Mga tip para sa ligtas na paggamit ng pampublikong Wi-Fi

Maaari kang pagsamantalahan online ng mga taong may masamang intensyon. Basahin sa ibaba ang ilang tip na maaari mong isaalang-alang kung kailangan mong gumamit ng pampublikong Wi-Fi.

Bilang tugon sa paglaganap ng Coronavirus at sa pagsasara ng mga negosyo at aklatan, marami sa atin ngayon ang gumugugol ng mas maraming oras online. Dahil dito, maaaring kailanganin nating gumamit ng pampublikong Wi-Fi para kumonekta sa internet. Kung kailanganin mong gumamit ng pampublikong Wi-Fi, mangyaring isaalang-alang ang sumusunod na rekomendasyon mula sa Chief Officer ng Pagkapribado ng estado para maprotektahan ang iyong data:

1. Kumpirmahin na nasa tama kang network.

Tiyaking kumokonekta ka sa tamang network. Maaaring gumawa ng network na mukhang ligtas batay sa pangalan nito ang mga taong may masamang intensyon, ngunit ang totoo ikinokonekta ka sa isang network na naka-set up para subaybayan ang iyong pag-surf sa internet. Nangangahulugan ito na kapag inilagay mo ang mga detalye sa paglog-in o mga password sa mga website, magagawang nakawin ng hacker ang iyong impormasyon. Para magkaroon ng proteksyon laban dito, basahin ang pangalan ng network nang mabuti at kung maaari, magtanong sa isang empleyado o tingnan ang karatula ng negosyo para tiyaking lehitimo ang network.

Hindi gaanong kahina-hinala ang mga kilalang network, tulad ng mga sikat na coffee chain (kapihan), dahil pinapagana ng kumpanya ang network bilang serbisyong kaugnay ng kanilang negosyo. Karaniwang mas ligtas ang mga kilalang network kaysa sa mga random na libreng Wi-Fi network na maaaring lumabas sa iyong phone kapag nasa pampubliko lugar.

2. I-off ang awtomatikong kumonekta.

Maraming device (mga smartphone, laptop, at tablet) ang mayroong mga setting para sa awtomatikong pagkonekta. Binibigyang-daan ng setting na ito ang iyong mga device

na madaling kumonekta sa mga nakapaligid na network. Ayos lang ito para sa mga pinagkakatiwalaang network, ngunit maaari din nitong ikonekta ang iyong mga device sa mga network na maaaring hindi ligtas. Maaari mong i-disable ang feature na ito sa pamamagitan ng mga setting sa iyong device. Panatilhing naka-off ang mga setting na ito, lalo na kapag naglalakbay ka sa mga hindi pamilyar na lugar. Bilang karagdagang pag-iingat, maaari mong lagyan ng check ang “forget network” pagkatapos gumamit ng pampublikong Wi-Fi.

Dapat mo ring subaybayan ang iyong Bluetooth habang nasa mga pampublikong lugar. Kapag nakakonekta sa Bluetooth, nagkakaroon ng kakayahan ang iba’t ibang device na kumonekta sa isa't isa, at maaaring maghanap ang isang hacker ng mga bukas na signal ng Bluetooth para makakuha ng access sa iyong mga device. Panatilihing naka-off ang function na ito sa iyong phone at iba pang device kapag nasa lugar ka na hindi pamilyar.

3. I-off ang file sharing.

Tiyaking i-off ang opsyong magbahagi ng file kapag nakakonekta sa pampublikong Wi-Fi. Maaari mong i-off ang file sharing mula sa mga pagpipilian ng system o control panel, depende sa gamit mong operating system. Ang AirDrop ay isang halimbawa ng feature na file sharing na makakabuti kung io-off mo. Kusang io-off para sa iyo ng ilang operating system tulad ng Windows/PC ang file-sharing kung pipiliin mo ang opsyong “public” kapag kumokonekta sa isang bagong pampublikong network sa unang pagkakataon.

Mga hakbang para i-off ang file sharing

Sa PC:

1. Pumunta sa Network and Sharing Center
2. Pagkatapos ay pumunta sa Baguhin ang mga advanced na setting ng pagbabahagi.
3. I-off ang file and printer sharing.

Para sa mga Mac:

1. Pumunta sa mga pagpipilian ng system.
2. Piliin ang Sharing.
3. Alisin sa pagkakapili ang lahat.
4. Susunod sa Finder, i-click ang AirDrop, at piliin ang Payagan akong matuklasan ng: Walang Isa.

Para sa iOs, hanapin lang ang Airdrop sa Control Center at i-off ito.

4. Gumamit ng VPN.

Subukang mag-install ng VPN sa iyong device. VPN ang pinakaligtas na opsyon para sa digital na pagkapribado sa pampublikong Wi-Fi. Ini-encrypt nito ang iyong data habang dumadaan papunta at paalis sa iyong device at nagsisilbi ito bilang pamprotektang “tunnel” para hindi nakikita ang iyong data habang dumadaan ito sa isang network.

5. Babala ng FBI tungkol sa mga naka-encrypt na website – HTTPS.

Nagbabala ang FBI tungkol sa mga website na may mga address na nagsisimula sa “https.” Ang pagkakaroon ng “https” at lock na icon ay ipinapagpalagay bilang mga tanda na nagpapahayag na naka-encrypt ang trapiko sa web at maaaring magbahagi ng data ang mga bisita nang ligtas. Gayunpaman, pinagsasamantalahan na rin ngayon ng mga kriminal sa cyberspace ang tiwala ng publiko sa pamamagitan ng panlilinlang sa kanilang pumunta sa mga mapanghamak na website na naka-https at lumalabas na ligtas, kunwari.

