

Cyber Protect Awareness Delivered for and in support of Oxforde County Council Scams events throughout October 2024

Note, there will be some cross over of information from the other speakers



Delivered by Mr M Godslan CISMP
Thames Valley Police / SEROCU
Police Cyber Security Advisor

Law Enforcement signposting
to Cyber Security Guidance,
reporting , presentations

Simple Steps to Protect You and Your Organisation

 serocu.police.uk/individuals



Raising the awareness of delegates to the general online safety process to secure email and other online accounts, creating and saving passwords, keeping devices up to date, saving your online data, signposting to the National Cyber Security Centre & covering the reporting process to Action Fraud.

([Links in blue enable you to read more content when you receive the summary notes](#))

Cyber Aware guidance for the wider public



Wider generic guidance concerning online safety and security



National Fraud Campaign – Home Office



AI / GI Guidance

Reporting of Fraud / Cyber Crime



Guidance correct as of 8th October 2024

Simple Steps to Protect You and Your Organisation

 serocu.police.uk/individuals



Protecting Our Communities

Short introduction from a local context

Thames Valley Cyber Crime Unit

Covering:

- Oxfordshire, Berkshire, Buckinghamshire
- Prepare / Protect / Pursue / Prevent
- Working with partners across the Force area
- Delivery of Victim Care guidance and signposting
- Delivering presentations to community groups, local organisations

Managed by SEROCU

Protect and Prepare

Pursue

Prevent

Crypto

Dark Web

Digital Forensics

Simple Steps to Protect You and Your Organisation

 serocu.police.uk/individuals

Cyber Aware – NCSC product and service



Take your email security to another level (For the individual)

Your email is where you keep your most personal and financial information.

If a hacker accesses your email, they could access your other online accounts using the 'forgot password' feature (which often sends you an email) access personal or business information and use this to scam you or people you know.

This guide outlines the Cyber Aware top tips and advice on how to:

-  Protect your **accounts** (How to guides are listed in each of the tips, via web links in blue)
-  Saving Passwords, Protect your **devices, data / information**

<https://www.ncsc.gov.uk/cyberaware/home>

Simple Steps to Protect You and Your Organisation

 serocu.police.uk/individuals

SOUTH EAST
ROCU | REGIONAL
ORGANISED
CRIME UNIT

Cyber Action Plan Tool

For individuals or sole traders, where you can receive personalised advice on how to improve your online security

58% of people are worried about their money being stolen online

53% are worried about having their personal details stolen online

48% are worried about their devices being infected by viruses or malware



<https://www.ncsc.gov.uk/cyberaware/actionplan>

Simple Steps to Protect You and Your Organisation

 serocu.police.uk/individuals

Action #1

Use a strong and different password for your email using 3 random words

Your email password should be strong and different from all your other passwords.

Using 3 random words is a great way to create a password that is easy to remember but hard to crack.

Do not use words that can be guessed (like your pet's name). You can include numbers and symbols if needed.

For example, “HippoPizzaRocket1”

Action 1: <https://www.ncsc.gov.uk/cyberaware/home>



Remembering Passwords – Browsers / Password Managers

Password managers: using browsers and apps to safely store your passwords



Need help remembering all your passwords? Get a password manager, or save them to your browser.

In addition, many password managers are helpful because they can:

- ✓ synchronise your passwords across your different devices, making it easier to log on, wherever you are, and whatever you're using
- ✓ help spot fake websites, which will protect you from phishing attacks
- ✓ let you know if you're re-using the same password across different accounts
- ✓ notify you if your password appears within a known data breach so you know if you need to change it
- ✓ work across platforms, so you could (for example) use a single password manager that would work for your iPhone and your Windows desktop

<https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers>

Simple Steps to Protect You and Your Organisation

 serocu.police.uk/individuals

Action #2

Turn on two-step verification (2SV)

2-Step Verification (2SV) gives you twice the protection.

2SV works by asking for more information to prove your identity.

For example, getting a code sent to your phone or authenticator App

You **won't** be asked for this every time you check your email.

The how:

https://www.ncsc.gov.uk/cyberaware/home#section_4

More detailed information:

https://www.ncsc.gov.uk/guidance/setting-2-step-verification-2sv#section_5



Backing up your Data and Updating your Devices

Backing up your data



ON THIS PAGE

1. [What is a backup?](#)
2. [Why might I need a backup?](#)
3. [Backing up using cloud storage](#)
4. [Backing up using removable media](#)
5. [Restoring backups](#)
6. [Recovering files deleted by mistake](#)

<https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data>

Install the latest software and app updates



Image credit: iStock.com/LPETTET

Applying security updates promptly will help protect your devices and accounts from cyber criminals.

You should apply updates to your apps and your device's software as soon as they are available. Updates include protection from viruses and other kinds of malware, and will often include improvements and new features.

