Поради щодо безпечного користування загальнодоступним Wi-Fi

Шахраї можуть скористатися вашим перебуванням в Інтернеті. Прочитайте нижче кілька порад, щоб вирішити, чи варто використовувати загальнодоступний Wi-Fi.

В результаті спалаху коронавірусу та закриття бізнесу та бібліотек багато хто з нас проводить більше часу в Інтернеті. Тому нам може знадобитися загальнодоступний Wi-Fi для підключення до Інтернету. Якщо у вас виникне потреба використати загальнодоступний Wi-Fi, будь ласка, врахуйте такі рекомендації від Chief Privacy Officer (головного спеціаліста з питань конфіденційност) і, щоб допомогти захистити свої дані:

1. Переконайтеся, що ви використовуєте правильну мережу.

Переконайтеся, що ви підключаєтесь до потрібної мережі. Шахраї можуть створювати мережі, які виглядають нешкідливими за своєю назвою, але насправді націлені на те, щоб побачити ваш Інтернет-серфінг. Це означає, що якщо ви будете вводити облікові дані або паролі для входу на веб-сайти, хакер зможе вкрасти вашу інформацію. Щоб захиститись від цього, уважно прочитайте назву мережі та, якщо можливо, попросіть співробітника або самостійно перевірте назву компанії, щоб переконатися, що мережа є законною.

Популярні мережі Wi-Fi, що належать до відомих мереж кав'ярень, ймовірно, викликають менше підозри, оскільки компанія надає послугу підключення до Wi-Fi в рамках свого бізнесу. Відомі мережі, як правило, безпечніші, ніж випадкові загальнодоступні мережі Wi-Fi, які можуть відображатися на вашому телефоні в громадському місці.

2. Вимкніть автоматичне підключення.

Багато пристроїв (смартфони, ноутбуки та планшети) мають налаштування автоматичного підключення. Воно дозволяє вашим пристроям зручно підключатися

до довколишніх мереж. Це налаштування підходить для надійних мереж, але воно також може підключати ваші пристрої до мереж, які можуть бути небезпечними. Ви можете вимкнути цю функцію у налаштуваннях на своєму пристрої. Тримайте цю функцію вимкненою, особливо коли ви подорожуєте в незнайомі місця. В якості додаткової перестороги ви можете вибрати налаштування «забути мережу» після використання загальнодоступного Wi-Fi.

Ви також повинні стежити за своїм Bluetooth під час перебування в громадських місцях. Підключення Bluetooth дозволяє різним пристроям зв'язуватись один з одним, і хакер може шукати відкриті Bluetooth, щоб отримати доступ до ваших пристроїв. Тримайте цю функцію на телефоні та інших пристроях вимкненою, ко знаходитесь у незнайомому місці.

3. Вимкніть обмін файлами.

Переконайтесь, що функцію обміну файлами вимкнено під час використання загальнодоступного Wi-Fi. Ви можете вимкнути обмін файлами в налаштуваннях системи або на панелі управління, залежно від вашої операційної системи. AirDrop - приклад функції обміну файлами, яку вам слід вимкнути. Деякі операційні системи, такі як Windows/ПК, вимкнуть обмін файлами для вас, коли ви виберете опцію «загальнодоступна» при першому підключенні до нової загальнодоступної мережі.

Кроки вимкнення обміну файлами

На ПК:

1. Перейдіть до Центру управління мережами та обміну файлами.
2. Потім виберіть «Змінити розширені налаштування обміну файлами».
3. Вимкніть обмін файлами та спільний доступ до принтерів.

На Macs:

1. Перейдіть до Налаштувань системи.
2. Оберіть «Спільний доступ».
3. Скасуйте вибір всього.
4. Далі в Шукачі натисніть AirDrop і виберіть «Дозволити побачити мене через»: Нічого.

Для iOS просто знайдіть AirDrop в Центрі управління та вимкніть його.

4. Використовуйте VPN.

Розгляньте варіант встановлення VPN (віртуальної приватної мережі) на своєму пристрої. VPN – це найбезпечніший спосіб збереження цифрової конфіденційності на загальнодоступному Wi-Fi. Він зашифровує ваші дані під час передачі на ваш пристрій і з нього та виконує функцію захисного «тунелю», щоб ваші дані не можна було побачити під час проходження через мережу.

5. Попередження FBI (ФБР) про зашифровані веб-сайти – HTTPS.

FBI (ФБР) попереджає про веб-сайти з адресами, які починаються з «https». Наявність «https» та піктограми блокування має означати, що веб-трафік зашифрований та що відвідувачі можуть безпечно обмінюватися даними. Однак кіберзлочинці зараз грають на довірі людей, заманюючи їх на шкідливі веб-сайти, які містять «https» та виглядають захищеними, але це оманливе враження.

