Загальнодоступна мережа Wi-Fi

Учасники дізнаються про загальнодоступні мережі Wi-Fi, їх переваги й ризики. Тобто вони навчаться розпізнавати незахищені доступні мережі Wi-Fi, дізнаються про негативні сторони користування незахищеними Wi-Fi-підключеннями та навчаться приймати обґрунтовані рішення щодо того, коли підключатися до незахищеної мережі Wi-Fi і використовувати її.

Ресурси

Зображення безпровідного модема
Роздатковий матеріал щодо безпеки підключення

Що таке Wi-Fi?

Частина 1

Запитайте учнів

Які пристрої ви використовуєте для доступу до Інтернету?

Як ці пристрої підключаються до Інтернету?

Image Class Interaction

Wi-Fi – це стандартний спосіб підключення пристроїв до Інтернету. Wi-Fi використовує радіосигнали для підключення пристроїв без фізичного або проводового зв’язку.

Уявіть, що у вас вдома є три ноутбуки, які ви хочете підключити до Інтернету. Щоб підключитися до Інтернету через Wi-Fi, вам потрібно нижченаведене.

1. Точка доступу. Точка доступу – це пристрій, який передає сигнал Wi-Fi і забезпечує доступ до Інтернету. Для підключення до Інтернету пристроям потрібно розпізнати ці сигнали. Іноді може знадобитися спеціальний дозвіл (наприклад, ім’я користувача й пароль), щоб увійти в мережу та використовувати сигнал безпровідного зв’язку, який передає точка доступу.

2. Маршрутизатор. Маршрутизатор – це пристрій, який створює мережу між усіма пристроями (наприклад, комп’ютерами, планшетами, мобільними телефонами) у певному розташуванні (наприклад, у школі, бібліотеці або у вас удома). Зазвичай точку доступу вбудовано в маршрутизатор (див. схему нижче).

> Маршрутизатори мають обмежений (зазвичай короткий) діапазон. Тому якщо пристрій розташовано далеко від маршрутизатора, він отримає слабкий сигнал Wi-Fi або не отримає його взагалі. Крім того, якщо між пристроєм і маршрутизатором є перешкода (наприклад, будівля або цегляна стіна), вона зменшить силу сигналу.
>
> Хоча підключення до маршрутизатора забезпечує доступ до мережі, це ще не доступ до Інтернету. Щоб кілька пристроїв у мережі могли підключатися до Інтернету, маршрутизатор має бути під’єднано до модема.

3. Модем. Модем – це пристрій, який створює та підтримує підключення до інтернет-провайдера, щоб надати вам доступ до Інтернету. Він перетворює сигнали ззовні в сигнали, які може розпізнати комп’ютер або інші цифрові пристрої.

У типовому налаштуванні точка доступу та маршрутизатор – єдиний пристрій, фізично під’єднаний до модема за допомогою кабелю Ethernet. Таке підключення мається на увазі, коли йдеться про "проводове" підключення до Інтернету.

Мобільні пристрої також можуть використовувати стільниковий зв’язок для підключення до Інтернету, особливо поза школою, бібліотекою чи домом. Стільниковий зв’язок – це вид безпровідного радіосигналу, який має набагато більшу зону покриття, ніж маршрутизатор. Для підключення мобільного пристрою до Інтернету за допомогою стільникового зв’язку використовуються спеціальні приймачі-передавачі, які називаються базовими станціями.

Частина 2

Запитайте учнів

Які переваги має Wi-Fi?

Які недоліки має Wi-Fi?

Які проблеми з безпекою можуть виникнути під час використання Wi-Fi у порівнянні із проводовим інтернет-підключенням?

Чому ви втрачаєте доступ до Wi-Fi на телефоні, коли залишаєте будинок?

Вибір мережі Wi-Fi

Частина 1

Запитайте учнів

Чи всі мережі Wi-Fi безпечні? Чому так і чому ні?

Розкажіть учням

Іноді ви можете вибрати мережу Wi-Fi, яку хочете використовувати. Важливо пам’ятати, що ви наражаєтеся на серйозні ризики, якщо підключитеся до неправильної мережі. Наприклад, незахищені мережі Wi-Fi не вимагають пароль під час входу. Якщо ви перебуваєте в незахищеній мережі, інші користувачі в тій самій мережі можуть переглядати вашу інформацію. Вони можуть викрасти інформацію, яку ви надсилаєте через мережу, або стежити за тим, що ви робите.

