सार्वजनिक वाई-फाई का सुरक्षित रूप से उपयोग करने के बारे में कुछ सुझाव

बुरे सक्रियक आपके ऑनलाइन होने का फायदा उठा सकते हैं। इस बात पर विचार करने के लिए कि आपको सार्वजनिक वाई-फाई उपयोग करने की आवश्यकता है नीचे कुछ सुझाव पढ़ें।

कोरोनावायरस के प्रकोप और व्यवसायों और पुस्तकालयों के बंद होने के फलस्वरूप, हम में से अधिकतर लोग ज़्यादा समय ऑनलाइन बिता रहे हैं। परिणामस्वरूप, इन्टरनेट से जुड़ने के लिए हमें सार्वजनिक वाई-फाई की आवश्यकता हो सकती है। यदि आप सार्वजनिक वाई-फाई उपयोग करने की आवश्यकता महसूस करते हैं, तो कृपया अपने डेटा सुरक्षा में सहायता के लिए Chief Privacy Officer (चीफ प्राईवेसी ऑफिसर) की निम्न सिफरिशों पर गौर करें:

1. पुष्टि करें कि आपके पास उचित नेटवर्क है।

सुनिश्चित करें कि आप सही नेटवर्क से जुड़ रहे हैं। बुरे सक्रियक ऐसे नेटवर्क बना सकते हैं जो अपने नाम के आधार पर हानिरहित दिखते हैं लेकिन वास्तव में आपका इन्टरनेट सर्फिंग देखने के लिए आपको किसी नेटवर्क सेटअप से जुड़ने का निर्देश दे रहे होते हैं। इसका मतलब है कि यदि आप वेबसाइटों में लॉगिन क्रेडेंशियल या पासवर्ड दर्ज करते हैं, तो हैकर आपकी जानकारी चुराने के योग्य होगा। इससे बचाव के लिए, नेटवर्क का नाम बहुत सावधानी से पढ़ें और यदि संभव हो, तो नेटवर्क की वैधता सुनिश्चित करने के लिए किसी कर्मचारी से पूछें या व्यवसाय के पहचानसूचक की जाँच करें।

जाने माने नेटवर्कों, जैसेकिसुपरिचित coffee chains (कॉफ़ी चेन्स), के संदिग्ध होने की संभावना कम होती है क्योंकि कंपनी अपने व्यवसाय की ही एक सेवा के रूप में नेटवर्क संचालित कर रही है। ज्ञात नेटवर्क आम तौर पर किसी सार्वजनिक जगह पर आपके फ़ोन पर दिखने वाले अनियमित मुफ्त वाई-फाई नेटवर्कों से ज़्यादा सुरक्षित होते हैं।

2. ऑटो-कनेक्ट बंद करें।

अधिकतर डिवाइसेज (स्मार्ट फ़ोन्स, लैपटॉप्स, और टैबलेट्स) में ऑटोमैटिक कनेक्टिविटी सेटिंग्स होती हैं। यह सेटिंग आपके डिवाइसेज को सुविधाजनक ढंग से आस पास के नेट वर्कों से जुड़ने देती है। विश्वसनीय नेट वर्कों के साथ तो यह ठीक है, लेकिन यह आपके डिवाइसेज को उन नेटवर्कों से भी जोड़ सकता है जो असुरक्षित हो सकते हैं. आप अपने डिवाइस पर सेटिंग्स की सुविधा के माध्यम से इस सुविधा को बंद कर सकते हैं। इन सेटिंग्स को बंद रखें, खासकर जब आप अपरिचित स्थानों की यात्रा कर रहे हों। एक अतिरिक्त सावधानी के रूप में, आप सार्वजनिक वाई-फाई का उपयोग करने के बाद “फॉरगेट नेटवर्क” की जांच कर सकते हैं।

सार्वजनिक स्थानों पर रहते हुए आपको अपने Bluetooth की भी देख रेख करनी चाहिए। Bluetooth कनेक्टिविटी विभिन्न डिवाइसेज को एक दुसरे से संवाद स्थापित करने देता है, और कोई हैकर आपके डिवाइसेज तक पहुँच प्राप्त करने के लिए खुले Bluetooth सिग्नलों की तलाश कर सकता है। जब आप किसी अपरिचित क्षेत्र में हों तो इस फंक्शन को अपने फोन और अन्य डिवाइसेज पर बंद कर के रखें।

3. फाइल शेयरिंग बंद करें।

सार्वजनिक वाई फाई पर होने की दशा में फाइल शेयरिंग विकल्प बंद करना सुनिश्चित करें। आप अपने ऑपरेटिंग सिस्टम के आधार पर, system preferences (सिस्टम प्रेफरेंसेज़) या कंट्रोल पैनल से फाइल शेयरिंग बंद कर सकते हैं। AirDrop(एयरड्रॉप) फाइल शेयरिंग सुविधा का एक उदाहरण है जिसे आप बंद करना चाहेंगे। कुछ ऑपरेटिंग सिस्टम्स जैसे कि Windows/ PC पहली बार किसी नए सार्वजनिक नेटवर्क से जुड़ने पर आपके द्वारा "सार्वजनिक" चुनने पर आपके लिए फाइल शेयरिंग बंद कर देंगे।

