Cybercrime Guidance for Individuals

How to keep you and your family safe and secure online

DRAFT

Cybercrime Guidance for Individuals

‘Cybercrime’ and ‘cyber security’ can both sound daunting or somewhat irrelevant until you or a family member becomes a victim of online criminality. This may be the moment where you might have wished you had taken a few simple steps to protect you, your finances, and your personal information. From banking, to shopping, streaming and social media, people of all ages are spending more time online than ever before. Our smartphones, tablets, laptops and computers hold more and more information about our lives, including our banking details, our precious pictures and videos of our lives, and important emails from a whole range of services and organisations. Losing this information, or losing access to all this data, which is a fundamental part of most of our lives, can be traumatic. A few simple steps can make things more difficult for cyber criminals who are seeking to access our details and accounts.

If a criminal can access your email account, they could:

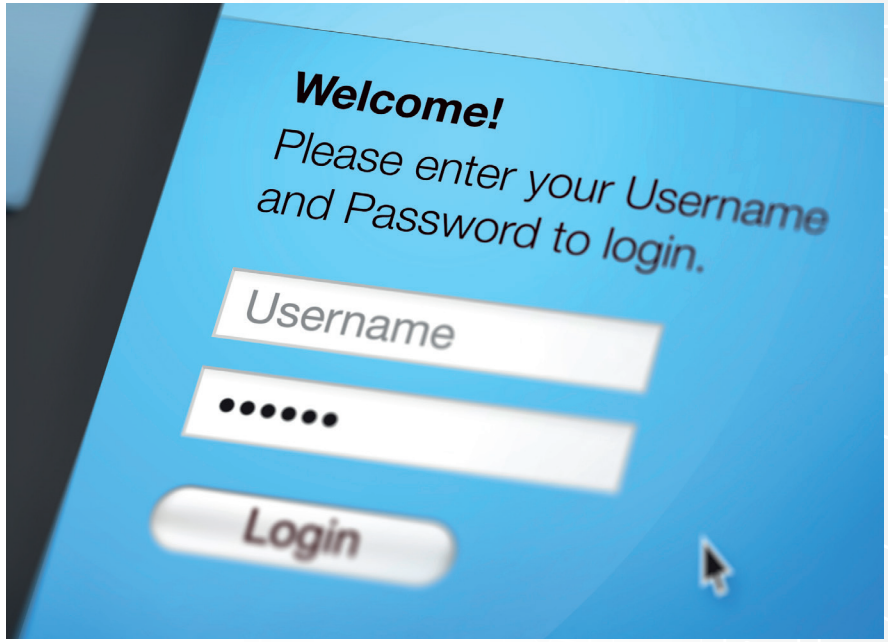
- access private information about you (including your banking details)
- post emails and messages pretending to be from you (and use this to trick other people)
- reset all your other account passwords (and get access to all your other online accounts)

Simple actions to protect against cybercrime

ACTION 1

Use strong and different passwords for your email using 3 random words

Create strong passwords using three random words. Hackers don’t have to try very hard in many cases as people still use obvious or commonly used passwords. They will even try different versions of words that can be linked you from social media such as favourite sports teams, family names or pets (for example ‘Brighton’, ‘Br1ght0n’, ‘br!ght0n’). Use three random words, and add numbers or special characters, for example ‘BlueJamDinner’ or ‘BlueJ@mD1nner’.



ACTION 2

Turn on 2-Step Verification (2SV) for your email

Even if cyber criminals have your password, 2-Step Verification (2SV)[1] adds an added layer of protection by asking for more information to prove your identity. For example, you may get a code sent to your phone when you sign into a new device or change your settings, such as your password. Some platforms will ask for this code every time that you sign in, but not all.

1. This is also known as 2-Factor Authentification (2FA) or Multi-Factor Authentication (MFA)

Now you have taken these first important steps, with just a few more actions you can improve your cyber security even further.

ACTION 3

Use different passwords for all your accounts and applications

With a strong password protecting your email, you should ensure it's different to passwords you use for other accounts, applications or programmes.

