ROYAL AIR FORCE

Have a safe and happy festive season

GET SAFE ONLINE .org

www.getsafeonline.org

This month, we're looking at how to stay safe and secure over the festive season … that's before, during and after Christmas.

If you're like most people, you'll have a lot on your mind in the run-up to Christmas: who to visit or invite for Christmas lunch, whether to cook a whole turkey or a crown, or when you'll get time to buy all the presents. With so much going on, it can be easy to forget the good online safety habits you've got into throughout the year. Fraudsters know this, so they're also having a busy time … maybe at your expense.

During and after Christmas, it's also important to be careful. Not only about scams, but also taking care with how you set up and use the new online devices you've given, received or treated yourself to, such as phones, tablets, laptops, smart home devices, kids' toys and fitness devices. A few minutes spent reading and applying the advice in this leaflet will help keep you, your family, finances, devices and the RAF protected.

Above all, we hope you have a safe and happy festive season.

ROYAL AIR FORCE

Buying online

- Ensure shopping websites are authentic by carefully checking the address is spelled correctly. Type it in rather than clicking on a link. And make sure payment pages are secure by checking that addresses begin with 'https' ('s' is for secure) and there's a closed padlock in the address bar.
- Sometimes, ads on social media and online forums are fraudulent, with gifts, tickets or travel non-existent, or not as advertised.
- Don't pay by transferring money directly to people or companies you don't know, however desperate you are to buy.
- Don't buy counterfeit goods intentionally or get duped into buying them. They're of low quality, can be dangerous and contravene copyright law.
- Avoid 'free' or 'low-cost' trials – whether remedies or tech gadgets – without reading the small print and trusted reviews. You could be signing up for large monthly direct debits which are difficult to cancel.
- Check that seasonal breaks, holidays or travel found online are genuine by thorough research.
- Never use your MoD email account to set up personal online store or other accounts.
- Avoid fake or non-existent event tickets by buying only from official sources.
- Avoid clicking on links in unexpected emails, texts or posts, or email attachments, as they could lead to fraud or identity theft, or downloading malware. If in any doubt, always call the organisation on the number you know to be correct.
- Unexpected phone calls claiming to be from banks, retailers, parcel firms or software support companies should be treated with caution.

Setting up and using connected devices

- Protect new or pre-owned internet-connected devices – including Apple – with a security app/software and a PIN or passcode as soon as you switch them on. Set all devices to back up automatically so you never lose valuable documents, photos and other files.
- Change passwords on connected devices like voice assistants, CCTV cameras, appliances, toys and fitness watches from the factory default as soon as you set them up. Disable location settings on fitness watches. And be careful what you say within earshot of that voice assistant!
- Download updates to operating systems, apps and software as soon as prompted. If you don't, you could leave yourself open to malware.
- Download apps only from App Store, Google Play or Microsoft Store. Others could result in fraud or identity theft.
- If you've bought or been given a preowned device, remove previous settings and data, if not already done. If you're selling, do a complete reset to prevent the buyer seeing your data.
- Don't overshare. What you post or message could be helping a fraudster, or giving your kids and friends an unwanted digital footprint. Posting that your family is away is a big clue that your home is empty. You or your family talking about locations could pose a security risk to the RAF. And remember to review your social media privacy settings.
- Don't use Wi-Fi hotspots if you're doing anything confidential, as they could be insecure or fake. Look after your devices as they make attractive targets for thieves. And be wary of people looking over your shoulder.
- Keep talking to your kids about safe and responsible use of the internet, including what they share, what they say, who they're communicating with and what content they're accessing including apps and games. Download a reputable parental control app and ISP filters. Make sure bills aren't being run up for in-game purchases.

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

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 kaspersky Gumtree Standard Life first direct PayPal HSBC

Royal Bank of Scotland NatWest M&S BANK LLOYDS BANK HALIFAX BANK OF SCOTLAND creativevirtual The science of conversation™ ROYAL AIR FORCE

HM Government CITY OF LONDON POLICE National Policing Lead For Fraud NPCC National Police Chiefs' Council NATIONAL TRADING STANDARDS eCrime Team Protecting Consumers Safeguarding Businesses cifas Leaders in fraud prevention VS VICTIM SUPPORT EUROPOL EC3 European Cybercrime Centre

NCA National Crime Agency ActionFraud National Fraud & Cyber Crime Reporting Centre actionfraud.police.uk METROPOLITAN POLICE Ofcom NEIGHBOURHOOD WATCH TO STOP FRAUD CYBER AWARE