DREAMING OF A SMART CHRISTMAS?

ARE YOU PLANNING ON GIVING THE GIFT OF A SMART DEVICE THIS CHRISTMAS? THEN READ ON...

VARDAGS INSIGHTS

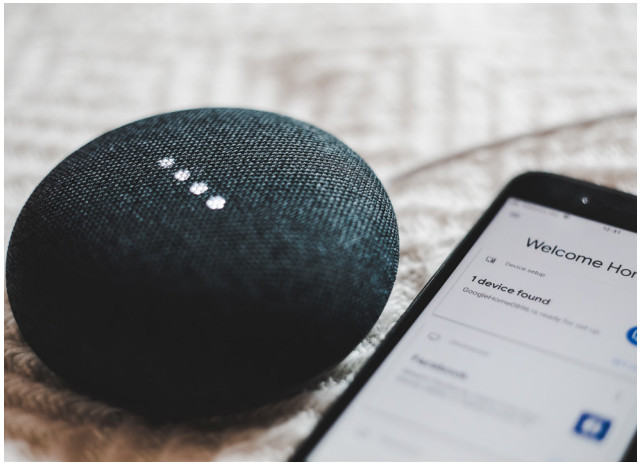
xcyber®

THE HUMAN SIDE OF CYBER®

BY ALEX MCCREADY OF *VARDAGS*, AND MATTHEW LANE OF *XCYBER*

For many of us, internet-connectable ('smart') devices have become an integral part of everyday life. From smartphones to tablets, televisions, fitness trackers and cloud-based voice assistants, this unprecedented rise in smart technology may have made our lives easier in many respects, but has it put our security and privacy at risk?

We have all caught sight of the headlines about how data can be obtained from these devices. Indeed, many devices, applications and online services commonly come with a trade-off: to gain functionality of their services, you must share your data with third parties (as the increasingly popular maxim goes: if you're not paying for it – you're the product being sold...). This data is often used to improve, enhance and de-bug the



provided service in question.

Such phenomena have, however, stoked a paranoia that many large tech companies can, and are, arbitrarily analysing our movements, tracking our whereabouts, and listening to our conversations. One brand of internet-enabled CCTV system had over 1,200 systems openly broadcasting live footage over the internet in the UK alone, and over 275,000 globally - these live feeds could be viewed by anyone. Another company recently filed a patent for a technique that supports key word determinations from voice data as the basis for enabling targeted advertising - while the company itself stressed that this technology is not currently in use, the patent filing has nonetheless concerned the tech community

TO THE RESCUE? NEW CYBER LAWS TO PROTECT PERSONAL TECH

This concern is not unwarranted, and governments have begun to react to the viable threats that smart devices pose. South Korea, on the one hand, were prompted to strengthen cybersecurity rules to protect residents whose smart home devices were being hacked to retrieve private home footage that could be sold on the dark web for bitcoin.

The UK Government has recognised the issues in this area and recently announced a new Product Security and Telecommunications Infrastructure (PSTI) Bill to increase protection for consumers from threats and hackers on internet-connectable devices. This comes as a response to numerous attacks on smart devices seen across the country, with insufficient security standards such as poor authentication measures, which have exposed even baby monitors and children's toys to hacking and misuse. The very fact that these devices often have fitted microphones and remote connectivity provides the potential for them to be open to misuse, with research showing four in five manufacturers do not implement adequate security measures.

The UK Government is responding to this huge cybersecurity risk with this new legislation, which intends to improve the protection of people's digital devices by:

- Introducing new, tougher cyber security standards, including a ban of universal default passwords
- Preventing the sale of connectable products in the UK that do not meet baseline security requirements, and issuing hefty fines where firms fail to comply
- Requiring that firms be transparent to their customers about how they are dealing with security flaws in connectable products, as well as the creation of better reporting systems for vulnerabilities

TOP TIPS FOR PROTECTION

So, if you are concerned about how secure your devices are, what can you do to maximise your protection?

Prioritise privacy and password protection

What's the first thing that you must do with a new device? Head to the security and privacy settings of any new device and change the default password if it has one! you. Not only does this increase the effectiveness of any protection, but also reduces the administrative burden of trying to change these retrospectively, which in some cases, may even be too late.

Keep it current

Moving forward, make sure to keep your security and privacy settings, including your password, current. It is also important that you know how to update the software on your smart device to ensure its protection against any security weaknesses that may have been discovered.

Share wisely

The terms and conditions can be lengthy, but you can search for key phrases like "sharing" and "privacy" to see if data from your smart assistant can be used by the company to improve services. These data-sharing permissions may be set to 'on' by default in the device's settings. It is important to remember, though, that these do have a legitimate purpose in helping the devices better understand regional accents and other languages or requests, but it is entirely your decision as to whether you wish to participate.

Children's devices

It is not just phones, computers and TVs that pose a risk. Parents should take care that they do not neglect data privacy and security within children's toys - if they can access the internet, they present a risk.

ABOUT

X Cyber Group (XCyber®) solves problems with state-grade intelligence expertise, across the core themes of trust, safety, and security. Their specialist intelligence and advisory services are designed to protect you, your data, your brand, and your reputation from the myriad of challenges the digital domain presents.

Vardags' is a top UK law firm offering blue-chip legal services to the high-net-worth and global elite. Their Reputation and Privacy department is headed by Alexandra McCready, who is widely respected for her industry-leading expertise in this area. The Vardags' team act both nationally and internationally for established, ultra-high-net-worth clientele and corporates on the full gambit of reputation and privacy issues, which includes specialist expertise in dealing with online threats, digital security audits and the removal of content from websites, blog sites and other social media.

Alex McCready, Head of Reputation & Privacy at Vardags

Matthew Lane, CEO & Co-Founder at XCyber®