## How to avoid falling victim to online scams


The Internet has brought the world closer together, but it also provides an easy means for disreputable individuals to steal or commit other criminal offences.

There are many different types of scams on the Internet and you need to be particularly wary of any contact from suppliers or authorities who want you to do something, especially if the call or e-mail is unsolicited. This guide covers the most common types of scams and explains how they work.

**Common elements**

The most common elements of scams include:

- **Unsolicited contact** (although not always); this may be by telephone, text message, e-mail or even a letter in the post
- **Element of urgency**; you are being asked to act now or soon, or the consequences will get worse (price will go up, you will be arrested or taken to court, service will be disconnected, etc.)
- **Buying your confidence**; scammers will try to use information you think is private (such as your address, credit limit, account number, etc.) to make you think they are legitimate
- **Requiring you to do something**; looking for errors on your computer, letting them take control, logging into your bank, divulge information, transfer money. Remember that even divulging your personal details can be valuable to someone who wants to commit identity fraud.

**The most common types of scams**

### Tech Support Scam

This became more popular in 2016 and involves someone calling and pretending to be from Microsoft or your broadband provider, and advising you that your computer is generating errors which they have been notified about and offer to help you. They usually take you through some steps to show you errors on your computer (which are in fact perfectly normal things you don't need to worry about), either before or after they take over your computer remotely using something like TeamViewer. Then they ask you to pay money to install some security software; the reality is the software will probably do nothing but make things worse.

Remember that someone **being able to confirm your account number or address is not proof they are from your broadband provider**.

Be aware that many of these tech support scams operate websites which look genuine so be careful if you search for them online using their phone number. If you need technical support, speak to someone you trust (by far the best option), or to a well-known support organisation.

### Bank Security Scams

Bank scams can take many forms from a call advising you that someone in your branch has been suspected of stealing money and asking you to transfer your money into a new secure account, to calls from your credit card company about a new card being sent out (with details like your address and credit limit provided by the caller to buy your confidence) and asking you to provide or type in your security code, password or PIN; they may have obtained your other credentials before, or even stolen your new card in the post. With your PIN, they can then go on a spending spree.

If you ever receive a call from your bank (especially an unexpected one), ask them the name/department of the caller (and extension number if possible), hang up, and call them back from your mobile phone using the number you find on the back of your card. Do not use your landline or any number provided by the caller. Similarly if you get an e-mail or text message, do not click on any links or reply to them. Open a web browser and type your bank's website address directly into the address bar. In some scams, banks send a 'courier' to collect your card after some fraud (typically after they have persuaded you to disclose your PIN code).

Another bank related scam is asking you to use your phone/token to generate a 'security code' to 'resync' the system. This is then used to login and empty your account.

### Your Broadband Is Going To Be Or Has Been Hacked Scams

A variation of the tech support scam, but someone claiming to be from your broadband provider (and in many cases they seem to guess the right provider or know via other data leaks) and that your broadband is going to be offline due to being hacked, or that they

expect it to be hacked in the next 24 hours. The wording is designed to install a sense of panic and a need to do something immediately about it.

The scammer is likely to proceed to get you install some software that will have malware attached to harvest details from your computer, or request payment for fixing the hack in advance so that you don't get knocked offline.

Never call them back on any phone number given by them, but if you are unsure and want reassurance from your broadband provider find their support number on a bill or their website and call them back on your mobile if they called you on the landline (this avoids a scam where people stay on the phone after you hang up and pretend to be provider support).

### Advance Fee (419) Scams

This type of scam happens through e-mail, phone, fax, post or any other means of communication. It may start from an unsolicited e-mail from a barrister telling you that you have been left something in a will, some famous person wanting to give away money, a lottery you have won or any other story for that matter.

In all cases, to get money the scammers will ask you to make a small payment for a 'customs charge' or some legal fees. This might only happen at a later stage (after they get personal details to use in identity fraud etc).

Often they will use services of companies like Western Union or Moneygram to wire funds, or pre-paid gift cards.

### Friend in Need/Danger Scams

You get an e-mail or text message from a friend in trouble (from their real e-mail address) abroad who needs money to pay medical bills or buy a plane ticket home. They might not be able to speak to you on the phone because it's 'been stolen' or some other excuse. In reality, their e-mail account has been hacked, or someone has stolen their phone and is trying to use their relationship with you to scam you out of your hard earned savings.

If you do encounter this situation, you need to speak to the friend in question.

### Legal action, unpaid bills or police coming to arrest you scams

These are becoming more common in the U.S. and seem to involve a voicemail/missed call. When you contact the caller back, they tell you they are from the Internal Revenue Service (IRS; U.S. equivalent of HMRC) and you owe some thousands of dollars in taxes. They advise you that police are being sent to arrest you unless payment is made immediately. An alternative to these is where a utility company is threatening to disconnect your supply imminently.

