FIREDOME

4 IoT nightmares for homeowners

Why security matters to your customers

When cybersecurity makes the news, it's usually in the context of international politics, a ransomware demand, or corporate espionage. Distant threats with little relevance to ordinary households.

Accordingly, security tends to take a backseat in IoT product development. But as IoT devices have become more common in the home, the risk of a cyber attack has loomed larger over everyday families.

These real-life IoT nightmare scenarios demonstrate that the danger is in fact very real and very present. And it's pushing cybersecurity up the list of priorities for your customers.

1. Blackmail by webcam hacking

Internet scammers recently took to extorting hundreds of thousands of dollars from high-earning targets. They would send an email claiming to have webcam footage of the victim watching pornography, threatening to publicly release it if they didn't receive payment.

Usually, they had no such footage. But they easily could have. Research from Wizcase identified eight common brands of webcam that were easily hackable. Footage, screenshots, and personal data were all left vulnerable to prying eyes, which can be used for blackmail, extortion, or identity theft.

2. Kidnap threat from hijacked baby monitor

One night in 2018, young Texas couple Ellen and Nathan Rigney were woken by the sound of talking from their baby's room. When they checked on their child, the voice instructed them to switch off the light. Refusing, it threatened to kidnap their baby. Their baby monitor had been hacked.

The hacker was bluffing. It was just a cruel prank. But the incident underlines how baby monitors can be accessed without appropriate security measures in place. There were no material consequences this time – only a grotesque invasion of privacy – but there easily could have been.

3. Smart doorbells offer entry to personal data

In late 2019, Amazon's increasingly popular smart doorbells, Ring, were discovered to have a critical security flaw. When first connecting to the home wi-fi network, the password was sent in clear text, rather than making use of encryption. (The issue has since been fixed.)

At this juncture, it was possible for hackers to intercept the message and perform a 'lateral hack' to gain access to other devices on the wi-fi network, including smartphones, tablets, and laptops. Once in, they could steal personal data, hold the device to ransom, or even take control over it.

4. Home security cameras used to plan burglaries

Many families have adopted cheap wi-fi-enabled cameras as a form of home security, which are just as vulnerable as baby monitors or smart doorbells, but even those designed for CCTV can be susceptible to attack.

Once accessed, cameras can be used as part of a botnet to steal personal data, gain access to other devices or identify the geographical location of the house. With detailed knowledge of the interior, online theft could be used to enable a real-life burglary.

Securing IoT devices

Despite these stories, security remains an afterthought for many IoT brands. But a network is only as strong as its weakest link, making products like webcams, baby monitors, and smart doorbells potential entry points for serious cyberattacks.

Changing the default password is a first step to securing a device. But there are often other hidden vulnerabilities and as the number of devices in a home multiplies, so does the attention required for effective cybersecurity. Most homeowners don't have the knowledge or time to stay secure.

Firedome's holistic IoT security solution combines firmware-embedded endpoint protection with AI-powered cloud analysis and 24/7 monitoring by security experts. It is the highest standard of security built right into the device.

As hacks gain more attention, homeowners gravitate towards the most secure IoT products.
With Firedome certification, you can show them you put their safety first.

Find out how Firedome can secure your devices, and help you grow your IoT sales. Visit www.firedome.io or get in touch today.

Securing the Connected Future
www.firedome.io