FIREDOME

High Profile Homeowner Nightmare Scenarios

Most national news these days about cyber attacks is related to geo-politics, corporate espionage, or damage or ransoms to large corporations. But the attacks that hit much closer to home for most Americans are usually stories you might only hear about on local news. But a home cyber attack is just as frightening for a homeowner, and the higher profile the owner is, the more there is to lose.

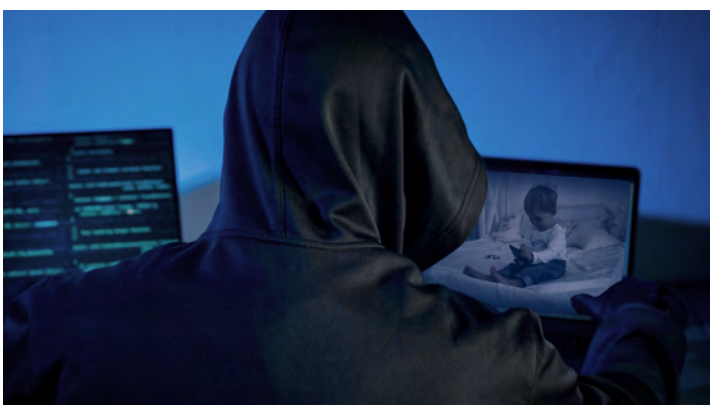
Below are 4 recent scary home cyber hacks or vulnerabilities, followed by Firedome's solution for all:

1) Webcam Sextortion Rings Target CEOS and 8 Popular Webcam Brands Can Be Easily Hacked

For executives or celebrities, an insecure webcam in their home can open the door for blackmail, extortion or exposure of damaging personally identifiable information. Hackers are more likely to target them because the potential rewards are higher for the risk they take doing the hack.

2) Hacker Hijacks Baby Monitor and Threatens to Kidnap Baby

Regardless of how physically secure a home is, hackers can wreak havoc without stepping in the house. Baby monitor hacks range from terrifying audio pranks hackers do for laughs to actual surveillance while considering a break in. If even an industry leader like Nest can't prevent password leaks and doesn't require changing default passwords at setup, incidents like this will happen again.



3) Smart Doorbells from Amazon's Ring - Exposing your home Wi-Fi password to the world

IoT devices that don't encrypt WiFi passwords when first configuring to home networks expose all devices to hackers. Considering this oversight most recently came from the most well-funded and staffed IoT security company in the world, one can imagine cheaper devices also have this flaw.

4) Primary Home Security Cameras Can Be Taken Offline Due to Flaws In Their Code

While baby monitor hacks are scary, they are not likely the main camera a hacker with burglary intentions is after. But primary home security cameras like Foscam are a different story.

If primary cameras can be taken over easily by hackers with basic internet scanners, they can target vulnerable IP addresses in high income areas specifically for the most valuable targets. And if these homes have smart locks on the same network too, lateral hacks can even open the door for them.

Firedome's Solution for These Types of Home Attacks

To avoid the high costs and resources required to address cyber attacks, manufacturers should assess their capabilities against IoT attacks & vulnerabilities and invest in adequate protection.

Preventing the above cases requires proactive endpoint security with the right defense measures. **Firedome Endpoint Protection for IoT** detects logins from abnormal locations (IDs malicious hackers connecting to devices), secures open connections and exposed attack surfaces (complements lack of secure authentication; uPnP), and mitigates zero-day (unknown) exploits used by malware and hackers to hijack devices (protects against remote code execution vulnerabilities).

IoT Devices May Not Hold Your Most Precious Data, But Lateral Hacks Can Get Them To It

The greatest risk from IoT devices on your home network being hacked is not always from the device itself. Because an IoT device can simply be used as an entry point to then move laterally across your network to cell phones, laptops or other devices, the risk is greater than it seems.

Poorly secured IoT devices means that your core devices are only as secure as your weakest IoT device. If you think about some of the higher profile celebrity hacks like Jennifer Lawrence, Mark Zuckerberg, Selena Gomez, Justin Bieber, Leonardo Dicaprio, Floyd Maytheather and more, you can imagine how bad hacks can also get for celebrities who also have weak IoT devices in their homes.

While individual vulnerabilities of these devices can sometimes be addressed with one-off password changes or disconnecting unused devices, it is becoming more difficult to keep track of all the connected devices on your network at any given time. That's why the most fool-proof way to fully secure your home is to only purchase devices with proactive cybersecurity protection like Firedome.