



Cyber Crime Guidance for Individuals



WHO IS THIS LEAFLET FOR ?

This leaflet will provide individuals across Surrey with easy-to-understand guidance, helping to protect you from becoming a victim of cybercrime. Information and advice has been gathered from Surrey Cyber Crime Unit, the National Cyber Security Centre and Action Fraud.

Many of us rely on the internet and technology to undertake day to day tasks, whether this be work, social life or daily activities. Cybercrime tends to sound daunting and can easily be ignored, but there are some simple steps that you can take to protect your online accounts, emails and devices from becoming compromised or affected in a cyber-attack.

What is included in this pack?

This pack does not include everything that you need to know in relation to cybercrime, but it does include the key important information and advice that individuals should be incorporating into their security practices, such as:

- Six actions to improve cyber security
- How to spot and deal with phishing emails
- How to use strong passwords to protect your accounts
- How to protect your devices from malware
- Cryptocurrency investment fraud and what to look out for
- WhatsApp scams and what to look out for
- How to report a cybercrime

SIX ACTIONS TO IMPROVE YOUR CYBER SECURITY

Just like locking your front door before you go outside, it's important to protect your information and devices before you go online.

Improve your password security

Passwords are the gateway to your accounts. Here are three actions to make your passwords work harder to protect you.

1 Create a separate email password

Your inbox contains lots of important information about you. So, if a hacker gets into your email, they could get into all your accounts that are linked to it. Create a strong email password and make sure it's different to all your others.

2 Create strong passwords using three random words

Hackers will try many different versions of words (Liverpool, L1verpool1, liverp00;!), so use three random words even when you need to add numbers or special characters e.g. BlueJ@mDance1/

3 Save passwords in your browser

Remembering passwords can be challenging because different websites have different rules. It's important to have separate passwords for your most important accounts like email.

Your internet browser will often give you the option to remember your passwords for you. This is a safe way to store your passwords, helping you to create stronger and different passwords without having to remember them all.

Add extra protection

Now you've got your passwords sorted, you're now ready to take cyber security to the next level.

4 Turn on two-factor authentication (2FA)

2FA is free. And it will stop hackers getting into your account even if they have your password. 2FA (also known as 2-step verification, or multi-factor authentication) simply means you'll be prompted for a second piece of information when signing into your account – usually a code which will be sent via text or email.

5 Update your devices

Tech companies are continually working to fix vulnerabilities in their software. So, when you receive prompts to update your devices don't ignore them. They contain important fixes which will help keep hackers out. You can make things even simpler by turning on automatic updates.

Make sure you can recover quickly

If you've followed these actions, you're protected from the vast majority of cyber-attacks. But, if something does go wrong, backing up means you will always have access to your most recently saved data.

6 Turn on backup

Backups are best done at regular intervals, so you always have a recent copy of your information (eg. photos and documents) saved if your data is lost or stolen. But the good news is if you turn on automatic backups your device will do the hard work for you.



GUIDANCE ON STRONG PASSWORDS

Passwords are key to our online accounts; therefore, it is important that your passwords are strong to reduce the likelihood of your accounts being compromised. When used correctly, passwords are a free, easy and effective first line of defence to prevent unauthorised users accessing your devices.

When creating passwords, make sure to consider:

- **Switch on your password protection** for your smartphones, tablets, laptops, and PC's. This could be a screen lock, PIN, Bit Locker or other authentication method (such as fingerprint or face unlock).
- **Use two-factor authentication.** This requires two different methods to 'prove' your identity before you can use a service, generally a password plus one other method. This could be a code that's sent to your smartphone or an authenticator app.
- **Avoid predictable passwords**, or one of the most commonly used passwords.
- **Use three random words.** The longer and more unusual your password is, the harder it is for a cybercriminal to crack. A good way to make your password difficult to crack is by combining three random words to create a single password, for example:
 - Applenemobiro
 - Coffeetrainfish
 - Eaglekitchenvase

Find out more:

For further information on how to use passwords to protect your accounts, please visit the National Cyber Security Centre:

<https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words>
<https://ncsc.gov.uk/cyberaware>

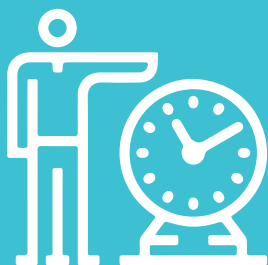
CRYPTOCURRENCY FRAUD



Have you been approached out of the blue about investing in an 'incredible' cryptocurrency investment opportunity?



Have you been asked to make an initial deposit with the promise of high returns?



