పబ్లిక్ Wi-Fi ని సురక్షితంగా ఉపయోగించటానికి చిట్కాలు

చెడ్డ వారు ఆన్‌లైన్‌లో మిమ్మల్ని సద్వినియోగం చేసుకోవచ్చు. మీరు పబ్లిక్ Wi-Fi ఉపయోగించాల్సిన అవసరం ఉంటే కొన్ని చిట్కాల కోసం క్రింద చదవండి.

కరోనావైరస్ వ్యాప్తికి వ్యాపారాలు మరియు గ్రంథాలయాల మూసివేతకు ప్రతిస్పందనగా, మనలో చాలా మంది ఆన్‌లైన్‌లో ఎక్కువ సమయం గడుపుతున్నారు. ఫలితంగా, మనము ఇంటర్నెట్‌కు కనెక్ట్ చేయడానికి పబ్లిక్ Wi-Fiని ఉపయోగించాల్సి ఉంటుంది. మీరు పబ్లిక్ Wi-Fiని ఉపయోగించాల్సిన అవసరం ఉందని మీరు భావిస్తే, దయచేసి మీ డేటాను రక్షించడంలో సహాయపడటానికి రాష్ట్ర చీఫ్ ప్రైవసీ ఆఫీసర్ (Chief Privacy Officer) నుండి ఈ క్రింది సిఫార్సులను పరిశీలించండి:

1. మీకు సరైన నెట్‌వర్క్ ఉందని నిర్ధారించుకోండి.

మీరు సరైన నెట్‌వర్క్‌కు కనెక్ట్ అవుతున్నారని నిర్ధారించుకోండి. చెడ్డ వారు హానిచేయని వాటిలా కనిపించేందుకు నెట్‌వర్క్‌లను వారి పేరు ఆధారంగా సృష్టించవచ్చు, అయితే వాస్తవానికి మీ ఇంటర్నెట్ సర్ఫింగ్‌ను చూడటానికి నెట్‌వర్క్ సెటప్‌తో కనెక్ట్ అవ్వమని మీకు నిర్దేశిస్తున్నారు. మీరు వెబ్‌సైట్లలోకి లాగిన్ ఆధారాలను లేదా పాస్‌వర్డ్‌లను నమోదు చేస్తే, హ్యాకర్ మీ సమాచారాన్ని దొంగిలించగలరు. దీని నుండి రక్షించడానికి, నెట్‌వర్క్ పేరును చాలా జాగ్రత్తగా చదవండి మరియు వీలైతే, నెట్‌వర్క్ చట్టబద్ధమైనదని నిర్ధారించుకోవడానికి ఒక ఉద్యోగిని అడగండి లేదా వ్యాపారం యొక్క సంకేతాలను తనిఖీ చేయండి.

సుపరిచితమైన కాఫీ చైన్స్ మాదిరిగా ప్రసిద్ధ నెట్‌వర్క్‌లు తక్కువ అనుమానాస్పదంగా ఉంటాయి, ఎందుకంటే కంపెనీ వారి వ్యాపారంతో నెట్‌వర్క్‌ను సేవగా నిర్వహిస్తోంది. యాదృచ్ఛిక ఉచిత Wi-Fi నెట్‌వర్క్‌ల కంటే తెలిసిన నెట్‌వర్క్‌లు సాధారణంగా సురక్షితంగా ఉంటాయి, ఇవి మీ ఫోన్‌లో బహిరంగ ప్రదేశంలో కనిపిస్తాయి.

2. ఆటో-కనెక్ట్ ఆఫ్ చేయండి.

