Vidokezo vya kutumia Wi-Fi ya umma kwa usalama

Waharifu wanaweza kutumia fursa ya wewe kuwa mtandaoni. Soma hapa chini kwa vidokezo vya kuzingatia kama unahitaji kutumia Wi-Fi ya umma.

Kwa sababu ya mlipuko wa Virusi vya Korona na kufungwa kwa biashara na maktaba, wengi wetu tunatumia muda mwingi zaidi mtandaoni. Hivyo, tunawezakuhitaji kutumia Wi-Fi ya umma ili kujiunga na intaneti. Iwapo wewe mwenyewe unahisi unahitaji kutumia Wi-Fi ya umma, tafadhali zingatia mapendekezo yafuatayo kutoka kwa Chief Privacy Officer jimbo ili kusaidia kulinda taarifa zako:

1. Thibitisha kuwa una mtandao sahihi.

Hakikisha kuwa unajiunga na mtandao sahihi. Waharifu wanaweza kuunda mitandao inayoonekana kuwa salama kulingana na jina lao lakini kwa hakika wanakuelekeza kuunganishwa na mtandao uliotengenezwa kuangalia shughuli zako za mtandaoni. Hii ina maana kuwa iwapo utajaza tarifa zako za kuingia au manenosiri yako katika tovuti, wadukuzi wataweza kuiba tarifa zako. Ili kujilinda dhidi ya haya, soma jina la mtandao kwa makini na ikiwezekana, muulize mfanya kazi au angalia kibao cha biashara ili kuhakikisha kuwa mtandao ni salama.

Mitandao inayojulikana vizuri, kama vile mikahawa mashuhuri, huenda yasiwe ya kushukiwa kwa sababu kampuni inaendesha mtandao kama huduma pamoja na biashara yao. Mitandao inayojulikana ni salama zaidi kuliko mitandao usiyofahamu inayoweza kujitokeza kwenye simu yako ya mkononi unapokuwa kwenye maeneo ya umma.

2. Zima kujiunga kiotomatiki.

Vifaa vingi (simu za janja, komyuta mpakato, na kompyuta ndogo) vina mpangilio wa kujiunga kiotomatiki. Mpangilio huu unawezesha vifaa vyako kujiuga na mitandao iliyo karibu kwa urahisi. Hii ni sawa kwa mitandao unayoiamini, lakini inaweza pia kuunganisha vifaa vyako kwenye mitandao ambayo si salama. Unaweza kulemaza kipengele hiki kupitia kipengele cha mipangilio kwenye kifaa chako. Hakikisha umeizima mipangilio hii, hasa unapotembelea mahali

pasipojulikana sana. Kama tahadhali ya ziada, unaweza kuchagua “forget network” baada ya kutumia Wi-Fi ya umma.

Pia unapaswa kufuatilia Bluetooth yako unapokuwa maeneo ya umma. Muunganisho wa Bluetooth unawezesha vifaa kadhaa kuwasiliana, na mdukuzi anaweza kutafuta ishara za Bluetooth ili kufikia vifaa vyako. Zima kiwezeshi hiki na zingine kwenye simu yako unapokuwa mahali usipofahamu vizuri.

3. Zima ugawaji wa faili.

Hakikisha kuwa umezima ugawaji wa faili unapotumia Wi-Fi ya umma. Unaweza zima ugawaji wa faili kupitia mapendeleo ya mfumo au paneli dhibiti, kulingana na mfumo wako endeshi. AirDrop ni mfano wa kipengele cha ugawaji wa faili utakachotaka kukizima. Baadhi ya mifumo endeshi kama vile Windows/Kompyut itakuzimia ugawaji wa faili iwapo utachagua “public” unapounganishwa na mtandao mpya wa umma kwa mara ya kwanza.

Hatua za kuzima ugawaji wa faili

Kwenye kompyuta:

1. Nenda kwenye Network and Sharing Center.
2. Kisha Change advanced sharing settings.
3. Zima file and printer sharing.

Kwa Macs:

1. Nenda kwenye System Preferences.
2. Chagua Sharing.
3. Ondoa alama kwenye machaguo yote.
4. Kisha katika Finder, bofya AirDrop na uchague Allow me to be discovered by: No One.

Kwa iOS, tafuta AirDrop kwenye Control Center na uizime.

4. Tumia VPN.

Zingatia kuweka VPN (Mtandao Pepe Binafsi) kwenye kifaa chako. VPN ndiyo chaguo lililo salama zaidi kwa faragha ya kidigitali katika Wi-Fi ya umma. Inaficha data yako inapopita kuelekea na kutoka kwenye kifaa chako na inachukua nafasi ya “shimo” la ulinzi ili data yako isionekane inapopita kwenye mtandao.

5. Onyo la FBI kuhusu tovuti zilizofichwa – HTTPS.

FBI imeonya kuhusu tovuti ambazo anwani zao zinaanza na “https.” Kuwepo kwa “https” na alama ya kufuli kunafaa kuonyesha kuwa trafiki ya mtandao imefichwa na kuwa wageni wanaweza kutuma data kwa usalama. Lakini, wahalifu wa mtandao sasa wanatumia uaminifu wa umma kwa kuwavuta watu kwenye tovuti zisizo salama ambazo zinatumia https na zinazoonekana kuwa salama ilhali si salama.

