Protecting yourself from cybercrime and fraud

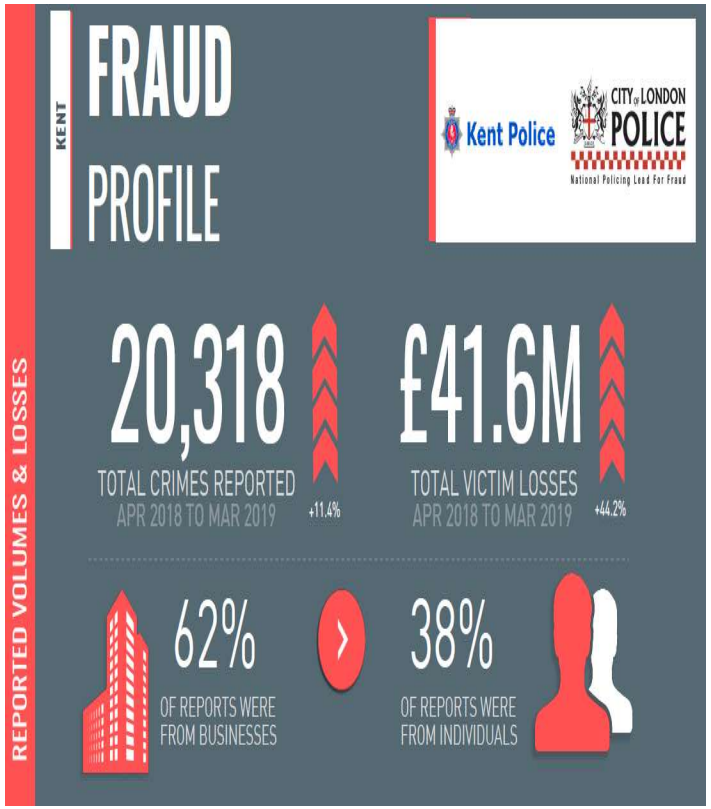
AIMEE PAYNE

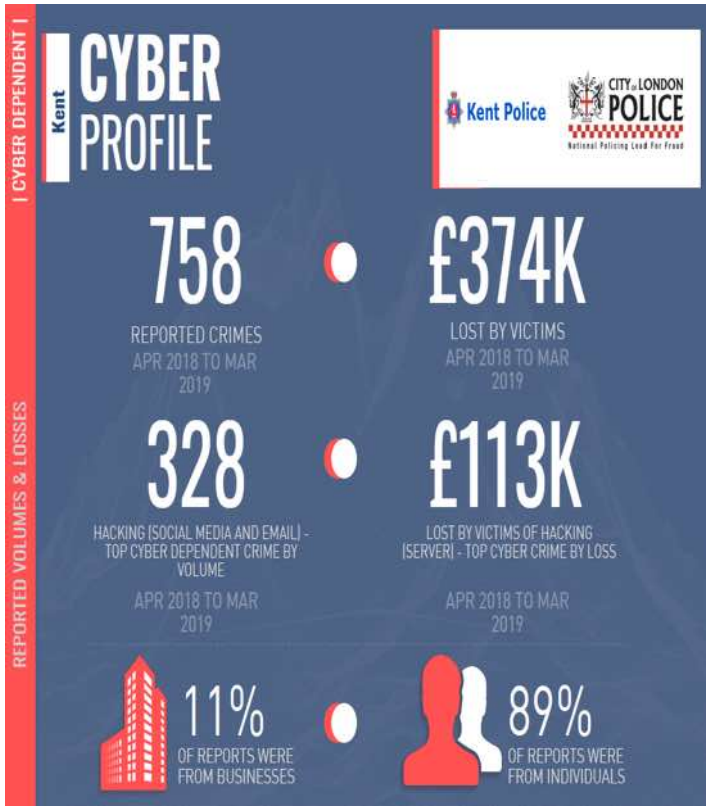
CYBER PROTECT & PREVENT OFFICER

KENT POLICE – SERIOUS CRIME DIRECTORATE

Kent Police

Crime has gone digital





Two types of cybercrime

Cyber-dependent

Crimes that can only be committed by using a computer to attack another computer

Eg: Hacking, Spread of Viruses, Ransomware, DDOS

Cyber-enabled

'Traditional' crimes which are increased in their scale by the use of computers

Eg: Fraud, identity theft, harassment, romance scams

The attraction

Traditional Crime

- Offender required to be present at crime scene
- One offence at a time
- Evidence/ Forensics/ CCTV
- Witnesses
- HIGH RISK/ LOW REWARD

Cybercrime

- Not present at the scene
- Multiple offences at the same time
- Commit offences from anywhere in the world
- Co-operation required between law enforcement internationally
- LOW RISK/ HIGH REWARD

Key Message

80% of all Cyber Crime is easily preventable by adopting basic measures and being aware.

Remember A, B, C

- A – Accept nothing
- B – Believe no one!
- C – CONFIRM EVERYTHING!

Are you aware of exactly how much you are sharing?

https://www.youtube.com/watch?v=yrjT8m0hcKU

Social Engineering

Understanding your digital footprint ?

Subject: RE: Your Delay at the Gate
From: info@BudgetAirlineUK.com
To: john.smith123@email.com

Dear Mr Smith,

We are sorry to hear that you were delayed at the airport when checking in at Manchester Airport on the 19th of October, for your flight number BUDNY1910 to New York. We hope it didn't spoil your trip!

As an apology Budget Airline UK would like to offer you a discount of 50% of your next flight, as well as complementary First Class upgrade.

