The Fraud & Scam Bulletin

April 2022

Your monthly update direct from West Mercia Police on the latest scams and frauds

There has been a rise in Impersonation Scams, especially those posing as Bank officials that everyone should be aware of.

IMPERSONATION SCAMS

WHAT ARE THEY?

You are convinced to make a payment or give personal and financial details to someone claiming to be from a trusted organisation such as:

- your bank
- the police
- a delivery or utility company
- communication service provider
- a government department such as HMRC
- someone you trust such as a friend or family member.

These scams often begin with a phone call, text, message or email that appears to be from a trusted organisation or person.
A criminal might say your bank account is at risk and ask you to move your money to a 'safe account'.
They might get in touch impersonating a police officer, saying your money needs to be analysed as part of a police investigation.
They may also get in touch via social media, sending you messages or by creating posts.
When criminals impersonate a friend or family member, they often invent reasons to ask for money, such as being stranded overseas or urgently needing to pay a debt, rent or a bill.

Criminals use many tactics to trick you including;

- including 'spoofing' which makes their call, text, DM or email appear genuine.
- These messages will often lead to a website that is made to look legitimate using another tactic called 'cloning'.
- Cloned websites often look almost identical to the real website of a trusted organisation.
- Phone numbers and sender ID's can also be cloned to make a scam message appear genuine.

- Criminals also use a tactic called social engineering to groom and manipulate you into transferring money or divulging your personal and financial details.

In some cases, criminals try to dupe you by sending couriers to collect your cards, cash, PINs or valuable items in person.

HOW TO SPOT AN IMPERSONATION SCAM

1. You receive a call, text, email or DM with an urgent request for your personal or financial information, to make a payment or move money
2. You receive a message from a friend or family member requesting financial assistance often with an urgent reason such as them being stranded overseas or requiring medical help
3. You are pressured to act immediately. The caller pressures you to rush causing a level of panic. Texts or messages may include a 'hook' to grab your attention, for example the criminal might say your money is at risk and you need to act to save it, or suggest you will get a reward if you do what they ask
4. You're asked to transfer money to another account for 'safe-keeping'
5. You're asked to purchase high value goods/vouchers to cover the cost of fines. They might also ask you pay a bill for tax or utilities or provide financial details to receive a rebate
6. You're asked for cash or a payment as part of a police investigation or told money in your account needs to be analysed as part of an ongoing investigation
7. The sender's email address is ever so slightly different to that of the genuine sender

IF YOU THINK YOU ARE BEING SCAMMED OR DO NOT RECOGNISE THE CONTACT

- **STOP**: Taking a moment to stop and think before parting with your money or information could keep you safe.

- **CHALLENGE**: Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

- **PROTECT:** Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud

If you've fallen for a scam, report it to **Action Fraud on 0300 123 2040** or via actionfraud.police.uk.

Scam Text messages can be forwarded to 7726 to help phone providers take early action and block numbers that generate spam on their networks.
Forward **Fake Emails** received to report@phishing.gov.uk.

SOURCE: TAKE FIVE

For further information visit:
https://www.actionfraud.police.uk/
https://takefive-stopfraud.org.uk/

West Mercia POLICE