Натомість захищені та надійні мережі Wi-Fi – це мережі, які вимагають пароль і підтримують шифрування даних, а також мережі, щодо яких ви впевнені, що їх назва представляє саме ту мережу, у яку ви входите. Наприклад, коли ви входите в мережу, яка називається іменем школи (але не є мережею школи), це може призвести до розкриття інформації про обліковий запис. Саме безпечні та надійні мережі пропонують найбільший захист.

Слід враховувати контекст або розташування мережі Wi-Fi. Наприклад, якщо ви перебуваєте в кінотеатрі й бачите на телефоні назву мережі своєї школи, коли шукаєте підключення до Wi-Fi, можете вважати, що ця мережа намагається імітувати або "підробляти" мережу школи, щоб збирати паролі з довірливих учнів.

Під час налаштування захищеної паролем мережі Wi-Fi її власник повинен увімкнути протокол шифрування маршрутизатора. Загальні протоколи шифрування – це Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) або WPA2. За допомогою цих протоколів інформація, яка надсилається по безпровідній мережі, шифрується.

Шифрування створено для того, щоб хакери не могли побачити, що ви надсилаєте Проте всі протоколи (WEP, WPA і WPA2) виявилися вразливими до хакерства. Тому важливо покладатися на безпечні веб-підключення для передачі інформації в Інтернеті.

HTTPS – це стандарт, який використовують веб-сайти для шифрування даних, що передаються через Інтернет. Шифрування може завадити третій стороні легко переглядати дані з вашого підключення. Воно гарантує додатковий рівень безпеки. Цей стандарт можна використовувати в будь-якому веб-браузері,

додаючи "https: //" перед URL-адресою, яку ви використовуєте (наприклад, https://www.mysite.com). Проте не всі веб-сайти підтримують протокол HTTPS.

1. Вводьте конфіденційну інформацію (наприклад, пароль, інформацію кредитної картки) тільки на веб-сторінках із префіксом HTTPS://.

2. Більшість стандартних браузерів мають індикатори безпеки у вигляді замка біля адресного рядка. Вони вказують на HTTPS-підключення.

3. На жаль, HTTPS не гарантує повну безпеку, оскільки деякі шкідливі веб-сайти можуть також підтримувати HTTPS. Стандарт HTTPS захищає підключення, але не гарантує, що сайт є надійним.

Розкажіть учням

Безпеку стандарту HTTPS гарантує технологія Secure Sockets Layer (SSL)/Transport Layer Security (TLS). SSL/TLS використовує цифрові ключі шифрування, які працюють, як справжні ключі. Якщо ви написали секрет на аркуші паперу для друга, той, хто знайшов папірець, зможе побачити цей секрет. А тепер уявіть, що ви особисто дали другу копію ключа та надіслали секрети в закритій скрині. Якщо хтось перехопить скриню, цій особі буде важко побачити секрет без ключа. Якщо хтось спробує підмінити скриню подібною, ви помітите, що ключ не працює. Протокол SSL/TLS функціонує так само, але з веб-сайтом.

Індикатори безпеки браузера також повідомлятимуть інформацію про сертифікат розширеної перевірки (EV). Сертифікати EV видаються веб-сайтам, що підтвердили свою ідентифікацію в органі сертифікації. Іноді в браузерах індикатор EV відображається біля рядка адреси як назва сайту або органу реєстрації. Якщо вміст певного веб-сайту здається підозрілим, ви можете перевірити, чи збігається URL-адреса в сертифікаті з URL-адресою у веб-браузері. Для цього скористайтеся функцією "Переглянути сертифікат". [Варто на екрані проектора показати учасникам, як знайти функцію "Переглянути сертифікат"]. Навігація до цієї функції залежить від браузера. Наприклад, у Chrome потрібно відкрити меню "Вид", "Розробник", "Інструменти розробника". У меню "Інструменти розробника" виберіть вкладку "Безпека", потім – "Переглянути сертифікат".

Запитайте учнів

Про що варто подумати під час підключення до нової мережі?

1. Можливі відповіді: розташування (тобто кому належить мережа), доступ (хто ще може підключитися до мережі) і дія (що ви збираєтеся робити в мережі).

Кому належить ваша домашня мережа Wi-Fi? А шкільна мережа? А мережа в кав'ярні?

1. Домашня мережа Wi-Fi належить батьками чи опікунам, шкільна мережа належить адміністраторам чи дирекції школи, а мережа в кав'ярні належить власнику кав'ярні.

