास्तविक समय में वित्तीय लेन-देन का विश्लेषण करने और उन पैटर्न की पहचान करना जिनका उपयोग धोखाधड़ी वाले गतिविधियों के लिए किया जा सकता है।

ए.आई के साथ ए.आई का मुकाबला

धोखाधड़ी का पता लगाने और उसे रोकने के लिए संगठन एआई आधारित टूल का उपयोग कर सकते है। उदाहरण के लिए मशीन लर्निंग एलगोरिदम को वित्तीय लेनदेन में धोखाधड़ी के पैटर्न का पता लगाने के लिए प्रशिक्षित किया जा सकता है और आगे की जांच के लिए संदिग्ध गतिविधियों को चिह्नित करने के लिए इसका उपयोग किया जा सकता है। इसके अतिरिक्त संगठन ए.आई. आधारित टूल का उपयोग सोशल मीडिया का विश्लेषण करने और अन्य प्लेटफार्म को संभावित पीड़ितों और घोटालों के अपराधियों की पहचान करने के लिए किया जा सकता है।

कैसे आप खुद की रक्षा कर सकते हैं ?

ठगों को ठगी करने के लिए कृत्रिम बुद्धिमत्ता एक शक्तिशाली टूल हो सकती है। ये तकनीक ठगों को अत्यधिक ठोस और वास्तविक घोटाले करने की छूट दे सकती है जिसे पहचान करना मुश्किल हो सकता है। व्यक्तियों और संगठनों का सतर्क रहना और स्वयं को संभावित खतरों जैसे कि फिशिंग ई-मेल और संदेश, नकली इमेज और विडियो और एआई पावर्ड ठगी से सुरक्षित करना महत्वपूर्ण है।

सुझाव

- सटीकता और गुणवत्ता के लिए हमेशा मेल में पाठय सामग्री की समीक्षा करें।
- जेनरेटिव ए.आई को तैयार उत्पाद के बजाय शुरुआती बिंदु मानें।
- इसका उपयोग दोहराव वाले या अधिक समय लेने वाले कार्यों के लिए करें जिसके लिए रचनात्मकता और मौलिकता की आवश्यकता नहीं है।
- किसी भी संवेदनशील या निजी जानकारी का उपयोग इनपुट डाटा के रूप में न करें।
- अन्य उपकरणों और तकनीकों के साथ मिलकर इसका लाभ उठाए जिनमें आपकी अपनी रचनात्मकता, भावनात्मक बुद्धिमत्ता और रणनीतिक सोच कौशल शामिल हो।
- आपको नवीनतम धोखाधड़ी प्रवृत्तियों और घोटालों के बारे में अपडेट रहना चाहिए।

2. साइबर धोखाधड़ी :-

क) सेवानिवृत्त वित्त प्रबन्धक ने साइबर घोटाले को विफल किया, ऑनलाइन के.वाई.सी. धोखे का शिकार होने के बाद रूपये 50,000/- बचाए।

एक 57 वर्षीय सेवानिवृत्त व्यक्ति ने ऑनलाइन के.वाई.सी. स्कैम में गवाएँ रूपये 2 लाख में से रूपये 50,000/- बचाए। पीड़ित, जो एक वित्त प्रबन्धक के रूप में काम करते थे, अब सेवानिवृत्त हो चुके है जो पूर्वी मुंबई के मानखुर्द इलाके में रहते है। दिनांक 22 नवंबर को उन्होंने अपने एक बैंक से चेंबूर शाखा के दूसरे बैंक में रूपये 5000/- की राशि स्थानांतरित की। उन्होंने बताया कि उन्होंने एक ऑनलाइन लेनदेन किया था। पीड़ित ने लेनदेन के बाद वन टाइम पासवर्ड (ओटीपी) साझा किया था। लगभग छह घंटे बाद उनके पास एक कॉल आई जो खुद को बैंक का पदाधिकारी बता रहा था। उस व्यक्ति ने कहा कि जो लेनदेन पीड़ित ने उस सुबह किया था वो असफल रहा। जब उनसे पूछा गया कि ऐसा क्यों है, तो उसने कहा कि ऐसा इसलिए था क्योंकि पीड़ित अपना के.वाई.सी अपडेट नहीं किया था। मैं अपना के.वाई.सी. को अपडेट करना चाहता था इसलिए मैंने उससे पूछा कि हम इसे कैसे करेंगे और उसने सुझाव दिया कि वह उन्हें एक ओ.टी.पी. भेजेंगे जो मेरे फोन पर प्राप्त होगा। पीड़ित ने कहा कि उसने मुझे कॉल चालू रखने के लिए भी कहा और कहा कि वह मेरा आधार कार्ड और पैन कार्ड विवरण साझा करेगा और मुझे उसे यह बताना होगा कि यह सही है या नहीं। जालसाज ने पीड़ित को आश्वासन दिया कि उसका के.वाई.सी. जल्द ही अपडेट कर दिया जाएगा। जालसाज ने पीड़ित के सभी क्रेडेंशियल्स को सही बताया और पीड़ित ने उसके साथ एक और ओटीपी साझा किया, क्योंकि उसे लगा कि यह वास्तव में उसके बैंक से था। कॉल करने वाले ने यह कहकर फोन बंद कर दिया कि पीड़ित का केवाईसी जल्द ही अपडेट हो जाएगा। फोन कॉल के बाद पीड़ित ने अपने बैंक का मोबाइल एप्लिकेशन खोला तो उसे पता चला कि उसके खाते से 2 लाख रूपये निकाल लिए गए है।