Part of
Cyber Aware 

<https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates>

Simple Steps to Protect You and Your Organisation

 serocu.police.uk/individuals

SOUTH EAST
ROCU | REGIONAL
ORGANISED
CRIME UNIT

Suspicious Email / Texts and Website Reporting

How to recognise and report emails, texts, websites, adverts or phone calls that you think are trying to scam you.

PAGES

PAGE 1 OF 8

Phishing: Spot and report scam emails, texts, websites and calls

[Report a scam email](#)

[Report a scam text](#)

[Report a scam phone call](#)

[Report a scam website](#)

[Report a scam advert](#)

[Phishing scams: If you've shared sensitive information](#)

[How to spot a scam email, text message or call](#)



What is 7726?

Together we can stamp out scams



7726 is a number that **any** UK mobile customer can text to report suspicious calls and messages **free of charge**.

This alerts your mobile provider to **investigate** and potentially **block** the number to help protect you.

Simple Steps to Protect You and Your Organisation

 serocu.police.uk/individuals

Phishing Scams

Reporting suspicious messages

If you are suspicious of an email, report it by forwarding it to:

report@phishing.gov.uk

Checking websites:

<https://www.getsafeonline.org/checkawebsite>

Report suspicious websites to:

<https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-website>

If you are suspicious of a text, report it by forwarding it to:
7726

Reporting of nuisance calls to the Information Commissioners Office:

<https://ico.org.uk/make-a-complaint/nuisance-calls-and-messages/spam-texts-and-nuisance-calls/>



National Cyber
Security Centre
a part of GCHQ




Reported an email to the NCSC?

- seek to block the address the email came from
- work with hosting companies to remove links to malicious websites
- raise awareness of commonly reported suspicious emails and methods used (via partners)

As of August 2024 the number of reports received stands at more than:

 **34m** reported scams

Which has resulted in:

 **193k** scams being removed across 352,679 URLs

Simple Steps to Protect You and Your Organisation

 serocu.police.uk/individuals

SOUTH EAST
ROCU | REGIONAL
ORGANISED
CRIME UNIT

Data breaches:

guidance for
individuals
and families



What is a data breach?

A [data breach](#) occurs when information held by an organisation is stolen or accessed without authorisation.

Criminals can then use this information when creating [phishing messages](#) (such as emails and texts) so that they appear legitimate.

The message has been designed to make it sound like you're being individually targeted, when in reality the criminals are sending out millions of these scam messages.

Even if your details are not stolen in the data breach, the criminals will exploit high profile breaches (whilst they are still fresh in people's minds) to try and trick people into clicking on scam messages.

- **Fraudsters aren't fussy. They'll pick on anyone.**
- Nobody is immune from fraud. The criminals behind it target people online and in their homes, often emotionally manipulating their victims before they steal money or personal data.
- But there is something we can do. By staying vigilant and always taking a moment to stop, think and check whenever we're approached, we can help to protect ourselves and each other from fraud.
- **Did you know?**
- In just one year, 1 in 17 adults were victims of fraud
- Source: Crime Survey for England and Wales, year ending September 2023




Find out how to stay ahead of
scams at gov.uk/stopthinkfraud >>



UK Government

<https://stopthinkfraud.campaign.gov.uk/>

Simple Steps to Protect You and Your Organisation
 serocu.police.uk/individuals



Are you at risk?

What's the risk of fraud happening to you? Find out why anybody can become a victim of fraud and why everyone should take steps to protect themselves.



How to spot fraud

Find out how to spot the tactics and techniques commonly used by fraudsters, to help reduce your risk of becoming a victim.



Protect yourself from fraud

Find out what you can do today to help protect yourself, your loved ones and your business from fraud.

