БЕЗПЕЧНЕ КОРИСТУВАННЯ ГРОМАДСЬКОЮ ТА ДОМАШНЬОЮ МЕРЕЖЕЮ WI-FI

Божкевич А. Є., Онищенко Ю.М.
Харківський університет внутрішніх справ, Харків, Україна

Сьогодні мережа Wi-Fi широко поширена по всій земній кулі і неможливо уявити і дня без користування нею. Бездротова мережа сучасності дозволяє нам незалежно від місця знаходження завжди бути онлайн: обмінюватися даними, відправляти і приймати пошту, знаходити потрібну інформацію в мережі Інтернет. Бездротові мережі зручні і добре захищені, що дає можливість використання мережевих технологій цього типу і в домашніх умовах [1]. Користування Wi-Fi вдома передбачає наявність роутера, що, власне, «роздає» Wi-Fi. Саме налаштування цього пристрою є необхідною умовою безпеки. Якщо не приділити увагу цьому важливого питанню, зловмисники можуть отримати контроль над каналами передачі даних, вкрасти конфіденційну інформацію, гроші, обмежити та/або позбавити користувача доступу до мережі Інтернет. Безпека домашньої мережі – це набагато більше, ніж встановлення пароля для домашнього Wi-Fi. Члени вашої родини дивляться свої улюблені шоу на Smart TV, купують різні товари в інтернеті, грають в мережеві ігри або працюють вдома. При цьому всі види важливих даних – особиста інформація, паролі, адреси, приватні фотографії тощо – постійно підключені до інтернету через домашню мережу.

Більшість користувачів мережі Інтернет знає про такі поняття, як "фішинг" та "шкідливе програмне забезпечення", які хакери використовують, щоб замаскувати себе та отримати доступ до домашньої мережі для крадіжки або знищення персональних даних. Але чи справді усі користувачі обізнані з тим, що це насправді і як з цим боротися? Безпека домашньої мережі – це фундаментальна основа для захисту себе та родини від загроз з боку зловмисників. Існують певні правила, дотримуючись яких, можна з легкістю захистити власну інформацію від витоку у мережі. Перш за все, налаштовуючи роутер, треба зважати на такі аспекти, що є складовими високого рівня кібербезпеки «домашньої» мережі, адже визначають те, як і коли роутер буде дозволяти пристроям користуватися Wi-Fi:

1. Спершу змініть стандартні налаштування логіна і пароля, що встановленні виробником із заводу.

2. Змініть тип шифрування на WPA2 / WPA, що зробить передачу даних мережею більш захищеною.

3. Керуйте списком пристроїв що користуються Вашою Wi-Fi мережею через визначення MAC-адрес пристроїв що можуть до неї під'єднуватися.

4. Вимкніть функцію WPS (QSS) – ця функція спрощує підключення нових пристроїв до мережі. Якщо Wi-Fi користуються з одних і тих самих гаджетів, краще відключити цю функцію, оскільки вона має серйозні уразливості.

5. Приховайте свою мережу від пристроїв які сканують простір в пошуках мереж. Ідея полягає у тому, що якщо Wi-Fi мережу не бачать, то вірогідність того що її захочуть «зламати» суттєво знижується [2].

Слід зауважити, що сучасні технології дають нам можливість користуватись мережею Wi-Fi не лише вдома, а й в громадських місцях. Сьогодні підключитися до безкоштовних мереж Wi-Fi можна у багатьох закладах харчування, в парках, громадському транспорті, торговельних центрах і навіть в укриттях. Для багатьох українців це зручний та вигідний спосіб отримати доступ до мережі Інтернет та бути постійно на зв'язку [1].

Однак, варто пам'ятати, що переважна більшість Wi-Fi мереж у громадських місцях мають дуже низький рівень захисту від злому. Отже, отримавши доступ до керування ними, шахраї можуть отримати доступ до конфіденційної інформації користувачів у тому числі до логінів та паролів від облікових записів, якими кожен з нас активно користується.

Для того, щоб не потрапити на гачок шахраїв, необхідно дотримуватися простих правил безпеки при роботі з громадськими Wi-Fi мережами. Ці правила стосуються всіх видів пристроїв – ПК, планшетів, смартфонів: встановіть антивірус; використовуйте VPN-сервіси; краще підключатися до мереж Wi-Fi вручну; обмежте можливість автоматичного підключення пристрою. Це можна зробити в налаштуваннях ноутбука або смартфону; якщо є можливість, уточніть назву мережі, до якої маєте намір під'єднатися; пам'ятайте – кібершахраї можуть створювати фейкові мережі для заволодінням інформацією; вимкніть функцію надання спільного доступу до файлів через локальну мережу на всіх пристроях; при підключенні до громадського Wi-Fi вони можуть стати доступними зловмисникам; уникайте здійснення грошових операцій: перекази, покупки, регулярні платежі. Не використовуйте загальнодоступні мережі Wi-Fi для обміну чутливою конфіденційною інформацією і вирішення важливих справ; краще скористатися перевіреною стаціонарною мережею або мобільним інтернетом; відвідуйте сайти, що використовують безпечний протокол з'єднання HTTPS; вимкніть загальний доступ до файлів і папок на пристрої що буде приєднуватися до відкритої Wi-Fi мережі.

Отже, можна зробити висновок, що сьогодні більшість користувачів перебувають онлайн майже цілодобово. Значною мірою на це вплинула наявність загальнодоступних Wi-Fi у громадських місцях та активним користуванням мережею в домашніх умовах [2]. Враховуючи той факт, що протягом наступних кількох років Wi-Fi обіцяють зробити безпечнішим, наразі досі залишається актуальним питання щодо збереження своєї цифрової безпеки в кіберпросторі.

Список літератури

1. Бездротові мережі (Wi-Fi). URL: https://i-help.us/adjustment/wifi/
2. Wi-Fi безпека: вдома та в громадських місцях. URL: https://zillya.ua/index.php?q=wi-fi-bezpeka-vdoma-ta-v-gromadskikh-mistsyakh