Mapendekezo ya FBI:

- Usiamini jina kwenye barua pepe: uliza lengo la maudhui ya barua pepe hiyo.
- Iwapo utapokea barua pepe yenye shaka na kiunganishi kutoka kwa mawasiliano usiyoyafahamu, hakikisha kuwa ujumbe ni halali kwa kupiga au kutuma barua pepe kwenda mawasiliano hayo. Usijibu moja kwa moja kwenye barua pepe yenye shaka.
- Angalia makosa ya uandishi au vikoa vya uongo katika kiunganishi (m.f., iwapo anwani inayofaa kuishia na “.gov” inaishia na “.com”).
- Usiamini tovuti kwa sababu tu ina alama ya kufuli au “https” kwenye kisanduku cha anwani.

6. Ufikiaji wa taarifa nyeti hakushauriwi.

Hata kama una VPN bado haishauriwi kufikia akaunti binafsi za benki, au data binafsi zingine kama namba za hifadhi ya jamii katika mitandao ya umma isiyo salama. Hata mitandao ya umma iliyo salama inaweza kuwa hatari. Tumia maamuzi yako mazuri zaidi iwapo ni lazima ufikie akaunti hizi kutumia Wi-Fi ya umma. Kwa shughuli za kifedha, ingekuwa bora kutumia mtandao wa “hotspot” katika simu janja yako.

7. Iliyo salama dhidi ya isiyo salama.

Kuna aina mbili ya mitandao ya Wi-Fi ya umma: Iliyo salama dhidi ya isiyo salama.

Inapowezekana jiunge na mitandao ya umma iliyo salama. Unaweza kujiunga na mtandao usio salama bila kipengele chochote cha usalama kama vile nenosiri au kuingia. Mtandao ulio salama unahitaji mtumiaji kukubali vigezo na masharti, kusajili akaunti, au kuweka nenosiri kabla ya kuunganishwa na mtandao huo.

8. Hakikisha firewall yako imewezeshwa.

Iwapo unatumia komyuta mpakato, wezesha firewall unapotumia Wi-Fi ya umma. Firewall hufanya kazi kama uzio unaolinda kifaa chako dhidi ya tisho la malware. Watumiaji wanaweza kulemaza firewall ya Windows kwa sababu ya viibukizi na arifa na kisha kisahau. Iwapo unataka kuiwasha tena kwenye kompyuta, nenda kwenye Control Panel, “System and Security” na uchague “Windows Firewall”. Iwapo unatumia Mac, nenda kwenye “System Preferences”, halafu “Security & Privacy”, kisha kichupo cha “Firewall” ili kuwezesha kipengele hiki.

9. Tumia programu ya kuzuia virusi.

Hakikisha umeweka toleo la hivi karibuni la programu ya kuzuia virusi kwenye kompyuta mpakato yako. Programu za kuzuia virusi zinaweza kukusaidia unapotumia Wi-Fi ya umma kwa kutambua malware ambayo inaweza kuingia kwenye mfumo wako unapotumia mtandao wa kutumia na watu wengine. Utapewa tahadhari ya kukuonya iwapo virusi vinavyojulikana vitaingia kwenye kifaa chako au iwapo kuna shughuli zingine zenye shaka, shambulio, au iwapo malware zitaingia kwenye mfumo wako.

10. Tumia uhalalishaji wa hatua mbili au hatua nyingi.

Tumia uhalalishaji wa hatua nyingi (MFA) unapoingia kwenye tovuti kwa kutumia taarifa zako binafsi. Hii inamaanisha kuwa utakuwa na msimbo wa pili wa uhalalishaji (itakayotumwa kwenye simu yako au itakayotolewa na programu au funguo halisi) ambao unakukinga. Kwa hiyo hata kama mdukuzi atapata jina lako la mtumiaji na neosiri, hataweza kufikia akaunti zako bila msimbo wa uhalalishaji.

11. Fuatilia vifaa vyako binafsi.

Usiache kompyuta mpakato, Tablet, au simu janja bila ulinzi katika maeneo ya umma au kwenye gari. Hata kama unajihadhari dhidi ya mtandao wa Wi-Fi, holo halitamzuia mtu kuchukua mali zako au kuchungulia taarifa zako. Angalia mazingira yako na uwe na tahadhari kwa walio karibu yako.

12. Vidokezo vingine vya mtandaoni.

Vifuatavyo ni vidokezo vichache vya kubaki salama mtandaoni, hasa iwapo unatumia muunganisho wa Wi-Fi ya umma:

- Tumia manenosiri magumu.
- Simba fiche vifaa vyako.
- Jihadhari na barua pepe za utapeli data.
- Kuwa makini na mashapisho yako ya kwenye mitandao ya kijamii. Taarifa binafsi nyingizinaweza kuwasidia wadukuzi kukisia manenosiri yako.
- Futa taarifa za zamani usizozihitaji tena.
- Iwapo mtandao utakuomba kusakinisha programu yoyote ya ziada au kuvinjariviendelezi usijiunge nayo.
- Hakikisha umesasisha programu katika vifaa vyako ili kujikinga dhidi ya matatizo yanayojulikana.