These particular scams seem to ask victims to go to a Target store (or in the UK that would be most supermarkets/newsagents) and buy 'gift cards' (iTunes, Amazon or other) and load

them with money and then give the code to the scammers over the phone so they can withdraw the money.

### You have made a purchase (e.g. on iTunes) for something you don't recognise

You get an e-mail advising you that you have made a purchase for something you don't recognise. It says if you want to dispute this, please click a link which then takes you to a form that asks you to login (e.g. to your iTunes/Apple account; to use for other bad purposes) or ask you to provide your card details for a refund, which are then used to make purchases online. If you divulge your security details to a scammer, your bank may not be as sympathetic when you dispute the transactions.

### Your device has been found!

Your mobile phone has been stolen and you get an e-mail from Apple saying it's been found, asking you to login to iCloud to locate it; in reality the thieves have found your e-mail address from your stolen device, and they need your iCloud login to unlock the iPhone so that they can re-sell it to someone. No one will buy an iPhone they can't use and Apple require you to login to wipe the device.

### Phishing Scams

Phishing is a term used to describe a process where you receive an e-mail supposedly from your bank, informing you of an issue that requires you to take action. These usually include a link to a site, which may look like your bank's web address, and a website that may look like your bank's website, but which in fact is controlled by the scammer. They will try to get you to enter some details like card/account numbers, logins, etc. which will then be used to commit fraud. If you disclose your personal security details to someone else, the bank may hold you liable, so you must be cautious!

### Ransomware

Ransomware isn't a scam usually, in the sense that when this happens, you've already let your security lapse, however it's useful to be aware of this. Typically you haven't updated your software regularly or you get a virus which encrypts your entire hard drive (and any attached network storage too) and once this is complete, you get a message saying you need to pay to decrypt the information.

If you're lucky, your backups are not affected and you can restore your data from there. If not, there might be a free tool to decrypt your system without paying. If this fails, you will usually have no option but to lose the data, or pay up (obviously the second option wouldn’t be recommended)..

Most of these ask for payment in Bitcoin (a digital crypto-currency) so you have no way to get your money back after you make the payment.

**Top 10 rules to follow...**

1. **Do not trust the 'caller ID' information** — the number that appears on your phone or when you dial '1471' to find out who the caller is; this is easy to fake
2. **The caller may know more about you** (name, address, credit limits, mother's maiden names, etc.) — this does NOT mean they are your bank or broadband provider. There have been many security breaches within large companies that mean this data is not something you can use to authenticate who is calling. Be suspicious.
3. **Never visit a website, install any software or call a number provided to you in an e-mail or during a phone call**. If you need to contact your bank, do so on the number on the back of your card (noting the tip below); Many scams rely on you visiting a website (possibly a genuine one) which gives remote control of your computer to scammers.
4. If you receive a call on a land line (i.e. not a mobile), when you hang up, the call does NOT disconnect for a long time. Therefore if you then pick up the receiver and hear a dial-tone and try to dial a number, this does not mean you're making a new call, and the scammer might still be on the line. **Use a mobile phone to call back if possible**.
5. **Don't trust someone based on their accent**; not all scams originate from overseas call centres and may be carried out by native English speakers.
6. **Microsoft Technical Support does not call you** to advise you that your system is sending errors; any such calls are scams (usually to try and sell you some unnecessary security solution/support package).
7. **Your ISP *probably* won't call you** to advise of a virus - some smaller ones may do, but if they do, they won't ask you to type things on your computer to show you any errors.
8. If anyone you know asks you for money, don't do so on the basis of an e-mail or text message; always speak to them on the phone to confirm.
9. **Bank staff will NEVER ask you to reveal your card PIN**; you will NEVER be asked to type the PIN into a telephone. They will also never send a courier to pick up your card or ask you to make a transfer.
10. Ensure that you **install Anti-Virus software** from a major well- known brand. Consider Anti-malware too.

**If you do become a victim**

If this happens, do not feel like you should be hiding this or ignore the problem, or it will get worse. You need to act to make sure you protect yourself.

1. If you have shared your login details, contact the companies involved (banks, e-mail providers, Apple, etc.) and change your credentials. Otherwise, things will get worse.
2. If you shared credit card details, contact your bank and report this immediately so they can stop any further misuse of your card.
3. You can install some anti-malware tools to help remove and keep off malware from your system
4. Contact Action Fraud (https://actionfraud.police.uk/) or your local police on 101 (do not use 999 unless it's an emergency)

5. Consider ID theft protection insurance (although bear in mind you may need to disclose this incident to them; read the policy carefully!

Do remember that online scams always evolve, so consider the above as examples and traits you should be looking out for, but always be cautious!

Adapted from [www.thinkbroadband.com/guides](www.thinkbroadband.com/guides)