Ви знаєте цих людей особисто? Ви довіряєте цим людям?

1. Залучіть учасників до обговорення про різні рівні довіри до цих людей.

Розкажіть учням

Ви маєте знати власника мережі Wi-Fi і довіряти йому. Іноді можна визначити власника мережі за ідентифікатором SSID.

Ідентифікатор SSID – це ім'я мережі Wi-Fi, яке ви бачите, коли намагаєтеся підключитися. Цей ідентифікатор часто повідомляє, кому належить мережа, а також містить відомості по неї. Будьте обережні, тому що майже всі люди (які знають, як це робиться) можуть створити SSID. Наприклад, хтось може створити SSID, що збігається з ідентифікатором, який ви використовуєте в школі. Це приклад видавання мережі за відому та довірену мережу для потенційного збору імен користувачів і паролів.

Якщо ви знаєте, кому належить мережа, ви можете визначити, чи вона безпечна. Якщо вона належить особі або організації, яким ви довіряєте, ви, скоріше за все, можете спокійно підключитися до неї. Проте, якщо мережа невідома, не варто з'єднуватися з нею, оскільки ви не знаєте, кому належить маршрутизатор, до якого ви підключаєтеся. Оскільки весь трафік мережі проходить через маршрутизатор, власник може відстежувати та записувати його повністю.

Коли ви з'єднуєтеся з мережею Wi-Fi, пристрій підключається до локальної мережі пристроїв, яка зв'язана з Інтернетом. Оскільки ваш пристрій обмінюється інформацією через цю мережу, важливо, щоб ви довіряли іншим пристроям, до яких ви підключені, тобто кожному пристрою в мережі. Так само, як під час групової роботи в школі, ви повинні довіряти кожному учаснику, з яким ви працюєте.

Використання пароля для мережі обмежує коло людей, які можуть до неї підключитися. Це означає, що ви краще знатимете, хто перебуває в цій мережі (сім'я, друзі або інші клієнти кав'ярні), ніж у випадку з відкритою мережею.

Рішення щодо приєднання до мережі, яка виглядає підозрілою, має базуватися на компромісах, на які ви готові піти в плані безпеки в Інтернеті. Вам потрібно

подумати, чи готові ви ризикнути зламом свого облікового запису, щоб підключитися до доступної мережі?

Запитайте учнів

Чи варто читати новини або блог в Інтернеті, використовуючи домашню мережу Wi-Fi? А шкільна мережа? А мережа в кав'ярні?

1. Поясніть, що вміст веб-сторінки зазвичай не містить конфіденційної інформації. Ви можете робите це в будь-якій мережі.

Чи варто надсилати номер кредитної картки, використовуючи домашню мережу Wi-Fi? А шкільна мережа? А мережа в кав'ярні? Чому?

1. Організуйте дискусію навколо питання, чому найбільш безпечно робити це через домашню мережу Wi-Fi і чому небезпечно через мережу в кав'ярні. Також обговоріть таку тему: хоча мережа школи, ймовірно, є надійною, не варто ризикувати, тому що саме ця інформація є надзвичайно конфіденційною.

Чи варто перевіряти електронну пошту, використовуючи домашню мережу Wi-Fi? А шкільна мережа? А мережа в кав'ярні?

1. Обговоріть, що найбезпечніше це робити через домашню мережу, залежно від вмісту облікового запису електронної пошти Наприклад, деякі люди мають кілька облікових записів електронної пошти, які вони використовують для різних цілей (наприклад, електронні листи з маркетингом і рекламою вони отримують в одному обліковому записі, а інший обліковий запис використовують для листування з друзями та родичами).

Розкажіть учням

Конфіденційні дані, зокрема паролі та банківську інформацію, краще передавати та переглядати в приватній і захищеній мережі на веб-сайтах, що використовують протокол SSL/TLS, а не в спільній загальнодоступній мережі. Ця приватна інформація буде під загрозою, якщо ви надішлете її або отримаєте доступ до неї в спільній мережі, яку використовують люди, яких ви не знаєте та яким не довіряєте.

Визначення конфіденційності інформації може бути неоднозначним, оскільки конфіденційність є особистим рішенням, яке ви приймаєте самостійно. Важливо розглядати кожну ситуацію окремо, щоб вирішити, чи потрібно підключитися до мережі. Перш ніж приймати рішення щодо підключення, запитайте себе, чи ви довіряєте власнику мережі, людям пов'язаним із ним, які дії ви виконуєте в

Інтернеті та якою інформацією ви ділитесь.

