Date: 15.07.2022	**Publication:** Navbharath Times

Cyber Crime: जामताड़ा के ठगों से बचना है तो जल्दी से कर लें यह काम, वरना हाथ मलते रह जाएंगे

Curated by **शिशिर चौरसिया** | नवभारतटाइम्स.कॉमUpdated: 15 Jul 2022, 10:33 am

देश में कोविड महामारी (Covid-19 Pandemic) की शुरुआत से पहले ही साइबर क्राइम (Cyber Crime) के केसेस बढ़ रहे थे। लेकिन महामारी के बाद जब से डिजिटल लेन-देन बढ़ा, तब से मानों इसमें बाढ़ आ गई है। साइबर धोखाधड़ी (Cyber Fraud) के सबसे कॉमन केसेज में पैसे और/या पहचान की चोरी, ईमेल स्पूफिंग, साइबरस्टॉकिंग, वायरस अटैक, सेवा से इनकार (डिनायल ऑफ़ सर्विस) और अनधिकृत ऑनलाइन लेनदेन जैसे कृत्य शामिल हैं।

Cyber Crime: जामताड़ा के ठगों से बचना है तो जल्दी से कर लें यह काम, वरना हाथ मलते रह जाएंगे

- प्राइम डे - सबसे अधिक बिकने वाले एलेक्सा उपकरणों पर वर्ष की सबसे कम कीमतें |

राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (NCRB) के अनुसार, भारत में साइबर अपराधों (Cyber Crime in India) में 2016 से 2020 के बीच 306% की भारी वृद्धि हुई है और महामारी के वर्ष में प्रतिदिन औसतन 136 साइबर अपराध के मामले सामने आए हैं। इससे भी ज्यादा चौकाने वाली बात है कि प्रत्येक वर्ष दर्ज किए गए लगभग 66% मामले साइबर अपराधों की जांच इसलिए नहीं हो पाई कि इसके मामले अचानक बढ़ गये थे। ऐसे में साइबर अपराधों से खुद को बचाने की जिम्मेदारी खुद आम लोगों पर आ पड़ी है।

बजाज आलियांज जनरल इंश्योरेंस के चीफ टेक्निकल ऑफिसर, टी.ए. रामलिंगम हमें बता रहे हैं कुछ एहतियाती कदम, जिनकी मदद से साइबर अपराध की गतिविधियों का शिकार होने से बचा या उसकी संभावना को कम किया जा सकता है।

एंटी-वायरस सॉफ़्टवेयर से अपडेट रखें

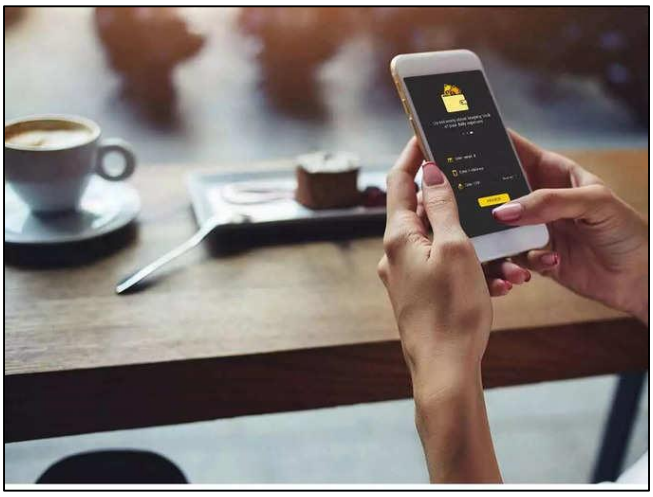
यह शायद साइबर अपराध की गतिविधियों का शिकार होने से बचने की सबसे अच्छी तरकीब है कि आप उन सभी कंप्यूटिंग उपकरणों को नवीनतम एंटी-वायरस और एंटी-मैलवेयर सॉफ़्टवेयर से लैस रखें जो इंटरनेट से जुड़े हैं। हालांकि अधिकांश डिवाइस मुफ्त सॉफ्टवेयर के साथ आते हैं, पर वे अक्सर सीमित अवधि के ही कारगर साबित होते हैं। उनकी वैधता समाप्त होने से पहले उन्हें अपडेट किया जाना चाहिए। बाजार में न जाने कितने विकल्प उपलब्ध हैं, पर ये सुनिश्चित करें कि आपके द्वारा चुने गए सॉफ़्टवेयर सालूशन उनके द्वारा प्रदान की जाने वाली सुरक्षा के लिए विश्वसनीय (trusted) हैं और आपके एप्लिकेशन (कमर्शियल या पर्सनल उपयोग) के लिए फिट हैं। अंत में यह देखते हुए कि साइबर अपराधी डिवाइस के ऑपरेटिंग सिस्टम में किसी भी तरह से उसमें एक्सेस बना लेते हैं, आपको थोड़ा अतिरिक्त सतर्कता बरतनी चाहिए और इसके लिए हर सप्ताह कम से कम एक बार सभी डिवाइस को स्कैन और अपडेट कर लेना चाहिए।

मजबूत पासवर्ड बनायें

यह भी अत्यंत महत्वपूर्ण है कि कई वेबसाइटों के लिए क्रेडेंशियल्स को रिफ्रेश करते समय सभी डिवाइस में पासवर्ड न दोहराएं। सबसे अच्छी सलाह यह दी जाती है कि साइबर अपराधियों को आपके खातों या कंप्यूटिंग उपकरणों तक पहुंच से रोकने के लिए आप नियमित रूप से अपने पासवर्ड बदलें और मुश्किल से अनुमान लगाने वाले पासवर्ड का ही उपयोग करें। इसलिए पासवर्ड चुनते समय हमेशा अक्षरों (letters), संख्याओं (numericals) और प्रतीकों (symbols) के संयोजन का उपयोग करने का सुझाव दिया जाता है। इसमें सभी रिकॉर्ड एक्सेल वर्कशीट या डिवाइस के नोटपैड के बजाय ऑफ़लाइन बनाए जाते हैं। इसके अतिरिक्त, यह भी सुनिश्चित करें कि मोबाइल उपकरणों को

एडवांस लॉगिन फीचर्स से सुरक्षित किया गया है जैसे कि जहां भी संभव हो चेहरा पहचान (face recognition) का उपयोग करें। इसके अलावा अपरिचितों या छोटे बच्चों को यथासंभव एक्सेस से रोकें।

साइबर अपराधियों के तौर-तरीकों को समझें



अधिकतर साइबर अपराधी या हैकर्स आमतौर पर सार्वजनिक वाई-फाई सिस्टम से जुड़े उपकरणों या असुरक्षित/अज्ञात वेबसाइटों पर विजिट करने वाले व्यक्तियों को टारगेट करते हैं। इसलिए यह सलाह दी जाती है कि आप हमेशा वेबसाइट पर जाने से पहले उसकी सिक्योरिटी को वेरीफाई करें, खासकर जब ईमेल या एसएमएस लिंक के माध्यम से उन पर रीडायरेक्ट किया जा रहा हो। मोबाइल डिवाइस के मामले में, कुछ लक्षण जैसे कि अनजान एप्लिकेशन आटोमेटिक रूप से डाउनलोड होना, बैटरी अधिक डिस्चार्ज होना या डाटा ज्यादा यूज होना आदि इस बात के संकेत हैं कि डिवाइस से छेड़छाड़ की गई है। ऐसे मामलों में, ऐसे उपकरणों से तुरंत लॉग ऑफ करने और मोबाइल सिक्योरिटी एक्सपर्ट के माध्यम से इसकी जांच कराने की सलाह दी जाती है।