Sfaturi pentru utilizarea în siguranță a Wi-Fi-ului public

Persoanele rău-intenţionate pot profita de prezenţa dvs. online. Citiţi mai jos câteva sfaturi de avut în vedere dacă trebuie să utilizați Wi-Fi-ul public.

Ca răspuns la pandemia de coronavirus și la închiderea afacerilor și a bibliotecilor, mulți dintre noi petrecem mai mult timp în mediul online. Drept urmare, este posibil să fim nevoiți să utilizăm Wi-Fi-ul public pentru a ne conecta la internet. Dacă vă găsiţi în situaţia de a trebui să utilizați Wi-Fi-ul public, vă rugăm să luați în considerare următoarele recomandări ale Inspectorul-șef pentru Protecția Confidențialității din statul nostru pentru a vă ajuta să vă protejați datele:

1. Asigurați-vă că sunteți conectat la rețeaua corectă.

Asigurați-vă că vă conectați la rețeaua corectă. Persoanele rău-intenționate pot crea rețele care arată inofensiv pe baza numelui lor, dar care, de fapt, vă îndrumă să vă conectați la o rețea configurată pentru a vedea istoricul dvs. de navigare pe internet. Acest lucru înseamnă că dacă introduceți datele de autentificare sau parolele pe site-uri web, hackerul va putea să vă fure informațiile. Pentru a vă proteja împotriva acestui lucru, citiți cu atenție numele rețelei și, dacă este posibil, întrebați un angajat sau verificați informațiile de prezentare ale firmei pentru a vă asigura că rețeaua este legitimă.

Rețele cunoscute, precum cele ale lanțurilor de cafenele recunoscute, sunt probabil mai puțin suspecte, deoarece compania operează rețeaua ca un serviciu oferit împreună cu activitatea lor comercială. Rețelele cunoscute sunt, în general, mai sigure decât rețelele Wi-Fi gratuite aleatorii care pot apărea pe telefonul dvs. într-un loc public.

2. Dezactivați opțiunea de conectare automată.

Multe dispozitive (smartphone-uri, laptop-uri și tablete) au setări automate de conectare. Această setare permite dispozitivelor dvs. să se conecteze în mod automat la rețele din apropiere. Acest lucru este în regulă în cazul rețelelor de încredere, dar vă poate conecta dispozitivele și la rețele care pot fi nesigure. Puteți dezactiva această opțiune cu ajutorul

caracteristicii pentru setări de pe dispozitivul dvs. Mențineți aceste setări dezactivate, în special atunci când călătoriți în locuri necunoscute. Ca o precauție suplimentară, puteți bifa „uită această rețea” după ce utilizați Wi-Fi-ul public.

De asemenea, ar trebui să monitorizați Bluetooth-ul dvs. în locuri publice. Conectarea prin Bluetooth permite diverselor dispozitive să comunice între ele, iar un hacker poate căuta semnale Bluetooth deschise pentru a avea acces la dispozitivele dvs. Mențineți această funcţie dezactivată pe telefon și pe alte dispozitive când vă aflați într-o zonă necunoscută.

3. Dezactivaţi opțiunea de partajare a fișierelor.

Asigurați-vă că dezactivați opțiunea de partajare a fișierelor pe Wi-Fi-ul public. Puteți dezactiva partajarea fișierelor de la preferințe sistem sau din panoul de control, în funcție de sistemul dvs. de operare. AirDrop este un exemplu de caracteristică de partajare a fișierelor pe care veți dori să o dezactivați. Unele sisteme de operare, cum ar fi Windows/PC, vor dezactiva partajarea fișierelor pentru dvs., alegând opțiunea „public” atunci când vă conectați prima dată la o nouă rețea publică.

Pașii de urmat pentru a dezactiva partajarea fișierelor

Pentru PC:

1. Accesați Centrul de rețele și partajare.
2. Apoi Modificare setări avansate partajare.
3. Dezactivați opțiunea de partajare a fișierelor și imprimantelor.

Pentru Mac:

1. Accesați Preferințe sistem.
2. Alegeți Partajare.
3. Deselectați totul.
4. Apoi în Finder, dați clic pe AirDrop, apoi selectați Permite-mi să fiu descoperit de: Nimeni.

Pentru iOS, doar găsiți AirDrop în Centrul de control și opriți-l.

4. Utilizarea unei VPN.

Luați în considerare instalarea unei VPN (rețea virtuală privată) pe dispozitivul dvs. O rețea VPN este cea mai sigură opțiune pentru confidențialitate digitală pe Wi-Fi-ul public. Ea vă criptează datele pe măsură ce trec spre și dinspre dispozitivul dvs. și acționează ca un „tunel” de protecție, astfel încât datele dumneavoastră nu sunt vizibile, atunci când trec printr-o rețea.

5. Avertismentul FBI despre site-urile web criptate – HTTPS.

FBI-ul a avertizat cu referire la site-urile web cu adrese care încep cu „https”. Prezența „https” și pictograma lacăt ar trebui să indice că traficul web este criptat și că vizitatorii pot împărtăși datele în siguranță. Cu toate acestea, infractorii cibernetici se bazează acum pe încrederea publicului prin atragerea oamenilor către site-uri web rău-intenționate care includ https și par sigure, când de fapt, nu sunt.