Remembering many different passwords can be challenging but your web browser will give you the option to save and remember them for you. You can also use a password manager. This is a safe way to store this information

ACTION 4

Always update software and applications when prompted.

Even when software is thoroughly tested vulnerabilities or bugs can be found and technology companies are continually working to improve and fix these issues. Don't ignore prompts and reminders to update all your devices as they contain important fixes which will help keep hackers out. You can make things simpler by activating automatic updates.

ACTION 5

Make sure you make regular backups of your data and information.

Most of us at some point have been unable to access important data, whether it's work documents, photos, videos, contact details or other personal information. Sometimes this is because of devices failing but it can also be because cyber criminals are denying you access.

Making a backup of this important information is essential so that you can recover all of your information and not fall foul of technical failure or online criminality.

A backup is a copy of your important data that's stored in a separate safe location, usually on the internet (known as cloud storage), or on removable media (such as USB stick, SD card, or external hard drive). As a rule of thumb, you should back up anything you value and would inconvenience you if you could no longer access it.

It doesn't take very long to make backups, you can decide what you want to backup (for example, documents, photos, videos) and they can usually be set to take place automatically. A little bit of planning your backup routine in advance could save you a lot of stress should the worst happen.

Once you've made your backup, you can restore a copy of your original data from the backup, should you lose access to it.

Phishing and how to spot and report scam emails, texts, websites and calls

'Phishing' is when criminals use scam emails, text messages or phone calls to trick people into giving away bank details or other personal information. Often it involves encouraging people to visit unsafe websites which may download a virus onto your device or harvest your information to sell online. Committing fraud is a criminal offence.

Phishing can take many forms, but in broad terms:

phishing is where an email or text that seems to be from a legitimate company asks you for your personal details, confirmation of login or bank details or passwords; or it may try to install malicious software on your device

vishing, refers to an automated phone message or a cold-caller seemingly from a legitimate company asking you for personal details or confirmation of your personal or banking details

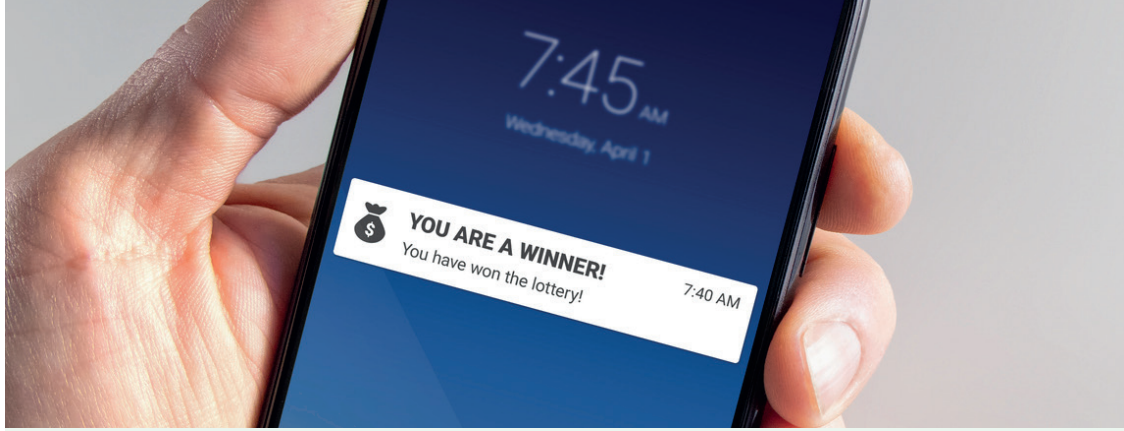
spear phishing, usually focuses on a targeted individual at work where the email appears to come from a legitimate organisation.

Using these methods, cyber criminals ask for information or confirmation of information such as **login details, passwords or banking details.** Unsafe emails may direct you to a website which may install malware on your computer.

If the information stolen during a phishing attack includes phone numbers, you might receive a suspicious call. The approach may be more direct, asking you for sensitive information (such as banking details or passwords), or access to your computer.

You can reduce the likelihood of being phished by thinking about what personal information you (and others) post about you, and by reviewing your privacy settings within your social media accounts.

