Умные часы, которые обмениваются данными со смартфонами и различными приложениями, могут стать целью мошенников, предупредил Владимир Ульянов из аналитического центра Zecurion. По его словам, компании обычно используют данные для создания персонализированных рекламных предложений, но существует риск, что информация может быть перехвачена или неправильно использована.

Ульянов отметил, что утечка данных может произойти как из-за злого умысла, если компании продают информацию третьим лицам, так и из-за невнимательности при чтении лицензионных соглашений. В некоторых случаях данные могут быть случайно утекать из-за ошибок или недостаточной квалификации сотрудников, что может привести к появлению «серых» баз данных, которые могут быть использованы в мошеннических целях.

Хотя полностью избежать утечки данных сложно, Ульянов дал несколько советов по снижению рисков. Он рекомендовал использовать устройства от проверенных брендов, которые заботятся о своей репутации и обеспечивают высокий уровень безопасности. Также полезно регулярно обновлять программное обеспечение и использовать уникальные логины и пароли для разных сервисов.