**Scams: What are they, how to avoid them, and what to do if you fall victim to a scam**

Fraud scams no longer target just the gullible. They still come in letters, texts and calls, but more crooks are now looking online for the chance to get their hands on people’s money. There are increasingly sophisticated ways scammers try to target their victims.

The coronavirus pandemic has seen a rise in scams. There has been an increase in criminals looking to exploit financial and health concerns by asking for money for fake services upfront, collecting personal information or bank details, or offering temptingly high returns on made-up investments or pension transfers.

This short guide explains what to look out for, how to protect yourself, and what to do if you're a victim of a scam.

# **What are scams?**

Scams are fraudulent schemes that dupe people into parting with their personal details and/or cash. They've been around for as long as we can remember, but they're no longer confined to shady door-to-door salesmen or dodgy second-hand car dealers.

Scammers now frequently target people through emails, online banking systems, text messages and online transactions. While fraud is becoming ever more sophisticated, people are still getting caught out by traditional scam letters and phone calls. So it is as important as ever to be wary.

## Four Signs That It’s a Scam

**1. Scammers PRETEND to be from an organization you know.**

Scammers often pretend to be contacting you on behalf of the government. They might use a real name, like the HMRC, or the Royal Mail, or make up a name that sounds official. Some pretend to be from a business you know, like a utility company, a bank, or even a charity asking for donations.

They use technology to change the phone number that appears on your caller ID. So the name and number you see might not be real.

**2. Scammers say there’s a PROBLEM or a PRIZE.**

They might say you’re in trouble with the government. Or you owe money. Or someone in your family had an emergency. Or that there’s a virus on your computer.

Some scammers say there’s a problem with one of your accounts and that you need to verify some information.

Others will say you won money in a lottery but have to pay a fee to get it.

**3. Scammers PRESSURE you to act immediately.**

Scammers want you to act before you have time to think. If you’re on the phone, they might tell you not to hang up so you can’t check out their story.

They might try to scare you by saying you could be arrested, sued or lose your driver’s license. They might say your computer is about to be corrupted.

**4. Scammers often tell you to PAY in a specific way.**

They often insist that you pay by sending money through a money transfer company or by putting money on a gift card and then giving them the number on the back.

### **What You Can Do to Avoid a Scam**

**Block unwanted calls and text messages.**Take steps to block unwanted calls and to filter unwanted text messages. If you need help on how to do this on your phone, one of our advisors can help.

**Don’t give your personal or financial information in response to a request that you didn’t expect.** Legitimate organizations won’t call, email, or text to ask for your personal information, like your National Insurance number, bank account, or credit card numbers.

If you get an email or text message from a company you do business with and you think it’s real, it’s still best not to click on any links. Instead, contact them using a website you know is trustworthy. Or look up their phone number. Don’t call a number they gave you or the number from your caller ID.

**Resist the pressure to act immediately.** Legitimate businesses will give you time to make a decision. Anyone who pressures you to pay or give them your personal information is a scammer.

**Stop and talk to someone you trust.**Before you do anything else, tell someone — a friend, a family member, a neighbour — what happened. Talking about it could help you realize it’s a scam.

#### **Our Top 3 Tips**

**TIP 1 – You can avoid the bait and therefore the scam by ignoring it completely.**

In any scam your reaction or interaction gives the criminal something to work with. If you do nothing, they get nothing. Start with that as your main defence. This can mean not clicking on an email or opening it. It can mean deleting an email immediately. It can mean hanging up the phone or deleting the text message.

Scammers try to get through to **you** on their terms and the time they prefer. If you ignore their attempts to reach you, they are more likely to give up and try someone else.

**TIP 2 – Take a moment to think before you do anything**

Not everything is a scam and we don’t want you to ignore all the wonderful things the internet or your telephone or your local community has to offer. When scammers do get through to you they typically try to get you to do something in a hurry before you have time to consult with a trusted friend or do any research yourself. They try to confuse you, and get you to a state where you are more likely to make a rash decision you will later regret.

If someone tells you that your phone line is about to get cut, or you need to pay a fine immediately or that you must confirm some payment details…STOP. Say you are busy doing something else and that you would like to take a few details to call them back. Don’t be the one in a hurry. End the conversation. When you are back in your real life you can think more clearly.

* You can decide to do nothing.
* You can do some research yourself (it’s amazing how many results you will find if you type “HMRC scam” or “Amazon Prime scam”).
* You can phone a trusted friend or family member.
* You can log into the account they claimed to be calling about and take a look to see if there has been any unusual activity.
* You can even call that company yourself and speak to their customer service team using the number published on their website. Don’t use any of the details from the call, text or email you suspect of being a scam.

**TIP 3 – If it’s too good to be true, it usually isn’t true. If it’s too bad to be true, it usually isn’t true.**

**Good news scams cover a range of wildly exciting possibilities. They want you to make a bad decision caused by excitement, including:**

* You’ve won a lottery somewhere. Send a payment to unlock further details. DO NOT
* You’ve been left some money by a long lost relative. Send a payment to unlock further details, or details to unlock the payment. DO NOT
* HMRC are about to send you a tax rebate. Provide further details to unlock the payment. DO NOT

**Bad news scams try to get you to make a bad decision caused by fear and anxiety, including:**

* Your details to an online account have been compromised. Confirm who you are and we will fix everything. **DO NOT CONFIRM**
* Someone is using your PIN number and we want to stop them. Tell us your PIN number. **DO NOT**
* Send a payment and we will deliver an important package to you.**DO NOT PAY**
* HMRC are going to prosecute you and you will go to prison unless you pay a fine immediately. **DO NOT PAY**

##### **What to do if you've been scammed**

**Below is a need-to-know checklist of what you should do.**

* If you've already responded to a scam, end all further communication immediately.
* Call your bank directly and cancel any recurring payments.
* Report the scam to the police through Action Fraud on **0300 123 2040**,

or report a scam anonymously on its website: https://www.actionfraud.police.uk/

* If you wish to seek further advice, contact the

Citizens Advice Scams Action helpline on **0300 330 3003** or through their website: www.citizensadvice.org.uk/scamsaction.

Alternatively, you can contact the Financial Conduct Authority's helpline on **0800 111 6768.**