As a general rule, **never give your personal or financial details to anyone unless you know and trust them.**



How to spot scam messages or calls

Cyber criminals are getting smarter in how they use scams to obtain personal data and information, some even fool the experts.

These scammers try to quickly gain your trust, aiming to pressure you into acting without thinking.

If a message or call makes you suspicious, stop, break the contact, and if an email or text, consider the language it uses.

Scams often feature one or more of these tell-tale signs.

Authority

Is the message claiming to be from someone official? For example, your bank, doctor, a solicitor, the tax office, or a government department. Criminals often pretend to be important people or organisations to add pressure on you into doing what they want.

Urgency

Are you told you have a limited time to respond (such as ‘within 24 hours’ or ‘immediately’)? Criminals often threaten you with fines, penalties or other negative consequences

Emotion

Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.

Scarcity

Is the message offering something in short supply, like concert tickets, money or a cure for medical conditions? Fear of missing out on a good deal or opportunity can make you respond quickly.

Current events

Are you expecting to see a message like this? Criminals often exploit current news stories, big events or specific times of year (like tax reporting) to make their scam seem more relevant to you.

How to check if a message is genuine

If you have any doubts about a message, contact the organisation directly. Don't use the numbers or address in the message – use the details from their official website.

Remember, your bank (or any other official source) will never ask you to supply personal information via email, or call and ask you to confirm your bank account details. If you suspect someone is not who they claim to be, hang up and contact the organisation directly. If you have paper statements or a credit card from the organisation, official contact details are often written on them.

Why you should report phishing scams

The National Cyber Security Centre (NCSC) is a UK government organisation that has the power to investigate and take down scam email addresses and websites.

Reporting a scam is free and only takes a minute.
By reporting phishing attempts, you can:

- ☑ reduce the amount of scam communications you receive
- ☑ make yourself a harder target for scammers
- ☑ protect others from cybercrime online

Protect your devices from malware and viruses

Malicious software (also known as 'malware') is software or web content that can seriously disrupt the correct function of your computer, laptop, tablet or mobile phone; stopping them from starting, rebooting at random times or not saving data. It can also restrict, encrypt or destroy information or data that you hold and in some cases, it collects information or data saved on your device, and passes it on to cyber criminals.

Malware comes in many forms such as ransomware, viruses, worms, trojan horses and spyware.

Protect yourself

Make sure your device has **reputable anti-virus software**. Without these, your computer has no defence to identify or block infections.

Take care downloading files. If you don't know someone who's sent you an email with an attachment, or you're not sure about a website offering a file to download, don't do it out of curiosity.

Browse safely on the web. Get to know the risks of being online and use the same level of caution as you would in the real world; don't automatically trust something unfamiliar.

Spot the signs

- You're being told by text, email or phone call to download something from a website that you haven't visited before and doesn't look quite right. You might receive this request from a stranger or from someone else whose accounts have been hacked.
- Your internet connection or the computer's general performance suddenly becomes very slow, you can't access files or programs, or you're unable to log in at all.
- There are signs other people have accessed password-protected accounts, or your bank statements shows things you've bought or withdrawals you can't remember making.

  If you suspect your PC, tablet or phone has been infected with a virus or some other form of malware, confirm your device is infected.
- You may already know for sure because your antivirus product is telling you it has found an infection, or your device is showing ransomware asking you to pay money.
- If you suspect an infection but aren't sure, the easiest way to confirm an infection on a device is to run an antivirus scan and see if it detects anything.

- If you don't have antivirus, signs of infection include:
  - » Your device is running slowly, rebooting by itself, frequently closes programs or apps you are using, or opens those you are not.
  - » You have pop-up boxes from programs/apps you don't recognise, asking you to do unexpected things.
  - » Someone you know tells you that they've received unexpected emails from you, advertising unlikely products, or perhaps asking for money.
  - » Some apps on mobile devices try to check if your device has been 'rooted' or 'jailbroken'. These aren't a guarantee that your device has been hacked, but if you haven't actively done either of these to your device then it can be a good indication.
- If you have received a phone call telling you your device is infected and you need their help to clear it up. This is a common scam, the caller often claims to be from a trusted company such as Microsoft, or your internet service provider. **Hang up immediately and report the call to Action Fraud.** If such a caller has persuaded you to pay them money, report the call to Action Fraud and your bank or credit card provider

If you've been tricked into sharing personal information with a scammer, you can take immediate steps to protect yourself.