చాలా పరికరాలు (స్మార్ట్‌ఫోన్‌లు, ల్యాప్‌టాప్‌లు మరియు టాబ్లెట్‌లు) ఆటోమేటిక్ కనెక్టివిటీ సెట్టింగులను కలిగి ఉంటాయి. ఈ సెట్టింగ్ మీ పరికరాలను సమీపంలోని నెట్‌వర్క్‌లకు సౌకర్యవంతంగా కనెక్ట్ చేయడానికి అనుమతిస్తుంది. విశ్వసనీయ నెట్‌వర్క్‌లకు ఇది సరైనదే, కానీ ఇది మీ పరికరాలను అసురక్షితమైన నెట్‌వర్క్‌లకు కనెక్ట్ చేస్తుంది. మీ పరికరంలోని సెట్టింగ్‌ల ఫీచర్ ద్వారా మీరు ఈ ఫీచర్

ని నిలిపివేయవచ్చు. ప్రత్యేకంగా మీరు తెలియని ప్రదేశాలకు ప్రయాణిస్తున్నప్పుడు, ఈ సెట్టింగులను ఆపివేయండి. అదనపు ముందుజాగ్రత్తగా, మీరు పబ్లిక్ Wi-Fi ఉపయోగించిన తర్వాత "నెట్‌వర్క్‌ను మరచిపోండి (forget network)" అనే దానికి నొక్కండి.

బహిరంగ ప్రదేశాల్లో ఉన్నప్పుడు మీరు మీ Bluetooth ను కూడా పర్యవేక్షించాలి. Bluetooth కనెక్టివిటీ వివిధ పరికరాలను ఒకదానితో ఒకటి కమ్యూనికేట్ చేయడానికి అనుమతిస్తుంది మరియు మీ పరికరాలకు ప్రాప్యత పొందడానికి హ్యాకర్ ఓపెన్ Bluetooth సిగ్నల్స్ కోసం చూడవచ్చు. మీకు తెలియని ప్రాంతంలో ఉన్నప్పుడు మీరు ఈ ఫంక్షన్‌ను మీ ఫోన్‌లో మరియు ఇతర పరికరాలలో ఆపివేయండి.

3. ఫైల్ షేరింగ్‌ను ఆపివేయండి.

పబ్లిక్ Wi-Fi లో ఉన్నప్పుడు ఫైల్ షేరింగ్ ఎంపికను ఆపివేయాలని నిర్ధారించుకోండి. మీ ఆపరేటింగ్ సిస్టమ్‌ను బట్టి, మీరు సిస్టమ్ ప్రాధాన్యతలు లేదా నియంత్రణ ప్యానెల్ నుండి ఫైల్ షేరింగ్‌ను ఆపివేయవచ్చు. మీరు ఆపివేయాలనుకుంటున్న ఫైల్ షేరింగ్ ఫీచర్‌కు AirDrop ఒక ఉదాహరణ. Windows/PC (పిసి) వంటి కొన్ని ఆపరేటింగ్ సిస్టమ్‌లు క్రొత్త పబ్లిక్ నెట్‌వర్క్‌కు మొదటిసారి కనెక్ట్ అయ్యేటప్పుడు "పబ్లిక్" ఎంపికను ఎంచుకోవడం ద్వారా మీ కోసం ఫైల్ షేరింగ్‌ను ఆపివేస్తాయి.

ఫైల్ భాగస్వామ్యాన్ని ఆపివేయడానికి దశలు

PC లో:

1. నెట్‌వర్క్ మరియు షేరింగ్ సెంటర్ (Network and Sharing Center) కు వెళ్లండి.
2. అప్పుడు అధునాతన భాగస్వామ్య సెట్టింగ్స్ (advanced sharing settings) ను మార్చండి.
3. ఫైల్ మరియు ప్రింటర్ భాగస్వామ్యాన్ని ఆపివేయండి.

Macs కోసం:

1. సిస్టమ్ ప్రాధాన్యతలకు వెళ్లండి.
2. భాగస్వామ్యాన్ని ఎంచుకోండి.
3. ప్రతిదాని ఎంపిక తీసివేయండి.
4. తదుపరి ఫైండర్ ఫైండర్లో, AirDrop పై క్లిక్ చేసి, నన్ను కనుగొనటానికి అనుమతించు: ఎవరికి వద్దు ఎంచుకోండి.

iOS కోసం, నియంత్రణ కేంద్రంలో AirDrop ను కనుగొని దాన్ని ఆపివేయండి.

