GUERRILLA OggaDoon COMMS

How Hackers are Getting into Your Smart Home

Smart watches, smart locks, smart thermostats, and smart speakers – they all offer a wide variety of benefits, but they are the perfect back door for hackers to get into your smart home.

After all, hackers can get into your smart fridge, and it has been estimated that there is an attempted hack every 39 seconds. An Android security flaw was revealed in September 2019 that demonstrated over 1 billion devices were at risk from hacking. In Australia alone, over $128m has been lost through hacking scams in just 2019 – and that number only includes those who reported the crimes.

But you don't just have to take our word for it. We spoke with Rik Turner, Principal Analyst for Security at Ovum, and he shared some fascinating insight into just why hackers find smart homes almost irresistible – and in some cases, very easy to enter.

The more connected devices you have, the more risk

Rik shared: "The increasing internet connectivity of devices is opening up risk to anyone who owns them, because you need to have them updated all the time with the latest security if you need them to respond to any attacks. Consumer security is notoriously poor, partly because people choose weak passwords like password123, and because WiFi can act as a bridge from one environment to the other."

We asked Rik to explain this a little more, and he talked us through the simple problem of moving one mobile device to multiple WiFi connections in one day. If you leave your own personal WiFi or hotspot open without a password, anyone can access your mobile and then any other device connected on the same network.

What does that mean in practice?

"Say you grab a coffee just outside work and then head into the office," Rik explained. "Someone in the coffee shop could use your phone to bridge into the corporate network, and steal sensitive data, steal IP, or wreak havoc! They could plant a trojan virus which may not explode for another 6 months, destroying all company data."

But that's just one phone and one network. With smart homes and greater interconnected devices, there are ever increasing entry points for hackers to get into your systems. For example, if you leave your mobile WiFi switched on while in your home, there's nothing stopping your neighbours bridging into your home network and stealing all your payment card details, personal info, and more.

This is particularly dangerous during the Christmas season, when huge numbers of payments are made leading up to December 25th. This increases the frequency with which you are inputting security passwords to authorise payments, which means more opportunities for hackers and scam artists not only to steal your data, but also to purchase gifts for themselves.

But I don’t have anything to hide, or anything of value!

You do, even if you don’t realise it. Take smart hubs, for example. They can now be used as the jumping-off point for all devices in your home, and that’s not just your laptop or your mobile.

“Unfortunately, one problem with home devices is that many companies who are internet-enabling devices are expert in that type of device, not the internet of things,” Rik points out. “Take smart kettles. Kettle manufacturers are expert in kettles, not WiFi, nor internet security. That means they can brew a great cup of tea, but they’ll also paint a target on your back. A large proportion of these WiFi cards don’t have pinned certificates, and that means they are vulnerable.”

And smart devices don’t stop there. Millions of people use smart home technology to control their heating – but a hacker could keep you in the cold. Smart locks could be locked against you. There are even smart learning toys, such as dolls which speak to children and use machine learning in the cloud to ‘learn’ the child’s name and, say, its preferred games.

Hacking dolls?

It really happened.

Rik tells us, “This doll technology had a deliberate security setting so it couldn’t start cursing at children or using age-inappropriate language. Through a testing exercise, someone got in and changed the software – in just 30 minutes.”

Smart home hacking is a growing problem

Data theft, actual physical sabotage of home appliances, compromised CCTV cameras for use in DDoS attacks…the list of ways that hackers could enter your smart home for nefarious purposes are starting to become endless. Hackers could use your fridge to attack the Pentagon, for instance, or launch a virus against the MOD in the UK. Or simply turn the fridge off while you're away for a long weekend, just to increase your grocery bill. Or hack into your smart meter to find out when you go on holiday and break into your house.

Without manufacturers taking cybersecurity more seriously, there are going to be growing numbers of people losing their sense of safety and security in their own homes.

But you can take back control. Making sure you have high-quality passwords, ignoring any emails that look suspicious, and demanding better cybersecurity for all your devices are positive steps you can take to protect yourself.

Social copy:

Twitter

Is your smart home opening a door to hackers? Read an expert opinion here #GiveAGiftNotYourData

Smart fridges, smart kettles, smart locks – but what if they aren’t so smart? #cybersecurity must start at home, and we reveal why in our latest blog #GiveAGiftNotYourData

LinkedIn

This Christmas, don’t open your door to cybersecurity scammers. We talk with Rik Turner, Principal Analyst for Security at Ovum, about how hackers are looking at your technology to access your personal data – or worse.