20 नईदुनिया
इंदौर, गुरुवार 10 मार्च 2016

बचें 'फिशिंग-विशिंग' में फंसाने वाले अपराधियों के जाल से

वरुण कपूर
आईपीएस

त्योहार और तोहफों का मौका आते ही ई-शॉपिंग यूजर्स के मेल-बॉक्स में ई-कॉमर्स पोर्टल्स के ऑफर्स की भरमार हो जाती है। दिवाली, क्रिसमस, न्यू ईयर या वेलेंटाइन-डे जैसे मौकों पर साइबर क्रिमिनल्स भी आम लोगों को अपने जाल में फंसाने के लिए सक्रिय हो जाते हैं। ऐसे समय अविश्वसनीय ऑफर्स के लालच में फंसने की काफी संभावना बढ़ जाती है। बड़े मौकों के अलावा अब रविवार हो या सोमवार, किसी न किसी बहाने कहीं न कहीं से डिस्काउंट, सेल, इनाम या ऑफर के मैसेज, ई-मेल आते रहते हैं।

दरअसल, दुनियाभर में साइबर अपराध लगातार बढ़ रहे हैं। इसी के साथ नए तथा चुनौतीपूर्ण अपराध व इनके नाम भी सामने आ रहे हैं। वर्चुअल दुनिया में सुरक्षित रहना पहले ही चुनौती बनी हुई थी ही कि आज नागरिकों को इस अपराध जगत की तेजी से बढ़ती शब्दावलियों तथा उनकी व्याख्याओं से भी जूझना पड़ा रहा है। सबसे पहले तो साइबर-कंप्यूटर से संबंधित इस शब्दजाल को समझना होगा और फिर स्वयं को इसके कुप्रभावों से दूर रखने के उपाय करने होंगे।

कई बार ऐसा करना लगभग असंभव होता है, क्योंकि जब तक बेचारा यूजर यह समझ पाए कि उक्त नाम किस तरह के अपराध से जुड़ा है, वह उसका शिकार हो चुका होता है। दूसरी बड़ी चुनौती यह है कि हर रोज साइबर अपराध की दुनिया में 'नए' प्रकार के शब्द आ जाते हैं। ऐसे में कोई कैसे और कितनी तरह के शब्दों को समझे तथा बचने का उपाय करे?

साइबर अपराध के चुनौतीभरे नामों में ताजा एंट्री 'फिशिंग' और 'विशिंग' की है। इस प्रकार का अपराध हर दिन तेजी से बढ़ रहा है। यही वजह है कि इसकी व्याख्या जल्द से जल्द करनी होगी। इसे आसान शब्दों में ऐसे समझा जा सकता है- 'फिशिंग' वह तरीका है जिसमें एसएमएस या ईमेल के जरिए लोगों को लुभा कर उनसे निजी जानकारियां तथा सूचनाएं हासिल की जाती हैं। बाद में इन सूचनाओं का गलत इस्तेमाल करते हुए साइबर क्राइम को अंजाम दिया जाता है।

दूसरी ओर 'विशिंग' ऐसी तकनीक है, जिसमें साइबर अपराधी वॉइस कॉल के जरिए इसी तरह सूचनाएं हासिल कर लोगों को अपना शिकार बनाते हैं। विशिंग में अपराधी वर्चुअल रूप में पीड़ित के सामने होता है, लेकिन फिशिंग में ऐसा नहीं होता है।

देखा जाए तो 'फिशिंग' और 'विशिंग' दोनों लगभग एक ही प्रकार के तरीके हैं। दोनों में ही पीड़ितको किसी न किसी प्रकार का लालच देकर उसे शिकार बनाया जाता है। ऐसे तरीके अपनाने वाले अपराधी सैकड़ों बार प्रयास करते हैं और आखिरकार एक-दो पीड़ितों को फंसाने में कामयाब हो ही जाते हैं। इन सूचनाओं को आपराधिक मकसद के लिए उपयोग किया जाता है। यह शब्दावली 'फिशिंग-विशिंग' मछली पकड़ने वाले उस शख्स से प्रेरित है जो पानी में तब तक हुक डाल कर बैठा रहता है, जब तक कि उसमें मछली न फंस जाए। यदि आप इस तेजी से बदलते और बढ़ते हुए तकनीकी माहौल में सुरक्षित रहना चाहते हैं तो आज से ही सतर्क हो जाइए।

साइबर अपराधी आम लोगों के डर और लालच को निशाना बनाते हुए 'फिशिंग-विशिंग' जैसे कारनामों को अंजाम देते हैं। इंटरनेट की दुनिया में कदम रखते समय इन दोनों कमजोरियों पर नियंत्रण रखें। ध्यान रहे, कोई चीज कभी मुफ्त में नहीं मिलती। किसी भी बैंक, एटीम सेवा देने वाली कंपनी, क्रेडिट कार्ड/डेबिट कार्ड एजेंसी या वेबसाइट को आपके बैंक अकाउंट की जानकारियां जैसे- अकाउंट नंबर, पासवर्ड, पिन नंबर, सीवीसी नंबर आदि का आपसे पूछने का कानूनी अधिकार नहीं दिया गया है। कोई भी, कभी भी, किसी रूप में भी ये जानकारियां आपके सामने आकर मांगे तो आप बिल्कुल न दें।

(लेखक अतिरिक्त पुलिस महानिदेशक पद पर इंदौर में पदस्थ हैं और विचार उनके व्यक्तिगत हैं)

ईमेल: varunkapoor170@gmail.com

सुरक्षा के सूत्र

1. किसी भी अनहोनी से बचने के लिए कोई भी अनजान शख्स के साथ अपनी निजी सूचनाएं नहीं बांटनी चाहिए।
2. इंटरनेट पर किसी से बात करते समय या इंटरेक्ट करते समय जागरूक रहने की आवश्यकता है। इससे यह पता चलेगा कि वे किससे बात कर रहे हैं और सामने वाले का मकसद क्या है।
3. साइबर स्पेस में कभी भी अपनी निजी तथा गोपनीय सूचनाएं किसी के साथ शेयर नहीं करनी चाहिए।
4. यदि आपको किसी कॉल/एसएमएस/ईमेल पर शंका हो तो तुरंत प्रतिक्रिया दीजिए।
5. जोखिम की आशंका नजर आते ही संबंधित लोगों से सवाल पूछें।