Эксперт рассказала, как хакеры получают доступ ко всем системам «умного» дома через зубную щетку

Современные гаджеты для ухода за зубами с Bluetooth-подключением вместе с удобством использования приносят риски для конфиденциальности данных. Эксперты предупреждают, что многие модели собирают информацию о привычках пользователей: от времени чистки и силы нажатия до геопозиции, если щётка подключена к смартфону. Эти данные передаются на серверы производителей, где защита информации далеко не всегда на высоте, пояснила заведующая кафедрой информационной безопасности РТУ МИРЭА Елена Максимова.

Злоумышленники уже научились использовать такие устройства в своих целях. Взломанные щётки могут стать частью вредоносных сетей, применяемых для майнинга, криптовалюты, DDoS-атак или проникновения в другие системы «умного» дома. Кроме того, анализ данных, например, с сенсоров температуры или Bluetooth-соединений, позволяет определить, находится ли человек дома, что увеличивает риск кражи.

Чтобы снизить угрозы, специалисты советуют отключать Bluetooth, когда устройство не используется, и ограничивать доступ приложений к личным данным. Также стоит выбирать гаджеты проверенных брендов, предлагающих надёжное шифрование информации. Такие меры помогут уменьшить вероятность утечек и защитить данные пользователей.