All you need to do is fill in the form by clicking the link below, and we will send out the voucher codes to you.

http://complaints.budgetairlineuk.com/voucher/50percent.html

We hope to see you again soon

King regards

Dave Cameroon
Senior Complaints Handler
Budget Airline UK

Social Media

- Never disclose private information when social networking
- Be wary about who you accept invitations from
- Consider what you are saying online
- Look for the verification tick

How secure is your Social Media?

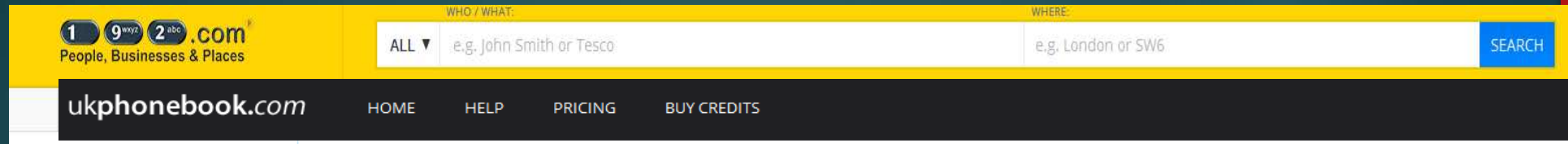
- We strongly advise that you opt for “Friends only”.
- Be a good friend and change your settings to ‘hide’ your friends list to protect their security too. Also helps prevent account cloning issues – do the same for contact details!
- Be mindful that “friends” settings can affect your own security
- It is advised you turn app location settings off when you post to social media as it indicates your current location …. AND where you are NOT!
- Remember regularly checking in to places, regardless of your settings ‘checking in’ is publically viewable
- Change your settings so that you control what others post about you!

Take a few minutes to review your digital footprint…

Quite simply, Google yourself!

Limit the amount of information made PUBLICLY available

Check www.ukphonebook.com
www.192.com



PHONE NUMBERS
ADDRESSES/POSTCODES
FIND A PERSON
COMPANY SEARCH
DIRECTOR SEARCH
TPS/CTPS
TELEAPPENDING
ZONESEARCH
MAPS
CREDIT REPORTS
AREA CODES
LAND REGISTRY

Saved results
No saved results.

Person Search - Find a Person

Find a person by searching the edited UK electoral register, the phone book, and consumer data.

Find this person:

aimee payne

Search

☑ Exact matches only

Refine search further:

Location: City, town, village or postcode

Street: Street or road

Premises: House name or number

Gender(s): Any

Age Range: Min age Min. Max age Max.

DOB: DD MM YYYY

Specify second resident: Full name of second resident

Search

How to delete this information ?

- Firstly remove yourself from the Public Electoral Roll - You are automatically enrolled upon voting, meaning anyone can request your information, this can make you a target so contact your local council.
- By going through public databases like the Electoral Roll, websites such as 192.com are able to collate your address, home phone number & more details all in one place. For a small fee, anyone can then discover a large amount of information about you that you may have considered relatively private.
- Once you have removed yourself from the public electoral roll, you can then remove yourself from the 192 website and UK phonebook website by completing the online request form.

Phishing Attacks

Spotting the signs…

- ▶Authority – claiming to be someone official
- ▶Urgency – a limited time to respond
- ▶Emotion – panic, fear, hopeful or curious
- ▶Current events – will use current news reports to seem realistic

National Cyber Security Centre

Phishing attacks

Dealing with suspicious emails

Phishing emails try to convince users to click on links to dodgy websites or attachments, or to give sensitive information away (such as bank details). This advice includes tips about how to spot the most obvious signs of phishing, and what to do if you think you've clicked a bad link. For more information, please visit www.ncsc.gov.uk/phishing .

What is phishing?

Phishing is when criminals attempt to trick people into doing 'the wrong thing', such as clicking a link to a dodgy website.

Phishing can be conducted via a text message, social media, or by phone, but the term 'phishing' is mainly used to describe attacks that arrive by email.

Criminals send phishing emails to **millions of people**, asking for sensitive information (like bank details), or containing links to bad websites. Some phishing emails may contain viruses disguised as harmless attachments, which are activated when opened.

Make yourself a harder target

Information from your website or social media accounts leaves a 'digital footprint' that can be exploited by criminals. You can make yourself less likely to be phished by doing the following:

- Criminals use publicly available information about you to make their phishing emails appear convincing. Review your privacy settings, and think about what you post.
- Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you.
- If you do spot a suspicious email, flag it as Spam/Junk in your email inbox, and report this to Action Fraud (www.actionfraud.police.uk).

What to do if you've already clicked ?

The most important thing to do is not to panic. There are number of practical steps you can take:

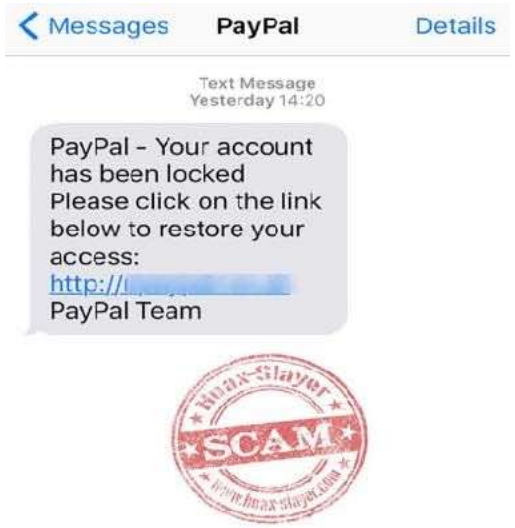
- Open your antivirus (AV) software, and run a full scan. Follow any instructions given.
- If you've been tricked into providing your password, you should change your passwords on all your other accounts.
- If you have lost money, you need to report it as a crime to Action Fraud. You can do this by visiting www.actionfraud.police.uk.

