A Day In The Life Of IoT Security

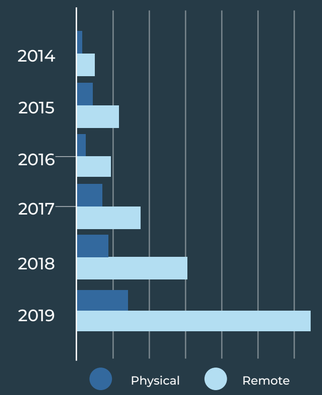
Talk to us today about end-to-end security solutions for your applications.

EPS Global provides simple, cost-effective Secure Provisioning services from our state-of-the-art programming centers strategically located in all major electronic manufacturing hubs worldwide.

Your Commute

In 2019 alone, automotive-related cyber incidents doubled from the year prior (a 605% increase from 2016). These include carjackings, data breaches, and even taking control of moving vehicles on a highway.

Remote & Physical Car Hacks 2014–2019



Dinner Time

In 2017 Pen Test Partners found a series of vulnerabilities in a smart oven allowing hackers to switch on all functions at once through a simple enumeration attack. This vulnerability could turn your smart oven into a mobile arson device in a matter of minutes.

A hacker attack occurs every

39 Seconds

Morning Coffee

In 2018 researchers at Avast hacked a coffee machine to remotely trigger the burner, dispense hot water, spin the bean grinder, and display a ransom message on the display.

If compromised smart appliances could act as a gateway to other smart devices and your home network. Hackers could conduct illegal activities by funneling web traffic through your connected smart appliance or hold your morning routine to ransom.

40.8%

of smart homes have at least one device vulnerable

Buying Lunch

In 2021 a team from Positive Technologies found multiple vulnerabilities in the payment terminals of the two largest manufacturers. These vulnerabilities made it far easier for hackers to steal bank details in over 150 countries worldwide.

7.6 Billion

POS transactions are processed annually.

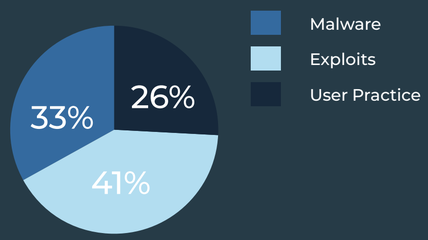
Adjusting the Heat

In 2019 a family in the USA returned home to find that their thermostat had been set to 90 degrees Fahrenheit while they were out. Hackers had taken remote control of the smart thermostat and speakers and were communicating with the couple.

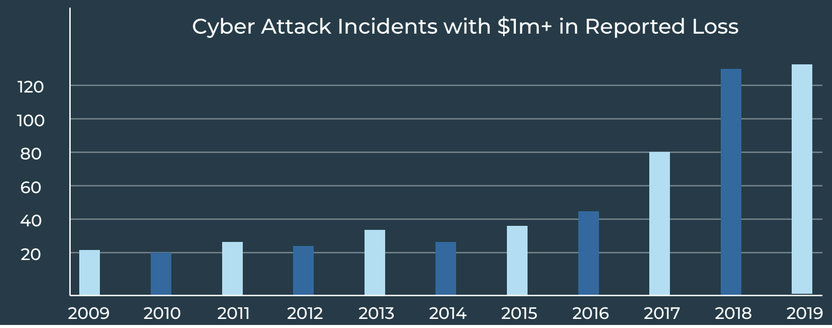
152,000

IOT devices will connect every minute by 2025

How the hacks occur

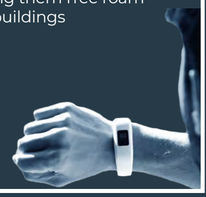


Cyber Attack Incidents with $1m+ in Reported Loss



Hitting the Gym

In 2016 hackers used a RaspberryPi to 'sniff' fitness wearables in a crowd and track individuals throughout the day and manipulate health data for users. Hackers also discovered the potential to scrape wireless identity authenticator codes when passing RFID devices - potentially giving them free roam around businesses and buildings



www.**epsprogramming**.com