नईदुनिया
इंदौर, गुरुवार 09 जून 2016

सोशल इंजीनियरिंग अटैक यानी विश्वासघात

वर्चुअल वर्ल्ड में ऐसे मामले तेजी से बढ़ रहे हैं, जहां पहले तो अपराधी विश्वास जीतते हैं और फिर धोखाधड़ी करने के लिए विश्वासघात कर जाते हैं। एक तरह से इंटरनेट की यह दुनिया 'सोशल इंजीनियरिंग अटैक की दुनिया' बन गई है। किसी को भी शिकार बनाने के लिए यहां सबसे पहले उसके बारे में जानकारी जुटाई जाती है।

वरुण कपूर
आईपीएस

एक उदाहरण से इसे स्थिति को समझते हैं। गुजरात में एक कॉलेज छात्रा का सहपाठी उससे मोबाइल नंबर मांगता है। वह इनकार कर देती है, लेकिन सहपाठी जवाब देता है कि वह किसी तरह हासिल कर ही लेगा। अगले दिन छात्र ने उस लड़की का नाम, उसके पिता का नाम, पता और फोन नंबर जैसा सबकुछ हासिल कर लिया। आखिर उसने कहां से यह जानकारी हासिल की? बहुत आसान है। उसने छात्रा की स्कूटी का नंबर गुजरात आरटीओ वेबसाइट पर डाला और सबकुछ बड़ी आसानी से हासिल कर लिया।

भारत सरकार के इनकम टैक्स डिपार्टमेंट की साइट 'ई–फिलिंग' भी ऐसा ही एक जरिया है। सायबर क्रिमिनल इस साइट पर जाकर किसी भी व्यक्ति का सरनेम और उसकी जन्म तारीख दर्ज करते हैं, इससे उस शख्स का पेन (स्थायी खाता संख्या) हासिल हो जाता है। इस पेन और उस पर छपे फोटो का इस्तेमाल कर वह फोटोशॉप की मदद से नया पेन कार्ड बनाता है। वह इस कार्ड का प्रिंट आउट निकालता है, लेमिनेशन कर सिम कार्ड खरीदने निकल पड़ता है। उसे बड़ी आसानी से पीड़ित शख्स के नाम से प्री–पेड सिम कार्ड मिल जाता है। इस कार्ड को आधार बनाते हुए वह अपराध को अंजाम देना शुरू कर देता है। इस तरह से कोई शख्स केवल इसलिए शिकार हो सकता है कि उसकी जानकारी सायबर स्पेस पर उपलब्ध है।

ऐसा ही एक मामला इंदौर की निजी कंपनी के वरिष्ठ अधिकारी का है। वे 'जल बचाओ' के विशेषज्ञ हैं और इसी संबंध में दुनियाभर में आते–जाते रहते हैं। सायबर अपराधियों ने सोशल इंजीनियरिंग तकनीक के जरिए उनसे जुड़ी बातें पता कर लीं और इस जानकारी का उपयोग उन पर सायबर अटैक करने के हथियार के रूप में इस्तेमाल किया। अपराधियों ने उन्हें एक ईमेल किया और इंटरनेशनल सेमिनार में हिस्सा लेने के लिए यूके आमंत्रित किया। वे जाल में फंस गए और इसके बाद सोची–समझी साजिश के तहत अपराधियों ने उनसे साढ़े पांच लाख रुपए बैंक ऑफ इंग्लैंड स्थित खाते में ट्रांसफर करवा लिए। भारी मशक्कत के बाद उक्त अधिकारी अपराधियों का पता लगाने में कामयाब रहे और उन्हें आश्चर्य हुआ कि घाना में बैठे सायबर अपराधियों ने इसे अंजाम दिया था। यानी पैसा यूके में जमा हुआ, लेकिन अपराधी घाना में बैठे थे। कोई आखिर किस तरह अपराध की तह तक पहुंचे? इस तरह सायबर अपराधियों ने एक परफेक्ट क्राइम को अंजाम दिया।

वर्तमान दौर में ऐसे मामले तेजी से बढ़ रहे हैं। अपराधी सायबर स्पेस में उपलब्ध छोटी–छोटी जानकारियों को दुरुपयोग करते हैं।

हो सकता है यह जानकारी हम ही ने वहां डाली हो या किसी थर्ड पार्टी ने। धोखाबाज बड़े सलीके से जानकारी हासिल करते हैं और होशियारी से उसका उपयोग करते हैं।

इन बातों का रखें ध्यान

- सोशल इंजीनियरिंग अटैक यानी भरोसे में लेकर भरोसा तोड़ना
- इंटरनेट पर उपलब्ध जानकारी हासिल कर अपराधी उसका दुरुपयोग करते हैं
- बचने का सबसे सही तरीका– अपनी कम से कम जानकारी ऑनलाइन साझा करें
- वर्चुअल वर्ल्ड में अनजान लोगों पर भरोसा न करें

अज्ञात ई–मेल, कॉल्स पर भरोसा न करें

अब सबसे बड़ा सवाल यह है कि इससे कैसे बचा जाए? सबसे पहले तो हमारी कोशिश यह होना चाहिए कि हम अपनी कम से कम जानकारी ऑनलाइन जारी करें। अपनी जानकारी से यहां तात्पर्य है – पता, फोन नंबर, ईमेल आईडी, वित्तीय जानकारी, पासवर्ड, शेड्यूल, पेन कार्ड नंबर्स, फोटो आदि। दूसरा– हमें यह आदत बनाना चाहिए कि अज्ञात लोगों से मिले ई–मेल, एसएमएस और फोन कॉल्स पर भरोसा नहीं करेंगे। ऐसे संवाद और उनके जरिए दिए जा रहे ऑफर्स को हमें शक की निगाह से देखना चाहिए। हो सकता है कि कोई शातिर अपराधी हमारी होशियारी की हवा निकालने की कोशिश कर रहा हो। एक बार हम उसके जाल में फंस जाएंगे तो अपराध होने के बाद ही हमें सचाई का अहसास हो पाएगा, लेकिन तब तक बहुत देर हो चुकी होगी।

(लेखक अतिरिक्त पुलिस महानिदेशक पद पर इंदौर में पदस्थ हैं और विचार उनके व्यक्तिगत हैं)
ईमेल: varunkapoor170@gmail.com