Захищені та незахищені мережі

Частина 1

Взаємодія в групі

Візьміть до уваги наведене нижче. Частину вмісту цього уроку розглянуто в уроці №2 "Вибір мережі Wi-Fi". Вам вирішувати, чи хочете ви ще раз ознайомитися з цим матеріалом або волієте пропустити його.

Розкажіть учням

Як говорилося раніше, незахищені мережі Wi-Fi не вимагають пароль під час входу. Якщо ви використовуєте незахищені мережі, ви наражаєте на ризик дані, які передаєте й отримуєте через мережу.

Захищені мережі Wi-Fi вимагають пароль під час входу та підтримують шифрування даних. Особа, яка налаштовувала мережу, вирішує, вмикати шифрування чи ні. Шифрування кодує інформацію, яку ви надсилаєте й отримуєте через мережу, тому хакерам у тій самій мережі Wi-Fi набагато важче побачити, що ви надсилаєте чи отримуєте.

Захищена мережа не означає, що дані в безпеці. Звісно, використовувати цю мережу безпечніше, ніж незахищену. Проте вмілий хакер все одно може знайти спосіб отримати доступ до персональної інформації.

Є три стандартних протоколи шифрування. Це Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) або WPA2. WEP та WPA застарілі, тому мережі, які їх використовують, слід вважати незахищеними. Крім того, протокол WPA2 також виявився вразливим до хакерства.

Щоб бути впевненими, що ваша інформація повністю захищена, переконайтеся, що веб-сайти, які ви використовуєте, зашифровані за допомогою технології SSL/TLS.

Запитайте учнів

Надайте приклади захищених мереж, які ви раніше використовували.

1. Деякі приклади включають домашні мережі Wi-Fi, шкільні мережі, а також загальнодоступні мережі, наприклад у кав’ярнях.

Надайте приклади незахищених мереж, які ви раніше використовували.

А приклади захищених?

Розкажіть учням

Щоб перевірити, чи мережа Wi-Fi зашифрована, перегляньте налаштування мережі чи налаштування безпровідного з’єднання на своєму пристрої.

Частина 2

Взаємодія в групі

Для підготовки до цієї частини пошукайте в Інтернеті, як перевірити типи шифрування мережі Wi-Fi в різних операційних системах. Потім продемонструйте, як дізнатись, який тип шифрування використовує мережа. Наприклад, у MacOS виберіть "Налаштування системи" -> "Мережа" -> "Вибрати Wi-Fi". Потім виберіть ім’я відповідної мережі. На вкладці Wi-Fi ви побачите список відомих мереж і стовпець, що містить дані про шифрування, яке використовується в мережі.

Розкажіть учням

Не всі підключення однакові. До незахищеної мережі може підключитися будь-хто, і невідомо, хто її контролює. Приєднуючись до незахищеної мережі, ви стаєте вразливими, оскільки інформація, яку ви надсилаєте й отримуєте, а також увесь веб-трафік (сторінки, паролі тощо) може переглянути будь-хто в мережі, якщо ви не використовуєте SSL/TLS-підключення.

Взаємодія в групі

Залежно від технічної обізнаності учасників ви можете обговорити використання віртуальних приватних мереж як додаткового рівня безпеки під час використання Wi-Fi. Додаткову інформацію див. за посиланнями про VPN у розділі "Ресурси".

Усвідомлення безпеки підключення

Заголовок частини

Взаємодія в групі

Розділіть учасників на групи по 2–3 особи. Роздайте учасникам матеріали до уроку "Безпека підключення" та призначте сценарій кожній групі. Дайте учасникам 5 хвилин на обговорення сценаріїв. Потім попросіть групи обмінятися відповідями. Відповіді позначено зеленим у роздатковому матеріалі.

Завдання

Частина 1

Завдання

Попросіть учасників виконати нижченаведені завдання.

1. Намалюйте часову шкалу звичайного дня, позначаючи мережі Wi-Fi, до яких підключаються учасники.

2. З вибраних мереж, зображених на часовій шкалі, учасники мають обрати дві та коротко описати їх. Хто ще підключається до цих мереж? Наскільки вони безпечні?

3. Крім того, для двох обраних мереж учасники мають описати, які можливості надають ці підключення та які ризики з ними пов’язані.