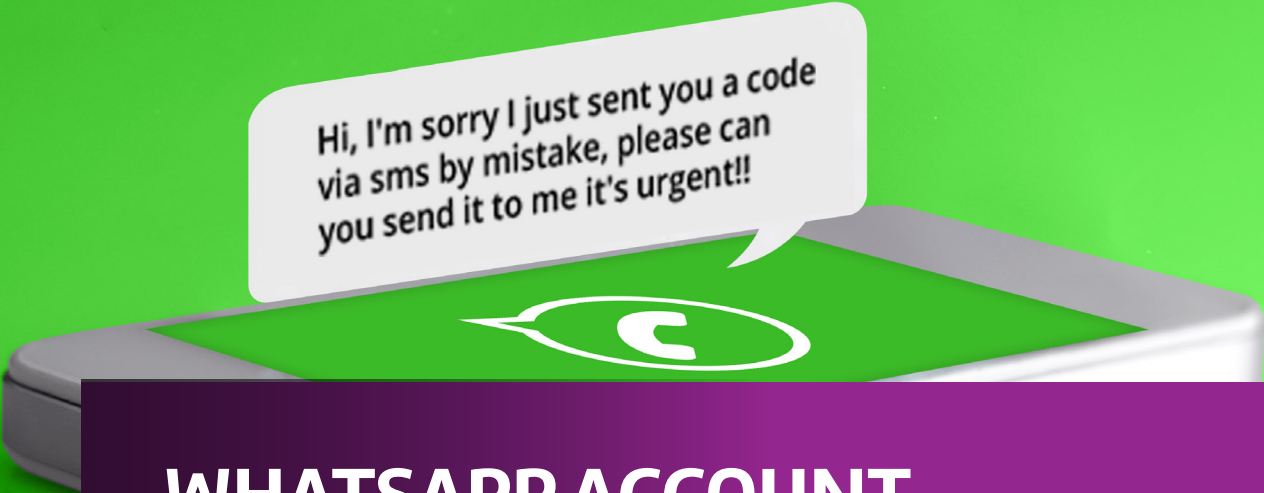
Are you being rushed into making a decision before having time to do your research on the investment platform in question?



STOP and THINK:
Could this be a scam?
Have you done your research on the investment platform?
Legitimate companies should never pressure you into investing.

Find out more at:

<https://actionfraud.police.uk/a-z-of-fraud/cryptocurrency-investment-fraud>



Hi, I'm sorry I just sent you a code via sms by mistake, please can you send it to me it's urgent!!

WHATSAPP ACCOUNT TAKEOVERS

What is an account takeover?

Where a hacker can trick you into giving them your WhatsApp verification code by pretending the code you receive belongs to them. This gives them access to your account to gain personal information and/or for financial gain by asking your contacts for money.

How does it happen?

Usually you will receive a message like the one above on WhatsApp that appears to be a friend or family member. You will also receive a code around the same time, and by sending them the code, you are giving them the control of your account because you will only ever receive verification codes that relate to your number?

How do I get my account back?

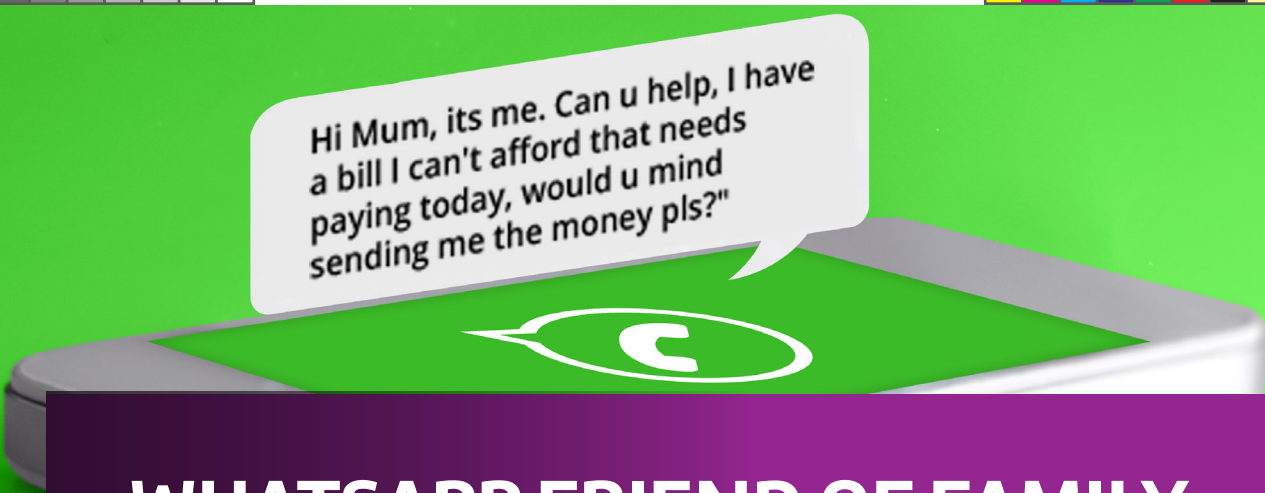
You need to sign into WhatsApp using your phone number and enter the 6-digit code sent to you via SMS. Once you enter this code, the individual accessing your account will be automatically logged out. If you are asked to enter a two-step verification code that you don't know (the hacker using your account 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.

Review your WhatsApp Account settings:

- 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.



Hi Mum, its me. Can u help, I have a bill I can't afford that needs paying today, would u mind sending me the money pls?"

WHATSAPP FRIEND OF FAMILY 'IN NEED' REQUEST

What is a friend or family in need scam?

Where an individual is pretending to be a friend or family member of the targeted victim who is in need of 'urgent' help. Usually they will claim that they are contacting from a new number, hence why it isn't recognised. Due to the personal connection, it is easy to not second guess the request, and provide the money that they are asking for.

How does it happen?

Usually you will receive a message like the one above on WhatsApp that appears to be a friend or family member. The requester will claim that they urgently need money for an array of reasons. The message will request money, and provide bank details for the funds to be sent to.

What should I do?

STOP. Take five minutes before responding. Make sure your WhatsApp two-step verification is switched on to protect the account.

THINK. Ask if the request makes sense. Scammers prey on people's kindness, trust and willingness to help.

CALL. Verify that it really is your friend or family member by calling them directly or ask for a voice note.

How to protect myself?

Check any messages are real by contacting the person through another means

- Set up 2-Factor Authentication
- Do not accept requests from people that you do not know
- Never share any codes or PIN numbers
- Always challenge requests for your information



REPORT ANY SUSPICIOUS ACTIVITY TO ACTION FRAUD 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>