# 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.


## 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.

## FAKE TECH SUPPORT

Attackers contact a target, pretending to work for their employers' 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.

## NUMBER SPOOFING

Here, the scammer takes impersonation cons 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, HMRC, the NHS or the DVLA (who have all been impersonated in these cons). This makes the scam far harder to spot and the victim much more inclined to comply.

## SIM HIJACKING

SIM hijacking switches control of a phone account from the victim's SIM card to one in the scammers' possession. Criminals use personal details pieced together from social media (birthday, 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 out 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 2016, 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.

KryptoKloud
Security Made Simple

NOS National Online Safety®

#WakeUpWednesday

Sources: https://www.ofcom.org.uk/news-centre/2021/45-million-people-targeted-by-scams | https://www.cprcallblocker.com/blogs/news/shocking-new-uk-fraud-statistics-financial-scam-committed-every-15-seconds | https://www.which.co.uk/news/2022/01/the-five-biggest-scams-of-2021/