सार्वजनिक Wi-Fi सुरक्षित रूपमा प्रयोग गर्ने सम्बन्धी सुझावहरू

खराब अभिनेताहरूले तपाईं अनलाइन भएको फाइदा उठाउन सक्छन्। तपाईंलाई सार्वजनिक Wi-Fi प्रयोग गर्न आवश्यक भएमा विचार गर्नुपर्ने केही सुझावहरू तल पढ्नुहोस्।

कोरोना भाइरस प्रकोपको र व्यवसाय तथा पुस्तकालयहरू बन्द भएको अवस्थामा, हामी मध्ये धेरैजसोले धेरै समय अनलाइनमा बिताइरहेका छौं। परिणाम स्वरूप, हामीलाई इन्टरनेटमा जडान हुन सार्वजनिक Wi-Fi प्रयोग गर्न आवश्यक पर्न सक्छ। यदि तपाईं आफूलाई सार्वजनिक Wi-Fi प्रयोग गर्न आवश्यक रहेको महसुस गर्नुहुन्छ भने, कृपया आफ्नो डेटा सुरक्षित राख्नको लागि राज्यको Chief Privacy Officer (प्रमुख गोपनीयता अधिकारी) का निम्नलिखित सिफारिसहरूको पालना गर्ने बारे विचार गर्नुहोस्:

1. आफूले सही सञ्जाल प्रयोग गरेको पुष्टि गर्नुहोस्।

आफू सही सञ्जालमा जडान हुँदै हुनुहुन्छ भनी सुनिश्चित गर्नुहोस्। खराब अभिनेताहरूले आफ्नो नाममा आधारित सुरक्षित देखिने तर वास्तवमा तपाईंको इन्टरनेट सर्फिङ्ग हेर्नको लागि तपाईंलाई सेट गरिएको सञ्जालमा जडान हुने मार्गमा लैजाने सञ्जालहरू सिर्जना गर्न सक्छन्। यसको अर्थ तपाईंले वेबसाइटमा लगइन पत्यारपत्र वा पासवर्डहरू प्रविष्ट गर्नुहुन्छ भने, ह्याकर तपाईंको जानकारी चोर्न सक्षम हुनेछ। यसबाट बच्नको लागि, सञ्जालको नाम एकदमै ध्यानपूर्वक पढ्नुहोस् र सम्भव भएमा, सञ्जाल वैधानिक हो भनी सुनिश्चित गर्न कर्मचारीलाई सोध्नुहोस् वा व्यवसायको पहिचान सूचक जाँच्नुहोस्।

परिचित कफी चेनहरू जस्ता सुपरिचित सञ्जालहरूलाई कम्पनीले आफ्नो व्यवसायमा सेवाको रूपमा सञ्चालन गरिरहेको हुने हुनाले सम्भवतः त्यस्ता सञ्जालहरू कम शंकास्पद हुन्छन्। ज्ञात सञ्जालहरू सामान्यतया सार्वजनिक स्थानमा तपाईंको फोनमा देखाउन सक्ने अनियमित निःशुल्क Wi-Fi सञ्जालहरू भन्दा अझ सुरक्षित हुन्छन्।

2. स्वतः जडानलाई बन्द गर्नुहोस्।

धेरै यन्त्रहरू (स्मार्टफोन, ल्यापटप र ट्याब्लेटहरू) मा स्वचालित कनेक्टिभिटी सेटिङहरू हुन्छन्। यो सेटिङले तपाईंका यन्त्रहरूलाई नजिकैका सञ्जालहरूमा सजिलैसँग जडान हुन अनुमति दिन्छ। यो विश्वसनीय सञ्जालहरूमा ठीक हुन्छ तर यसले तपाईंका यन्त्रहरूलाई असुक्षित हुन सक्ने सञ्जालहरूमा पनि जडान गर्न सक्छ। तपाईंले यो सुविधालाई आफ्नो यन्त्रको सेटिङहरू सुविधामा गएर असक्षम गर्न सक्नुहुन्छ। यी सेटिङहरूलाई, विशेषगरी तपाईं अपरिचित स्थानहरूमा यात्रा गर्दा बन्द राख्नुहोस्। अतिरिक्त सावधानीको रूपमा, तपाईंले सार्वजनिक Wi-Fi प्रयोग गरेपछि "सञ्जाल बिर्सिनुहोस्" मा ठीक चिन्ह लगाउन सक्नुहुन्छ।

