Cyber Protect Webinar with

Mr Mark Godsland CISMP
Police Cyber Security Advisor
Thames Valley Police

Summary document following the ‘Protecting your “Internet” connected devices + your online identity / footprint’ on 15th October 2020

Please view with the notes page visible for additional, information guidance

Cyber Aware Stay connected. Stay Cyber Aware.

@SECyberprotect SECyberprotect SEROCU Cyber Protect South East ROCU Cyber Protect

National Cyber Security Centre a part of GCHQ

South East Regional Organised Crime Unit Cyber Crime Unit

Cyber Aware

"Cyber Aware is the UK government's advice on how to stay secure online during coronavirus"

@CYBERAWARE 6 TOP TIPS

- 1. Create a separate password for your email
- 2. Create a strong password using three random words
- 3. Save your passwords in your browser
- 4. Turn on two-factor authentication
- 5. Update your devices
- 6. Turn on backup

These Cyber Aware tips are the baseline for members of the public from which all guidance from the National Cyber Security Centre(NCSC) is applied: https://www.ncsc.gov.uk/cyberaware/home

If you wish more in-depth guidance visit the associated page on the main NCSC website:

https://www.ncsc.gov.uk/section/information-for/individuals-families#section_4

Create a separate password for your email
Your personal email account contains lots of important information about you and is the gateway to all your other online accounts.
If your email account is hacked all your other passwords can be reset, so use a strong password that is different to all your others.

Create a strong password using three random words
Weak passwords can be hacked in seconds. The longer and more unusual your password is, the stronger it becomes and the harder it is to hack. The best way to make your password long and difficult to hack is by using a sequence of three random words you'll remember.

You can make it even stronger with special characters. Starting with your most important accounts (such as email, banking and social media), replace your old passwords with new ones. Just connect three random - but memorable - words together.

Save your passwords in your browser
Using the same passwords for all your accounts makes you vulnerable - if that one password is stolen all your accounts can be accessed. It’s good practice to use different passwords for the accounts you care most about.

Of course, remembering lots of passwords can be difficult, but if you save them in your browser then you don’t have to. Online service providers are constantly updating their software to keep sensitive personal data secure, so store your passwords in your browser when prompted; it’s quick, convenient and safer than re-using the same password

What is two factor authentication?

Simply, it adds an extra step to your login process meaning you have to confirm your identity, usually using a second device. For example, receiving a text message with a code to type in online.

This is important because it gives you an extra layer of protection so if a criminal is able to get hold of your passwords, they still won't be able to log in to your account.

We recommend enabling this for your most important accounts:

- Social media accounts
- Email accounts
- Online banking (all banks should already have this enabled as standard)

National Cyber Security Centre

Protecting devices

From viruses and malware

This page contains tips about how to protect your computers, laptops, smartphones and tablets from the damage caused by viruses and other types of malware. Following these steps will help keep your devices - and the information stored on them - free from harm. For more information, please refer to **www.ncsc.gov.uk/antivirus** .

Viruses are a type of malicious software that can harm devices such as computers, laptops, smartphones and tablets.

Once your device has been infected, this **mal**icious soft**ware** (also known as **malware**) can steal your data, erase it completely, or even prevent you from using your device.

Devices can become infected by accidentally downloading an email attachment that contains malware, or by plugging in a USB stick that is already infected. You can even get infected by visiting a dodgy website.

For these reasons, it's important that you **always use antivirus software on your laptops and PCs**. Smartphones and tablets don't need antivirus software, provided you **only install apps and software from official stores** such as Google Play and Apple's App Store.

Turn on your antivirus product

Antivirus (AV) products detect and remove viruses and other kinds of malware from your computer, laptop or MAC, and should always be used.

- **Make sure your AV product is turned on and up to date.** Windows and iOS have built-in tools that provide suitable AV.
- **New computers often come with a trial version of additional AV software. You may want to carry out your own research to find out if these products are right for you.**
- **Make sure your AV software is set to automatically scan all new files, such as those downloaded from the internet or stored on a USB stick, external hard drive, SD card, or other type of removable media.**
- **You don't need AV products on your smartphone or tablets, provided you only install apps from official stores.**
- **If you think your computer has been infected, open your AV software, and run a full scan. Follow any instructions given.**
- **If you receive a phone call offering help to remove viruses and malware your computer, hang up immediately (this is a common scam).**

Keep all your IT devices up to date

Don't put off applying updates to your apps and your device's software; they include protection from viruses and other kinds of malware.