Tell tale signs of phishing

Spotting a phishing email is becoming increasingly difficult, and even the most careful user can be tricked. Here are some tell tale signs that could indicate a phishing attempt.

- Is the email addressed to you by name, or does it refer to 'valued customer', or 'friend' or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- Others will try and create official-looking emails by including logos and graphics. Is the design (and quality) what you'd expect?
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?
- Your bank (or any other official source) should never ask you to supply personal information in an email. If you need to check, call them directly.
- If it sounds too good to be true, it probably is. It's most unlikely that someone will want to give you free trainers, or codes to access films for free.

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq



And it's not just emails…

Email Top Tips…

- Ensure your spam filter is on
- Do not open an email you suspect could be spam and send straight to your spam or junk folder
- Don’t open attachments or click links from unknown sources
- If it’s too good to be true- it probably is!
- Consider having two separate email accounts (public & private)

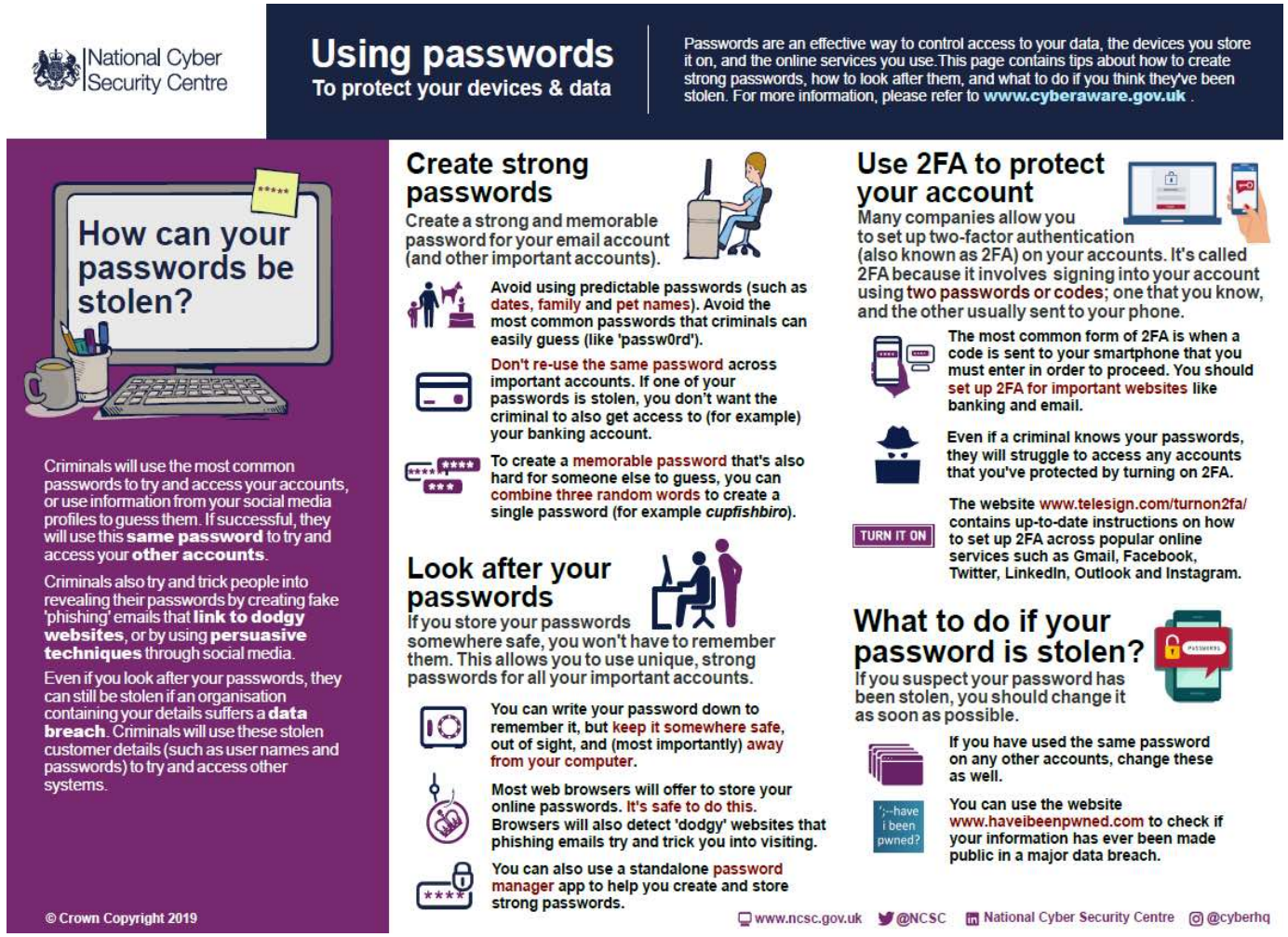
Passwords Top Tips…

- Think of your password as your front door
- Think passphrase! Choose three random unrelated words

  VioletMouseCuppa

  Vi0letMou$eCupp@

- Use a different password for each website
- Use a password manager
- If your password is compromised – change it immediately



Two/ Multi Factor Authentication

- Adds a second layer of security to your accounts
- Receive a text/ email if a new device is used to access your account
- Gives you the opportunity to confirm if the user is you
- Visit TeleSign website for more information

www.haveibeenpwned.com

A website that allows you to check if your personal data has been compromised by data breaches.

"Notify me" service allows visitors to subscribe to notifications about future breaches. Once signed up, you will receive an email message any time their personal information is found in a new data breach.

This service often alerts users to breaches long before it reaches the news, meaning that you can take action immediately instead of your accounts being at risk for months without you knowing.

actionfraud.police.uk/report-phishing

Spotted a suspicious email?