तपाईंले सार्वजनिक स्थानहरूमा हुँदा आफ्नो Bluetooth को पनि निगरानी राख्नुपर्छ। Bluetooth कनेक्टिभिटीले विभिन्न यन्त्रहरूलाई एक-अर्कासँग सञ्चार गर्न अनुमति दिन्छ र ह्याकरले तपाईंका यन्त्रहरूमा पहुँच प्राप्त गर्न खुला Bluetooth संकेतहरू खोज्न सक्छन्। तपाईं अपरिचित क्षेत्रमा हुँदा आफ्नो फोन र अन्य यन्त्रहरूमा यो प्रकार्यलाई बन्द राख्नुहोस्।

3. फाइल साझेदारीलाई बन्द गर्नुहोस्।

सार्वजनिक Wi-Fi मा हुँदा फाइल साझेदारी विकल्पलाई बन्द गर्न सुनिश्चित हुनुहोस्। तपाईंले आफ्नो सञ्चालन प्रणालीको आधारमा प्रणाली प्राथमिकताहरू वा नियन्त्रण प्यालनबाट फाइल साझेदारीलाई बन्द गर्न सक्नुहुन्छ। AirDrop तपाईंले बन्द गर्न चाहनुहुने फाइल साझेदारी सुविधाको उदाहरण हो। Windows/PC जस्ता केही सञ्चालन प्रणालीहरूले तपाईंको लागि नयाँ सार्वजनिक सञ्जालमा पहिलो पटक जडान हुँदा "सार्वजनिक" विकल्प चयन गरेर फाइल साझेदारीलाई बन्द गर्नेछन्।

फाइल साझेदारीलाई बन्द गर्ने चरणहरू

PC मा:

1. सञ्जाल र साझेदारी केन्द्रमा जानुहोस्।
2. त्यसपछि उन्नत साझेदारी सेटिङहरू परिवर्तन गर्नुहोस् विकल्पमा जानुहोस्।
3. फाइल वा प्रिन्टर साझेदारीलाई बन्द गर्नुहोस्।

Macs को लागि:

1. प्रणाली प्राथमिकताहरूमा जानुहोस्।
2. साझेदारी रोज्नुहोस्।
3. सबै कुराबाट चयन हटाउनुहोस्।
4. त्यसपछि Finder मा, AirDrop मा क्लिक गर्नुहोस् र मलाई निम्नद्वारा खोजिने अनुमति दिनुहोस् चयन गर्नुहोस्: कसैले पनि होइन।

iOS को लागि, नियन्त्रण केन्द्रमा AirDrop फेला पार्नुहोस् र यसलाई बन्द गर्नुहोस्।

4. VPN प्रयोग गर्नुहोस्।

आफ्नो यन्त्रमा VPN (अवास्तविक निजी सञ्जाल) स्थापना गर्ने बारे विचार गर्नुहोस्। VPN सार्वजनिक Wi-Fi मा डिजिटल गोपनीयताको लागि सबैभन्दा सुरक्षित विकल्प हो। यसले तपाईंका डेटा तपाईंको यन्त्रमा र यसबाट जाँदायसलाई इन्क्रिप्ट गर्छ र सुरक्षात्मक "टनेल" को रूपमा कार्य गर्छ जसकारण तपाईंका डेटा सञ्जालमार्फत जाँदा दृश्यवान हुँदैनन्।

5. इन्क्रिप्ट गरिएका वेबसाइटहरू – HTTPS सम्बन्धी FBI को चेतावनी।

FBI ले "https" बाट सुरु हुने ठेगानाहरू भएका वेबसाइटहरू सम्बन्धी चेतावनी दिएको छ। "https" र लक चिह्नको उपस्थितिले वेब ट्राफिक इक्रिप्ट गरिएको र आगन्तुकहरूले डेटा सुरक्षित रूपमा साझा गर्न सक्ने संकेत गरेको मानिन्छ।

यद्यपि, साइबर अपराधीहरूले अहिले मानिसहरूलाई https भएको र सुरक्षित नहुँदा सुरक्षित देखिने दुर्भावनापूर्ण वेबसाइटहरूमा प्रभोलन देखाएर सर्वसाधारणको विश्वाससँग खेलिरहेका छन्।

