Использование публичного Wi-Fi. Что можно, а чего нельзя?

Владимир Безмалый

Общественный (публичный) Wi-Fi доступен практически везде, от местной кофейни до отелей и аэропортов, которые вы посещаете во время путешествия. Wi-Fi сделал нашу жизнь немного проще, но он также представляет угрозу безопасности для личной информации, доступной на наших ноутбуках и смартфонах. Вот полезный список того, что нужно и чего нельзя делать, если вы планируете использовать общедоступный Wi-Fi.

Есть в основном два вида общественных сетей Wi-Fi: защищенные и незащищенные.

Незащищенная сеть может быть подключена без каких-либо функций безопасности, таких как пароль или логин. И наоборот, защищенная сеть требует, чтобы пользователь согласился с юридическими условиями, зарегистрировал учетную запись или ввел пароль перед подключением к сети. Также может потребоваться плата или покупка в магазине для получения доступа к паролю сети.

В некоторых странах от вас потребуют ввод пароля, для получения которого вам нужно послать SMS на указанный номер. Более того, я встречался с ситуацией, когда в аэропорту такое СМС можно было послать только с местного номера телефона (принадлежащего именно этой стране).

Независимо от типа подключения, вы всегда должны использовать общедоступный Wi-Fi с осторожностью.

Давайте посмотрим на некоторые плюсы и минусы подключения к таким сетям:

- По возможности подключайтесь к защищенным публичным сетям. В случае, если вы не можете

подключиться к защищенной сети, использование незащищенной сети будет допустимо, если подключение требует какого-либо входа или регистрации.

- Не пользуйтесь личными банковскими счетами или конфиденциальными личными данными в незащищенных публичных сетях. Даже защищенные сети могут быть рискованными. Подумайте, а нужен ли вам доступ к учетным записям в общедоступной сети Wi-Fi.
- Не оставляйте свой ноутбук, планшет или смартфон без присмотра в общественном месте. Даже если вы работаете в защищенной сети Wi-Fi, это не помешает кому-либо завладеть вашей собственностью или взглянуть на ваше устройство.
- Не делайте покупки онлайн при использовании общедоступного Wi-Fi. Конечно, покупки, похоже, не связаны с конфиденциальными данными, но для совершения покупок в Интернете требуется личная информация, которая может включать данные банковского счета и логин продавца. Покупки — это не то, что вы хотите делать в незащищенной сети Wi-Fi.
- Как отключить автоматическое подключение? Большинство смартфонов, ноутбуков и планшетов имеют автоматические настройки подключения, которые позволяют беспрепятственно подключаться к одной точке доступа к другой. Это удобная функция, но она также может подключать ваши устройства к сетям, которые вы обычно не используете. Держите эти настройки выключенными, особенно когда вы путешествуете в незнакомых местах.
- Следите за своим Bluetooth-соединением. Bluetooth в домашних условиях — удивительная функция на многих интеллектуальных устройствах. Однако, если Bluetooth включен в общественных местах, это может создать огромный риск для вашей кибербезопасности. Связь Bluetooth позволяет различным устройствам связываться друг с другом, и хакер может искать

открытые сигналы Bluetooth, чтобы получить доступ к вашим устройствам. Держите эту функцию на своем телефоне и других устройствах заблокированными, когда вы выходите из дома, офиса или аналогичной защищенной зоны.

- Подумайте об использовании виртуальной частной сети (VPN), чтобы обеспечить вашу конфиденциальность и анонимность при использовании общественного Wi-Fi. Службы VPN, могут шифровать все данные, которые вы отправляете и получаете, используя общедоступную точку доступа Wi-Fi, защищая вашу информацию от других пользователей того же соединения.

https://ib-bank.ru/bisjournal/news/14383