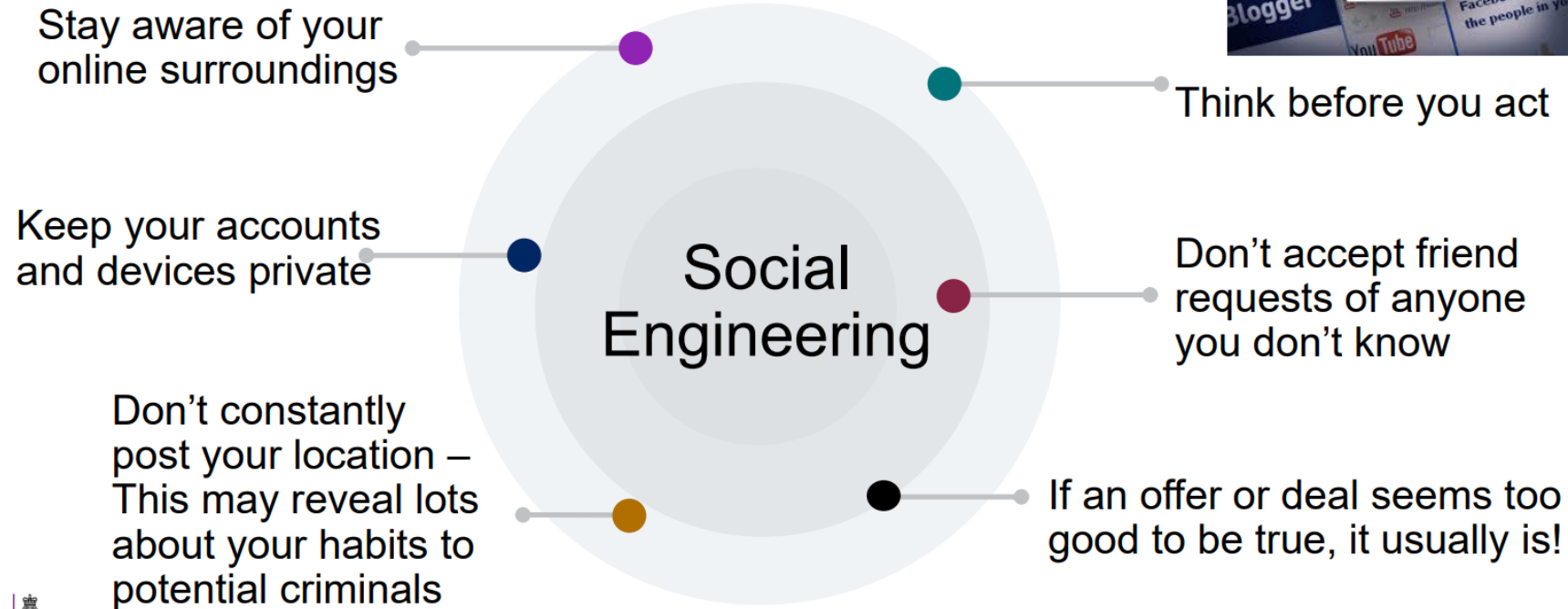


Recovery from fraud

Learn how to access practical advice and support and what steps you can take if you've lost money or data.

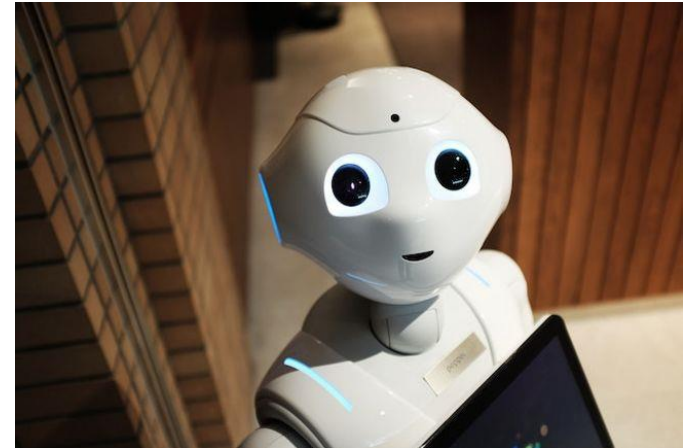
MY SOCIAL ENGINEERING CHECKLIST

How to defend yourself



Guidance for AI and GI (Generative Intelligence)

1. Be mindful of personal information. ...
 2. Understand privacy settings. ...
 3. Don't overshare. ...
 4. Think critically. ...
 5. Report inappropriate content. ...
 6. Be cautious with AI-generated messages. ...
 7. Don't solely rely on AI. ...
- Stay informed.



Reporting of Fraud / Cyber crime

Action Fraud customer channels



Social Media

Help and advice.
How to protect against fraud.
News and alerts.
Real time fraud intelligence.



0300 123 2040

Report fraud and cyber crime.
Help, support and advice.



24/7 Live cyber

Specialist line for business, charities or organisations
suffering live cyber attacks

Report 24/7 & Web Chat

www.actionfraud.police.uk

Secure online reporting.
News and Alerts.
Advice on avoiding the latest scams.

<https://www.actionfraud.police.uk/>

Simple Steps to Protect You and Your Organisation

 serocu.police.uk/individuals



<https://southeastcyber.police.uk/>

Thanks for participating, we hope that this session was of value to you?

Do please take a few moments before we conclude to fill in this short engagement survey, thank you.

https://www.smartsurvey.co.uk/s/ThamesValley_Individuals/



If you've seen something that doesn't feel right, STOP!

- don't click on any links
- don't give out any personal or bank details
- break contact if needed
- tell family and friends to make them aware
- **Report to Action Fraud**

Action Fraud is the reporting centre for fraud and cyber crime in England, Wales and Northern Ireland. If you've been scammed, defrauded or experienced cyber crime, [report it to Action Fraud](#) online or by calling [0300 123 2040](tel:03001232040).

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

