लोकमत समाचार
नागपुर, रविवार, 4 सितंबर 2016

वर्चुअल दुनिया में फिशिंग और विशिंग की चुनौती

साइबर कवच

वरुण कपूर
अतिरिक्त पुलिस महानिदेशक एवं साइबर सिक्योरिटी विशेषज्ञ

दुनिया में साइबर अपराधों के तेजी से बढ़ने के साथ ही नए और चुनौतीपूर्ण अपराध तथा इनके नए नाम सामने आ रहे हैं. वर्चुअल दुनिया में सुरक्षित रहने की चुनौती ही मानो पर्याप्त नहीं थी कि अब लोगों को जटिल शब्दावली तथा उसे समझने की समस्या से भी जूझना पड़ रहा है. सबसे पहले उन्हें साइबर कम्प्यूटर से संबंधित अपरिचित शब्दावली के वास्तविक मायनों को समझना होगा और फिर उसके दुष्प्रभावों से खुद को दूर रखने के लिए उपाय खोजने होंगे. कई बार यह काम असंभव सा लगता है और जब तक नागरिक यह समझ सकें कि नामविशेष के साथ किस तरह का अपराध जुड़ा है, वे उसका शिकार हो चुके होते हैं. दूसरी बड़ी चुनौती यह है कि हर रोज नए साइबर अपराध नए तरह के बेतुके नामों के साथ सामने आ रहे हैं. तर्कों को खारिज करने वाले इन नामों को कोई कितना याद रखे और अपना बचाव करे!

साइबर अपराधों के इन चुनौतीपूर्ण नामों में ताजा नाम है 'फिशिंग बनाम विशिंग' का. इस तरह के अपराध अनियंत्रित गति से रोज बढ़ रहे हैं, इसलिए इसे तत्काल समझना जरूरी हो गया है. फिशिंग ऐसा तरीका है जिसमें टेक्स्ट (एसएमएस या ईमेल) के माध्यम से असावधान नागरिकों को जाल में फंसा कर उनसे व्यक्तिगत जानकारियां हासिल करने की कोशिश की जाती है, बाद में जिनका इस्तेमाल करते हुए उस व्यक्ति के खिलाफ साइबर अपराध को अंजाम दिया जाता है. दूसरी ओर विशिंग ऐसा तरीका है जिसमें साइबर अपराधी वॉयस कॉल के जरिए लोगों से व्यक्तिगत सूचनाएं हासिल कर उन्हें अपना शिकार बनाते हैं. विशिंग में अपराधी वर्चुअली रूप में पीड़ित व्यक्ति के सामने होता है जबकि फिशिंग में ऐसा नहीं होता. लेकिन बुनियादी रूप में दोनों का लक्ष्य एक तरह से शिकार को लुभाना (जैसे मछली पकड़ने वाला चारा फंसाकर हुक डालता है) होता है और फिर वह उसके फंसने का इंतजार करता है.

ऐसे अपराधी सैकड़ों बार प्रलोभन देने का प्रयास करते हैं और आखिरकार एक-दो लोगों को फंसाने में कामयाब होते ही उनका मकसद पूरा हो जाता है. उनसे हासिल जानकारी को वे सुरक्षित रख लेते है और फिर आपराधिक उद्देश्य के लिए उसका इस्तेमाल करते हैं. यह मछली पकड़ने के समान ही होता है. उन्हें चारा डाल कर घंटों इंतजार किया जाता है और फिर फंसते ही खींच लिया जाता है. इसी के साथ मछली पकड़नेवाले का काम पूरा हो जाता है.

बुनियादी तथ्य यह है कि नागरिकों को साइबर स्पेस में अपने आपको सुरक्षित रखने के लिए जरूरी है कि वे किसी को भी बिना सोचे-समझे अपनी व्यक्तिगत जानकारियां न दें. इसके लिए उन्हें इंटरनेट पर किसी से बात करते समय इस इस बारे में सदैव सतर्क रहना होगा कि वे किसके साथ बात कर रहे हैं और उसका उद्देश्य क्या है. साइबर स्पेस में किसी भी अनजान व्यक्ति के साथ अपनी पर्सनल इन्फार्मेशन को कभी भी शेयर न करें. तकनीक से संचालित इस विकसित होती चुनौतीपूर्ण दुनिया में यदि सुरक्षित रहना है तो सतर्क रहना सीखना होगा. ■■