लोकमत समाचार
epaper.lokmat.com/lokmatsamachar
नागपुर, रविवार, 18 सितंबर 2016

सतर्क रहकर बचें ठगी से

साइबर-कवच

वरुण कपूर
अतिरिक्त पुलिस महानिदेशक
एवं साइबर सिक्योरिटी विशेषज्ञ
varunkapoor170@gmail.com

वित्तीय धोखाधड़ी से संबंधित साइबर अपराध जिस तेजी से बढ़ रहे हैं वे न केवल देश के सुरक्षा प्रतिष्ठानों के लिए खतरे की घंटी हैं, बल्कि नागरिकों के लिए भी. इससे प्रभावी ढंग से निपटा जा सकता है. और नागरिकों की बेहतर तरीके से सुरक्षा की जा सकती है. यह कैसे किया जा सकता है - इसका उत्तर है नागरिकों में जागरूकता और जाल में फंसाने वाले ऐसे सभी संपर्कों के प्रति 'स्मार्ट' प्रतिक्रिया के जरिए.

बुनियादी रूप से ये हमले 'विशिंग' कॉल के ही रूप हैं. फोन करने वाला आपको खतरनाक स्थिति में डालकर झटका देना चाहता है, जैसे - 'आपका एटीएम कार्ड ब्लॉक कर दिया गया है' या कुछ इसी तरह की अन्य बातें कह कर वह रिसीवर के सामने आपातकालीन स्थिति पेश करना चाहता है. या 'आपकी बीमा पॉलिसी पर लाभांश घोषित किया गया है' जैसी बातें कहकर फोन करने वाला अपने शिकार को ललचाता है.

दोनों ही मामलों - डर और प्रलोभन- में पीड़ित तार्किक ढंग से सोच नहीं पाता और अपराधी यही चाहता भी है. तार्किक सोच नहीं होने पर तर्कसंगत कार्रवाई भी नहीं हो पाती और साइबर अपराधी के लिए अपनी चिकनी-चुपड़ी बातों के जरिए मनचाही जानकारी हासिल करना आसान हो जाता है. इसी जानकारी का इस्तेमाल ऑनलाइन वित्तीय लेन-देन के माध्यम से पीड़ित को आर्थिक नुकसान पहुंचाने के लिए किया जाता है.

दोनों ही मामलों - डर और प्रलोभन- में पीड़ित तार्किक ढंग से सोच नहीं पाता और अपराधी यही चाहता भी है. तार्किक सोच नहीं होने पर तर्कसंगत कार्रवाई भी नहीं हो पाती और साइबर अपराधी के लिए अपनी चिकनी-चुपड़ी बातों के जरिए मनचाही जानकारी हासिल करना आसान हो जाता है.

जैसा कि ऊपर कहा जा चुका है, साइबर अपराध या किसी भी अन्य अपराध से लड़ने के लिए कॉमन सेंस और एक स्मार्ट दृष्टिकोण जरूरी है. निरंतर खतरे और प्रलोभन के ऐसे परिदृश्य में आम आदमी जो काम सबसे बेहतर कर सकता है वह यही है कि वित्तीय धोखाधड़ी करने वाले साइबर अपराधियों के बहकावे में वह न आए.

सबसे बेहतर यही है कि निश्चित पहचान वाले वित्तीय क्षेत्रों, जैसे एटीएम, ऑनलाइन बैंकिंग, ऑनलाइन शॉपिंग, बीमा, म्यूचुअल फंड, अन्य निवेश आधारित वित्तीय गतिविधियां, ई-पेमेंट पोर्टल आदि के नाम पर यदि किसी उपभोक्ता के पास ऐसा कोई फोन (या मैसेज अथवा ईमेल) आता है तो उसका जवाब इस तरह देना चाहिए - "मैं कोई प्रीमियम नहीं चाहता और न ही मुझे आपको कोई जानकारी देने की जरूरत है, यदि आप सच्चे हैं और आपके पास कहने के लिए कोई ठोस बात या प्रस्ताव है तो अपने प्रतिनिधि को मुझसे मिलने भेजिए. तभी और सिर्फ तभी मैं इस मुद्दे पर आगे बात करूंगा." हो सकता है इसके बाद फोन डिस्कनेक्ट हो जाए. इस तरीके को अपनाने से आप अत्यंत दुर्लभ मामले में ही किसी सुविधा या लाभ से वंचित हो सकते हैं, लेकिन साइबर अपराधियों द्वारा ऑनलाइन दी जाने वाली बहुत सी पीड़ाओं और तकलीफों से आप बचे रह सकेंगे.

इसलिए आदर्श वाक्य यह होना चाहिए- 'सतर्क रहें, स्मार्ट प्रतिक्रिया दें और सुरक्षित रहें.'