FBI का सिफारिसहरू:

- इमेलमा भएको नामलाई सहज रूपमा विश्वास नगर्नुहोस्: इमेल सामग्रीको उद्देश्यमा प्रश्न गर्नुहोस्।
- यदि तपाईंले ज्ञात सम्पर्कबाट लिङ्क सहितको शंकास्पद इमेल प्राप्त गर्नुहुन्छ भने, सम्पर्कलाई फोन गरेर वा इमेल पठाएर सन्देश वैधानिक छ भनी पुष्टि गर्नुहोस्। शंकास्पद इमेलमा सिधै जवाफ नदिनुहोस्।
- लिङ्क भित्र गलत हिज्जे वा गलत डोमेनहरू (उदाहरण, ".gov" मा समाप्त हुनुपर्ने ठेगाना अन्यथा ".com" मा समाप्त भएमा) जाँच गर्नुहोस्।
- वेबसाइटमा ब्राउजर ठेगाना पट्टीमा लक आइकन वा "https" भएको हुनाले मात्रै यसको विश्वास नगर्नुहोस्।

6. संवेदनशील जानकारी पहुँच गर्ने कार्य सिफारिस गरिँदैन।

तपाईंसँग VPN भएता पनि असुरक्षित सार्वजनिक सञ्जालहरूमा व्यक्तिगत बैंक खाताहरू वा सामाजिक सुरक्षा नम्बरहरू जस्ता समान संवेदनशील व्यक्तिगत डेटा पहुँच गर्न अझै पनि सिफारिस गरिँदैन। सार्वजनिक सुरक्षित सञ्जालहरू पनि जोखिमपूर्ण हुन सक्छन्। तपाईंले सार्वजनिक Wi-Fi मा यी खाताहरू पहुँच गर्नुपर्ने भएमा आफ्नो उत्कृष्ट विवेक प्रयोग गर्नुहोस्। वित्तीय कारोबारहरूका लागि, यसको सट्टामा तपाईंको स्मार्टफोनको हटस्पट प्रकार्य प्रयोग गर्नु अझ राम्रो हुनसक्छ।

7. सुरक्षित र असुरक्षित सञ्जाल।

साधारणतया दुई प्रकारका सार्वजनिक Wi-Fi सञ्जालहरू हुन्छन्: सुरक्षित र असुरक्षित।

सम्भव हुँदा सुरक्षित सार्वजनिक सञ्जालहरूमा जडान हुनुहोस्। असुरक्षित सञ्जाल पासवर्ड वा लगइन जस्तो कुनै पनि प्रकारको सुरक्षा सुविधा बिना नै जडान हुनसक्छ। सुरक्षित सञ्जालमा सामान्यतया प्रयोगकर्तालाई सर्त तथा नियमहरूमा सहमति जनाउन, खाता दर्ता गर्न वा सञ्जालमा जडान हुनुअघि पासवर्ड टाइप गर्न आवश्यक हुन्छ।

8. आफ्नो फायरवाललाई सक्षम राख्नुहोस्।

यदि तपाईं ल्यापटप प्रयोग गर्दै हुनुहुन्छ भने, सार्वजनिक Wi-Fi मा हुँदा आफ्नो फायरवाललाई सक्षम राख्नुहोस्। फायरवालले तपाईंको यन्त्रलाई मालवेयर खतराहरूबाट सुरक्षित राख्ने अवरोधको रूपमा कार्य गर्छ। प्रयोगकर्ताहरूले पप अप तथा सूचनाहरूका कारण Windows फायरवाललाई असक्षम गर्न सक्छन् र त्यसपछि यसको बारेमा बिर्सिन्छन्। यदि तपाईंले PC मा यसलाई फेरि सुरु गर्न चाहनुहुन्छ भने, त्यसोभए नियन्त्रण प्यानल, "प्रणाली र सुरक्षा" मा जानुहोस् र "Windows फायरवाल" चयन गर्नुहोस्। यदि तपाईं Mac प्रयोगकर्ता हुनुहुन्छ भने, सुविधालाई सक्षम गर्नको लागि "प्रणाली प्राथमिकताहरू", त्यसपछि "सुरक्षा र गोपनीयता" र "फायरवाल" ट्याबमा जानुहोस्।

