HAMPSHIRE CYBERWATCH

Claire Wills

Cyber Champion

❖ **What is Cyber crime?**

❖ **How does Cyber crime work?**

❖ **How do we protect ourselves ?**

❖ **How do you report Cyber crime ?**

❖ **Where to get further information / support ?**

HAMPSHIRE CYBERWATCH

How does Cyber Crime work?

IT PAYS TO STOP AND THINK

1. Never disclose security details
2. Don't assume an email, text or phone call is genuine
3. Don't be rushed
4. Listen to your instincts
5. Stay in control

TAKE FIVE
TO STOP FRAUD

Take the test - https://www.takefive-stopfraud.org.uk

Spam Email

Social Media ads or messages

Text or Whats App messages

Unsolicited Phone calls

How can we protect ourselves?

Be **"Cyber Aware"** – search "cyber aware" or visit https://www.ncsc.gov.uk/cyberaware/home

Here you can find out:

How to secure your e-mail   *How to use two-step verification (2SV)*

How to store passwords securely

How to backup your data   *How to keep your devices updated*

How can we protect ourselves?

Phone   Computer   Bank   Shopping   Social Media   Bills   Contacts

Your email is where you keep your most personal and financial information.
If a cyber criminal accesses your email, they could:

• access your other online accounts using the 'forgot password' feature (which often sends you an email)

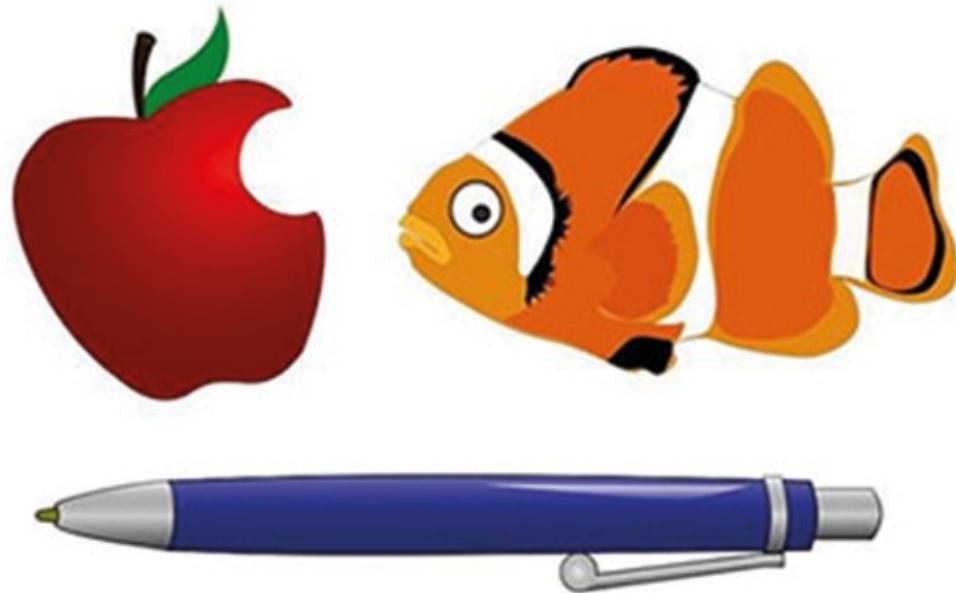• access personal or business information and use this to scam you or people you know

How can we protect ourselves?

Secure your e-mail with a strong passphrase – three random words

Complex passwords are hard for people to remember and no more difficult to crack than letters on their own.

Choosing three random words and stringing them together into a phrase is easier to remember than a password with number substitution and the length makes it harder for computers to crack.

A password of 12 or more characters is recommended by NCSC.

Three random words – 'applenemopen' or 'fruitflounderbiro'

How can we protect ourselves?

Turn on Two-step verification (2SV) (also known as 2FA)

2-step verification involves using a second device to verify your identity.

This could be a mobile phone app, a chip and pin device, a fingerprint reader or even a telephone.

Most banks use an authentication device to enable online banking. This works in the same way as a 2SV app on your phone.

Using 2SV will normally stop a criminal accessing your data, even with your password!

How can we protect ourselves?

Use a Password Manager or Browser Password store

We all have lots of passwords these days and the temptation is to use the one password that you can remember for all accounts.

Password managers will securely suggest and store long passwords for you, often across multiple devices, and you only have to remember the one passphrase (*made of three random words, of course*!)

Take care on shared computers!

Use a strong memorable password to secure your password manager

How can we protect ourselves?

Backup your device's data regularly

Backing up your data will ensure that you are able to recover critical information in the event of your computer becoming corrupted or getting stolen.

You can back up to a USB stick, an external hard disk or a cloud account.

Most computers, tablets or phones have software built in to take backups.

Back up any data that would inconvenience you if it were lost

How can we protect ourselves?

Keep your devices up to date

Computer manufacturers regularly release operating system and security updates, as do the providers of anti-virus software.

These should be downloaded and applied as soon as they are available to stay as secure a possible.

If you get an update notification, install the updates as soon as you can

How can we protect ourselves?

Check your Privacy settings

All social media platforms have privacy settings to help you keep your personal information private.

Advice on protecting your accounts can be found on the NCSC advice and guidance page.

Don't over share - Keep your personal information private!

How can we report Cyber crime?

If you think you have been the victim of a Cyber crime or fraud, it can be easily reported by visiting the Action Fraud website.

You report a Cyber Crime or fraud offence by telephone to Action Fraud using **0300 123 2040**.

If you have suffered financial loss, you should also contact your bank or credit card provider.

Phishing attempts can be simply forwarded to report@phishing.gov.uk or if they are text messages, by forwarding them to 7726.

Reporting Cyber crime helps investigators and protects future victims

HAMPSHIRE CYBERWATCH

A Quick recap:

Secure your e-mail accounts   **Use 2-step verification**   **Backup your devices**

Use a password manager   **Keep devices updated**   **Use privacy settings**

Need further help?

Search "**cyber aware**" to get up to date information.

Contact your local **Hampshire CyberWatch** Cyber Champion for advice or contact Blue Lamp Trust Cyber Bobby Scheme via
[CYBER BOBBY SCHEME | THE BLUE LAMP TRUST](#)

Thank you for listening!   Any Questions?