

What parents need to know about phone scams

At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one of many issues which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, links and tips for adults.

What Parents & Carers Need to Know about PHONE SCAMS

In a three-month period during 2021, no fewer than 45 million people in the UK experienced a suspicious attempt at being contacted via their mobile. Phone scams are a common form of cyber-attack where fraudsters engage directly with their intended victim through their smartphone. As our phones carry so many sensitive (and therefore potentially valuable) details about us, it's vital that trusted adults are alert to the tactics that scammers use to get access to user accounts, personal data and private information for financial gain.

WHAT ARE THE RISKS?

SMISHING
SMS phishing, or 'smishing' is one of the most common forms of mobile-based cyber-attack. Smishing is when a scammer texts their target, pretending to be a reputable person or organisation. They aim to trick the victim into supplying sensitive data such as bank details and personal information, so that they can then access the target's bank accounts and remove money.

IMPERSONATION
Fraudsters often impersonate someone else to trick the victim into actually transferring money directly. They might claim, for example, to be a friend or relative using a different number who urgently needs funds. Other common cons include sending fake texts informing the target that they have a package which requires a fee to be delivered, or that they have an unpaid bill to settle.

NUMBER SPOOFING
Here, the scammer takes impersonation a step further by cloning the phone number of a genuine company, so when the target receives a call or text, their phone recognises the sender's number as legitimately belonging to Amazon, HSBC, the NHS or the OLA (who have all been impersonated in these cons). This makes the scam far harder to spot and the victim much more inclined to comply.

FAKE TECH SUPPORT
Attackers contact a target, pretending to work for their employer's IT support team. They then advise them to download some software to fix a 'technical issue' with their device. In reality, however, the software grants the scammers access to the victim's private data and sensitive information. This con is more common on desktop and laptop devices, but is still possible to accomplish on mobiles.

SIM HIJACKING
SIM hijacking switches control of a phone account from the victim's SIM card to one in the scammer's possession. Criminals use personal details pieced together from social media (birthdate, address, pet's name and so on) to pose as you, then instruct your phone network to transfer your number to their SIM - giving them access to all calls and texts meant for you, including one-time login passcodes.

Advice for Parents & Carers

DO SOME DIGGING
If you've received a call or text asking for specific information, research the caller's number. There are several websites that allow you to enter a phone number and will then display any relevant information about it - this usually includes feedback and comments from other people, so you can easily see if that particular number has been implicated in potential scams.

TRY A CALL BLOCKER
If a suspicious call comes through on your mobile, you can manually block the number. If you believe it to be dubious or a nuisance caller, alternatively, you could consider installing a call blocker service on your phone. They automatically stop calls getting through from numbers which have been reported as suspicious, halting potential scammers in their tracks before they can reach you.

VERIFY THE SOURCE
Never disclose confidential details to an individual or organisation you're unfamiliar with. If the caller claims to represent a company you trust but is still asking for personal information or payment on an outstanding charge, end the conversation. Then find the company's genuine number on a bill or on their website and call them directly to confirm if there really is an issue you need to address.

BREAK OUT THE TECH
Lots of anti-virus software now also protects mobiles. Some anti-virus apps can detect phishing links in text messages and alert you to the risk. When you're sat and about, try not to use public WiFi for sensitive transactions: it's far less secure than your home WiFi network. Instead, you could consider installing a VPN (virtual private network), which encrypts all data travelling to and from your phone.

REPORT INCIDENTS
If you or a family member does give out confidential information to a caller you aren't sure about, contact the actual company mentioned to check if the call was genuine. If they confirm that the call was not made by their organisation, you should report it as a potential scam via the Action Fraud website and (depending on exactly what information was divulged) consider involving the police.

BE WARY OF LINKS
If you get a message from an unknown number asking you to click on a link, report it as spam and do not open the link. One recent example 'warned' victims they'd been exposed to the Omicron variant and needed to click a link to buy a special test - only to find they had paid their money to scammers. Links can also install malware onto your device, so always treat them with extreme caution.

Meet Our Expert
Formed in 2018, Kryptokloud provides cyber security and resilience solutions to its customers. With offices in the UK, the company offers managed service operational packages including cyber security, monitoring and testing, risk audit, threat intelligence and incident response.

NOS National Online Safety®
#WakeUpWednesday

Source: <https://www.actionfraud.police.uk/news/2022/01/20/45-million-people-targeted-by-phone-scams-in-uk> | <https://www.actionfraud.police.uk/news/2022/01/20/45-million-people-targeted-by-phone-scams-in-uk> | <https://www.actionfraud.police.uk/news/2022/01/20/45-million-people-targeted-by-phone-scams-in-uk>

www.nationalonlinesafety.com @nationalonlinesafety /NationalOnlineSafety @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 22.03.2022

Financial Fraud Action estimates that, in the UK, a financial scam is committed every 15 seconds. Some of these dishonest schemes continue to take the traditional route through our letterboxes or onto our doorsteps – but an increasing majority now target that commanding gateway to our attention that's with us throughout our waking hours: our phone.

From bogus bank personnel to counterfeit couriers, scammers now adopt a whole gallery of convincing aliases from behind a keyboard. In this week's #WakeUpWednesday guide, we profile some of the most frequent attempted cons, highlight ways to avoid them and suggest what to do if you or someone in your family does inadvertently fall foul of a phone scam.

According to recent Ofcom research, 7 out of 10 people in the UK received a suspicious text to their mobile phone last year. Almost half (44%) of those say they get a such a message every week. Banks and consumer watchdogs alike are warning of an increase in attempted phone scams, which frequently target more vulnerable groups: the elderly and, of course, young people.

Scammers' tricks have become more sophisticated in the digital age: now they can convincingly pretend to represent our bank, our health services or even our loved ones. Stay wise to their rapidly evolving schemes and protect yourself – and your family – with today's #WakeUpWednesday guide to phone scams.