- **Applying software updates is one of the most important things you can do to protect your devices. Update all apps and your device's operating system when you're prompted.**
- **Set all software and devices to update automatically, including your AV software.**
- **You should consider replacing devices that are no longer supported by manufacturers with newer models. You can search online to see how long your current device will be officially supported.**

Only install official apps

Download on the App Store

GET IT ON Google Play

Only download apps for smartphones and tablets from official stores (like Google Play or the App Store). Apps downloaded from official stores have been checked to provide protection from viruses and malware.

5 things to consider when backing up your data.

Think about how much you value what data you have saved on your device or in a separate device or in the Cloud. Now imagine how long you would be able to operate without them, if it were lost, damaged, compromised.

In you are concerned by this, then perhaps you should take regular backups of the important data, and make sure that these backups are recent and can be restored.

Furthermore, if you have backups of your data that you can quickly recover, you can't be blackmailed by ransomware attacks.
This section outlines 5 things to consider when backing up your data.

Tip 1: Identify what data you need to back up

Tip 2: Keep your backup separate from your computer /device

Tip 3: Consider 'the cloud'

Tip 4: Make backing up a regular occurrence?

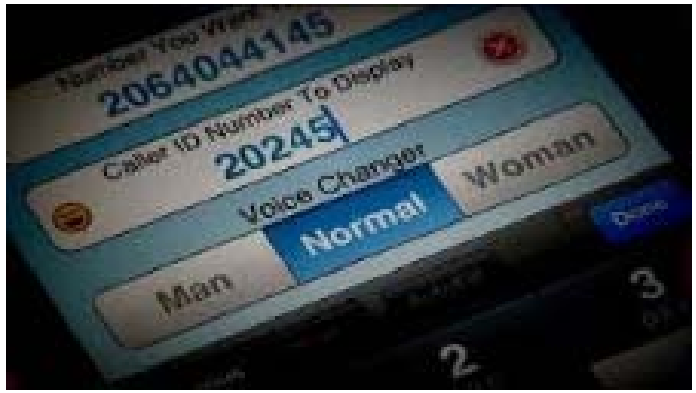
Tip 5: Test your back up

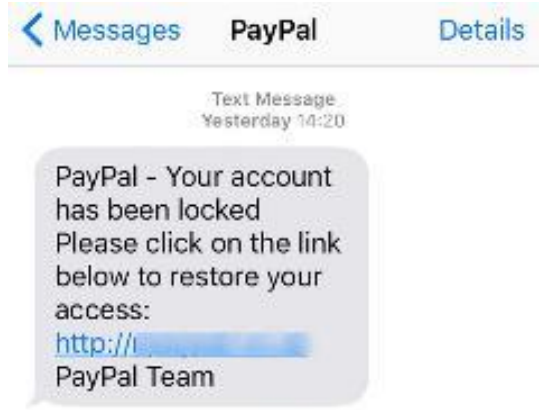
If you want a more locally focused source of the previous content, please visit the Thames Valley Police recent “6 Days to Cyber Secure” release page