4. VPN ఉపయోగించండి.

మీ పరికరంలో VPN (వర్చువల్ ప్రైవేట్ నెట్‌వర్క్) ను ఇన్‌స్టాల్ చేయడాన్ని పరిగణించండి. పబ్లిక్ Wi-Fi లో డిజిటల్ గోప్యత కోసం VPN అత్యంత సురక్షితమైన ఎంపిక. ఇది మీ డేటాను మీ పరికరానికి మరియు

దాని నుండి వెళుతున్నప్పుడు గుప్తీకరిస్తుంది మరియు రక్షిత "టనెల్ (tunnel)" వలె పనిచేస్తుంది, తద్వారా మీ డేటా నెట్‌వర్క్ గుండా వెళుతున్నప్పుడు కనిపించదు.

5. గుప్తీకరించిన వెబ్‌సైట్ల గురించి FBI హెచ్చరిక - HTTPS.

"Https" చిరునామాలతో ప్రారంభమయ్యే వెబ్‌సైట్‌ల గురించి FBI హెచ్చరించింది. "Https" మరియు లాక్ ఐకాన్ ఉండటం వెబ్ ట్రాఫిక్ గుప్తీకరించబడిందని మరియు సందర్శకులు డేటాను సురక్షితంగా పంచుకోవచ్చని సూచిస్తుంది. ఏదేమైనా, సైబర్ నేరస్థులు ఇప్పుడు https ను పొందుపర్చిన హానికరమైన వెబ్‌సైట్‌లకు ప్రజలను ఆకర్షించడం ద్వారా తీసుకెళ్లి అవి సురక్షితం కానప్పటికీ సురక్షితం అనేలా కనిపించి ప్రజల నమ్మకంతో బ్యాంకింగ్ చేస్తున్నారు.

FBI యొక్క సిఫార్సులు:

- ఇమెయిల్‌లో పేరును నమ్మవద్దు: ఇమెయిల్ కంటెంట్ యొక్క ఉద్దేశాన్ని ప్రశ్నించండి.
- మీకు తెలిసిన పరిచయం నుండి లింక్‌తో అనుమానాస్పద ఇమెయిల్ వస్తే, పరిచయానికి కాల్ చేయడం లేదా ఇమెయిల్ చేయడం ద్వారా సందేశం చట్టబద్ధమైనదని నిర్ధారించండి. అనుమానాస్పద ఇమెయిల్ కు నేరుగా ప్రత్యుత్తరం ఇవ్వవద్దు.
- లింక్‌లోని అక్షరదోషాలు లేదా తప్పు డొమైన్‌ల కోసం తనిఖీ చేయండి (ఉదా., ".Gov" తో ముగియవలసిన చిరునామా, బదులుగా ".com" తో ముగుస్తుంది).
- వెబ్‌సైట్‌లో లాక్ ఐకాన్ లేదా బ్రౌజర్ అడ్రస్ బార్‌లో "https" ఉన్నందున దాన్ని నమ్మవద్దు.

6. సున్నితమైన సమాచారాన్ని యాక్సెస్ చేయడం సిఫారసు చేయబడలేదు.