फाइल शेयरिंग बंद करने के चरण

किसी PC पर:

1. Network and Sharing Center (नेटवर्क एंड शेयरिंग सेंटर) पर जाएँ।
2. फिर advanced sharing settings (एडवांस्ड शेयरिंग सेटिंग्स) बदलें।
3. file and printer sharing (फाइल और प्रिंटर शेयरिंग) बंद करें।

मैक के लिए:

1. System Preferences (सिस्टम प्रेफरेंसेज़) पर जाएँ।
2. Sharing (शेयरिंग) चुनें।
3. अब सब कुछ (अचयनित) Unselect करें।
4. फिर फाइंडर में, AirDrop पर क्लिक करें, और Allow me to be discovered by (मुझे खोज करने की अनुमति दें) का चयन करें: कोई नहीं।

iOS के लिए, कंट्रोल सेंटर में सिर्फ AirDrop तलाश करें और उसे बंद कर दें।

4. VPN उपयोग करें।

अपने डिवाइस पर कोई VPN (वर्चुअल प्राइवेट नेटवर्क) Virtual Private Network इनस्टॉल करने पर विचार करें। सार्वजनिक वाई फाई पर डिजिटल प्राइवेसी के लिए VPN सब से सुरक्षित विकल्प है। यह आपके डेटा को आपके डिवाइस से आने जाने के दौरान एन्क्रिप्ट करता है और एक सुरक्षात्मक "सुरंग" के रूप में कार्य करता है ताकि आपका डेटा किसी नेटवर्क से आने जाने के दौरानदिखाई न दे।

5. एन्क्रिप्टेड वेबसाइटों – HTTPS के बारे में FBI की वार्निंग।

उन वेबसाइटों के बारे में जिनके एड्रेसेज "https" से आरंभ होते हैं FBI ने चेतावनी दे रखी है। "https" और लॉक आइकॉन की उपस्थिति से इस बात का इशारा करने की अपेक्षा की जाती है कि वेब ट्रैफिक एन्क्रिप्ट किया हुआ है और आगंतुक सुरक्षित रूप से डेटा शेयर कर सकते हैं। हालाँकि, साइबर अपराधी अब लोगों को ऐसी दुर्भावनापूर्ण वेबसाइटों की तरफ लुभा कर लोगों को विश्वास दिलाने की कोशिश कर रहे हैं जिनमें https शामिल है और वो सुरक्षित लगती हैं जबकि वो सुरक्षित नहीं हैं ।

FBI की अनुशंसा

- केवल ईमेल में मौजूद नाम पर ही विश्वास ना करें: ईमेल में मौजूद विषय वस्तु की मंशा पर भी प्रश्न उठाएं।
- अगर आप किसी परिचित संपर्क से लिंक के साथ संदिग्ध ईमेल प्राप्त करे हैं, तो उस संपर्क को कॉल या ईमेल करने के द्वारा इस बात की पुष्टि करें कि संदेश वैध है। किसी भी संदिग्ध ईमेल का सीधे जवाब ना दें।
- लिंक के अंदर गलत स्पेलिंग या गलत डोमेन की जाँच करें (जैसे कि, कोई ऐसा एड्रेस जिसे ".gov" पर समाप्त होना चाहिए वह उसके बजाय ".com" पर समाप्त हो रहा हो)।
- किसी वेबसाइट पर सिर्फ इस लिए विश्वास ना करें कि उसके ब्राउज़र एड्रेस बार में लॉक आइकॉन या "https" है।

6. संवेदनशील जानकारी तक पहुँचने की अनुशंसा नहीं की जाती है।

यद्यपि आपके पास VPN है फिर भी असुरक्षित सार्वजनिक नेटवर्क्स पर व्यक्तिगत बैंक खातों, या उसी जैसे संवेदनशील व्यक्तिगत डेटा जैसे कि सोशल सिक्यूरिटी नंबर्स तक पहुँचने की अनुशंसा नहीं की जाती है। यहां तक कि सार्वजनिक सुरक्षित नेटवर्क्स भी जोखिम भरे हो सकते हैं। अगर सार्वजनिक वाई फाई पर इन खातों का उपयोग करना मजबूरी हो तो अपने सर्वोत्तम निर्णय का उपयोग करें। वित्तीय लेन देन के लिए, विकल्प के रूप में अपने स्मार्टफोन का हॉटस्पॉट फंक्शन उपयोग करना ज़्यादा अच्छा हो सकता है।

7. सुरक्षित बनाम असुरक्षित।

मूल रूप से दो प्रकार के सार्वजनिक वाई-फाई नेटवर्क हैं: सुरक्षित और असुरक्षित।

जब भी संभव हो सुरक्षित सार्वजनिक नेटवर्क्स से जुड़ें। एक असुरक्षित नेटवर्क से किसी भी प्रकार के सुरक्षा सुविधा के बिना जैसे कि पासवर्ड या लॉग इन के जुड़ा जा सकता है। एक सुरक्षित नेटवर्क सामान्यतः नेटवर्क से जून से पहले उपयोगकर्ता से नियम एवं शर्तों से सहमत होना, अकाउंट रजिस्टर करना, या पासवर्ड टाइप करना आवश्यक करता है।