https://rlsd.co/p/QF1kKQ#

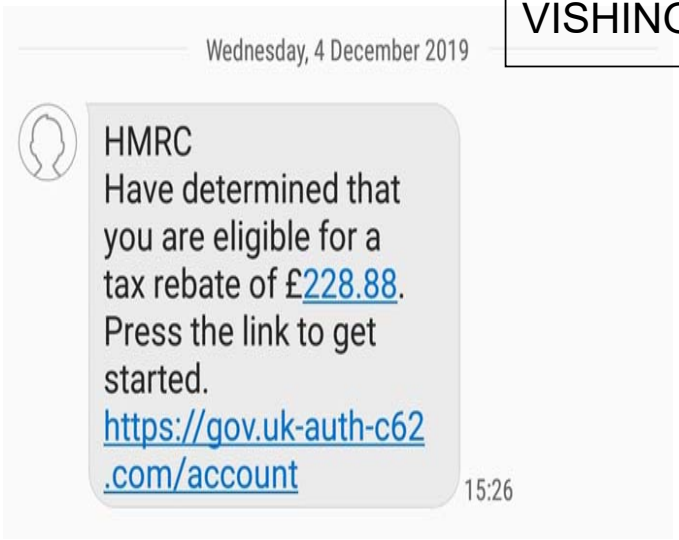
Information covered

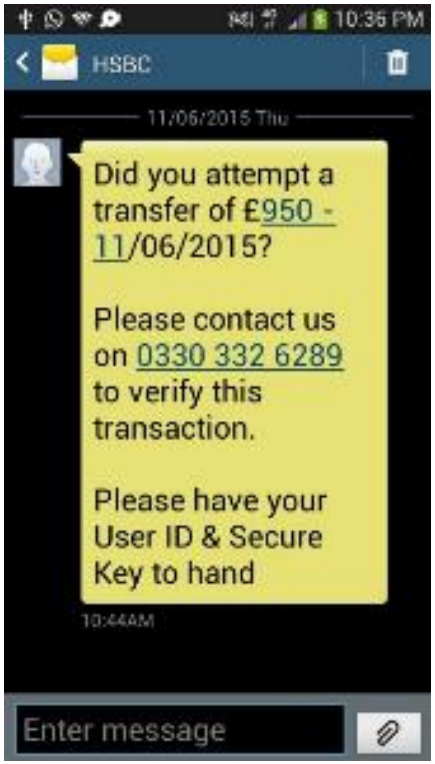
Explainer for the topic to be covered
Explanatory Video
How to guides
Quiz





SPAM PHISHING	emails to all
SPEAR PHISHING	targeted email phishing
SOCIAL MEDIA PHISHING	targeted phishing
POSTAL PHISHING	phishing by post
SMISHING	SMSs can be spoofed
VISHING	CALLS can be spoofed





National Cyber Security Centre

Reported an email to the NCSC?

The NCSC will analyse the suspect email and any websites it links to.

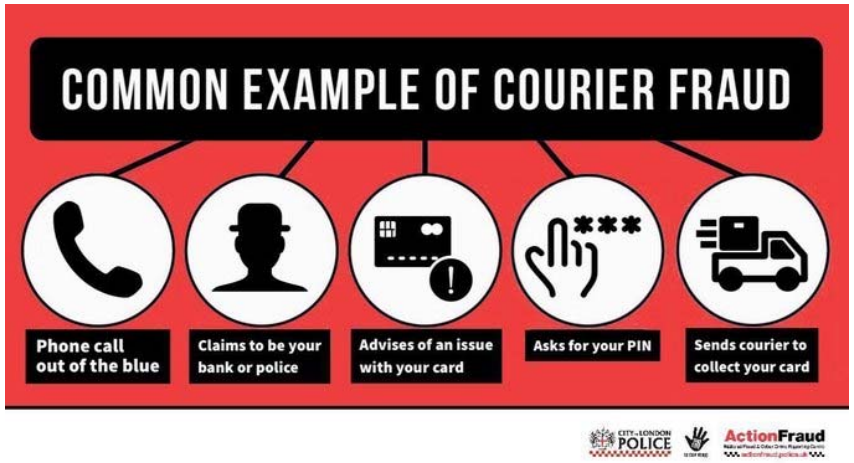
If they discover activity that they believe is malicious, they may:

- seek to block the address the email came from, so it can no longer send emails
- work with hosting companies to remove links to malicious websites
- raise awareness of commonly reported suspicious emails and methods used (via partners)

Whilst the NCSC is unable to inform you of the outcome of its review, we can confirm that they do act upon every message received.

Suspicious Texts, Forward to 7726

Keep up to date:
https://www.actionfraud.police.uk/news

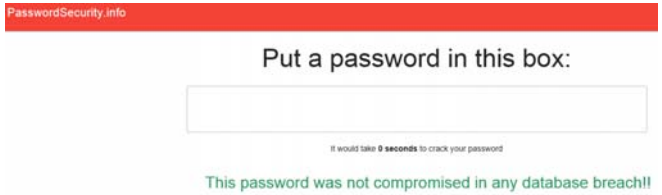


DATA BREACHES

General Data Protection Regulation became enforceable on 25/5/18
Possible fines of 4% of global turnover or €20M by the Information Commissioners Office

www.haveibeenpwned.com allows you to check if personal data has been compromised

"Notify me" allows you to subscribe to future breaches which often alerts you to breaches long before it reaches the news meaning you can take action immediately instead of your accounts being at risk for months without you knowing



https://passwordsecurity.info/- is another resource that you can use where you can see if your #Password has been 'hacked'.

