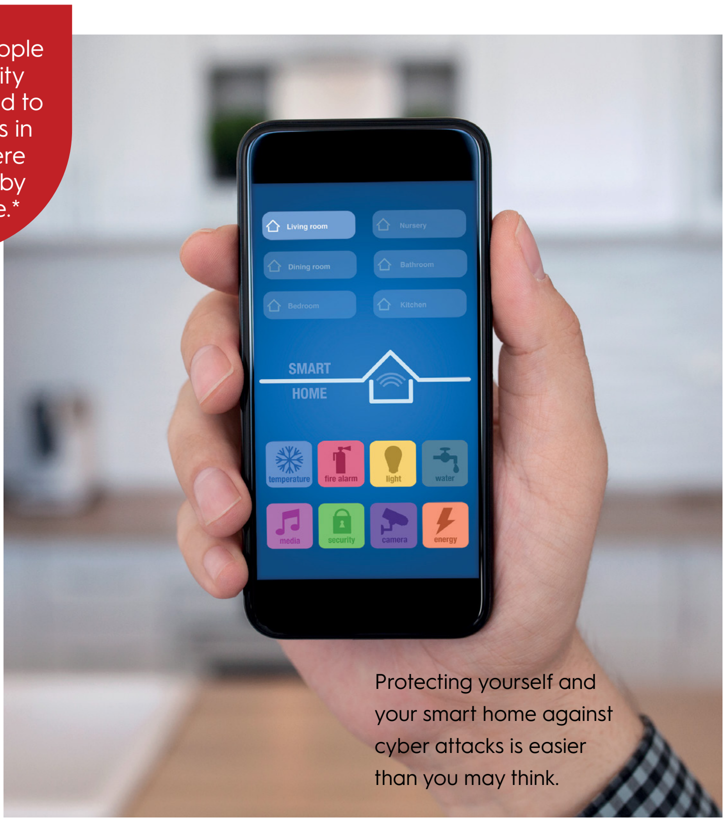
Cyber security: are our smart homes safe?

The growing number of devices raises an equally increasing amount of concerns about the level of protection that comes with them. Here, **Yvette Murrell** investigates which precautions to take



52% of people said security threats related to smart devices in the home were outweighed by convenience.*

Protecting yourself and your smart home against cyber attacks is easier than you may think.

Naturally, I am all for smart home technology. I think it's great, and it's certainly going to be an integral part of the way we live in the future – there's no doubt about that. But it would be naïve to assume my personal data and safety weren't at some sort of risk by introducing more of these devices into my home.

Like me, I'm sure over recent years you've heard news stories on security breaches including the cameras in smart TVs, hackers accessing voice-controlled devices to order expensive items, and the ongoing debate on whether the likes of Amazon and Google should hand over recording data to the police in criminal cases. The latter has brought up the bigger question about what these smart-home devices are actually watching and listening to.

"The main concern among experts when it comes to smart home technology is the degree to which they are listening in," says Martin Quaife, senior consultant at security firm Blackstone Consultancy. "They obviously listen for any commands you might say – but what else are they taking in and how could that put privacy at risk? With the likes of Amazon's Alexa, Apple's Siri, Microsoft's Cortana, and Google's Home Assistant in many households these days, and knowing that some of the technology is listening and recording, who might exploit that?" Indeed, this is a concern for many of us. According to a Censuswide survey by Open-Xchange on parents, 78% said they would consider not investing in any more smart home devices in the event of a cyber attack.

This leads us to another other issue: as the majority of these gadgets are connected to our home WiFi networks, we are at risk if our internet routers are not secured. Not only could our personal data be stolen, but with the likes of smart lighting and heating, criminals could also potentially work out when we're not at home using the data these products hold in the cloud. Yikes.

But enough scaremongering. Fortunately, you can help prevent security breaches without having to forego smart devices entirely. The first step is easy: make sure your router is secure and protected with a password. Then, consider investing in protection measures. WiFi retailer TP-Link has worked with Japanese cyber security company Trend Micro to create HomeCare, an anti-virus and malware solution specifically for smart home technology. Available to buy online, it protects your router from being hacked at the source so that every device is taken care of.

Many smart home systems such as cameras, heating, and lighting usually work with a virtual cloud server, which is linked to an account you create using your email and personal details. To prevent data like this being retrieved by hackers, systems such as Homematic IP store everything anonymously on their cloud, with no need for a user account – so any data sitting there is useless for others.

> "The main concern among experts when it comes to smart home technology is the degree to which they are listening in."

And when it comes to voice-controlled devices, you can turn the mute button on when you are not using it and should get in the habit of doing so when you leave the house. This will prevent the device from listening in. You should also think about what you actually need connected to your device and which accounts realistically benefit you from having smart functions, as they will all be interlinked in some way. It's easy to review access permissions and data collection settings on your Amazon or Google accounts, and I would recommend doing so on a regular basis. This way, by making a few small but all-important adjustments to your security, you can continue interacting with your smart home devices worry free. KBB

*Source: Radware / Image: istock.com / Prykhodov

For stockists turn to p154