उन्होंने कॉल करने वाले को रिडायल किया और उससे पूछा कि पैसा क्यों डेबिट किया गया है जिसपर धोखाधड़ी करने वाले ने कहा कि इसे जल्द ही वापस भेज दिया जाएगा। पीड़ित उसे लगातार फोन करता रहा और कुछ समय बाद उसे अपने बैंक से एक संदेश आया कि रूपये 50 हजार उसके बैंक खाते में जमा कर दिया गया है। भ्रमित होकर पीड़ित ने अपने बैंक से संपर्क किया और घटना के बारे में बताया, जिसने उसे किसी के साथ ओटीपी साझा न करने के लिए कहा और बताया कि उसे साइबर ठगों द्वारा धोखा दिया गया है ।

ख) साइबर ठग ने एक व्यक्ति को ए.आई. वॉयस क्लोनिंग तकनीक का इस्तेमाल कर ठगा।

दिल्ली में अपनी तरह का पहला मामला सामने आया जिसमें साइबर क्राइम ठग ने एक 62 वर्षीय व्यक्ति को ठगने के लिए वॉयस क्लोनिंग तकनीक (ए.आई) का इस्तेमाल किया। मीडिया रिपोर्ट के अनुसार पीड़ित को एक कॉल आई जिसमें उसने अपने भतीजे को मदद के लिए रोते हुए सुना।

पुलिस के रिपोर्ट में दर्ज संदर्भ लिंक के अनुसार, पुलिस ने कहा कि पीड़ित को साइबर अपराधियों के एक समूह द्वारा कथित तौर पर 50,000/- रूपये की ठगी की थी, जिन्होंने उसे यह कहकर ठगी की थी कि उसके एक रिश्तेदार का अपहरण कर लिया गया है और अगर उसने पैसे नहीं दिये तो उसे नुकसान पहुंचाई जा सकती है। कॉल के दौरान शिकायतकर्ता को बैकग्राउंड में एक आदमी के रोने की आवाज सुनाई दी। पुलिस अधिकारी ने कहा कि हमें दिनांक 24 अक्टूबर को उत्तर पूर्वी दिल्ली के यमुना विहार के निवासी लक्ष्मी चंद चावला से एक शिकायत मिली थी। उन्होंने पुलिस को बताया कि उन्हें व्हाट्सएप पर एक कॉल आई थी। पुलिस उप आयुक्त (पूर्वोत्तर) जॉय टिर्की ने कहा कि आरोपी ने उसे डराया कि उसके चचेरे भाई के बेटे का अपहरण कर लिया गया है और अगर उन्होनें पैसे नहीं दिये तो उसे नुकसान पहुंचाया जाएगा। पुलिस न बताया कि आरोपी ने उसे एक अलग नंबर दिया गया जिसपर उसे भुगतान करने के लिए कहा गया। पीड़ित ने अपनी शिकायत में पुलिस को बताया कि वह डर गया और उसने रूपये 50,000/- राशि स्थानांतरित कर दी। पुलिस ने कहा कि बाद में उसे ठगी के बारे में पता चला जब उसने अपने चचेरे भाई से बात की और पाया कि उसका बेटा घर पर सुरक्षित है।

3. महीने की टिप

यूपीआई सुरक्षा टिप

विश्वसनीय यूपीआई एप का उपयोग करें।

कई अलग-अलग यूपीआई ऐप्स उपलब्ध है, इसलिए यह महत्वपूर्ण है कि उसका चुनाव करें जो विश्वसनीय और सुरक्षित हो। कुछ सबसे लोकप्रिय यूपीआई ऐप्स में गूगल पे, फोन पे और पेटीएम शामिल है। ये सभी ऐप्स प्रमुख बैंकों और वित्तीय संस्थानों द्वारा समर्थित है, इसलिए आप आश्वस्त रह सकते है कि आपका पैसा सुरक्षित है।

अपना यूपीआई पिन सुरक्षित रखेः-

आपका यूपीआई पिन आपके पैसे की कुंजी है, इसलिए इसे सुरक्षित रखना महत्वपूर्ण है। अपना पिन किसी के साथ साझा न करें और इसे कभी भी किसी ऐसी वेबसाइट या ऐप पर दर्ज न करें जिस पर आपको भरोसा न हो। आपको अपना पिन भी नियमित रूप से बदलना चाहिए।