If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS)

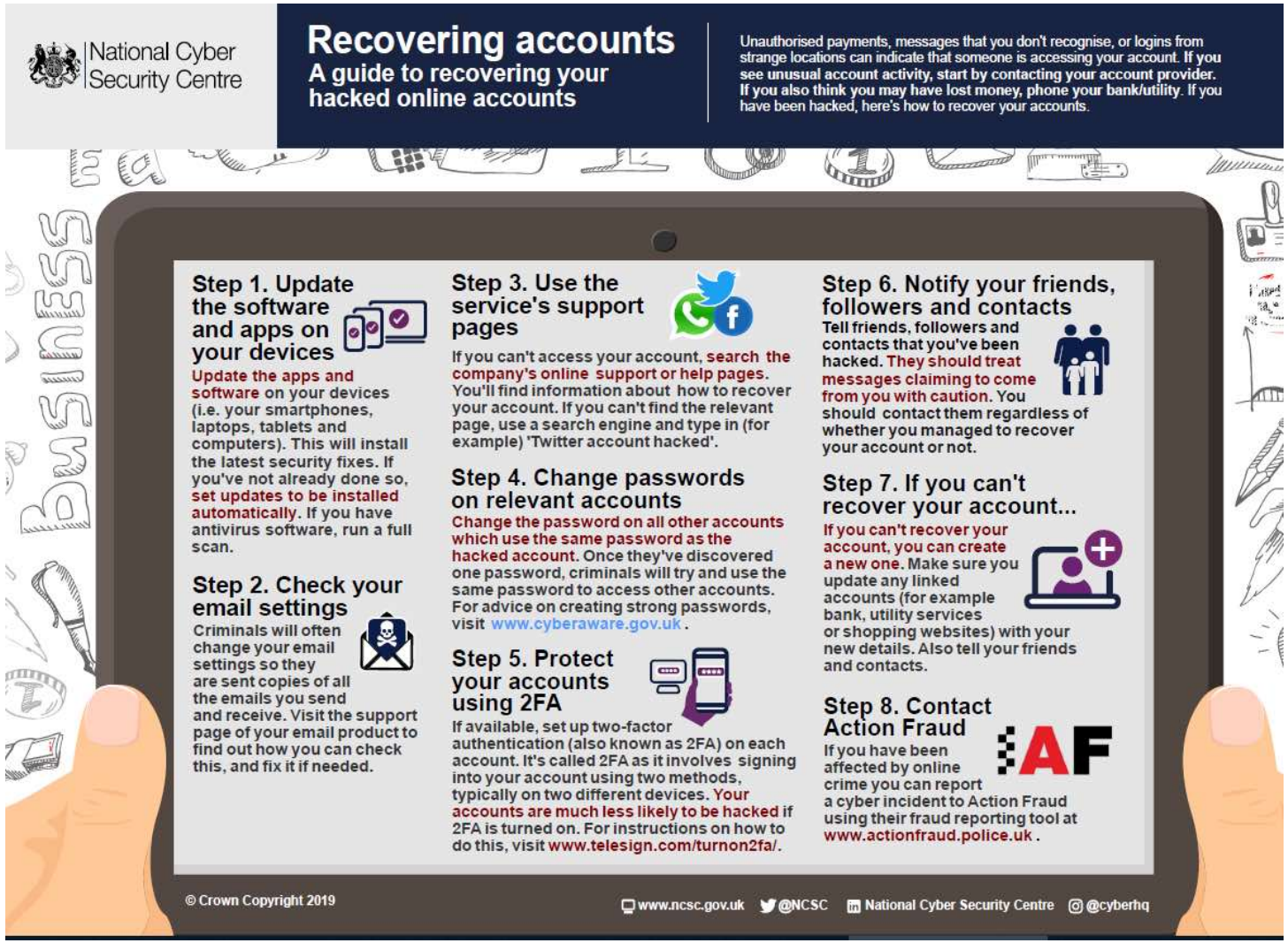
report@phishing.gov.uk

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

Cyber Aware

Recovering a hacked account ?

- Update your devices
- Contact your provider
- If your email was hacked ? Check the filtering rules
- Change passwords
- Set up 2-Factor authentication
- Notify your contacts



What is Ransomware ?

- Ransomware is a malicious software that prevents you from accessing your computer.
- If your computer is infected with ransomware the computer will be locked and a ransom is requested to unlock your computer.

Ransomware Top Tips..

- Make a regular back up – ensure this isn't permanently connected
- Keep your operating system and apps up to date
- Install antivirus and keep it turned on and up to date
- Be careful what apps you install
- Don't pay ransom, there's no guarantee you will get your files back.
- Contact Action Fraud or the Police

National Cyber Security Centre

Ransomware
Prevention & recovery

Following this advice can reduce the likelihood of you becoming a victim of ransomware. Ransomware makes your data or computers unusable and asks you to make a payment to release it. If your computer is already infected with ransomware, we've included some useful recovery steps below. For more information, please refer to www.ncsc.gov.uk/ransomware .

What is ransomware?

Ransomware is malicious software that prevents you from accessing your computer (or data that is stored on your computer).

If your computer is infected with ransomware, the computer itself may become **locked**, or the data on it might be **stolen**, **deleted** or **encrypted**.

Normally you're asked to make a payment (the ransom), in order to 'unlock' your computer (or to access your data).

However, even if you pay the ransom, there is **no guarantee** that you will get access to your computer, or your files. This is one of the reasons why it's important to always have a recent backup of your most important files and data.

Don't be blackmailed - keep a backup!

If you have a recent backup of your most important files, then you can't be blackmailed.

