AirCyISOC
Air Cyber and Information Services Operations Centre

ROYAL AIR FORCE

The internet of things

How to keep your smart devices secure.

GET SAFE ONLINE .org

www.getsafeonline.org

Connected devices can make life and work more convenient. But how can you ensure they're secure?

The internet of things (IOT) describes internet-connected devices other than computers, tablets or mobile phones, which most of us have in our homes and places of work.

In your home, these may include smart speakers (or voice assistants), security cameras and lighting, heating controllers, appliances and printers. Children's toys and baby monitors are also becoming increasingly connected. In your workplace, there will almost certainly be IOT devices too, office printers being a commonplace example.

Because smart devices in both the home and workplace carry out specific tasks for which functionality and usability is enhanced through being online, they receive controls and transmit usage data to their owners and manufacturers. *This is where the potential risks occur.*

If either the IOT devices or the network they're attached to aren't secure, they could be illicitly accessed online, or your data could end up in the wrong hands.

For you and your family, this could lead to privacy breaches, financial or identity theft or your devices being controlled without your authorisation. As RAF personnel, however, weak security on your devices or network could represent a threat to national security, with our adversaries constantly seeking ways to infiltrate our systems and acquire information about us.

In 2016, 'Mirai' malware was used to attack numerous IOT devices including routers and connected cameras. And there have been many widely reported cases of baby-monitoring cameras being compromised by hackers, with the culprit observing the child in their nursery and even conversing over the speaker.

In 2018, the UK government launched a voluntary Secure by Design Code of Practice for consumer IOT devices in attempt to get stronger security measures to be build into smart products at the design stage. A similar global standard has since been launched by the European Telecommunications Standards Institute (ETSI). Legislation is also planned to ensure that all IOT devices correspond to rigorous security requirements. But it's *your* responsibility to ensure your devices are secured.

ROYAL AIR FORCE

Secure your IOT devices by following these expert top tips

- Most smart devices need a password to connect to Wi-Fi. Always replace factory-set passwords with secure ones you create yourself, as many default administrator passwords are common to every device shipped and potentially insecure. If in doubt, check manufacturers' instructions on how to change passwords.
- Never use the same password for more than one connected device, nor for other online accounts.
- Make sure your Wi-Fi network is secure: see the advice page on Wireless Networks & Hotspots at **www.getsafeonline.org/personal/articles/wireless-networks-and-hotspots**
- Make sure you have a strong, unique password for your home router. Also, consider changing your SSID (network name) so you can't be identified as its owner. Information on doing this can also be found on the Get Safe Online website.
- Protect all your computers and mobile devices with updated internet security software/app and protect access to them with a unique PIN or passcode.
- Check the apps associated with your connected devices and install updates as soon as prompted. In addition, regularly check manufacturers' websites for updates in case they haven't been pushed out.
- Read the terms and conditions for your smart devices and apps to be clear on how manufacturers can use your data.
- Choose well-known, reputable brands, as it is likely that more care has been taken in designing-in security.
- When working at home, be aware of potential passive listening by voice assistants – have SECRET conversations only in RED/AMBER zones at work and never discuss anything above OFFICIAL level around smart speakers.
- In the workplace, follow guidance for Information Protected Zones (IPZs). Do not use PEDs (including IoT devices), enabled or open webcams and mics in AMBER or RED zones.

For comprehensive, practical, expert advice on keeping safe and secure online, visit **www.getsafeonline.org**

#RAFsafeonline

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by a number of government departments, law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

GET SAFE ONLINE .org

ROYAL AIR FORCE

www.getsafeonline.org

GET SAFE ONLINE: WORKING TOGETHER WITH...

TESCO · NatWest · Gumtree · Standard Life · first direct · HSBC · ROYAL AIR FORCE · Royal Bank of Scotland · M&S BANK · LLOYDS BANK · HALIFAX · BANK OF SCOTLAND · creativevirtual · ClearScore · CITY OF LONDON POLICE · NPCC · NATIONAL TRADING STANDARDS eCrime Team · cifas · VICTIM SUPPORT · EUROPOL EC3 · ActionFraud · METROPOLITAN POLICE · Ofcom · neighbourhood ALERT