How to recognise a scam

Knowing what to look out for when it comes to scams is one of the best ways to protect yourself. Here's what you should look out for:

- **Verify any unexpected contact:** When answering phone calls, letters or emails that look unfamiliar, make sure you verify the identity of the company or person you are talking to. You can do this by looking at the contact details given in official paperwork or on their website to check if the person approaching you is legitimate.

  Please note: whilst on the Homes for Ukraine Scheme, you may receive important phone calls related to your stay here, which may come from unrecognised numbers. If this happens, save the number when you are called so that you know it is not a scam in future.

- **Email address** - If you get an email, expand the pane at the top of the message and see exactly who it has come from, it could say it's from TV Licensing but if you click or hover over the name it might reveal something different. If it's a scam, the email address the message has come from might not match up with the sender's name, have misspellings, random numbers or be from one of your contacts that's been hacked.

- **Text messages** – Modern scammers can make their numbers look like one you trust, like your bank's. The scam text message might even appear in the same conversation as legitimate texts you've had before. This is known as 'number spoofing'. Just in case, avoid clicking links in text messages, and don't be afraid to contact the company directly to check if it's a real message.

- **If it sounds too good to be true, it usually is**. For example, a holiday that's much cheaper than you'd expect.

- **Personal details, full PIN codes and passwords** - these are things no legitimate company will ask you for.

- **Quick decisions** - if you are pushed into making a decision on the spot, be suspicious. Scammers don't want you to have time to think about it. Any legitimate company who calls you won't mind if you hang up and call them back later. Use the phone number you find on letters from the company or the back of your card.

2. Types of scams

The tactics used by scammers and fraudsters can vary from someone knocking on your door to an unexpected email or phone call.

The internet and advances in digital communications have opened other ways for scammers to target you and steal information. Chances are, you've come across the most common type of scams – the spam email saying you're about to come into some money or pretending to be from HMRC or your bank.

However, while some email scams can be quite easy to spot and avoid, others are much more sophisticated and difficult to recognise.

Types of scams currently circulating include:

East Sussex County Council

**Please note: this list is not inclusive of all possible scams, there may still be others.*

- **The covid text message scam** - a scam that was active during lockdown which has started to reappear again. You receive a text message on your mobile to say you have been in contact with someone who has covid and to click on a link, which will then ask you for your details. This is a scam, otherwise it would be linked to a government website.

- **The electricity / gas rebate scam** - A text message on your mobile saying that you are entitled to a rebate on your fuel bill and to click on the link. This is a scam. The link asks for your details and has nothing to do with your own electric/gas supplier. If you did receive this scam check with your electric/gas supplier first. Any genuine rebate will either be done through a government agency or direct from your own electric/gas supplier.

  Find out more about how to avoid and report energy scams here.

- **The family text message scam** - A text message on your mobile which looks as if it has come from your daughter / son / granddaughter / grandson to say their mobile phone has been damaged or broken so they are texting on a 'friend's mobile'. The scam asks you to send £800 for a new phone to the account below (which is the scammers account). If you did receive a scam like this, make sure you ring your family member up first to check if it is legitimate.

- **The crypto currency scam** - you may see a crypto currency advert on your facebook asking you to send money to an account saying it's a 'good investment'. This is a scam. If you are unsure if it is genuine or not then do not engage with the company.

- **The courier scam** - you receive a text saying there is a parcel waiting to be delivered but before it can be delivered there is a payment which is outstanding so you need to click on the link. This is a scam as no genuine courier company would ask for payment.

- **The HMRC scam** - texts, calls and emails from "HMRC" are all scams . This department would write to you and never call, text or email.

- **The television licence scam** – you receive an email saying your tv licence is due and to click on the link to make the payment. If your payment is not due or even if it is a genuine email, it would give your own reference number. If there is no reference number, and if the email address has a typing error regarding the word 'licence', this is a scam,

- **Generic scam calls** - if you receive a phone call on your mobile or landline and you do not recognise the number or it comes up with no caller ID then it is advised not to take the call. You can also block scam calls on your mobile. Most of the landline providers have a "blocking service" so that only genuine calls get through to you.

- **The prize draw scam** - If you receive a letter through the post such as a "prize draw", saying you have won (for example) £20,000 and to send £20 to receive the prize - this is definitely a scam. Shred the letter and then throw it away.

- **The doorstep caller scam** - another type of scam are doorstep callers, this is when someone knocks on your door asking if you want work undertaken on your property. For example, gardening work, the cleaning of your driveway etc. Or they may be trying to sell you something. If you do receive a visit such as these, tell the person you are not interested and ask them to leave.

3. How to protect yourself against scams

The next step to avoiding scams is to know how to protect yourself. While some of these points are good advice in general, many are aimed at keeping you safe online.

- **Never give out personal information**. This can be used to steal your identity and access accounts. In particular, you should never share your full PIN or password with anyone. Your bank will ask you to use a card reader or ask for a few digits of your password if they need it.
- **Make sure all your accounts have strong passwords.** Don't use the same password for multiple accounts and change them regularly.
- **Don't make any advanced payments** until you are sure the company you're dealing with is legitimate.
- **If you're unsure about a financial services company**, check the FCA register of regulated companies. If they're not on it, don't have anything to do with them.
- **If you're unsure about any other kind of company**, you can look them up on Companies House to find out their background, or search for reviews online.
- **Use safe and secure WiFi connections** and avoid public WiFi. Your standard 3G or 4G connection is often more secure than the one in the coffee shop or restaurant.

4. What to do if you've been a victim of a scam

If you think you've been scammed, here's what you should do:

1. Stop sending money straight away. If the payment has been set up as a Direct Debit, get in touch with your bank to stop this immediately.
2. If you've been targeted, even if you're not a victim of it, report the scam to Citizens Advice consumer helpline on **0808 223 1133**, and use the online reporting tool.

If you think you've been targeted by a scam, you should gather as much information as possible to report it so it can be investigated. For more information on how to report scams, visit the Citizens Advice website.