Поддельные зарядные станции могут взломать ваш смартфон

Владимир Безмалый

Никто не хочет, чтобы батарея разряжалась, когда они в пути. Фактически недавнее исследование показало, что мы проверяем наши телефоны не менее 80 раз в день. Такое отношение стало преобладать в сегодняшнем мире подключений просто потому, что мы используем наши мобильные устройства не только для звонков.

В мире, где мы полагаемся на наши телефоны практически во всём — от онлайн-банкинга и учётных записей электронной почты до социальных сетей, игр и многого другого, — общественные зарядные станции могут стать незаменимыми спасителями, когда у вас разряжается батарея.

Но эксперты по безопасности предупреждают, что зарядка не стоит того, особенно, если зарядная станция настроена для кражи ваших данных.

Что такое Juice Jacking?

Этот взлом заключается в том, что мошенники устанавливают в общественных местах поддельные киоски для зарядки, чтобы украсть данные вашего телефона.

Эти уязвимые киоски также можно запрограммировать для установки вредоносного ПО на ваше устройство.

Общественные зарядные станции часто оснащены несколькими USB-подключениями, чтобы заряжать большее количество смартфонов. Хотя это может показаться дополнительной функцией удобства, большинство зарядных станций также скрывают другой конец этих шнуров и, что более важно, подключённый источник питания.

У связи всегда есть две стороны

Мошенники могут устанавливать поддельные киоски в тех местах, где жертвам потребуется подзарядка на ходу. Но когда вы спешите и ищете только значок зарядки, который появится на вашем телефоне, можно легко не заметить взломанную зарядную станцию.

Данная атака эффективна, потому что манипулирует тем, что мы используем каждый день. Кабели USB позволяют передавать данные и питание между двумя подключёнными устройствами. Хотя они могут выглядеть безобидными, мошенники могут использовать эти кабели для сбора ваших данных, демонстрации вашего экрана или даже заражения вашего устройства.

Другой вариант этого взлома включает «Video Jacking», когда мошенники используют соединение HDMI (в отличие от соединения USB) для взлома ваших смартфонов. Вместо того, чтобы передавать данные при подключении к сети, мошенники используют соединение HDMI для зеркального отображения экрана вашего телефона на другом устройстве. Этот метод взлома можно использовать для сбора конфиденциальной информации, такой как пароли, учетные данные для входа и номера финансовых счетов, путём записи ваших действий на своём телефоне.

Что делать?

Хотя общественные зарядные станции могут быть удобны при низком заряде аккумулятора, воспользуйтесь этими советами, чтобы защитить свои устройства от утечки сока:

- Проверьте источник питания. Самый безопасный способ зарядить телефон — подключить его напрямую к розетке. Не заряжайте телефон в местах, где источник питания плохо виден.
- Принесите свой шнур. Используя собственный шнур, вы можете избежать использования общественной зарядной станции и вместо этого подключитесь к розетке. Вы также можете приобрести USB-кабели с питанием только от источника питания, которые не поддерживают возможность передачи данных.
- Купите внешний аккумулятор. Аккумуляторы работают как портативные источники питания, обеспечивая дополнительную мощность в пути. Кроме того, вы также можете безопасно заряжать внешние батареи на общественных зарядных станциях, не беспокоясь о передаче данных туда и обратно.

Если у вас нет другого выхода, выключите телефон перед подключением к зарядной станции.

https://ib-bank.ru/bisjournal/news/14409