Have you been affected by a data breach?

| How to protect yourself |

Financial details

If your financial data was compromised, be vigilant against any unusual activity in your bank accounts or suspicious phone calls and emails asking for further information. If you notice any unauthorised transactions, notify your bank or card company.

Phishing messages and calls

Criminals may use your personal details to target you with convincing emails, texts & calls. Be suspicious of unsolicited requests for your personal or financial details. If you receive an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS): **report@phishing.gov.uk**

Report fraud

If you think you have been a victim of fraud or cybercrime, report it to Action Fraud at **Actionfraud.police.uk**

City of London Police | ActionFraud | Cyber Aware

Consumer Guidance for Smart Devices in the Home

Smart or internet-connected devices, such as smart TVs, music speakers, connected toys or smart kitchen appliances can bring great benefits to your daily life. However, without taking steps to secure all of your internet-connected products, you and your data could be at risk from someone getting unauthorised access to your device or account. Developed by the UK government and industry experts, this guidance will help you manage the security of your devices and help protect your privacy.

SETTING-UP YOUR DEVICE

- **Read and follow the set-up instructions** for the device. These are often found in an app downloaded onto your smartphone, tablet or from a paper manual and guide that comes with the product.
- **Check device instructions to see if you need to** create an account on the manufacturer's website, or download any other recommended apps.
- If you are prompted to enter a password during the set-up process that is easy to guess, (such as 'admin' or '00000'), **you should change it**. Guidance on creating a strong password can be found on the **Cyber Aware** website.

MANAGING YOUR ACCOUNT

- To **set-up and manage your device**, you may need to create or use an existing account on the manufacturer's website. This account may allow you to add a new device or link your smartphone to your devices. You should ensure that your account has a **strong password**.
- For added security, if the device or app offers **Two Factor Authentication** which provides a second layer of security, (such as a text message to your phone) you should enable it. This is particularly important if the account contains your **personal data** or **sensitive information** or is linked to something that may impact your or another persons physical safety.
- **Some products allow you to access or control them** when you are away from your home's Wi-Fi network; such as, to view security camera footage. Consider whether you need to make use of this feature, as products may allow you to disable it either in the app settings or within your account.

KEEP UPDATING YOUR SOFTWARE AND APPS

Much like your laptop and smartphone, software and app updates help keep your devices secure. You should:

- **Check whether you can set-up and enable automatic updates** (on the app or on your online account).
- **Install the latest software and app updates**. These updates should download and install automatically on your device. If not, then you should install them straight away so you have the latest security protections. You should be prompted when a new update is ready to install, usually via a pop-up message or in the settings menu in the app or device menu.

IF YOU BECOME AWARE OF AN INCIDENT AND THINK IT AFFECTS YOUR DEVICE

- **Visit the manufacturer's website** to see if there is information available on what you should do next.
- Check the **National Cyber Security Centre** and the **Information Commissioner's Office** websites to see any published guidance.
- Further advice on your consumer rights can be found on the **Which?** and **Citizens Advice** websites.

HM Government

CYBER AWARE

www.cyberaware.gov.uk

National Cyber Security Centre

Recovering “Hacked Accounts”

Once you know your account has been hacked, this is what you should do:

1. Update your devices

2. Contact your provider

3. If your email account was hacked

4. Change passwords

5. Set up 2-factor authentication

6. Notify your contacts

7. If you can't recover your account

8. Contact Action Fraud

Identity theft

Identity theft happens when fraudsters access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to commit identity fraud. Identity theft can take place whether the fraud victim is alive or deceased.

If you're a victim of identity theft, it can lead to fraud that can have a direct impact on your personal finances and could also make it difficult for you to obtain loans, credit cards or a mortgage until the matter is resolved.

https://www.actionfraud.police.uk/a-z-of-fraud/identity-fraud-and-identity-theft

Identity fraud

Identity fraud can be described as the use of that stolen identity in criminal activity to obtain goods or services by deception. Fraudsters can use your identity details to:

Open bank accounts.
Obtain credit cards, loans and state benefits.

Order goods in your name.
Take over your existing accounts.

Take out mobile phone contracts.
Obtain genuine documents such as passports and driving licences in your name.
Stealing an individual’s identity details does not, on its own, constitute identity fraud. But using that identity for any of the above activities does.

The first you know of it may be when you receive bills or invoices for things you haven’t ordered, or when you receive letters from debt collectors for debts that aren’t yours.

