Фото: © Freepik

УМНЫЕ ДОМА: *насколько они безопасны?*

Фото: © Freepik

С РАЗВИТИЕМ ТЕХНОЛОГИЙ УПРАВЛЕНИЕ БЫТОВЫМИ УСТРОЙСТВАМИ СТАЛО ЗНАЧИТЕЛЬНО УДОБНЕЕ. ПЕРВЫЕ ПУЛЬТЫ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ ДЛЯ ТЕЛЕВИЗОРА ПОЯВИЛИСЬ ЕЩЕ В 1950-Е ГОДЫ. ОДНАКО НАСТОЯЩИМ ПРОРЫВОМ СТАЛО ПОЯВЛЕНИЕ ИНТЕРНЕТА ВЕЩЕЙ *(INTERNET OF THINGS, IOT)*. ЭТА ТЕХНОЛОГИЯ ОБЪЕДИНИЛА ВСЕ УСТРОЙСТВА В ДОМЕ В ЕДИНУЮ СЕТЬ, ЧТО ПОЗВОЛИЛО КОНТРОЛИРОВАТЬ ИХ ИЗ ОДНОГО ЦЕНТРА.

Сегодня с помощью одного контроллера можно управлять музыкальным центром, телевизором, системами отопления и освещения, а также дверными замками. Однако, несмотря на удобство, **умные дома имеют свои риски**. В интернете много угроз, и все подключенные к сети устройства уязвимы для атак. В этой статье мы рассмотрим основные угрозы и способы защиты умных домов.

КАК ФУНКЦИОНИРУЕТ УМНЫЙ ДОМ?

Устройства *Интернета вещей* имеют доступ к сети и встроенные микрокомпьютеры. Это могут быть как отдельные приборы, например, кофеварка, так и целые системы, такие как отопление. Они используют интернет-протоколы для связи и подключаются к контроллеру, которым может быть роутер или смартфон.

Контроллер собирает информацию об использовании устройств, что позволяет хранить данные о ваших привычках и предпочтениях. Чем больше устройств в доме, тем больше данных о вас они собирают, что может стать мишенью для злоумышленников.

ЧЕМ БОЛЬШЕ УСТРОЙСТВ В ДОМЕ, ТЕМ БОЛЬШЕ ДАННЫХ О ВАС ОНИ СОБИРАЮТ, ЧТО МОЖЕТ СТАТЬ МИШЕНЬЮ ДЛЯ ЗЛОУМЫШЛЕННИКОВ

Фото: © macrovector / Freepik

ОСНОВНЫЕ КИБЕРУГРОЗЫ ДЛЯ УМНОГО ДОМА

1. Небезопасные устройства. Некоторые производители спешат выпустить на рынок новые устройства, не уделяя должного внимания их безопасности. Это делает их уязвимыми для взломов.

2. Слабая защита Wi-Fi. Если злоумышленники получат доступ к вашему Wi-Fi, они смогут получить доступ ко всем данным, хранящимся в сети.

3. Уязвимость смартфонов. Управление умным домом часто осуществляется через смартфон, который также может быть взломан или украден, что откроет доступ ко всей домашней сети.

КАК ЗАЩИТИТЬ УМНЫЙ ДОМ?

1. Создание отдельной сети для умных устройств. Настройка гостевых сетей помогает изолировать данные умных устройств от основной сети.

2. Защита всех устройств. Установите надежные пароли и антивирусные программы на всех устройствах. Используйте WPA-шифрование для защиты Wi-Fi.

3. Регулярные обновления. Устанавливайте актуальные исправления безопасности и обновления программного обеспечения для всех устройств.

БУДУЩЕЕ УМНЫХ ДОМОВ

Постоянное развитие технологий делает умные дома еще более комфортабельными. Прогнозируется, что **к 2029 году объем рынка умных домов достигнет 370,95 млрд долларов США**. Однако для использования всех возможностей этих устройств важно обеспечить их безопасность.

Защищайте свои умные дома, чтобы наслаждаться всеми преимуществами современных технологий без риска.

По материалам https://allsoft.ru/ и www.kaspersky.ru