नईदुनिया
इंदौर, गुरुवार 08 सितंबर 2016

नुकसान से बेहतर है सुरक्षा

रियल वर्ल्ड में हमारी पहचान हमारा नाम और उसके साथ लगा पिता या पति का नाम होता है। जबकी वर्चुअल दुनिया में हमारी पहचान यूजरनेम और पासवर्ड से होती है जहां यूजरनेम यानी हमारा नाम और पासवर्ड के मायने हमारे पिता का नाम हो सकता है जिसके साथ कोई भी छेड़छाड़ करे तो हमें बर्दाश्त नहीं होता उसी तरह हमें वर्चुअल वर्ल्ड में अपने पासवर्ड को सुरक्षित रखने की कोशिशें करना चाहिए।

वरुण कपूर
आईपीएस

सामान्यत: लोग अपने पासवर्ड को लेकर सजग नहीं होते हैं और कुछ तो इसके भूल जाने के भय से इतने सरल कॉम्बिनेशन के पासवर्ड रखते हैं कि उसका अंदाजा लगाना मुश्किल नहीं होता। 123456 अमूमन सबसे ज्यादा उपयोग में लाए जाने वाला पासवर्ड हैं। यह बात 2013,2014 और 2015 में इंटरनेट इस्तेमाल करने वालों के बीच किए गए सर्वे के दौरान सामने आई जो हमें आगाह करने के लिए काफी है। ऐसे में सवाल उठता है कि पासवर्ड कैसा हो जिसे कोई भेद ना पाए।

1) अपने पासवर्ड को कॉम्प्लेक्स बनाए-

आप 123456 जैसा सरल पासवर्ड ना रखें और ना ही ऐसा कोई कॉम्बिनेशन जिसके बारे में कोई अंदाजा लगा सके। **ब्रूट फोर्स अटैक** एक ऐसा सॉफ्टवेयर है जिसके जरिए आसान और छोटे पासवर्ड का पता लगाया जा सकता है। ऐसे में जरुरी है कि पासवर्ड कम से कम 8 कैरेक्टर का हो। साथ

ही कोई डिक्शनरी शब्द का उपयोग पासवर्ड में ना हो क्योंकि एक दूसरे सॉफ्टवेयर **डिक्शनरी अटैक** से पासवर्ड का पता लगाया जा सकता है। इसके अलावा अपनी जन्म तारीख, पैन नम्बर, घर, फोन या गाड़ी के नम्बर का इस्तेमाल भी पासवर्ड में ना करें क्योंकी इसे **सेशल इंजीनियरिंग अटैक** सॉफ्टवेयर से तोड़ा जा सकता है। तो ऊपर बताए सुझावों के आधार पर ही पासवर्ड बनाए और इसे 3 से 6 महिने में बदलते रहें।

2) हर अहम अकाउंट के लिए अलग पासवर्ड हो

जिस तरह हम अपने घर को सुरक्षित रखने के लिए 3-4 ताले लगाते हैं और सभी की चाबियां अलग होती है उसी तरह सभी अकाउंट के पासवर्ड भिन्न होना चाहिए ताकी किसी एक पासवर्ड के क्रेक होने पर दूसरों का पता लगाना आसान ना हो।

3)- किसी भी साइट के अपना पासवर्ड स्टोर ना करने दें

सामान्यत: हम जब भी कोइ साइट लॉगइन करते हैं तो **रिमेम्बर मी, स्टे साइन इन** या **ऑटोमेटिक साइन इन** ऑप्शंस सामने आते हैं जिन्हें आपको सिलेक्ट नहीं करना है। कई बार हम इसे अपनी सहुलियत के लिए चुन लेते हैं जो खतरनाक हो सकता है। इसे हम एक उदाहरण से समझ सकते हैं जो पूना का है। पीड़ित ने अपना मोबाइल ऑफिस की टेबल पर छोड़ कर कैफेटेरिया में कॉफी पीने चला गया, इतने में उसका एक साथी वहां आया और उसकी गैरमौजूदगी में फोन को उठाकर ई-मेल आइकन पर क्लीक किया जिसमें **कीप साइन इन** इनेबल्ड था और पीड़ित का साथी उसके मेल अकाउंट में चला गया जहां से उसने कम्पनी के बॉस को धमकीभरे गंदे मेल कर दिए। बात आगे बढ़ गई और फोन के मालिक पीड़ित को नौकरी से बेदखल कर दिया गया। यह मामला हमें सीख देता है कि पासवर्ड टाइप करने में चंद सेकंड का आलस हमारा बड़ा नुकसान कर सकता है।

यह अपने पासवर्ड को सुरक्षित रखने के 6 में से 3 सावधानियां हैं शेष 3 अगले सप्ताह के कॉलम में सुझाए जाएंगे।

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