09 декабря 2020

Раскрыт самый популярный способ взлома гаджетов: мнение эксперта по кибербезопасности

Чаще всего злоумышленники добираются до устройств вовсе не с помощью сетей WI-FI.
«Умные устройства», оснащенные Bluetooth, чаще становятся целью интернет-мошенников. В следующем году риски пользователей будут заметно возрастать. Об этом сообщил эксперт по кибербезопасности Андрей Масалович в беседе с изданием Nation News.

Отмечается, что главная проблема подобных гаджетов состоит в редких обновлениях и в стремлении производителей быстрее продать их, не учитывая все уязвимости. Из-за коммерческой составляющей о безопасности думают единицы, поэтому пользователям приходится продумывать этот момент самим.

Тем не менее, большинство людей продолжают использовать заводские настройки «умных устройств», которые уже давно изучены хакерами. Bluetooth легко взломать, и киберпреступники пользуются этим моментом. Чтобы избежать этого, необходимо как можно быстрее изменить все фабричные настройки и пароли после покупки. Также можно оценить, установлены ли на устройстве подозрительные приложения и проследить за

уровнем нагрева гаджета и другими нехарактерными свойствами.

Как сообщила Delovoe.TV **маркетолог департамента ИТ-аутсорсинга ГК «КОРУС Консалтинг» Катерина Комарова**, устройство действительно проще взломать, если в прошивке Bluetooth содержатся уязвимости, позволяющие пройти процедуру сопряжения устройств без контроля пользователя или ОС.

«После того, как к устройству Bluetooth удается подключится в обход, с него можно получить различные данные. Интерес для злоумышленников обычно представляют смартфоны, так как на них хранятся личные фото, контакты, расписание календаря, SMS-переписка. Защититься от такого взлома можно - во-первых, не нужно принимать никаких запросов от незнакомых устройств. Во-вторых, все сессии связи необходимо защищать паролями», – считает **Катерина Комарова, маркетолог департамента ИТ-аутсорсинга ГК «КОРУС Консалтинг»**.

Эксперт также отметила, что многие пользователи действительно уделяют меньше внимания настройкам Bluetooth, чем данным WI-FI. Многие совершают ошибку, оставляя включенный Bluetooth в режиме «доступен всем». Производители стараются ограничить время доступности, но есть и исключения.

Также **Катерина Комарова** дала советы по распознанию подозрительного приложения: «Если в данный момент времени вы не совершаете сопряжение с устройством, а к вам пришел запрос, то это или ошибка, или целенаправленная атака. Если рассматривать приложения, которые устанавливаются через магазин, то тут вероятность получить троянский вирус мала. Это связано с тем, что Bluetooth имеет малый радиус действия».

Источник: Delovoe.TV