Make regular backups of your most important files (such as photos and documents), and check that you know how to restore the files from the backup. If you're unsure how to do this, you can search online.

Make sure the device containing your backup (such as an external hard drive or a USB stick) is not permanently connected to your computer.

Turn on auto-backup so that data on your smartphone is automatically copied to the cloud. This means you'll be able to recover your data quickly by signing back into your account from another device.

Protecting your data and devices

The following steps will reduce the likelihood of your devices being infected with ransomware.

Keep your operating system and apps up to date. Apply software updates promptly, they contain patches that keep your device secure, including protection from ransomware and other types of virus.

Make sure your antivirus product is turned on and up to date. Windows and macOS have built in malware protection tools which are suitable for this purpose.

Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide protection from viruses.

What to do if you are infected

If your computer has been infected by ransomware (or any type of malware), you should:

Open your antivirus (AV) software, and run a full scan. Follow any instructions given. If your AV can't clean your device, you'll need to perform a 'clean re-install', which will remove all your personal files, apps and settings. If you're unsure how to do this, you can search online using another device.

Restore your backed-up data that you have kept on a separate device (such as USB stick, external hard drive) or cloud storage. Do not copy any data from the infected computer.

If you receive a phone call offering help to clean up your computer, hang up immediately (this is a common scam).

Anyone who thinks they may have been subject to a ransomware attack should contact Action Fraud (www.actionfraud.police.uk). Organisations should call 0300 123 2040. In Scotland, contact the police by dialing 101.

Should I pay the ransom?

The NCSC encourages you **not** to pay the ransom. If you do:

- there is no guarantee that you will get access to your data or computer
- your computer will still be infected
- you will be paying criminal groups
- you're more likely to be targeted in the future

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

Sextortion

https://www.bbc.co.uk/news/av/stories-46323625/what-happened-when-sextortion-scammers-targeted-a-bbc-trending-reporter

Sextortion scam Top Tips..

- Do not engage – delete & report to Action Fraud
- Don't pay the ransom!
- Don't worry if they have your password – Change it
- If you have paid the ransom – call 101 immediately

National Cyber Security Centre

Sextortion phishing scams
How to protect yourself

This advice is for people who have received sextortion emails. If someone you don't know is blackmailing you by claming to have login details or a video of you visiting an adult site, **don't pay the ransom**, but follow the steps below instead. The criminals behind these attacks don't know if you have a webcam, or if you've visited adult websites.

What is a sextortion scam?

A **sextortion scam** is when a criminal attempts to **blackmail** someone, usually by email. The criminal will claim they have login details or a video of the victim visiting an **adult website**, and will threaten to disclose this unless the victim pays a **ransom** (often in BitCoin).

The criminals behind these attacks do **not** know if you have a webcam, or know if you've visited adult websites. They are attempting to **scare their victims** into paying a ransom, and will send millions of emails in the hope that someone will pay. They'll often include technical sounding details to make the email sound convincing. It may also include a password the victim uses or has used.

Sextortion is an example of a **phishing attack**, where victims receive emails that try and **trick them** into doing the wrong thing.

What to do if you're being blackmailed

Don't communicate with the criminal

Our advice is to **not** engage with the criminal. If you have received an email which you're not sure about, forward it to the NCSC's suspicious Email Reporting Service (SERS): report@phishing.gov.uk.

Don't pay the ransom

If you pay the ransom, you might be targeted with more scams, as the criminal will know their previous scam worked.

Check if your accounts have been compromised

Do not worry if your password is mentioned. It has probably been discovered from a previous data breach. You can check by visiting https://haveibeenpwned.com/

Change any passwords that are mentioned

If a password you still use is included, then change it immediately. For advice on how to create good passwords, please visit www.cyberaware.gov.uk .

Report any losses to Action Fraud

If you have already paid the ransom, then report it to Action Fraud (www.actionfraud.police.uk).

www.ncsc.gov.uk
@NCSC
National Cyber Security Centre
@cyberhq

Do you use Public WIFI ?

WIFI Top Tips…

- Don’t use public WIFI for sensitive transactions
- Use 3G 4G - this is always encrypted
- Use a Virtual Private Network (VPN)
- Turn off WIFI when your not using it

Computer Security

- Install Anti-Virus on all devices and set to automatically update
- Update your software as soon as your computer prompts you
- Back up your data to an external device and remove that device from your computer
- Check Op Systems are supported and running the latest version (Windows 7 end of life was January 2020)
- Only install official apps from your app store

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 **malicious software** (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

