OA FACT SHEET

This fact sheet is about staying secure online. It aims to provide information and guidance and to highlight other sources of support available.

OFFICERS' ASSOCIATION

STAYING SAFE ONLINE

The internet plays an important role in our everyday lives both at work and home and when we are on the move. During the Covid-19 pandemic, you may have had to use online services for the first time or more frequently for online grocery shopping, connecting with family and friends, using social media platforms, or registering for online banking.

STAYING CONNECTED

The internet can be an invaluable resource. During the national lockdowns, workforces were able to operate remotely, teaching and education went online, and people were able to connect with relatives, friends, employees, local community networks and places of worship. Many services, such as the National Health Service, now rely on digital platforms so having online access can make your life easier in many ways.

REDUCING ONLINE RISK

The internet has widespread uses and can be safe to use but it comes with risks if you do not protect yourself when online. It also attracts people who seek to misuse it, steal information, scam us and commit fraud and other criminal activities.

Taking the following steps can help you stay safe online, reduce risks and be aware of potential threats.

TOP TIPS FOR ONLINE SAFETY

KEEP CLEAN

Check that you have current and up-to-date security software: The latest security software, web browser and operating system protect us against viruses, malware and other online threats and are essential for all devices that connect to the internet.

PROTECT YOUR PERSONAL INFORMATION

A strong password: This is usually a minimum of 8-12 characters long and includes a variety of letters in upper and lower case, numbers, and symbols. Passwords should not contain your personal details such as name or date of birth.

A different password for different accounts: Having a different password for all accounts is encouraged and will provide safer and stronger protection.

Keep it safe: Your password(s) should only be known by you. If you need to write it down, do so securely and do not keep it on the device.

TOP TIPS FOR ONLINE SAFETY CONTINUED

CONNECT WITH CARE

Stay safe online: Check trusted websites for the latest information and before sharing.

Logging in: When using public wi-fi networks, do not view or send sensitive information.

Back it up: Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

THREATS, RISK, AND IMPACT

Email Scams: Scammers send bogus emails in the hope that people will enter their personal or financial details. Some emails, known as spam, junk or phishing, may contain harmful links or files for you to click on or open and may include a virus and impact your device. These emails can look genuine, so always be alert.

Fake Websites: Visiting a forged website that looks official but is designed to capture sensitive information such as bank account or login details.

Computer viruses: The most common virus is malware, often described as a rogue software programme that can spread from computer to computer. Malware can be sent via email or as an email attachment; it releases a virus when you click on it. Criminals may use this to take over your computer and steal your data.

FIGHT CYBERCRIME – REPORT IT

When in doubt, delete it: Links in emails, social media posts and online advertising can be an attempt by cybercriminals to steal your personal information. Even if you know the source, if something looks suspicious, delete it.

Report to the authorities: Stolen finances or identity, attempts and other cybercrimes to Action Fraud – National Fraud & Cyber Security Centre. Telephone 0300 123 2040 or online at www.actionfraud.police.uk.
All emergencies, please call 999.

YOUR ONLINE PRESENCE

Be aware of what's being shared: Protect your personal information such as your purchase history or location by setting the privacy and security settings on web services and devices to your comfort level. It's OK to limit how and with whom you share information.

Share with care: Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it could be perceived now and in the future.

Safer for me, more secure for all: What you do online has the potential to affect everyone – at home, at work and around the world. Practising good online habits benefits the global digital community.

USEFUL ORGANISATIONS

- **Age UK** offers IT training classes to help you get online www.ageuk.org.uk/services/in-your-area/it-training/. Call Age UK's freephone number 0800 678 1174 for your nearest Age UK and ask about local training opportunities.
- The **Online Centres Network** has 6,000 centres around the UK providing access to and advice on computers and the internet www.onlinecentresnetwork.org
- Ask at your local library about computer training opportunities

FURTHER READING

- www.ageuk.org.uk/information-advice/work-learning/technology-internet/internet-security/
- www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

Officers' Assocation, Grants and Welfare
T: **020 7808 4175** | E: **help@officersassociation.org.uk**
officersassociation.org.uk

EVERY OFFICER
EVERY FAMILY

OFFICERS' ASSOCIATION

The Officers' Association (OA) has prepared this information guide to provide general advice only; as such, it should not be relied upon as a basis for any decision or action and should not be used as a substitute for professional advice. Neither the OA nor OA Advance accepts any liability arising from its use. It is the reader's sole responsibility to ensure any information is up to date and accurate. The inclusion of named agencies, websites, companies, products, services or publications in this information guide does not constitute a recommendation or endorsement by the OA or subsidiary organisations.