**Смарт-устройства – за и против.**

В 2019 году Всемирный день прав потребителей прошел под девизом: «Trusted Smart Products" – «За надежные смарт-устройства".

**Что это за чудо двадцать первого века – смарт-устройства?**

Смарт-устройство (также «умное», «интеллектуальное» устройство) способно подключаться к другим устройствам, обмениваться с ними данными, взаимодействовать с ними и со своим пользователем.

Самые популярные среди потребителей смарт-устройства – это смартфоны, игровые приставки, смарт-телевизоры, портативные трекеры состояния здоровья (например, фитнес-трекеры), термостаты, детские игрушки и оборудованные доступом в Интернет автомобили. Все эти продукты способны собирать и анализировать пользовательские данные и передавать их на другие подключенные к сети устройства. Сети, состоящие из подключенных друг к другу смарт-устройств, называются Интернетом вещей (IoT).

Потребители используют смартфоны для осуществления платежей, отправки и получения денежных переводов, связи, доступа к заработной плате, кредитам т. п. – то есть для выполнения важнейших функций. Это означает, что обеспечение доступности, безопасности и защищенности подключенных к Интернету телефонов особенно важно для потребителей, использующих свои смартфоны для получения основных услуг.

Помимо смартфонов, также популярны другие подключенные устройства, включая смарт домашние системы безопасности и смарт мониторы слежения за состоянием здоровья. Например, фитнес-трекеры отслеживают уровень физической активности, характер сна и качество состояния здоровья, помогая пользователям достичь лучшего понимания информации о состоянии их здоровья. В доме смарт системы безопасности оснащены беспроводными веб-камерами, замками и датчиками движения. Если эти устройства зафиксируют необычную активность, то они могут посылать сигнал тревоги владельцу дома на его смартфон.

Так же существует и увеличивается количество смарт устройств, которые предлагают индивидуальные решения для людей с ограниченными возможностями. Например, смарт часы для людей с проблемами зрения, которые вибрируют при получении письма на электронную почту, затем переводят его содержание в шрифт Брайля на экран часов. Смарт лампочки, подключенные к дверному звонку или телефону, предупреждают людей с проблемами слуха, когда звонит телефон или кто-либо находится у дверей.

За последнее десятилетие освоение потребителем смарт устройств неуклонно возрастает, и прогноз показывает, что этот процесс будет продолжаться.

В частности, всемирное распространение смартфонов быстро возросло за последние три года. Сегодня в мире насчитывается около 4 миллиардов подключений к смартфонам, что почти вдвое больше, чем три года назад.

**Но вместе с популярностью в один ряд стоят и проблемы связанные с использованием смарт-устройств, а именно:**

1. **Ценовая доступность**.

**2. Безопасность**: Все интеллектуальные устройства являются частью более крупных подключенных систем и сетей, оттого уязвимость любой отдельно взятой части может поставить под угрозу всю систему. В последние годы мы узнали о множестве громких кибератак, запущенных хакерами, которые получили доступ к незащищенным потребительским устройствам. В 2016 году крупная кибератака нарушила работу Интернет-сервисов в Северной Америке и Европе, когда были атакованы незащищенные принтеры, домашние Wi-Fi роутеры и радио-няни. Это позволило вирусу стремительно распространиться и заразить в итоге почти 65 000 устройств менее чем за 24 часа.

**3. Помимо рисков нарушения работы сетей и сервисов, незащищенные смарт-устройства ставят под угрозу** **безопасность самих потребителей**. Исследователи выявили, что устройства можно взламывать и управлять ими удаленно – в одном из случаев специалисты в области компьютерной безопасности смогли получить доступ к подключенному к сети автомобилю и управлять его рулевой системой, тормозной системой и дверными замками.

**4. Защита личных данных:** Значительный риск с точки зрения сохранения конфиденциальности данных возникает из-за того, что устройства могут и конструктивно предназначены для обмена данными друг с другом, способны автономно передавать данные третьим сторонам. Объекты внутри подключенной системы могут собирать данные или информацию, которые сами по себе безвредны, но при сопоставлении и анализе вместе с другими данными способны раскрыть достаточно точные сведения о личности, что приводит к расширению возможностей по отслеживанию пользователей и их профилированию.

**5. Функциональная совместимость**: Обеспечение того, чтобы различные «умные» устройства, которыми владеют потребители, могли продуктивно обмениваться данными друг с другом, также очень важно для потребителей с точки зрения максимально эффективного использования приобретенных устройств. Если вы купили «домашний помощник» и обнаружили, что он не может подключиться к другим устройствам в вашем доме, это серьезно ограничит его функциональность. Если устройства могут эффективно работать только с другими гаджетами от той же компании, потребитель оказывается вынужденно привязанным к одной системе, а это ограничивает его выбор и конкуренцию на рынке.

**6. Обновления функций безопасности:** Общая проблема с подключенными устройствами – это отсутствие обновлений функций безопасности. Если обновления недоступны, устройства могут стать уязвимыми для вирусов и кибератак. Тем не менее компании не обязаны предоставлять обновления, и кроме того, нигде не оговаривается, как долго они должны предоставлять такие обновления для устройств старых моделей.

 Норвежский Совет Потребителей (NCC) и британская компания, занимающаяся безопасностью, протестировали четыре модели умных детских часов. Тест показал, что устройства имеют серьезные недостатки, ненадежные с точки зрения безопасности функции, не обеспечивают защиты потребителей. У двух моделей были выявлены недостатки, позволяющие потенциальному злоумышленнику контролировать приложения и таким образом в режиме реального времени получать доступ к данным о местонахождении детей и к аудио данным.

Завоевание доверия: Всемирная организация потребителей совместно с ANEC, ICRT и BEUC опубликовала ряд принципов, подчеркивающих необходимость приоритизации защиты прав потребителей, конфиденциальности и безопасности сетей и устройств в развитии Интернета Вещей. Эти принципы и рекомендации предназначены для разработчиков, производителей, политиков и регулирующих органов.

В них учтены основные риски, с которыми сталкиваются потребители при использовании Интернета Вещей, даны рекомендации по решению существующих проблем.

Призыв к улучшению качества обновлений смартфонов: Consumentenbond, член Всемирной организации потребителей из Нидерландов, подал в суд иск против Samsung за то, что компания не предоставляла обновления функций безопасности для своих смартфонов в течение достаточно продолжительного срока. Компания утверждала, что их более дорогие продукты получают обновления в течение более длительного периода времени.

Which? проверяла умные игрушки на безопасность: В 2016 и 2017 годах организация Which? совместно с другими организациями потребителей и специалистами в области безопасности провела исследование подключаемых к компьютерным сетям игрушек. Исследование показало, что некоторые из популярных детских игрушек имеют серьезные проблемы с безопасностью. Особую озабоченность вызвали игрушки, оборудованные динамиками и микрофонами; при отсутствии аутентификации через Bluetooth хакерам удалось подключиться к интерактивному медвежонку Toy-Fi Teddy и передавать через него голосовые сообщения ребенку, получая ответы.

В мае 2018 года вступила в силу **Директива ЕС о безопасности сетей и информационных систем**, которая требует от провайдеров цифровых услуг (торговых онлайн площадок, поисковых систем и облачных сервисов) внедрения основанных по оценке рисков мер по обеспечению безопасности в отношении интегрированных в их сети устройств Интернета Вещей.

**Взвесив все «за» и «против» по использованию смарт-устройств выбор остается за Вами!**

*Материал подготовлен по материалам сайта Consumers International.*