The Unwanted Visitors You're Letting Into Your Home: How Second-hand Smart Home Technology is Compromising Your Safety

Submitted by: vpnMentor
Wednesday, 22 August 2018

---

127 million smart home units are expected to be sold in the US in 2018, with the global smart home market expected to be worth 53.45 billion USD by 2022. With 55% of smart device owners in the dark about how they actually work, could those who bought second-hand smart home devices be welcoming a threat to their families into their homes?

Internet security experts vpnMentor (https://www.vpnmentor.com/) have utilised a team of ethical hackers to uncover the most hackable smart home devices including the first-generation Amazon Echo, a Samsung Smart Camera and the first-generation Ring Smart Doorbell.

vpnMentor have produced a video which shows just how you're inviting hackers into your home, and how easy it can be for them to access your sensitive information. Disturbingly, the team were able to manipulate all of the devices tested to gain access to your home.

Amazon Echo - A wiretap waiting to happen?

Our research revealed a critical vulnerability related to the first-generation Echo's physical design. Hackers were able to open the device up and manipulate it using a specially crafted SD card. This means that malicious actors could live stream audio from its microphone, and remotely use its services.

The video showcasing this in action, as well as advice to protect yourself, is viewable here (https://www.vpnmentor.com/how-hackable-is-your-smart-home/personal-assistant-device/).

Keeping Cyber Criminals At Bay

With such terrifying findings, vpnMentor wants to highlight just how simple it is for your home to be targeted by malicious hackers.

However, the experts at vpnMentor have compiled a list of recommendations to protect users from becoming an easy target:

- Always research a product, and any existing security threats to it, before you buy.
Only buy your smart gadget from an officially certified source.

- Be aware of any signs of physical intervention with the product.

- Directly address the seller if you or someone else has identified any major misconfiguration.
Make sure your smart device is properly configured and regularly updated.

- Keep your externally facing smart devices on a separate network.

Ariel Hochstadt, co-founder of vpnMentor, commented: "If you are going to introduce smart technology

into your home, it is important that you remain attentive with your devices to ensure that only those you trust have access. By following our set of simple rules you can ensure the best security practices have been met and saving you from becoming an easy target for crime."

For more information on cybersecurity, and how to make sure your devices are protected, you can read the full vpnMentor guide here (https://www.vpnmentor.com/wp-content/uploads/2018/06/vpnMentor_Whitepaper_EN.pdf). You can also watch their video investigation here (https://www.vpnmentor.com/how-hackable-is-your-smart-home/personal-assistant-device/) to see how one unsuspecting family was affected after their devices were hacked.

NOTES TO EDITORS:

All devices mentioned were purchased and hacked by a team of ethical hackers in March-April 2018. Full details can be found in the whitepaper. Although all hacks took place in real-life, the scenes depicted in the video are a reconstruction of a scenario that would have been possible with the vulnerabilities uncovered.

For any questions or queries, please contact:

Jessica Fairfax

Kaizen

jess.fairfax@kaizen.co.uk

020 3950 2165