9. एन्टिभाइरस सफ्टवेयर प्रयोग गर्नुहोस्।

साथै आफ्नो ल्यापटपमा एन्टिभाइरस प्रोग्रामको नवीनतम संस्करण स्थापना गर्न सुनिश्चित हुनुहोस्। एन्टिभाइरस प्रोग्रामहरूले साझा गरिएको सञ्जाल प्रयोग गर्दा तपाईंको प्रणालीमा पस्न सक्ने मालवेयर पत्ता लगाएर सार्वजनिक Wi-Fi प्रयोग गर्दा तपाईंलाई सुरक्षित राख्न मद्दत गर्न सक्छन्। ज्ञात भाइरसहरू तपाईंको यन्त्रमा लोड भएमा वा कुनै पनि शंकास्पद क्रियाकलाप, आक्रमण भएमा वा मालवेयर तपाईंको प्रणालीमा पसेमा चेतावनीले तपाईंलाई सचेत गराउनेछ।

10. दुई-खण्ड वा बहु-खण्ड प्रमाणीकरण प्रयोग गर्नुहोस्।

आफ्नो व्यक्तिगत जानकारी भएका वेबसाइटहरूमा लगइन गर्दा बहु-खण्ड प्रमाणीकरण (MFA) प्रयोग गर्नुहोस्। यसको अर्थ तपाईंसँग दोस्रो प्रमाणीकरण कोड (तपाईंको फोनमा पाठ सन्देश पठाइएको वा एप वा भौतिक कुञ्जीमार्फत उपलब्ध गराइएको) हुन्छ जसले तपाईंलाई अधिक सुरक्षित राख्दछ। त्यसैले ह्याकरले तपाईंको प्रयोगकर्ता नाम र पासवर्ड प्राप्त गरेता पनि, तिनीहरूले प्रमाणीकरण कोड बिना तपाईंका खाताहरूमा पहुँच गर्न सक्दैनन्।

11. आफ्ना व्यक्तिगत यन्त्रहरूसँग सम्पर्क कायम राख्नुहोस्।

आफ्नो ल्यापटप, ट्याब्लेट वा स्मार्टफोनलाई सार्वजनिक स्थान वा सवारी साधनमा एक्लै नछोड्नुहोस्। तपाईंले Wi-Fi सञ्जालमा सावधानीहरू अपनाइ रहनुभएको भएता पनि, त्यसले कसैलाई तपाईंको सम्पत्ति लिन वा तपाईंको जानकारीको झलक लुकिछिपी हेर्नबाट रोक्न सक्दैन। आफ्ना परिवेशका वस्तुहरू प्रति सचेत र आफू वरपर रहेका व्यक्तिहरूदेखि होशियार हुनुहोस्।

12. अनलाइन सुरक्षा सम्बन्धी अन्य सुझावहरू।

यहाँ अनलाइनमा रहँदा, विशेषगरी तपाईंले सार्वजनिक Wi-Fi जडान प्रयोग गर्दै हुनुहुन्छ भने सुरक्षित रहनको लागि केही सुझावहरू छन्:

- बलियो पासवर्डहरू प्रयोग गर्नुहोस्।
- आफ्ना यन्त्रहरू इन्क्रिप्ट गर्नुहोस्।
- फिशिङ इमेलहरूदेखि सतर्क रहनुहोस्।
- आफूले सामाजिक मिडियामा पोस्ट गर्ने कुरामा होशियार हुनुहोस्। अति धेरै व्यक्तिगत विवरणहरूले ह्याकरहरूलाई पासवर्डहरू अनुमान लगाउन मद्दत गर्न सक्छन्।
- तपाईंलाई अब उपरान्त आवश्यक नपर्ने पुरानो जानकारी मेटाउनुहोस्।
- यदि सञ्जालले तपाईंलाई कुनै पनि अतिरिक्त सफ्टवेयर वा ब्राउजर एक्स्टेन्सन स्थापना गर्न अनुरोध गरेमा जडान नगर्नुहोस्।
- ज्ञात समस्याहरूबाट सुरक्षित रहन तपाईंका यन्त्रहरूमा नवीनतम प्याच र सफ्टवेयर अद्यावधिकहरू स्थापना गरिएका छन् भनी सुनिश्चित गर्नुहोस्।