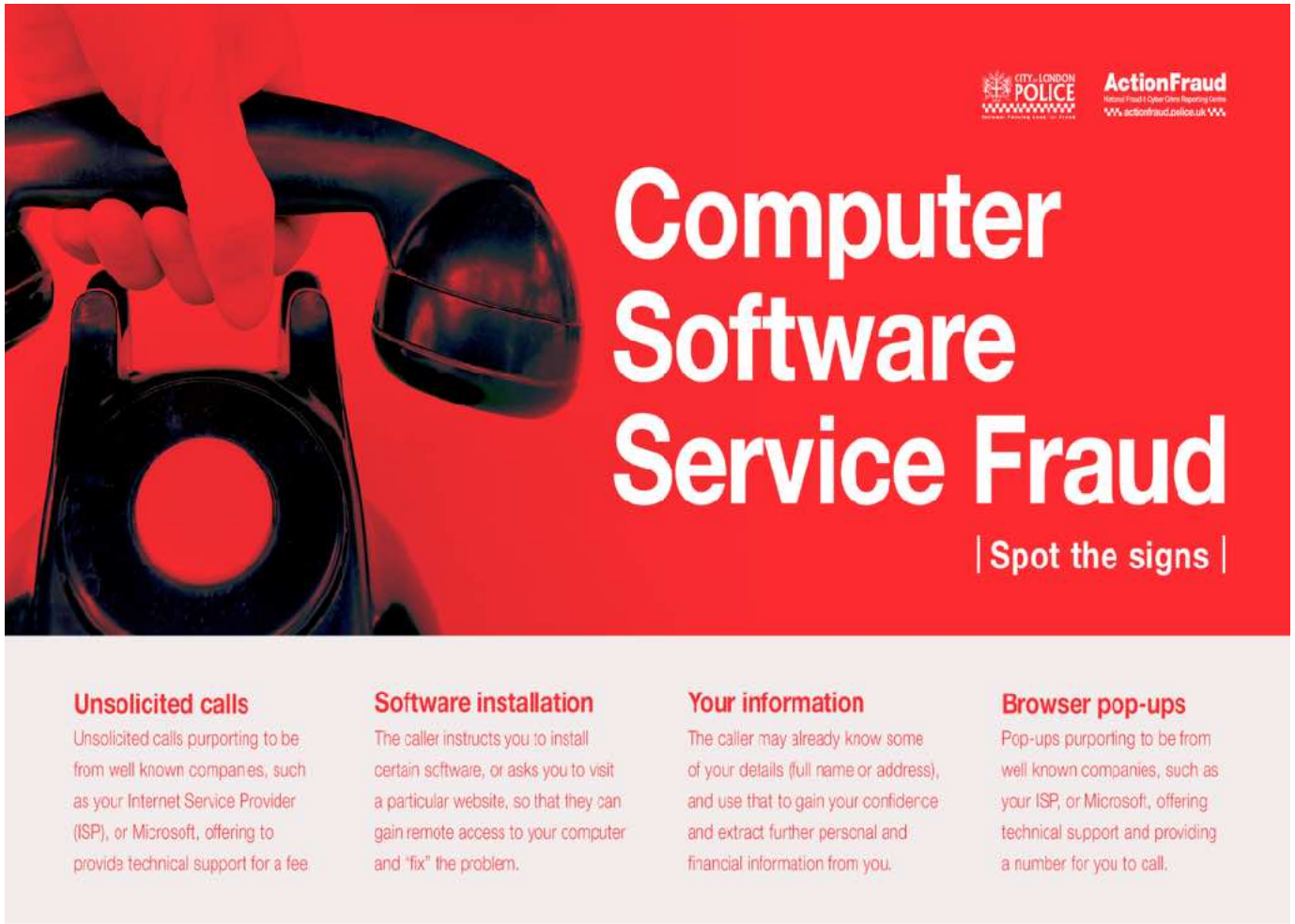
Download on the App Store · GET IT ON Google Play

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.

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

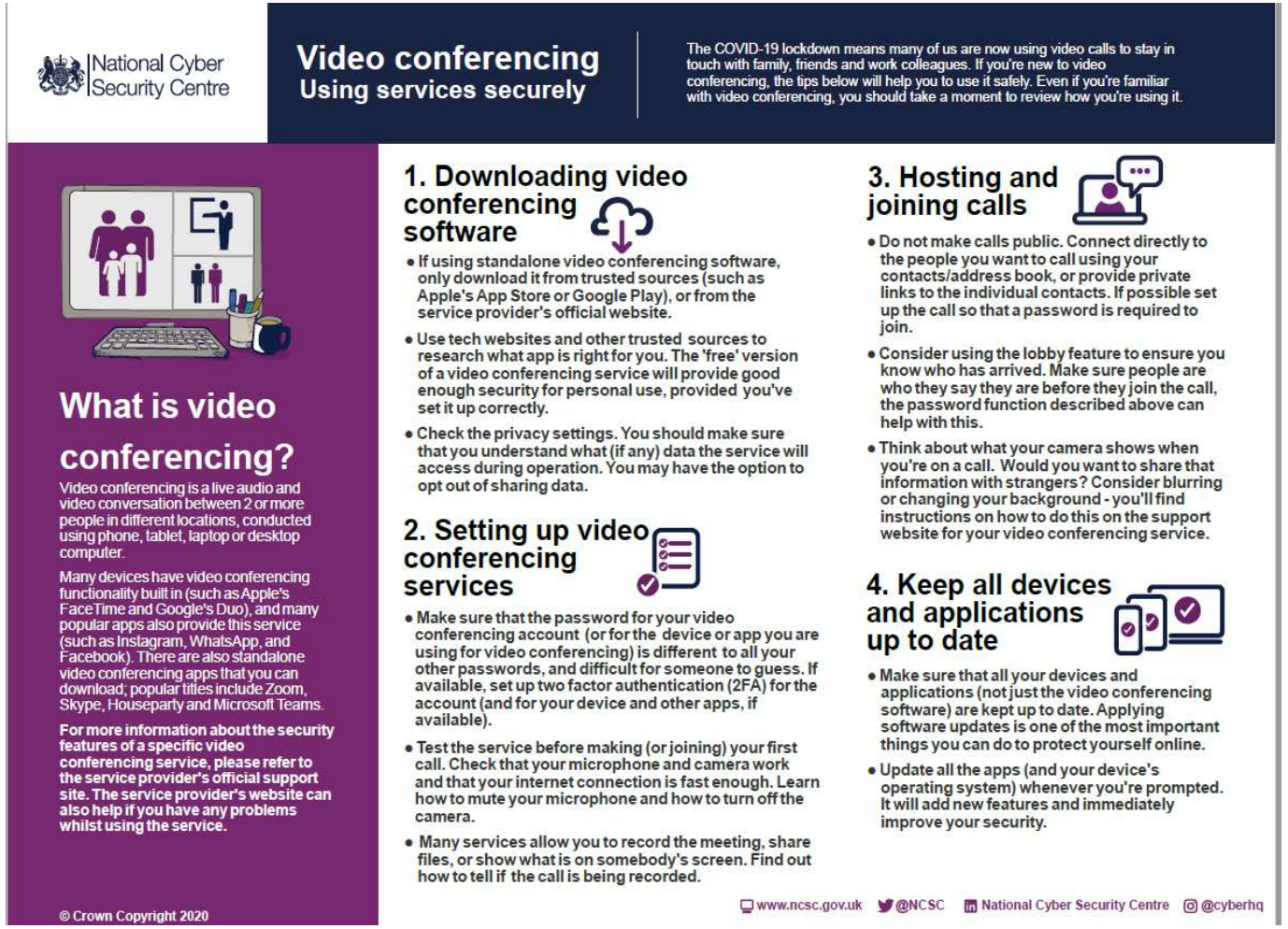
CSSF Top Tips….

