



Top Tips

Types of scams



Phishing

Phishing is a type of internet scam, generally an email, that tries to trick you into giving away your personal information.



Smishing

Smishing is when cyber criminals send texts or online messages that trick you into giving away information.



Vishing

Vishing is the name for phone calls where scammers try to get your personal information.

Spotting a scam



Out of the blue

Watch out for unexpected calls, messages or emails, as they could be from scammers. They often pretend to be from a company or business you are familiar with. It's very unusual for a genuine organisation or business to contact you and ask for your personal information or bank details if you're not expecting them to.



Under Pressure

Scammers will try to trick you into making quick decisions or act urgently - it doesn't give you time to think about checking their message or thinking twice that they may steal your personal information or bank details. Be aware - they might set a time limit for you to take action or you will miss out on a great offer. Or if you don't act fast, something bad will happen with your internet, the police or HMRC.



Too good to be true

Scammers may use the temptation of a prize or cash to get you to communicate with them over text, email or even a phone call. They might want you to 'click' a link or give away personal information or your bank details. Be aware - if something seems too good to be true, it usually is!



Untrusted Source

Almost all phishing attempts will claim to be from a trusted source, or pretend to be from someone you know, like a friend, company or government agency. If they are asking you to give away personal information or bank details you should be very suspicious. Be aware - try contacting them in a different way. Maybe call them from a number on their secure website, or send them a personal email or message if it looks like it's from someone you know.



An Ask

If you are at all suspicious you should contact the organisation in a different way, maybe call a number on their secure website, or send a message if it's someone you know. Be aware and ignore or delete emails that ask for your bank details or personal information. If the request is genuine, the organisation or person will get in touch with you in another way.