Mga Rekomendasyon ng FBI:

- Huwag basta-basta magtiwala sa pangalang nasa email: pagtakhan kung ano ang layunin ng nilalaman ng email.
- Kung makatanggap kayo ng kahina-hinalang email na may link mula sa kilalang contact, kumpirmahin kung lehitimo ang mensahe sa pamamagitan ng pagtawag o pag-email sa contact. Huwag direktang tumugon sa isang kahina-hinalang email.
- Tingnan kung may mga maling spelling o mga maling domain sa loob ng isang link (hal. kung ang address na nagtatapos dapat sa “.gov” ay nagtatapos sa “.com” sa halip).
- Huwag magtiwala sa isang website dahil lang sa mayroon itong lock na icon o “https” sa address bar sa browser.

6. Hindi inirerekomenda ang pag-access sa sensitibong impormasyon.

Kahit na mayroon kang VPN, hindi pa rin inirerekomendang mag-access ng mga personal na bank account, o katulad na sensitibong personal na data gaya ng mga social security number sa mga hindi ligtas na pampublikong network. Maaari pa ring maghatid ng peligro kahit na ang mga ligtas na pampublikong network. Pag-isipan at pagpasyahan nang mabuti kung kailangan mo talagang i-access ang mga account na ito sa pampublikong Wi-Fi. Para sa mga pinansyal na transaksyon, maaaring mas mabuti kung ang function na hotspot ng iyong smartphone na lang ang gagamitin.

7. Ligtas kumpara sa hindi ligtas.

Bilang batayan, mayroong dalawang uri ng pampublikong Wi-Fi network: Ligtas at hindi ligtas.

Hangga't maaari, kumonekta sa mga ligtas na pampublikong network. Nakakakonekta sa mga hindi ligtas na network nang walang kahit anong uri ng feature na panseguridad tulad ng password o pag-log in. Kadalasang nag-aatas sa user na sumang-ayon sa mga tuntunin at kundisyon, magrehistro ng account, o mag-type ng password bago makakonekta sa network ang ligtas na network.

8. Panatilihing naka-enable ang iyong firewall.

Kung gumagamit ka ng laptop, panatilihing naka-enable ang firewall mo habang nasa pampublikong Wi-Fi. Nagsisilbi ang firewall bilang panghadlang na nagpoprotekta sa iyong device laban sa mga banta ng malware. Maaaring nadi-disable ng mga user ang firewall sa Windows dahil sa mga pop-up at notification, at pagkatapos ay nakakalimutan na ang tungkol dito. Kung gusto mo itong i-restart sa isang PC, pumunta lang sa Control Panel, "System and Security" at piliin ang "Windows Firewall". Kung gumagamit ka ng Mac, pumunta sa "System Preferences", pagkatapos ay sa "Security & Privacy", at sa tab na "Firewall" para i-enable ang feature.

9. Gumamit ng antivirus na software.

Tiyakin din na naka-install ang pinakabagong bersyon ng antivirus na program sa iyong laptop. Makakatulong ang mga antivirus na program na protektahan ka habang gumagamit ng pampublikong Wi-Fi sa pamamagitan ng pagtukoy kung may malware na maaaring makapasok sa system mo habang ginagamit ang nakabahaging network. Aalertuhan ka bilang babala kung may na-load na mga kilalang virus sa iyong device o kung may anumang kahina-hinalang aktibidad, pag-atake o kung may nakapasok na malware sa iyong system.

10. Gumamit ng two-factor o multi-factor na authentication.

Gumamit ng multi-factor na authentication (MFA) kapag nagla-log in sa mga website gamit ang iyong personal na impormasyon. Ibig sabihin, mayroon kang pangalawang verification code (na iti-text sa phone mo o ibibigay ng app o pisikal na key) na magbibigay sa iyo ng dagdag na proteksyon. Kaya, kahit makuha ng hacker ang username at password mo, hindi niya maa-access ang iyong mga account nang walang authentication code.

11. Subaybayan ang mga personal mong device.

Huwag iwan ang iyong laptop, tablet, o smartphone nang walang bantay sa pampublikong lugar o sasakyan. Kahit na nag-iingat ka sa paggamit ng Wi-Fi network, hindi nito mapipigilan ang isang tao na kunin ang pagmamay-ari mong device o silipin ang iyong impormasyon. Maging mapagmasid sa kapaligiran mo at sa mga taong nakapaligid sa iyo.

12. Iba pang tip para sa pagiging ligtas online.

Narito ang ilang tip para sa pananatiling ligtas online, lalo na kung nakakonekta ka sa pampublikong Wi-Fi:

- Gumamit ng mga hindi madaling hulaan na password.
- I-encrypt ang iyong mga device.
- Mag-ingat sa mga email na phishing.
- Mag-ingat sa kung ano ang ipinopost mo sa social media. Kapag nagbahagi ka ng masyadong maraming personal na detalye, natutulungan mo ang mga hacker na hulaan ang iyong mga password.
- I-delete ang lumang impormasyong hindi mo na kailangan.
- Kung hilingin sa iyo ng isang network na mag-install ng anumang dagdag na software o extension sa browser, huwag kumonekta.
- Siguruhing naka-install sa mga device mo ang mga pinakabagong patch at update sa software para magkaroon ng proteksyon laban sa mga kilalang problema.