Советы по безопасному использованию общественных сетей Wi-Fi

Злоумышленники могут воспользоваться соединением, чтобы похитить ваши данные. Ознакомьтесь с рядом советов, приведенных ниже, и подумайте, нужно ли вам использовать общественные сети Wi-Fi.

В связи со вспышкой коронавируса и закрытием предприятий и библиотек, многие из нас проводят больше времени онлайн. В результате для подключения к интернету нам может понадобиться общественный Wi-Fi. Если Вам действительно необходимо использовать общественный Wi-Fi, пожалуйста, рассмотрите следующие рекомендации от руководителя службы по защите конфиденциальной информации, чтобы помочь защитить ваши данные:

1. Убедитесь в подключении к правильной сети.

Убедитесь, что вы подключаетесь к нужной сети. Злоумышленники могут создавать сети, которые выглядят безобидными, исходя из их названия, но на самом деле предлагают вам подключиться к сети, чтобы увидеть ваш веб-серфинг. Это означает, что при вводе учетных данных или паролей для входа на веб-сайт хакер сможет украсть вашу информацию. Чтобы защититься от этого, внимательно читайте название сети и по возможности спросите название у сотрудника или проверьте вывеску компании, чтобы убедиться, что сеть является законной.

Хорошо известные сети, такие как сети известных кофеен, вероятно, менее подозрительны, поскольку компания использует сеть в качестве услуги для своей деятельности. Известные сети, как правило, безопаснее, чем случайные бесплатные сети Wi-Fi, которые могут отображаться на вашем телефоне в общественном месте.

2. Отключите автоподключение.

Многие устройства (смартфоны, ноутбуки и планшеты) имеют настройки автоматического подключения. Эта настройка позволяет вашим устройствам легко подключаться к ближайшим сетям. Эта функция удобна для защищенных сетей, но благодаря ей устройства также могут подключаться к сетям, которые могут быть небезопасными. Эту функцию можно отключить в настройках вашего устройства. Выключайте эту функцию, особенно когда едете в незнакомое место. В качестве дополнительной меры предосторожности после использования общественной сети Wi-Fi можно нажать «Забыть сеть».

Также следует следить за Bluetooth-соединением в общественных местах. Соединение Bluetooth позволяет различным устройствам связываться друг с другом, и хакер может искать доступные сигналы Bluetooth, чтобы получить доступ к вашим устройствам. Выключайте данную функцию на телефоне и других устройствах, когда находитесь в незнакомом месте.

3. Отключите общий доступ к файлам.

Убедитесь, что вы отключили функцию общего доступа к файлам при использовании общественной сети Wi-Fi. Вы можете отключить общий доступ к файлам в системных настройках или на панели управления, в зависимости от вашей операционной системы. AirDrop — это пример функции обмена файлами, которую лучше отключить. Некоторые операционные системы, такие как Windows / PC, отключат общий доступ к файлам на вашем устройстве, выбрав профиль “Общедоступная сеть” при подключения к новой общественной сети впервые.

Шаги по отключению общего доступа к файлам.

На ПК:

1. Перейдите в Центр управления сетями и общим доступом.
2. Затем выберите Изменить расширенные настройки общего доступа.
3. Отключите общий доступ к файлам и принтерам.

Для Mac:

1. Перейдите в Системные настройки.
2. Выберите Общий доступ.
3. Снимите отметку напротив всех пунктов.
4. Далее в Finder нажмите AirDrop, и выберите Разрешить мое обнаружение: Никому.

Для iOS, просто найдите AirDrop в Центре управления и выключите его.

4. Используйте VPN.

Подумайте об установке VPN (виртуальная частная сеть) на ваше устройство. VPN является наиболее безопасным вариантом для сохранения цифровой конфиденциальности при использовании общественной сети Wi-Fi. Он шифрует ваши данные при передаче их на ваше устройство и с него и действует в качестве защитного “туннеля”, поэтому ваши данные не видны при передачи между элементами сети.

5. Предупреждение FBI о зашифрованных сайтах - HTTPS.

FBI предупредило о веб-сайтах, адреса которых начинаются с “https”. Наличие “https” и значка замка должны указывать на то, что веб-трафик зашифрован и что посетители могут безопасно обмениваться данными. Тем не менее, киберпреступники рассчитывают на доверие общественности, заманивая людей на вредоносные веб-сайты, которые содержат https и выглядят безопасными, хотя это не так.