మీకు VPN ఉన్నప్పటికీ, వ్యక్తిగత బ్యాంక్ ఖాతాలను లేదా అసురక్షిత పబ్లిక్ నెట్‌వర్క్‌లలో సామాజిక భద్రతా సంఖ్యల వంటి సున్నితమైన వ్యక్తిగత డేటాను యాక్సెస్ చేయడానికి ఇప్పటికీ సిఫార్సు చేయబడలేదు. పబ్లిక్ సెక్యూర్డ్ నెట్‌వర్క్‌లు కూడా ప్రమాదకరంగా ఉంటాయి. మీరు పబ్లిక్ Wi-Fi లో ఈ ఖాతాలను తప్పనిసరిగా యాక్సెస్ చేయాల్సివస్తే మీ ఉత్తమమైన తీర్పును ఉపయోగించండి. ఆర్థిక లావాదేవీల కోసం, బదులుగా మీ స్మార్ట్‌ఫోన్ హాట్‌స్పాట్ ఫంక్షన్‌ను ఉపయోగించడం మంచిది.

7. సురక్షితమైన వర్సెస్ అసురక్షితమైన.

ప్రాథమికంగా రెండు రకాల పబ్లిక్ Wi-Fi నెట్వర్క్ లు ఉన్నాయి: సురక్షితమైనవి మరియు అసురక్షితమైనవి.

సాధ్యమైనప్పుడల్లా సురక్షితమైన పబ్లిక్ నెట్వర్క్ లకు కనెక్ట్ అవ్వండి. పాస్‌వర్డ్ లేదా లాగిన్ వంటి భద్రతా ఫీచర్ లేకుండా అసురక్షిత నెట్‌వర్క్‌ను కనెక్ట్ చేయవచ్చు. సురక్షితమైన నెట్‌వర్క్‌కు సాధారణంగా వినియోగదారుడు నిబంధనలు మరియు షరతులను అంగీకరించడం, ఖాతాను నమోదు చేయడం లేదా నెట్‌వర్క్‌కు కనెక్ట్ చేయడానికి ముందు పాస్‌వర్డ్‌ను టైప్ చేయడం అవసరం.

8. మీ ఫైర్‌వాల్‌ను ఎనేబుల్ లో ఉంచండి.

మీరు ల్యాప్‌టాప్‌ను ఉపయోగిస్తుంటే, పబ్లిక్ Wi-Fiలో ఉన్నప్పుడు మీ ఫైర్‌వాల్‌ను ప్రారంభించండి. ఫైర్‌వాల్ మీ పరికరాన్ని మాల్వేర్ అపాయముల నుండి రక్షించే అవరోధంగా పనిచేస్తుంది. పాప్ అప్‌లు మరియు నోటిఫికేషన్‌ల కారణంగా వినియోగదారులు Windows ఫైర్‌వాల్‌ను నిలిపివేయవచ్చు మరియు దాని గురించి మరచిపోవచ్చు. మీరు దీన్ని PCలో పునఃప్రారంభించాలనుకుంటే, కంట్రోల్ పానెల్ (Control Panel), "సిస్టమ్ అండ్ సెక్యూరిటీ(System and Security)" కి వెళ్లి "Windows ఫైర్‌వాల్ (Firewall)" ఎంచుకోండి. మీరు Mac యూజర్ అయితే, ఫీచర్ ని ప్రారంభించడానికి "సిస్టమ్ ప్రాధాన్యతలు (System Preferences)", "భద్రత మరియు గోప్యత (Security & Privacy)", ఆపై "ఫైర్‌వాల్(Firewall)" టాబ్‌కు వెళ్లండి.

9. యాంటీవైరస్ సాఫ్ట్‌వేర్ వాడండి.

మీ ల్యాప్‌టాప్‌లో యాంటీవైరస్ ప్రోగ్రామ్ యొక్క తాజా వెర్షన్‌ను ఇన్‌స్టాల్ చేయాలని నిర్ధారించుకోండి. భాగస్వామ్య నెట్‌వర్క్‌ను ఉపయోగిస్తున్నప్పుడు మీ సిస్టమ్‌లోకి ప్రవేశించే మాల్వేర్లను గుర్తించడం ద్వారా పబ్లిక్ Wi-Fi ఉపయోగిస్తున్నప్పుడు యాంటీవైరస్ ప్రోగ్రామ్‌లు మిమ్మల్ని రక్షించడంలో సహాయపడతాయి. తెలిసిన వైరస్ లు మీ పరికరంలో లోడ్ చేయబడినా లేదా ఏదైనా అనుమానాస్పద కార్యాచరణ, దాడి లేదా మాల్వేర్ మీ సిస్టమ్‌లోకి వస్తే అలెర్ట్ మిమ్మల్ని హెచ్చరిస్తుంది.

