InfoSec
महिलाओं
के लिए

राष्ट्रीय साइबर सुरक्षा जागरूकता माह

अक्टूबर, 2020

वाईफाई सुरक्षा

वाईफाई लोगों के दैनिक जीवन का अभिन्न हिस्सा बन चुक है। इंटरनेट उपयोक्ता, खास कर महिलाएं अपने घरों और व्यवसायों में, खरीदारी के लिए, बैंक, जीवन को व्यवस्थित करने और जुड़े रहने के लिए इंटरनेट तक पहुंचने के लिए वाईफाई यंत्रों पर निर्भर रहते हैं। व्यक्तिगत जानकारी को सुरक्षित रखने के लिए वाईफाई कनेक्शन को सुरक्षित रखना एक महत्वपूर्ण तत्व है। कुछ बेतार यंत्र अपने मूल बनावट में जोखिम भरे होते हैं। चूंकि इन यंत्रों में सुरक्षा का स्तर तय करन के बारे में अंतिम उपयोक्ता, खास कर महिलाएं पूरी तरह जानकार नहीं होते, वे साइबर खतरों के लिए आसान शिकार हो सकते हैं। साइबर अपराधी अपने गैरकानूनी उद्देश्यों को पूरा करने के लिए इन असुरक्षित वाईफाई यंत्रों की तलाश करते रहते हैं।

कंप्यूटर, लैपटाप या मोबाइल को कोई भी वाईफाई कनेक्टिविटी के माध्यम से असुरक्षित एक्सेस प्वाइंट (वायरलेस राउटर) से जोड़ सकता है। यदि एक्सेस प्वाइंट अपने मूल स्वरूप की सेटिंग में है या असुरक्षित है, तो उस रेंज में कोई भी उससे सीधे जुड़ सकता है। असुरक्षित नेटवर्क का इस्तेमाल करते हुए एक बार कनेक्शन स्थापित हो जाने पर हमलावर पीड़ित के कंप्यूटर पर लंबी अवधि तक नियंत्रण स्थापित करने के लिए उस पर मेल भेज सकते हैं, वर्गीकृत/गोपनीय सामग्री डाउनलोड कर सकते हैं, नेटवर्क के अन्य कंप्यूटरों पर हमला शुरू कर सकते हैं, दूसरों को गलत कोड भेज सकते हैं।

इंटरनेट सुरक्षा मुद्दे और सावर्जनिक वाईफाई के खतरे बढ़ रहे हैं। कुछ सावधानियां बरतने से आपको अपनी सूचनाओं को सुरक्षित रख पाने में मदद मिलेगी।

अपने वायरलेस संचार को अतिरिक्त के साथ नेटवर्क सुरक्षा देकर सुरक्षित करें जैसे कि एसएसएच, या वीपीएन, या एसएसएल टनलिंग और उपयोग में न होने पर वायरलेस डिवाइस बंद करें

मुफ्त वाईफाई हाटस्पाट साइबर हमलों के प्रति जोखिम भरे होते हैं

अधिकांश महिलाएं अपनी पसंद की सोशल मीडिया या चैटिंग एप्लीकेशन के लिए सार्वजनिक स्थानों पर उपलब्ध मुफ्त वाईफाई से जुड़ना चाहती हैं। रेलवे स्टेशनों और हवाई अड्डों पर सार्वजनिक बेतार कंप्यूटर नेटवर्क से जुड़ कर इंटरनेट का इस्तेमाल आपको साइबर हमलों के जोखिम में डाल सकता है। इन जोखिमों का सफलतापूर्वक लाभ उठा कर हमलावर केडिट कार्ड संख्या, पासवर्ड, चैटिंग के संदेश, ईमेल आदि जैसी संवेदनशील सूचनाएं हासिल कर सकते हैं। यह सुझाव दिया जाता है कि उपयोक्ता सार्वजनिक वाईफाई से दूर रहें और केवल सुरक्षित नेटवर्क का इस्तेमाल करें। मुफ्त सार्वजनिक वाईफाई के इस्तेमाल के लिए कुछ सुझाव इस तरह हैं

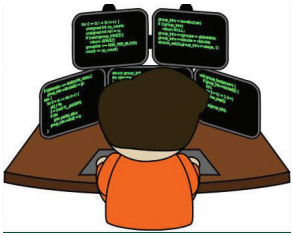
सार्वजनिक स्थानों पर खुले वाईफाई नेटवर्क में स्वतः कभी न जुड़े
सार्वजनिक वाईफाई का इस्तेमाल करते समय केवल सुरक्षित वेबसाइट पर ही जाएं
जब आपको जरूरत न हो, वाईफाई को बंद रखें
आंकड़ों की हिस्सेदारी के विकल्प को निष्क्रिय कर दें
संवेदनशील पासवर्ड के इस्तेमाल से बचें