Prevention

Do not share account information with friends, family or other people.

Ensure you always have effective and updated antivirus/antispyware software running.
If possible, arrange for paperless bills and statements.

File sensitive documents securely, and shred those you no longer need – preferably with a cross-cut shredder.

Never divulge private information data in response to an email, text, letter or phone call unless you are certain that the request is from a bona fide source.

Always beware of people looking over your shoulder when you are entering private information on a computer, smartphone/tablet or ATM.

What should you do if you've been a victim of identity fraud?

Act quickly – you mustn't ignore the problem. Even though you didn't order those goods or open that bank account, the bad debts will end up under your name and address.

If you believe you're a victim of identity fraud involving plastic cards (e.g. credit and debit cards), online banking or cheques, you must report it to your bank as soon as possible. Your bank will then be responsible for investigating the issue and they will report any case of criminal activity to the police. The police will then record your case and decide whether to carry out follow-up investigations.

If you think you're a victim of another kind of identity fraud, you must report the matter to the relevant organisation. Depending on their advice, you should then alert your local police force.

You should report all lost or stolen documents – such as passports, driving licences, plastic cards, cheque books – to the relevant organisation.

Understanding your digital footprint

It's worth exercising some caution when using social media. Not everyone using social media is necessarily who they say they are. Take a moment to check if you **know** the person, and if the friend/link/follow is genuine.

Less obviously, you should think about your digital footprint, which is a term used to describe the entirety of information that you post online, including photos and status updates. Criminals can use this publicly available information to steal your identity, or use it to make phishing messages more convincing.

You should:
•Think about **what** you're posting, and **who** has access to it. Have you configured the privacy options so that it's only accessible to the people you want to see it?

•Consider what your followers and friends **need** to know, and what detail is unnecessary (but could be useful for criminals).
•Have an idea about what your friends, colleagues or other contacts say about **you** online.

Nb: CPNI's Digital Footprint Campaign, contains a range of useful materials (including booklets) to help understand the impact of your digital footprint.

Action Fraud customer channels

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

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.

National Fraud and Cyber Crime Reporting Centre

2,000+ calls per day
250+ web chats per day

Cifas Data
UK Finance

https://reporting.actionfraud.police.uk/login

Summary

The Cyber Aware site has the entry level of 6 top tips
https://www.ncsc.gov.uk/cyberaware

Not forgetting the TVP 6 Days to Cyber Secure, which is entirely based on Cyber Aware 6 Top Tips: https://rlsd.co/p/QF1kKQ#

The National Cyber Security Website, guidance on cyber security advice to protect you and your family, and the technology you rely on.

https://www.ncsc.gov.uk/section/information-for/individuals-families

For the 'Infographics' used in the presentation applicable for individuals, families:

https://www.ncsc.gov.uk/information/infographics-ncsc#section_1

Links to the videos you may wish to view and consider

Passwords: Social engineering to obtain & demonstration the poor quality of such, when protecting “Key Accounts”
https://youtu.be/opRMrEfAIiI

Coffee Shop video – “How much are you sharing on your social media accounts”
https://youtu.be/X0VtC_Q6NrY

Cyber Choices – Divert young people away from falling foul of the Computer Misuse Act
https://youtu.be/UIoGmA4VwEk

Cyber Griffin – Working From Home
https://youtu.be/uyKPDlPxrTY

TVP Protect Team: cyber.protect@thamesvalley.pnn.police.uk **(Not for reporting)**

Follow us on Twitter **@TVPCyber_Fraud**

Get the latest reports from the National Cyber Security Centre:

- Cyber Alerts & Advisories: https://www.ncsc.gov.uk/section/keep-up-to-date/ncsc-news
- Thames Valley Alerts: https://www.thamesvalleyalert.co.uk/
- Action Fraud Alerts: https://www.actionfraud.police.uk/sign-up-for-action-fraud-alert
- Please take just a few moments to complete our anonymous engagement survey, thank you. https://www.smartsurvey.co.uk/s/Individual-ThamesValley2021/

Follow our social media for simple and practical advice on how to protect yourself from fraud and cybercrime

Cyber Aware Stay connected. Stay Cyber Aware.

@SECyberprotect SECyberprotect SEROCU Cyber Protect South East ROCU Cyber Protect

National Cyber Security Centre
a part of GCHQ