Mobile phone scams

Smartphones are mini-computers, so take all the same precautions with them as you would with your own computer at home.

What you should know

If you use an online banking app, only use the official app provided by your bank. If in doubt, contact your bank to check.

Only download apps from official app stores, such as:

* Apple iTunes
* Android Marketplace
* Google Play Store

Downloading them from unofficial or unknown sources could infect your phone with a virus.

Keep your phone’s operating system updated with the latest security patches and upgrades. Your operating system provider normally sends these.

Never give your mobile banking security details, including your passcode, to anyone else and don’t store them on your phone.

For added security set up a password or PIN to lock your mobile.

Just like on your computer, you can get antivirus tools for your mobile; use a reputable brand. Some banks offer free antivirus software for their customers’ phones. Check your bank’s website for more information.

Be wary of clicking on links in a text message or email. Don’t respond to unsolicited messages or voicemails on your phone. Your bank will never email or text to ask for your PIN or full password.

Examples of mobile phone scams

Text scams offering you money for an accident you may have had is often a ploy to get your personal details. Don’t reply, even by sending a ‘STOP’ text. Simply delete the message.

You may get a text or advert encouraging you to enter a competition for a great prize. The scammers will charge extremely high rates for the messages you send them, as high as £2 per text message. Don’t reply.

‘Trivia scams’ involve you answering general knowledge questions to win a prize. The first few questions will be very easy, so you keep playing. But the last one or two questions you need to answer to claim your ‘prize’ could be very difficult or even impossible.

If you try to claim your prize, you may have to call a premium-rate number, often beginning 0906. You then have to listen to a long recorded message, designed to keep you on the line. It’s highly unlikely there’ll be a prize at the end of it. Don’t phone back to claim.

‘SMiShing’ (SMS phishing) is when a scammer texts asking for personal or financial information. The message may appear to be from a legitimate company, like a mobile phone provider, but legitimate companies never ask you to provide sensitive information by text. Don’t reply to these texts. Simply delete them.

Unless you’re using a secure webpage, don’t send or receive private information when using public WiFi. And be aware of who’s around you when using a mobile device to go online.

For more information and help and to report this and many other types of fraud, visit [Action Fraud](https://actionfraud.police.uk/) the UK’s national fraud and cybercrime reporting centre.

Mass market fraud or scam mail

The sophistication of mass market mail and online fraud and scam mail can vary enormously but as a general rule, if something seems too good to be true, it probably is.

Many people in the UK, particularly the elderly and vulnerable, are lured by the prospect of a surprise win, and give large amounts of money or personal data to claim their fake prize.

Examples of scam mail

The most common mass-market fraud, the fake prize scam, is where you get a message by post, email or text saying you’ve won a prize or competition, usually one you’ve never heard of.

The message asks for an upfront payment to claim the prize, which either never arrives or is very different to what was promised.

‘Psychic’ and ‘clairvoyant’ scams set up victims for a fake prize scam. In this situation, a ‘psychic’ sends the victim a list of ‘lucky’ lottery numbers. Soon afterwards, a letter arrives telling the victim they’ve won a lottery with those exact numbers. Of course, this is all part of the scam.

You may receive unsolicited mail advertising ‘high quality’ or ‘exclusive’ goods, which in reality are poor value for money.

Another mass marketing scam is to offer a share of a cash prize that you can only get by ordering goods. The goods are usually very poor quality and the cash prize is never mentioned again.

Also be wary when sending money, or receiving money from, someone you don’t know and trust. This may be a ploy by a scammer to get you to pass money through your bank account that’s stolen from another victim’s account.

If you do this, technically you’re money laundering and being a ‘money mule’ for the scammers. If convicted of money laundering you could be sent to prison. Having a criminal conviction can make it harder to get financial products or get a job.

It can only take a single response to a scammer to be inundated with more scam mail. Your name and address will be included on a ‘suckers list’ and you’ll get lots of scam mail every day.

Remember, you:

* can’t win money or a prize in a lottery you haven’t entered
* can’t be ‘chosen at random’ from a list you didn’t sign up to
* should never have to pay a fee or make a purchase to claim a legitimate prize

For more information and help or to report on this and many other types of fraud, go to [Action Fraud](https://actionfraud.police.uk/) the UK’s national fraud and cybercrime reporting centre.

Internet scams

Many internet scams take place without the victim even noticing. Scammers put programs on your computer that can steal, wipe or lock your data. To prevent this, have antivirus software and a firewall installed on your computer, and keep it up to date.

Take the precautions below and use common sense to avoid becoming a victim.

What you should know

Scammers defraud people using spam emails. Simply delete the email without opening or replying to it, otherwise the scammer will send you more and more emails from lots of different addresses.

Any email you get from someone you don’t know is likely to be spam, especially if it’s not addressed to you personally and promises you some kind of gain.

If you get an email with an attachment, apparently from someone you know, but it’s not the usual sort of message you get from them, don’t open the attachment. Contact the person who’s supposed to have sent it and confirm it’s genuine. The email may have been infected with a virus and forwarded through their address book.

Online marketplaces can be a lot of fun and can save you money but they’re also used by scammers. Scammers will try to steer you away from online sites and get you to use unusual payment methods, such as money transfer agents or e-money, a digital equivalent of cash.

The most common scams at the moment are for:

* concert and event tickets
* apartments, residential and holiday lettings
* dating and romance
* vehicles for sale or hire (especially if they deliver the hire vehicles to you)

Adverts and websites can be very sophisticated so do some research to make sure everything makes sense. Always think about your personal safety when meeting anyone you’ve only talked to on the internet.

Be careful of official-looking but bogus websites that claim to help you apply for passports, visas and driving licences.

There are lots of ways scammers gain personal or financial information from their victims, such as:

* phishing, where an email that seems to be from a legitimate company asks you to give your personal details
* vishing, where either an automated phone message or a cold-caller who seems to be from a legitimate company asks you for personal details
* spear phishing, which focuses on an individual or department in an organisation; the email appears to come from a legitimate organisation

Using these methods, scammers ask for information such as login details and passwords, or install malware on your computer.

As a general rule, never give your personal or financial details to anyone unless you know and trust them.

For more information and help or to report on this and many other types of fraud, go to [Action Fraud](https://actionfraud.police.uk/) the UK’s national fraud and cybercrime reporting centre.