Recomandările FBI-ului:

- Nu aveți pur și simplu încredere în numele dintr-un e-mail: puneți la îndoială intenția conținutului e-mailului.
- Dacă primiți un e-mail suspect cu un link de la o persoană cunoscută, asigurați-vă că mesajul este legitim, sunând persoana sau trimițându-i un e-mail. Nu răspundeți direct la un e-mail suspect.
- Verificați dacă există greșeli sau domenii incorecte în cadrul unui link (de exemplu, dacă o adresă care ar trebui să se termine în „.gov” se termină în „.com”).
- Nu aveți încredere într-un site web doar pentru că are o pictogramă lacăt sau „https” în bara de adresă a browser-ului.

6. Accesarea informațiilor sensibile nu este recomandată.

Chiar dacă aveți un VPN, nu este recomandat să accesați conturi bancare personale sau alte date personale sensibile, precum numerele de asigurări sociale prin rețelele publice nesecurizate. Chiar și rețelele securizate publice pot fi riscante. Gândiți-vă bine atunci când sunteți nevoiți să accesați aceste conturi prin Wi-Fi-ul public. În cazul tranzacțiilor financiare, ar fi mai bine să utilizați funcția de hotspot a smartphone-ului dvs.

7. Securizat vs. nesecurizat.

Există, practic, două tipuri de rețele Wi-Fi publice: securizate și nesecurizate.

Ori de câte ori este posibil, conectați-vă la rețele publice securizate. O rețea nesecurizată se poate conecta fără niciun tip de caracteristică de securitate, precum o parolă sau date de autentificare. O rețea securizată necesită, de obicei, ca un utilizator să fie de acord cu termenii și condițiile, să înregistreze un cont sau să introducă o parolă înainte de a se conecta la rețea.

8. Menţineți firewall-ul activat.

Dacă utilizați un laptop, păstrați firewall-ul activat în timp ce accesați Wi-Fi-ul public. Un firewall acționează ca o barieră care vă protejează dispozitivul împotriva amenințărilor de tip malware.

Utilizatorii pot dezactiva firewall-ul Windows din cauza unor pop-up-uri și notificări și apoi uită de el. Dacă doriți să-l reporniți pe un calculator, atunci mergeți la Panoul de control, „Sistem și securitate” și selectați „Windows Firewall”. Dacă sunteți utilizator de Mac, accesați „Preferințe sistem”, apoi „Securitate și confidențialitate”, încheind cu fila „Firewall” pentru a activa opțiunea.

9. Folosiți programe antivirus.

De asemenea, asigurați-vă că instalați cea mai recentă versiune a unui program antivirus pe laptop. Programele antivirus vă pot ajuta să fiți protejați în timp ce utilizați Wi-Fi-ul public, detectând programele de tip malware care ar putea intra în sistemul dvs. în timp ce utilizați rețeaua partajată. O alertă vă va anunța dacă viruși cunoscuți sunt încărcați pe dispozitivul dvs. sau dacă există vreo activitate suspectă, atac sau dacă este introdus un program tip malware în sistemul dvs.

10. Utilizați autentificarea cu doi sau mai mulți factori.

Folosiți autentificarea cu mai mulți factori (MFA) atunci când vă conectați la site-uri web cu datele dvs. personale. Acest lucru înseamnă că aveți un al doilea cod de verificare (trimis prin SMS pe telefonul dvs. sau furnizat de o aplicație ori cheie fizică) care vă protejează suplimentar. Deci, chiar dacă un hacker obține numele de utilizator și parola dvs., acesta nu vă poate accesa conturile fără un cod de autentificare.

11. Aveţi grijă de dispozitivele dvs. personale.

Nu lăsați laptop-ul, tableta sau smartphone-ul nesupravegheat/ă într-un loc public sau vehicul. Chiar dacă luați măsuri de precauție privind o rețea Wi-Fi, acest lucru nu va împiedica pe cineva să vă ia lucrurile personale sau să arunce o privire în informațiile dvs. Fiți conștienți de împrejurimile dvs. și atenți la cei din jur.

12. Alte sfaturi de siguranţă când sunteţi online.

Iată câteva sfaturi pentru a vă menține în siguranță în mediul online, mai ales dacă utilizați o conexiune Wi-Fi publică:

- Folosiți parole puternice.
- Criptați-vă dispozitivele.
- Feriți-vă de e-mailurile de tip phishing.
- Fiți atenţi ce postați în media socială. Prea multe detalii personale pot ajuta hackerii să ghicească parolele.

- Ștergeți informațiile vechi de care nu mai aveți nevoie.
- Dacă o rețea vă solicită să instalați orice software suplimentar sau extensii de browser, nu vă conectați.
- Asigurați-vă că cele mai recente patch-uri și actualizări software sunt instalate pe dispozitivele dvs. pentru a vă proteja împotriva problemelor cunoscute.