8. अपना फ़ायरवॉल सक्षम रखें।

अगर आप लैपटॉप का उपयोग कर रहे हैं, तो सार्वजनिक वाई फाई पर होने के दौरान अपना फ़ायरवॉल सक्षम रखें। फ़ायरवॉल एक बाधा के रूप में काम करता है जो आपके डिवाइस को मैलवेयर के खतरों से बचाता है। पॉप अप और विज्ञापनों के कारण उपयोगकर्ता Windows फ़ायरवॉल को अक्षम कर सकते हैं और फिर इसके बारे में भूल सकते हैं। अगर आप किसी पीसी पर इसको दोबारा शुरू करना चाहते हैं, तो कंट्रोल पैनल, "(सिस्टम एंड सिक्यूरिटी)" "System and Security" पर जाएँ और "Windows Firewall (फ़ायरवॉल)" चुनें। अगर आप मैक उपयोगकर्ता हैं, तो

“System Preferences” (“सिस्टम प्रेफरेंसेज़“)पर जाएँ, फिर (“सिक्यूरिटी & प्राइवेसी”) “Security & Privacy” पर, फिर “फ़ायरवॉल” सुविधा सक्षमकरें।

9. एंटीवायरस सॉफ़्टवेयर का उपयोग करें।

अपने लैपटॉप पर एंटीवायरस प्रोग्राम का नवीनतम संस्करण इनस्टॉल करना भी सुनिश्चित करें। एंटीवायरस प्रोग्राम सार्वजनिक वाई फाई उपयोग करते समय ऐसे मैलवेयर का पता लगा कर आपकी सुरक्षा में सहायता कर सकते हैं जो साझा नेटवर्क का उपयोग करते समय आपके सिस्टम में आ सकते हैं। यदि आपके डिवाइस पर ज्ञात वायरस लोड हैं या यदि कोई संदिग्ध गतिविधि, हमला, या फिर यदि मैलवेयर आपके सिस्टम में आता है, तो एक चेतावनी आपको सावधान करेगी।

10. दो-कारक या बहु-कारक प्रमाणीकरण का उपयोग करें।

अपने व्यक्तिगत जानकारी के साथ किसी वेबसाइट में लॉग इन करते समय बहु-कारक प्रमाणीकरण (MFA) का उपयोग करें। इसका मतलब कि आपके पास एक दूसरा सत्यापन कोड (जिसे आपके फ़ोन पर टेक्स्ट किया गया है या किसी ऐप या फिजिकल की के द्वारा प्रदान किया गया है) है जो आपकी और ज़्यादा सुरक्षा करता है है। तो यदि कोई हैकर आपका उपयोकर्ता नाम और पासवर्ड पा जाए, वो बिना प्रमाणीकरण कोड के आपके अकाउंट तक नहीं पहुँच सकते हैं।

11. अपने व्यक्तिगत डिवाइसेज पर निगाह रखें।

अपने लैपटॉप, टैबलेट, या स्मार्टफोन को किसी सार्वजनिक जगह या गाड़ी में अकेला ना छोड़ें। यद्यपि आप किसी वाई फाई नेटवर्क पर सावधानी बरत भी रहे हैं, तो भी यह किसी को आपका सामान ले लेने या आपकी जानकारी पर नज़र डालने से नहीं रोकेगा। अपने परिवेश से सावधान रहें और अपने आस पास के लोगों से सचेत रहें।

12. अन्य ऑनलाइन सुरक्षा सुझाव।

ऑनलाइन, खास कर जब आप कोई सार्वजनिक वाई फाई कनेक्शन उपयोग कर रहे हैं तो सुरक्षित रहने के कुछ सुझाव ये हैं:

- सशक्त पासवर्ड उपयोग करें।
- अपना डिवाइस एन्क्रिप्ट करें।
- फ़िशिंग ईमेल से सचेत रहें।
- सोशल मीडिया पर आप जो कुछ पोस्ट करते हैं उसके बारे में सतर्क रहें। बहुत ज़्यादा व्यक्तिगत विवरण हैकर्स को पासवर्ड का अनुमान लगाने में सहायता कर सकता है।
- पुरानी जानकारी जिसकी अब आपको आवश्यकता नहीं है हटा दें।
- अगर कोई नेटवर्क आपसे अतिरिक्त सॉफ्टवेयर या ब्राउज़र एक्सटेंशन इनस्टॉल करने को कहता है तो ना जुड़ें।
- सुनिश्चित करें कि ज्ञात समस्याओं से सुरक्षा के लिए आपके डिवाइसेज पर नवीनतम पैचेज और सॉफ्टवेयर अपडेट इनस्टॉल किये हुए हैं।