Рекомендации FBI:

- Не доверяйте слепо названию в электронном письме: поставьте под сомнение содержимое электронного письма.
- Если вы получили подозрительное электронное письмо со ссылкой от известного вам отправителя, подтвердите его подлинность, позвонив или отправив письмо отправителю. Не отвечайте на подозрительные письма напрямую.
- Проверьте наличие орфографических ошибок или неправильных доменов в ссылке (например, если адрес, который должен заканчиваться на “.gov” заканчивается на “.com”).
- Не доверяйте веб-сайту только потому, что в адресной строке браузера есть значок замка или «https».

6. Не рекомендуется осуществлять доступ к конфиденциальной информации.

Даже если у вас установлен VPN, в незащищенных общественных сетях по-прежнему не рекомендуется осуществлять доступ к личным банковским счетам или аналогичным конфиденциальным личным данным, таким как номера социального страхования. Даже защищенные общественные сети могут быть небезопасны. Тщательно обдумайте, стоит ли осуществлять доступ к этим аккаунтам, используя общественную сеть Wi-Fi. Что касается финансовых операций, то целесообразнее использовать функцию хот-спот на вашем смартфоне.

7. Защищенная и незащищенная сеть.

Существует два вида общественных сетей Wi-Fi: Защищенные и незащищенные.

По возможности подключайтесь к защищенным общественным сетям. К незащищенной сети можно подключиться без каких-либо средств защиты, таких как пароль или логин. Защищенная сеть обычно требует от пользователя согласия с условиями, регистрации учетной записи или ввода пароля перед подключением к сети.

8. Включайте свой брандмауэр.

Если вы используете ноутбук, то при использовании общественной сети Wi-Fi оставляйте брандмауэр включенным. Брандмауэр служит барьером, защищающим ваше устройство от вредоносного ПО. Пользователи могут отключать брандмауэр Windows из-за всплывающих окон и уведомлений, а затем забыть об этом. Если вы хотите опять включить его на ПК, перейдите в Панель управления “Система и безопасность” и выберите “Брандмауэр Windows”. Если вы пользователь Mac, перейдите в “Системные настройки”, затем “Безопасность и конфиденциальность”, а затем на вкладку “Брандмауэр”, чтобы включить эту функцию.

9. Используйте антивирусное программное обеспечение.

Также убедитесь, что на вашем ноутбуке установлена последняя версия антивирусной программы. Антивирусные программы могут помочь защитить ваше устройство при использовании общественной сети Wi-Fi, обнаруживая вредоносные программы, которые могут проникнуть в вашу систему при использовании сети общего пользования. Сигнал тревоги оповестит вас, если на ваше устройство будут загружены известные вирусы или в случае подозрительной активности, атаки или попадания вредоносного ПО в вашу систему.

10. Используйте двухфакторную или многофакторную аутентификацию.

Используйте многофакторную аутентификацию (MFA) при входе на веб-сайты с вашей личной информацией. Это означает, что у вас есть второй проверочный код (отправленный на ваш телефон или предоставленный приложением или физическим ключом), который дополнительно защищает ваше устройство. Поэтому, даже если хакер

получит ваше имя пользователя и пароль, он не сможет получить доступ к вашим аккаунтам без кода аутентификации.

11. Следите за своими личными устройствами.

Не оставляйте свой ноутбук, планшет или смартфон без присмотра в общественном месте или в автомобиле. Даже если вы принимаете меры предосторожности при подключении к сети Wi-Fi, это не помешает кому-либо забрать вашу собственность или подсмотреть вашу информацию. Будьте осведомлены о своем окружении и внимательны к людям вокруг.

12. Другие советы по безопасности в Интернете.

Вот несколько советов по обеспечению безопасности в Интернете, особенно если вы используете общественную сеть Wi-Fi.

- Используйте надежные пароли.
- Зашифруйте свои устройства.
- Остерегайтесь фишинговых электронных писем.
- Будьте осторожны с тем, что вы публикуете в социальных сетях. Слишком большое количество личных данных поможет хакерам подобрать пароли к вашим аккаунтам.
- Удаляйте старые данные, которые вам больше не нужны.
- Если сеть запрашивает установку какого-либо дополнительного программного обеспечения или расширения браузера, не подключайтесь.
- Убедитесь, что на ваших устройствах установлены последние исправления и обновления программного обеспечения для защиты от известных проблем.