Рекомендації FBI (ФБР):

- Не довіряйте імені в електронних листах: ставте під сумнів наміри, заявлені в електронному листі.
- Якщо ви отримаєте підозрілий електронний лист із посиланням від відомого контакту, переконайтеся, що повідомлення є законним, зателефонувавши або надіславши електронний лист. Не відповідайте безпосередньо на підозрілий електронний лист.
- Перевіряйте наявність помилок або неправильних доменів у посиланні (наприклад, якщо адреса, яка повинна закінчуватися на «.gov», закінчується на «.com»).
- Не довіряйте веб-сайту лише тому, що він містить значок блокування або «https» в адресному рядку браузера.

6. Не рекомендується передавати конфіденційну інформацію.

Навіть якщо у вас є VPN, все одно не рекомендується отримувати доступ до особистих банківських рахунків або передавати подібні конфіденційні особисті дані, такі як номери соціального страхування, в незахищених загальнодоступних мережах. Навіть загальнодоступні захищені мережі можуть бути небезпечні. Добре подумайте перед тим, як отримувати доступ до цих облікових записів на загальнодоступному Wi-Fi. Для фінансових операцій краще використовувати функцію точки доступу на вашому смартфоні.

7. Захищені проти незахищених.

Є два види загальнодоступних мереж Wi-Fi: захищені та незахищені.

Якщо можливо, підключайтеся до захищених загальнодоступних мереж. До незахищеної мережі можна підключити без будь-якої функції захисту, такої як пароль або логін. Захищена мережа зазвичай вимагає, щоб користувач погодився з положеннями та умовами, зареєстрував обліковий запис або ввів пароль перед підключенням до мережі.

8. Тримайте брандмауер увімкненим.

Якщо ви користуєтесь ноутбуком, тримайте брандмауер увімкненим під час роботи через загальнодоступний Wi-Fi. Брандмауер діє як бар'єр, який захищає ваш пристрій від загроз з боку зловмисних програм. Користувачі можуть вимкнути брандмауер Windows через спливаючі вікна та сповіщення, а потім забути про це. Якщо ви хочете перезапустити його на ПК, перейдіть на Панель управління, «Система та безпека» та виберіть «Брандмауер Windows». Якщо ви користуєтеся Mac, перейдіть до «Налаштування системи», потім «Безпека та конфіденційність», а потім на вкладку «Брандмауер», щоб увімкнути цю його.

9. Використовуйте антивірусну програму.

Також обов’язково встановіть на свій ноутбук останню версію антивірусної програми. Антивірусні програми можуть допомогти захистити вас під час використання загальнодоступного Wi-Fi, виявивши зловмисне програмне забезпечення, яке може потрапити у вашу систему під час використання загальнодоступної мережі. Програма буде попереджати, якщо на ваш пристрій будуть завантажуватися відомі віруси чи виникатиме якась підозріла активність, атака, або якщо зловмисне програмне забезпечення потрапить у вашу систему.

10. Використовуйте двофакторну або багатофакторну автентифікацію.

Використовуйте багатофакторну автентифікацію (MFA) під час входу на веб-сайти з вказанням своєї особистої інформації. Це означає, що у вас є другий код підтвердження (надісланий у вигляді текстового повідомлення на телефон або наданий додатком або фізичним ключем), який додатково захищає вас. Тож навіть якщо хакер отримає ваше ім’я користувача та пароль, він не зможе отримати доступ до ваших облікових записів без коду автентифікації.

11. Слідкуйте за своїми особистими пристроями.

Не залишайте ноутбук, планшет чи смартфон без нагляду в громадському місці чи транспортному засобі. Навіть якщо ви вживаєте запобіжних заходів у мережі Wi-Fi, це не перешкоджає комусь забрати вашу власність чи переглянути вашу інформацію. Будьте обізнані щодо вашого оточення і пам'ятайте про людей довкола.

12. Інші поради щодо безпеки в Інтернеті.

Ось кілька порад щодо безпеки в Інтернеті, особливо якщо ви користуєтесь загальнодоступним Wi-Fi:

- Використовуйте надійні паролі.
- Зашифровуйте свої пристрої.
- Остерігайтеся фішингових листів.
- Ставтеся розсудливо до того, що публікуєте в соціальних мережах. Занадто багато особистих даних може допомогти хакерам відгадати паролі.
- Видаляйте стару інформацію, яка вам більше не потрібна.
- Якщо мережа вимагає встановити додаткове програмне забезпечення або розширення браузера, не підключайтеся.
- Переконайтеся, що на ваших пристроях встановлені останні виправлення та оновлення програмного забезпечення, щоб захистити вас від відомих проблем.