10. రెండు-కారకం లేదా బహుళ-కారకాల ప్రామాణీకరణను ఉపయోగించండి.

మీ వ్యక్తిగత సమాచారంతో వెబ్‌సైట్లలోకి లాగిన్ అయినప్పుడు బహుళ-కారకాల ప్రామాణీకరణ (multi-factor authentication) (MFA) ఉపయోగించండి. దీని అర్థం మీకు రెండవ ధృవీకరణ కోడ్ (మీ ఫోన్‌కు టెక్స్ట్ చేయబడింది లేదా యాప్ లేదా భౌతిక కీ అందించినది) మిమ్మల్ని మరింత రక్షిస్తుంది. కాబట్టి హ్యాకర్ మీ వినియోగదారుడు పేరు మరియు పాస్‌వర్డ్‌ను పొందినప్పటికీ, వారు ప్రామాణీకరణ కోడ్ లేకుండా మీ ఖాతాలను యాక్సెస్ చేయలేరు.

11. మీ వ్యక్తిగత పరికరాలను ట్రాక్ చేయండి.

మీ ల్యాప్‌టాప్, టాబ్లెట్ లేదా స్మార్ట్‌ఫోన్‌ను బహిరంగ ప్రదేశంలో లేదా వాహనంలో చూడకుండా ఉంచవద్దు. మీరు Wi-Fi నెట్‌వర్క్‌లో జాగ్రత్తలు తీసుకుంటున్నప్పటికీ, అది మీ ఆస్తిని తీసుకోకుండా లేదా మీ సమాచారాన్ని పరిశీలించకుండా ఎవ్వరిని ఆపదు. మీ పరిసరాల గురించి తెలుసుకోండి మరియు మీ చుట్టూ ఉన్నవారి గురించి జాగ్రత్త వహించండి.

12. ఇతర ఆన్‌లైన్ భద్రతా చిట్కాలు.

ఆన్‌లైన్‌లో సురక్షితంగా ఉండటానికి ఇక్కడ కొన్ని చిట్కాలు ఉన్నాయి, ప్రత్యేకించి మీరు పబ్లిక్ Wi-Fi కనెక్షన్‌ను ఉపయోగిస్తుంటే:

- బలమైన పాస్‌వర్డ్‌లను ఉపయోగించండి.
- మీ పరికరాలను గుప్తీకరించండి.
- ఫిషింగ్ ఇమెయిల్‌ల పట్ల జాగ్రత్త వహించండి.
- మీరు సోషల్ మీడియాలో ఏమి పోస్ట్ చేస్తారో జాగ్రత్తగా ఉండండి. పాస్‌వర్డ్‌లను అంచనా వేయడానికి హ్యాకర్లకు వ్యక్తిగత వివరాలు చాలా సహాయపడతాయి.
- మీకు ఇక అవసరం లేని పాత సమాచారాన్ని తొలగించండి.
- ఏదైనా అదనపు సాఫ్ట్‌వేర్‌ను ఇన్‌స్టాల్ చేయమని నెట్‌వర్క్ మిమ్మల్ని అడిగితే లేదా బ్రౌజర్ పొడిగింపులు కనెక్ట్ అవ్వవు.
- తెలిసిన సమస్యల నుండి రక్షించడానికి మీ పరికరాల్లో తాజా ప్యాచెస్ మరియు సాఫ్ట్‌వేర్ నవీకరణలు ఇన్‌స్టాల్ చేయబడ్డాయని నిర్ధారించుకోండి.