किसी व्यक्ति का पीछा करना

मोबाइल फोन की तरह वाईफाई यंत्र के पास विशिष्ट पहचान करने वाले होते हैं, जिनका इस्तेमाल पीछा करने के लिए किया जा सकता है। ये संभावित सुरक्षा मुद्दों के लिए संभावित खतरे हो सकते हैं। वाईफाई हाटस्पाट के इस्तेमाल द्वारा पीछा करने से लगातार नजर रखने जैसे साइबर अपराध भी हो सकते हैं। किसी सेवा के इस्तेमाल या उसे हासिल करने के लिए वेबसाइटों को अक्सर उपयोक्ता की व्यक्तिगत सूचनाएं, जैसे नाम, उम्र, जिप कोड या व्यक्तिगत पसंद साझा करने की आवश्यकता होती है।

प्राधिकारियों द्वारा: प्राधिकारियों के पास लोगों के ब्राउजिंग विवरण और आदतों तक पहुंचना आसान होता है और राष्ट्रीय सुरक्षा के नाम पर बिना सहमित के लोगों पर निगरानी रखने में इस्तेमाल किया जा सकता है।

हैकरों द्वारा: पीड़ितों के बैंक खातों और निगमित वित्तीय सूचना और गोपनीयता से सूचनाएं चुराना और हैक करना।



वायरलेस संचार के लिए राउटर को स्थापित करते समय खुद को सुरक्षित करने के उपाय के लिए

- **एक्सेस प्वाइंट का यूजर नाम और पासवर्ड बदल दें**
  वाईफाई के घरेलू नेटवर्क और ब्राडबैंड राउटर यूजर नाम और पासवर्ड से सुरक्षित होते हैं, ताकि केवल अधिकृत व्यक्ति ही नेटवर्क में प्रशासनिक फेरबदल कर सके।
- **मूल एसएसआईडी बदल दें, और अपने नेटवर्क का नाम प्रसारित करने से बचें**
  सभी एक्सेस प्वाइंट और राउटर सर्विस सेट आइडेंटिफायर नामक नेटवर्क के नाम का इस्तेमाल करते हैं। केवल एसएसआईडी की जानकारी से आपके नेटवर्क पर हमला नहीं किया जा सकता है, लेकिन यह दिखाता है कि यह खराब तरीके से स्थापित है।
- **इस्तेमाल नहीं होने की स्थिति में वाईफाई बंद कर दें**
  जब आपको घरेलू नेटवर्क से विस्तारित अवकाश लेना हो, तब इसका दुरुपयोग करने के लिए इसे बंद कर देना अच्छा है। जब इस्तेमाल में नहीं हो, तब एक्सेस प्वाइंट को भी बंद कर दें।
- **घरेलू वाईफाई के लिए डायनेमिक आईपी पता का इस्तेमाल करने से बचें और स्थैतिक (स्टैटिक) आईपी पते का इस्तेमाल करें**
  अधिकांश घरेलू नेटवर्क प्रशासक अपने यंत्रों को आईपी पता देने के लिए डायनेमिक होस्ट कनफिगरेशन प्रोटोकाल (डीएचसीपी) का इस्तेमाल करते हैं। राउटर या एक्सेस प्वाइंट पर डीएचपीसी बंद कर दें। इसके बदले में निश्चित निजी आईपी पता का रेंज तय करें और तब सभी जुड़े हुए यंत्रों को उस रेंज के अधीन पते के भीतर स्थापित करें।
- **एनक्रिप्शन के लिए हमेशा मजबूत पासवर्ड का इस्तेमाल करें**
  पासवर्ड में व्यक्तिगत आंकड़ों के इस्तेमाल से बचें। याद रखने में आसान पास और वाक्यांश का इस्तेमाल करें।
- **अतिरिक्त बचाव के लिए फायरवाल और एंटी वायरस का इस्तेमाल करें**
  बेतार नेटवर्क को तारयुक्त नेटवर्क से फायरवाल और एक एंटी वायरस गेटवे के माध्यम से अलग कर दें।
- **यंत्र द्वारा उपलब्ध कराये गये मूल सुरक्षा उपायों का इस्तेमाल करें।**
  सभी वाईफाई यंत्र एनक्रिप्शन के कुछ प्रकार का समर्थन करते हैं। इसलिए उन्हें सक्रिय करें। फर्मवेयर को नियमित रूप से अद्यतन करते रहें।
  वायरलेस नेटवर्क में संवेदनशील आंकड़ों के लिए एनक्रिप्शन तकनीक का इस्तेमाल करें। एनक्रिप्शन के लिए हमेशा एक्सेस प्वाइंट द्वारा समर्थित अधिकतम कुंजी आकार का इस्तेमाल करें।
  केवल जरूरत पड़ने पर ही फाइल की साझेदारी और एयरड्राप को खोलें।