# Безопасное использование смарт-устройств

Смарт-устройство можно определить, как электронное устройство, имеющее возможность подключения к другим устройствам и сетям передачи данных через беспроводные способы доступа, такие как Bluetooth, NFC, Wi-Fi, 3G и т.д.

Такие возможности устройства определенно должны быть хорошо защищены, так как подключение к интернету сопряжено с определенными рисками.

Поскольку умные устройства подключены к интернету, они не являются исключением для взломов. Более того, пользователи расценивают умное устройство как обычный домашний прибор, забывая о простых мерах компьютерной безопасности, поэтому ситуация ухудшается.

В результате порог безопасности для доступа к таким устройствам является низким, что дает возможность вмешиваться в их работу любому, кто имеет базовые знания в области сетевой безопасности.

Проблема безопасности смарт-устройств – одна из основных на сегодня. Цифровые устройства являются самыми уязвимыми технологиями. Угроза появляется, когда люди покупают технику и подключают ее к сети интернет, не изменяя заводских настроек и паролей, и это одна из основных причин того, что злоумышленники могут удаленно управлять вашей техникой.

**Для соблюдения мер безопасности при использовании смарт-устройств рекомендуется:**

- смените первоначальный PIN-код SIM-карты если устройство использует мобильную связь для соединения;
- установите экранный замок (код или отпечаток пальца) и при возможности используйте настройку автоматического замка;
- не загружайте файлы с неизвестным содержимым с сомнительных сайтов;

- при запросе предоставления личной информации на веб-сайте всегда просматривайте разделы «Условия использования» или «Политика защиты конфиденциальной информации»;
- всегда удостоверяйтесь в том, кому предоставляется информация и в каких целях она будет использована;
- периодически обновляйте программное обеспечение смарт-устройств и приложений (используйте новейшие версии программного обеспечения);
- отключайте автосохранение паролей;
- не подключайтесь к сомнительным сетям, не открывайте подозрительные электронные письма;
- попытайтесь избегать использования в приложениях возможности «запомни меня». Это очень упрощает потенциальным преступникам доступ к вашим данным;
- не оставляйте смарт-устройства без присмотра в общественных местах (кафе, кинотеатры и т.д.).

Такими действиями вы уменьшите потенциальный возможный ущерб.

*Информация подготовлена Консультационным центром ФБУЗ «Центр гигиены и эпидемиологии в Смоленской области»*