PHONE SCAMS

Phone scams involve fraudsters attempting to obtain your personal or financial information over the phone. These can be hard to spot as fraudsters can ‘spoof’ phone numbers so you think you are being called by your bank or other organisation.

Some examples:

Someone calls you claiming to be from your bank's fraud department. They tell you that your account has been compromised and encourage you to transfer your money into a 'safe' account. Scammers have also been known to impersonate the police, utility providers and government departments.

An automated phone call says that your Amazon account has been compromised or a recent purchase needs to be authorised or some similar tale. Hang up immediately and, if you want to check, go to your Amazon account using your normal method and look to see if there are any issues. If there are then contact Amazon using the links from the genuine site you have just logged into. (The same thing can happen using a company other than Amazon. Do the same thing - hang up then check using genuine links)

The fraudster claims your account (or phone, computer etc) has been compromised and tells you that you must download software onto your device so that they can access the account. The software may well be from a real company but is used by the scammer to steal your money. If you're asked to download software, end the call, disconnect from your wi-fi and delete anything you've downloaded.

The fraudster impersonates a tech company such as Microsoft and informs you that your device has been infected with malware. To fix the issue, they will either ask you to download remote access software to give them control over your device or trick you into installing malware.

A scammer calls you claiming to be from HMRC, telling you that you have underpaid your tax. Some scammers leave automated voicemails which state that you're being taken to court and ask you to press a number that then puts you through to a fraudster. Other HMRC scams begin with an email or text message asking you to call a dodgy number to secure your account or claim a tax refund.

A fraudster calls you claiming that you've won a prize or the lottery. They'll invent a story to make up for the fact that you don't remember entering a competition. You'll usually be asked for your personal or financial information to receive the prize or money.

PREMIUM RATE NUMBER SCAMS

Premium numbers to look out for typically start with 084, 087, 090, 091 or 098. These calls can cost upwards of £100. To avoid these scams, don't click on sponsored results when looking up companies or government departments. Instead, ensure you're navigating to their official website.

Also be on your guard against 'missed call' scams. This is when a scammer calls you from a premium number but ends the call before you can answer it, in the hope you'll phone back and run up a big bill.

SCAM BANK MESSAGES

If you get a message claiming to be from your bank, always treat this with caution. Your bank should never:

• Ask for your Pin or internet banking password.

• Send someone to your home to collect cards or banking information.

• Ask you to email or text personal or banking information.

• Email a link where you have to then input your internet banking details.

• Ask you to authorise a funds transfer which you haven't requested.

• Tell you to invest in diamonds, land or other commodities.

• Ask you to carry out a test transaction.

• Send you to a mobile app other than their own official app.

If you receive an unexpected message from your bank and you're concerned whether it's genuine or not, you can call your bank back via an official telephone number printed on the back of your debit or credit card.

REMEMBER Scammers may be able to keep your phone line open even after you've hung up, so if you hang up on a dodgy call, use a different phone to call the company back on a trusted number or wait for at least 10 to 15 minutes.