Impersonation Fraud

TAKE FIVE TO STOP FRAUD™

Impersonation fraud is where individuals are convinced to make a payment or give personal and financial details to someone claiming to be from a trusted person or organisation.

These can include banks, the police, a delivery or utility company, communication service provider, a government department such as HMRC or a friend/family member. Criminals use a tactic called social engineering to groom and manipulate people into transferring money or divulging personal and financial details.

This is a common scam type that many people fall victim to due to various reasons. Individuals are often pressured into taking swift action as scammers convince them the situation is either very urgent, or that the victim may face serious repercussions if they don't give the information the criminal needs. People also can be too polite to decline, or simply feel they trust the person or organisation without questioning. If you get asked to send money urgently, always be suspicious, especially if you've been contacted unexpectedly. Don't assume a person you are dealing with is who they say they are.

5 WAYS TO STAY SAFE FROM IMPERSONATION FRAUD

1 When faced with a request for personal or financial information, stop and think before clicking on any links or replying to text messages asking you to make a payment.

2 Never let someone gain remote access to your computer or phone that has called you out the blue. If it doesn't feel right, you can hang up on them. Only criminals will persist in getting your information.

3 Avoid logging on to financial accounts using public WiFi.

4 Banks or police will never ask you to move your money to a 'safe account' because your 'money is at risk'. If this happens, hang up, and call them back on a number you know to be correct. Scammers can change the caller ID to make the number seem trustworthy.

5 Only give your personal or financial information out to services you have consented to and are expecting to be contacted by.

Examples of impersonation fraud

Bank impersonation/Transfer money to a 'safe' account

An individual receives a call from someone claiming to be from their bank's fraud team enquiring if several payments on their account were actually made by them. Individuals usually don't recognise these and are advised that their account has been compromised, and they should urgently move money into a 'safe' account in order to protect it. This money then gets transferred directly into the criminal's account. By this time, it is too late for the victim. Bank impersonation is a widespread type of deception that takes advantage of people's trust in financial organisations.

Friend/Family in need scam

This scam typically involves criminals texting individuals claiming to be a family member and will usually begin the conversation with "Hello Mum" or "Hello Dad". They will say that they are texting from a new mobile number as their phone was lost or damaged and will go on to ask for money to purchase a new phone or claim that they need money urgently for an emergency.

The criminal will supply their bank details for payment to be received, with some coming back with further demands for money. Criminals are often successful in their approach as they are exploiting the emotional vulnerability of the public in an attempt to deceive victims.

Contact your bank immediately if you think you've been scammed and report it to Action Fraud at actionfraud.police.uk or on 0330 123 2040.