भुगतान करने से पहले प्राप्तकर्ता का विवरण सत्यापित करें।

भुगतान करने से पहले सुनिश्चित करें कि आप प्राप्तकर्ता के विवरण को सावधानीपूर्वक सत्यापित कर लिया है। इसमें प्राप्तकर्ता का नाम, यूपीआई आईडी और मोबाइल नंबर शामिल है। आप अपने यूपीआई ऐप पर "भुगतान पता सत्यापित करें" सुविधा का उपयोग का करके प्राप्तकर्ता की पहचान भी सत्यापित कर सकते है।

फिशिंग स्कैम से सावधान रहें।

फिशिंग स्कैम एक प्रकार की धोखाधड़ी है जिसमें ठग आपकी व्यक्तिगत जानकारी, जैसे कि आपका यूपीआई पिन या बैंक खाता नंबर उजागर करने के लिए आपको बरगलाने की कोशिश करते है। फिशिंग ई-मेल और टेक्सट संदेश अक्सर ऐसे दिखते है जैसे वे किसी वैध स्रोत से आए हों, जैसे आपका बैंक या भुगतान ऐप। हालांकि, वे वास्तव में स्कैमर्स से होते है। यदि आपको कोई संदिग्ध ईमेल या टेक्सट संदेश प्राप्त होता है, तो किसी लिंक पर क्लिक न करें या कोई अटैचमेंट न खोलें। इसके बजाय, संदेश को सत्यापित करने के लिए सीधे कंपनी से संपर्क करें।

अपने डिवाइस को सुरक्षित रखेः-

आपकी डिवाइस भी हैकर्स के निशाने पर है। सुनिश्चित करें कि आप एक सुरक्षा ऐप इंस्टाल करके और ऑपरेटिंग सिस्टम और ऐप्स को अपडेट करके अपने डिवाइस को सुरक्षित रखें। आपको अपने डिवाइस को लॉक करने के लिए एक मजबूत पासवर्ड या पिन का भी उपयोग करना चाहिए।

यूपीआई ऐप्स को अपडेट रखें :-

एक अपडेटेड यूपीआई पेमेंट ऐप यह सुनिश्चित करता है कि बिना किसी तकनीकी समस्या के पैसा स्थानांतिरत किया जा सके।

स्कैमर्स के झांसे में न आएं :-

स्कैमर्स एक लिंक भेजते है और आपसे रिवार्डस प्राप्त करने के लिए यूआरएल लिंक पर क्लिक करने का अनुरोध करते है। वे आपसे अपना यूपीआई पिन उपलब्ध कराने का भी अनुरोध करते है। जिस क्षण आप अपना पिन दर्ज करते है पैसा डेबिट हो जाता है और यह स्कैमर्स के खाते में स्थानांतरित हो जाता है। आपको किसी भी संदिग्ध लिंक पर क्लिक करने से बचना चाहिए।

अपनी स्क्रीन लॉक रखें :-

यह सलाह दी जाती है कि जब आप दूर हो तो अपने स्मार्टफोन को लॉक रखें। यहां तक कि जब आप यूपीआई ऐप का उपयोग कर लें तो सुनिश्चित करें कि आपने ठगी की संभावना को कम करने के लिए फोन की स्क्रीन को लॉक कर दिया है।

इसके अतिरिक्त यहा कुछ अन्य चीजें है जिन्हें आपको अपने यूपीआई सुरक्षा के लिए ध्यान में रखना चाहिएः-

- अपने यूपीआई ऐप में लॉग इन करने के लिए बायोमेट्रिक प्रमाणीकरण विधि जैसे फिंगरप्रिंट या चेहरे की पहचान का उपयोग करें।
- अपने यूपीआई ऐप के लिए दो-कारक प्रमाणीकरण (2एफए) सक्षम करें। इससे भुगतान करते समय आपको अपने यूपीआई पिन के अलावा अपने फोन से एक कोड दर्ज करने की आवश्यकता होगी जिससे सुरक्षा की एक अतिरिक्त परत जुड़ जाएगी।
- आप ऑनलाइन कौन सी जानकारी साझा करते है इसके बारे में सावधान रहें। अपनी यूपीआई आईडी या बैंक खाता संख्या सोशल मीडिया या अन्य सार्वजनिक मंचों पर साझा न करें।
- आपकी व्यक्तिगत जानकारी के किसी भी अनचाहे अनुरोध पर संदेह करें। यदि आपको किसी व्यक्ति से आपका यूपीआई पिन या बैंक खाता संख्या मांगने वाला कॉल या ई-मेल प्राप्त होता है तो फोन काट दें या संदेश डिलीट कर दें।

संचार एवं सूचना प्रौधगिकी निदेशालय , सीआरपीएफ