- NEVER allow a cold caller remote access to your device
- NEVER reveal your personal or financial details
- NEVER install any software or visit a website as a result of a cold call
- A legitimate company wouldn't cold call you, if your unsure hang up and call them back from a different phone and the number you have for them.
- Consider investing in a call blocking system (Truecall, Call Guardian or speak to your service provider)



Video Conferencing Top Tips…

- Only download the software from trusted sources
- Do your research – free one is fine as long as you set it up correctly
- Check the privacy settings
- Use a password – 2FA if available
- Consider using the “lobby” feature
- Keep all video conferencing apps up to date – it will add new features and keep it up to date



National Cyber Security Centre

Video conferencing
Using services securely

The COVID-19 lockdown means many of us are now using video calls to stay in touch with family, friends and work colleagues. If you're new to video conferencing, the tips below will help you to use it safely. Even if you're familiar with video conferencing, you should take a moment to review how you're using it.

What is video conferencing?

Video conferencing is a live audio and video conversation between 2 or more people in different locations, conducted using phone, tablet, laptop or desktop computer.

Many devices have video conferencing functionality built in (such as Apple's FaceTime and Google's Duo), and many popular apps also provide this service (such as Instagram, WhatsApp, and Facebook). There are also standalone video conferencing apps that you can download; popular titles include Zoom, Skype, Houseparty and Microsoft Teams.

For more information about the security features of a specific video conferencing service, please refer to the service provider's official support site. The service provider's website can also help if you have any problems whilst using the service.

1. Downloading video conferencing software

- If using standalone video conferencing software, only download it from trusted sources (such as Apple's App Store or Google Play), or from the service provider's official website.
- Use tech websites and other trusted sources to research what app is right for you. The 'free' version of a video conferencing service will provide good enough security for personal use, provided you've set it up correctly.
- Check the privacy settings. You should make sure that you understand what (if any) data the service will access during operation. You may have the option to opt out of sharing data.

2. Setting up video conferencing services

- Make sure that the password for your video conferencing account (or for the device or app you are using for video conferencing) is different to all your other passwords, and difficult for someone to guess. If available, set up two factor authentication (2FA) for the account (and for your device and other apps, if available).
- Test the service before making (or joining) your first call. Check that your microphone and camera work and that your internet connection is fast enough. Learn how to mute your microphone and how to turn off the camera.
- Many services allow you to record the meeting, share files, or show what is on somebody's screen. Find out how to tell if the call is being recorded.

3. Hosting and joining calls

- Do not make calls public. Connect directly to the people you want to call using your contacts/address book, or provide private links to the individual contacts. If possible set up the call so that a password is required to join.
- Consider using the lobby feature to ensure you know who has arrived. Make sure people are who they say they are before they join the call, the password function described above can help with this.
- Think about what your camera shows when you're on a call. Would you want to share that information with strangers? Consider blurring or changing your background - you'll find instructions on how to do this on the support website for your video conferencing service.

4. Keep all devices and applications up to date

- Make sure that all your devices and applications (not just the video conferencing software) are kept up to date. Applying software updates is one of the most important things you can do to protect yourself online.
- Update all the apps (and your device's operating system) whenever you're prompted. It will add new features and immediately improve your security.

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

UK CORONAVIRUS SCAMS

City of London Police – National Policing Lead For Fraud

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

Cyber Aware

NHS Test and Trace

Contact tracers will NEVER:

- Ask you for any form of payment
- Ask you for any passwords or PINs
- Ask any details about your bank account
- Ask you to download anything
- Ask you to hand over control of your PC
- Send someone to your home

For more information, visit:
actionfraud.police.uk/testandtrace

OFFICIAL

#coronavirusfrauds

Romance Scam Definition….

*'The intended victim is befriended on the Internet and eventually convinced to assist their new love financially by sending them money for a variety of emotive reasons'*1.

Romance Fraud Top Tips…

- Don’t rush into an online relationship – get to know the person, not the profile and ask plenty of questions.
- Analyse their profile and check the person is genuine by putting their name, profile pictures or any repeatedly used phrases and the term ‘dating scam’ into your search engine.
- Talk to your friends and family about your dating choices. Be wary of anyone who tells you not to tell others about them.
- Evade scammers by never sending money to, or sharing your bank details with, someone you’ve met online, no matter what reason they give or how long you've been speaking to them.
- Stay on the dating site messenger service until you’re confident the person is who they say they are. If you do decide to meet in person, make sure the first meeting is in a public place and let someone else know where you’re going to be.

