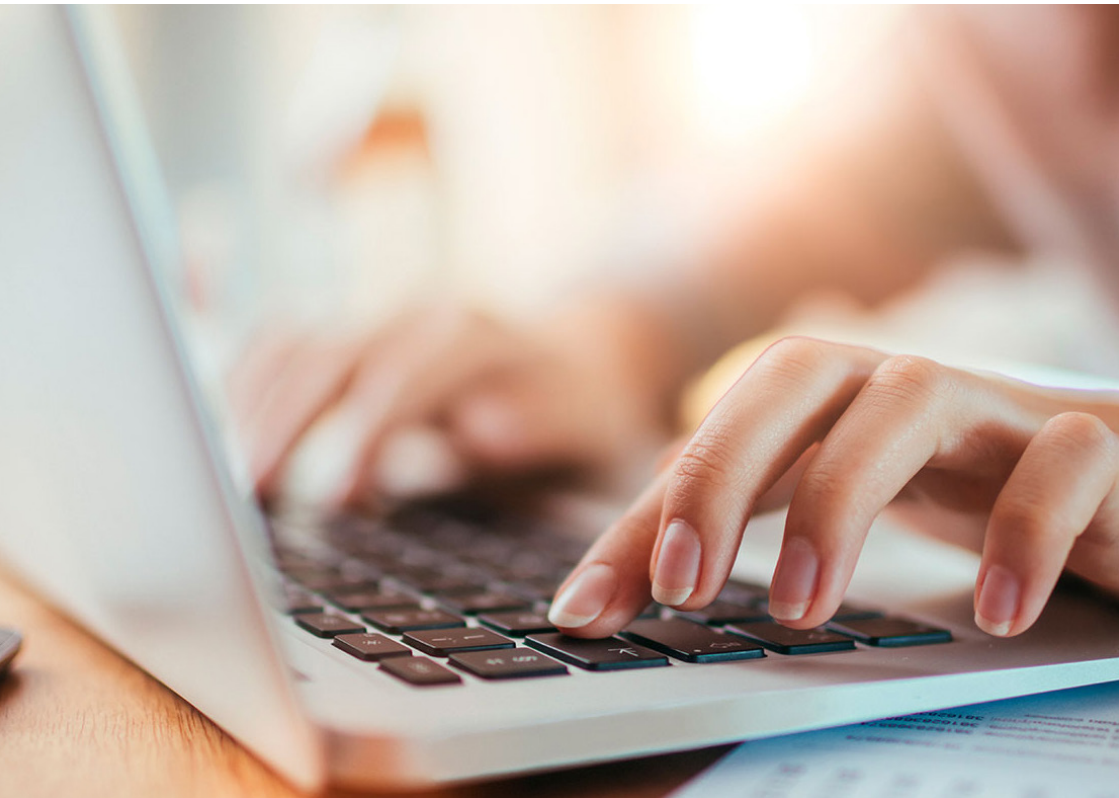
EMAIL SCAMS

Crime toolkits



DON'T BE A SCAM VICTIM!

Scammers will use any means to separate you from your money or your personal data – they operate over the phone, through the post, on the internet or face-to-face, often on the doorstep.

They will do their best to persuade you that they, or whatever it is they are offering you, are genuine – and will usually appear to be polite, friendly, and professional. It can be easy to be taken in by them – after all, they do this for a living!

However, there are also lots of signs that might indicate that all is not what it seems. Many scams follow certain patterns, and once you know what to look for, they can be easy to spot.

Here is one of the most common scams targeted at older people, and how you can avoid falling victim to it:

EMAIL SCAMS

HOW DOES IT WORK?

Email scams take many forms.

A common scam, called 'phishing', is where you receive an email purporting to be from your bank, which states your account has been compromised and asks you to transfer all your money to this new, safer account they've opened for you.

There are many variations on phishing scams, too. The "bank" might invent some excuse to need your PIN number, or your online banking password.

REMEMBER: Your bank will NEVER contact you out of the blue asking for your PIN, full password or to move money to another account.

DON'T BE A SCAM VICTIM!!

Your bank will NEVER contact you asking for your PIN

If you receive an email with any of these signs, or you just don't think it looks right, just delete it. If you're not sure, ask someone you trust, like a friend or relative, or your Neighbourhood Watch coordinator.

Email scams are not the only scams that use the internet to try to get you to part with your money, or your personal information.

Follow these back-to-basics rules from Get Safe Online to reduce your chances of falling victim to email or other online scams:

1. **ALWAYS REMEMBER: IF SOMETHING SEEMS TOO GOOD TO BE TRUE, IT USUALLY IS**
2. Make sure you have strong passwords on all your online accounts, and change these regularly. For a secure password, use three random words and include a symbol, numbers and upper and lower-case letters.
3. Look after your mobile devices. Don't leave them unattended in public places,

SPOT THE SIGNS!!

Any one of these 7 signs could suggest that an email you've been sent is a scam:

- The sender's email address doesn't match the website address of the organisation it says it's from. Roll your mouse pointer over the sender's name to see its true address
- The email doesn't use your name – it says something like 'Dear customer' instead
- There's a sense of urgency, asking you to act immediately
- There's a prominent website link which may look at first glance like the proper address, but has one letter missing or wrong
- There's a request for personal information – your bank will never ask for this
- There is poor grammar and spelling
- The entire text of the email is contained within an image rather than the usual text format, and the image contains an embedded hyperlink to a bogus site. Again, roll your mouse pointer over the link to reveal its true destination.

and protect them with a PIN or passcode.

4. Ensure you always have internet security software loaded on computers and update this as soon as new versions become available.
5. Never use wifi hotspots in places like cafes, bars and hotel rooms to do confidential things like banking – these connections are not secure.
6. Never reveal too much personal or financial information in emails, on social media and dating sites and in person.
7. Always consider that online or on the phone, people aren't always who they claim to be. Fake emails and phone calls are a favourite way for fraudsters to approach their victims.
8. Don't click on links in emails, posts, tweets or texts – and don't open attachments – if the source isn't 100% known and trustworthy, or it seems strange that you'd be receiving them.
9. Always access internet banking sites by typing the bank's address into your web browser.
10. Never pay for anything by direct bank transfer unless it's to someone you know personally and is reputable.
11. Never respond to any emails, text messages, letters or social media that look suspicious, including messages with bad spelling or grammar.
12. Never go to a website from a link in an e-mail and then enter personal details - the email could be fraudulent.
13. If you are at all suspicious, heed your instincts! You are very probably right. Go and check with someone you trust.
14. If someone you've never met in person asks you for money, that should be a red flag. Tell them you're

Agree a code word with the person so they can signal distress

not interested and stop all contact.

DON'T BE EMBARRASSED

If you did fall victim to the scam, do not feel ashamed, or think that you were to blame in any way. Victims of scams are just like victims of any crime – they have been targeted by criminals and bear no culpability for the crime.

The quicker you act, the sooner you might stop someone else becoming a victim. You might even be able to get your money back – if you sent off a cheque, for example, the police may be able to ask Royal Mail to intercept it or require your bank to put a stop on it.

You should also tell your Neighbourhood Watch coordinator, so that they can warn others in your area that this particular type of scam is being attempted. They will not reveal to anyone else that you have been a victim of it.

REPORTING A SCAM

If you or someone you know has fallen victim to a scam, you should report it to the **Police** on **101** and to **Action Fraud** on **0300 123 2040.**

ourwatch.org.uk