Impersonation scams

What are they

These type of scams involve criminals pretending to be a trusted organisation such as a bank, the police, a government department or a service provider. They can also pretend to be a friend or family member.

What to look out for

You receive an urgent request for your personal or financial information, to make a payment or move money. They may pressure you to rush causing a level of panic. You're asked to transfer money to another account for 'safe-keeping'.

You may be contacted by someone pretending to be a member of your family, claiming they've broken their phone and are texting you from a new number. This will be followed by a request for money.

How to protect yourself

- **Your bank or the police will never ask you to transfer money to a safe account or ask for your full PIN, password or passcode**
- Contact your bank or an organisation directly using a known email or phone number
- **Don't give anyone remote access** to your computer or install any applications or software to any of your devices following a cold call, unsolicited email or text message
- **If you have a social media account and someone you don't know tries to connect with you** saying they know a way to make money quickly do not respond
- If a **friend on social media reaches out saying they have made money quickly** and they want to show you how to do the same do not respond their account has been hacked
- **If you receive a text message from a new number claiming to be from a friend or family member asking for money,** always contact the person on their original number, not the new number they are contacting you from
- **If a caller tells you to hang up the phone and dial another number** – It is possible they have kept the line open and when you phone the number they have given you, you will be put through to another scammer. **If in doubt, call 159**
- **They may put you under pressure to act quickly** – This false sense of urgency triggers a reaction in us to worry that we need to take action in case something bad happens or we will lose our money. The enemy of scammers is: **Stop Challenge Protect** – Only criminals will try to rush or panic you
- **Remember: It's OK to refuse, reject, or ignore requests.** Taking a moment to stop and think before parting with your money or information could keep you safe

How to report a fraud or scam

You should call **159** if you're worried about a fraud or a scam, especially if you've received a phone call from the bank asking you to make a payment.

Tomorrow Begins Today

NatWest

Jane's story

Jane was at home, having a cup of tea when the phone rang

It was a very polite man called Philip, phoning from her bank, NatWest. Jane checked the number through her caller ID and it was the bank's normal phone number

Philip explains that he is in the bank's fraud team and that there is a problem; there appears to be fraudulent activity taking place on Jane's account

Jane is shocked and scared that she will be in trouble with her bank and even the police if they think she is responsible for this fraud. She is also worried that fraudsters have managed to take money from her savings

He says he has to validate Jane's identity to ensure she is the correct account holder, so he asks her for her online banking log in details. Because Philip is logging into Jane's online banking from a different device, he asks Jane for her one time passcode which will give him access to her online banking. She provides this

Philip is very kind and reassuring, he explains to her that he can get this all sorted for her today. He advises Jane that her money will have to be moved to a 'safe account' to protect the funds and it will have to be done quickly so as to avoid Jane losing her money

Whilst Jane is on the phone, Philip transfers the money out of her account into a 'secure account'

What to do in this sort of situation

In the case of a bank impersonation

- ✓ **Stop, hang up, and call 159** to be securely directed to your bank to check the call is genuine
- ✓ Criminals posing as the police may ask you to take part in an undercover operation to investigate 'fraudulent' activity being committed by bank staff. Legitimate organisations would never ask you to do this
- ✓ Only give out your personal or financial information to services you have consented to and are expecting to be contacted by
- ✓ If you're a NatWest customer, you can forward suspicious emails to phishing@natwest.com and suspicious texts referring to NatWest to the number 88355

In all other cases of impersonation

- Forward a suspicious text to 7726
- Forward a suspicious email to report@phishing.gov.uk
- If you receive a suspicious phone call you can report it via Action Fraud
- If you think you have been scammed, call Action Fraud

Tomorrow Begins Today

TAKE FIVE TO STOP FRAUD

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

NatWest