Courier Fraud Top Tips…

- Never divulge passwords or PIN codes to people over the phone – you cannot be sure who you are speaking to
- Police, HMRC or Banks will NEVER send a courier/unmarked unit to collect bank cards/PINs for investigation!
- There is no such thing as a "Safe Account". Banks nor Police will ever ask for funds to be transferred to one
- Police will never ask you to be involved in 'undercover' operations

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

Further information and advice

General advice on Cyber Security and Passwords:
National Cyber Security Centre www.ncsc.gov.uk
& Cyber aware www.cyberaware.com

Online safety on all areas for everyone:
GetSafeOnline www.getsafeonline.org

CEOP online safety for under 18s, parents and schools:
ThinkUknow www.thinkuknow.co.uk & www.internetmatters.org

Advice on spam emails, spam phonecalls and scams
Take 5 to Stop Fraud https://takefive-topfraud.org.uk/

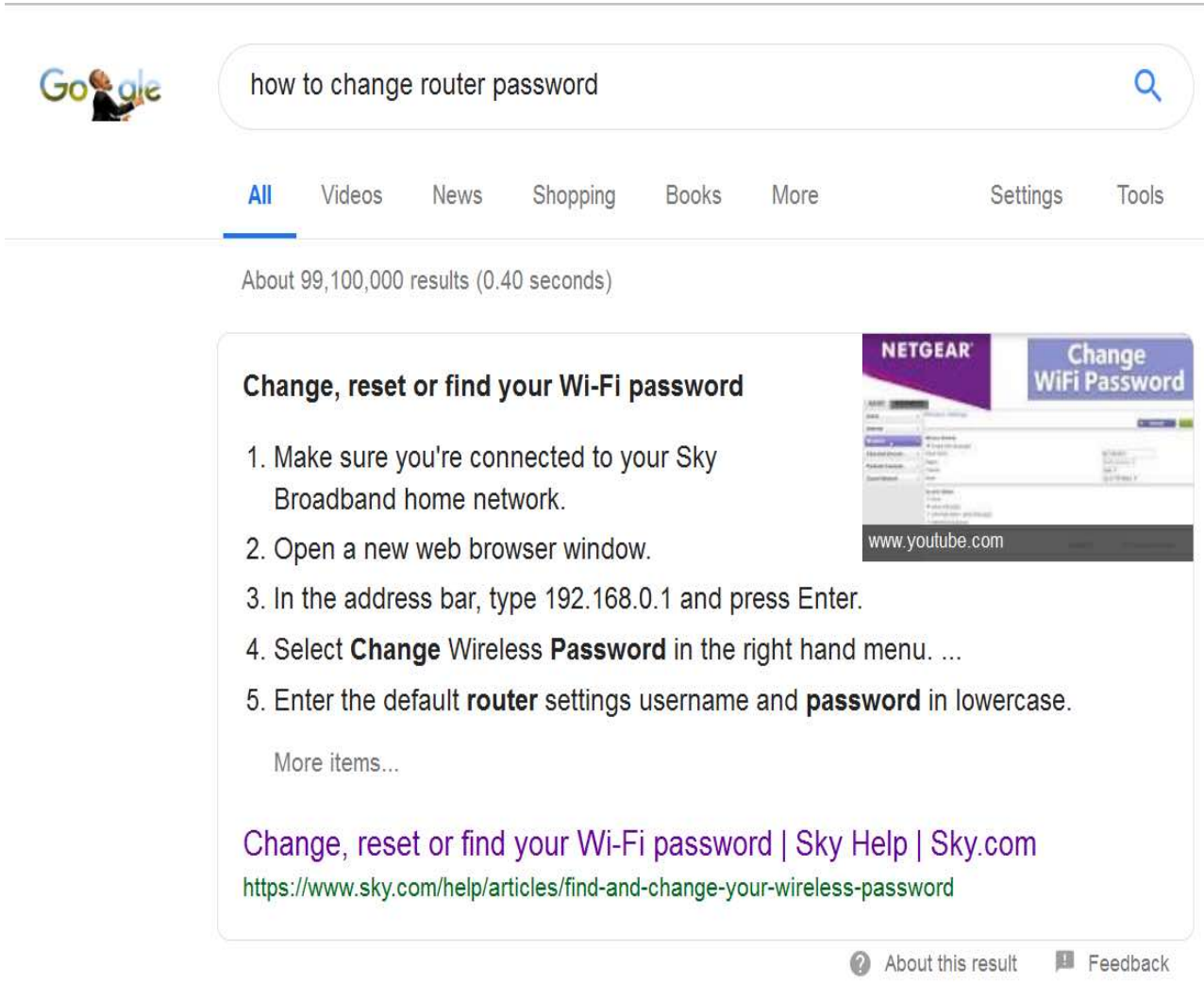
Follow us @kentpolicecyber

VS VICTIM SUPPORT

Support and advice for victims

Checklist:

- Check Op Systems are supported and running the latest version
- Check Firewalls, Antivirus, Antimalware and Antispyware are installed, running and regularly updated
- Check your passwords are secure / strong and not used across platforms
- Check your digital footprint
- Check public electoral roll, UK Phonebook & 192.com for entries in your name – request removal
- Check your social media settings
- Check your email address with www.haveibeenpwned.com and set up Two/multi Factor Authentication (2FA)
- Ensure your home router has a password set, if the original default, change it
- Don't use public WiFi for sensitive transactions such as banking/social media/ email unless you've set up a VPN, or revert to 3G/4G on your device
- *Share this information with family, friends, and the public!*



How to change your router password ?

EXAMPLE....

Questions ?

AIMEE PAYNE
CYBER PROTECT & PREVENT OFFICER
SERIOUS ECONOMIC CRIME UNIT
KENT & ESSEX SERIOUS CRIME DIRECTORATE
AIMEE.PAYNE@KENT.POLICE.UK
TWITTER - @KENTPOLICECYBER