SITUATION	ACTION
You've provided your banking details	Contact your bank and let them know.
You think your account has already been hacked	You may have received messages sent from your account that you don't recognise, or you may have been locked out of your account. Go to the account provider's website and search their help or support pages. These will explain in detail the account recovery process (it's likely to be different for each account).
You received the message on a work laptop or phone	Contact your IT department and let them know.
You opened a link on your computer, or followed instructions to install software	Open your antivirus (AV) software if you have it, and run a full scan. Allow your antivirus software to clean up any problems it finds.
You've given out your password	You should change the passwords on any of your accounts which use the same password.
You've lost money	Tell your bank and report it as a crime to Action Fraud.

Cryptocurrency investment fraud

Cryptocurrency is a digital or virtual currency designed to work as a medium of exchange.

How does this scam work?

Fraudsters will cold call people and use social media platforms to advertise 'get rich quick' investments in mining and trading in cryptocurrencies.

They will encourage people to sign up to cryptocurrency investment websites and to part with their personal details such as credit card details and driving licences to open a trading account. An initial minimum deposit will be required, after which the fraudster will call them to persuade them to invest again to achieve a greater profit.

In some cases, victims have realised they have been defrauded, but only after any websites have been deactivated and the suspects can no longer be contacted.

- **Don't assume websites are legitimate**. Professional looking websites, adverts or social media posts don't always mean that an investment opportunity is genuine. Criminals can use the names of well-known brands or individuals to make their scams appear legitimate.
- **Don't be rushed or pressured into making a decision**. A genuine bank or financial organisation won't force you to part with your money on the spot. Always be wary if you're pressured to invest quickly or promised returns that sound too good to be true.
- **Stay in control.** Avoid uninvited investment offers, especially those over cold calls. If you're thinking about making an investment, get independent advice and thoroughly research the company first.

Facebook and WhatsApp account takeovers

How does this fraud work?

Fraudsters are hacking Facebook and WhatsApp accounts through unknown means and then changing the password and phone number of a person's account.

The fraudsters then message the hacked victims' friends to ask them to receive payments through PayPal for various reasons. They then ask for their phone number so they can communicate through WhatsApp.

The fraudsters convince the victim to receive funds into their PayPal account and transfer them into a bank account of the scammers choice.

A chargeback is then initiated through PayPal, leaving the PayPal account holder out of pocket as they have already sent the money to the fraudster's bank account.

How do I get my account back?

You need to sign into WhatsApp using your phone number and enter the 6-digit code sent to you via SMS. Once you enter this code, the individual accessing your account will be automatically logged out. If you are asked to enter a two-step verification code that you don't know (the hacker using your account may have set it up) you must wait 7 days before you are able to sign back in.

How do I protect my account?

Never share your 6-digit registration code or two-step verification PIN with others.

Set up two-step verification.

Set up a screen lock.

If you suspect someone is using your account, you can check which devices are logged in to your account and log them out.

How to report a cybercrime

Report any suspicious activity to ActionFraud by:

- Calling **0300 123 2040** Mon-Fri 8am-8pm
- Via telephone from abroad: **+44 300 121 2040**
- If deaf or hard of hearing, textphone: **0300 123 2050**
- In Scotland through Police Scotland's **101 call centre**

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**

If you have received a text message which you're not sure about, forward it to the Suspicious Text Message Reporting Service: **7726**

You can report a suspicious website through the Suspicious Website Reporting Service at: **https://ncsc.gov.uk/section/about-this-website/report-scam-website**

Click Call Connect

Reporting online **could save lives**

Report online at **www.sussex.police.uk** or **call 101**.
In an emergency always **call 999**.

Find us on social media

Produced by Sussex Police Media and Communications 2022