The Fraud & Scam Bulletin MARCH 2024

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

TELEPHONE FRAUD

The number of “Nuisance” calls has risen in recent years from 21% to 40% and according to OFGEN, nearly 40% of Scams start with a phone call.

These scams involve fraudsters trying to gain your personal and financial information, and are often referred to as “*Vishing”* – an amalgamation of “*Voice*” and “*Phishing*”.

Very often the fraudster has disguised their call identity by using an apparently legitimate number so appearing genuine; this is known as “Spoofing”. If you do receive a call from a company which is not expected than just hang up, wait for 10 minutes or so, or use another phone, and then call the real company back on a listed number from their website or letterhead.

Common Phone Call Scams

- Technical Support scams - They may impersonate a company such as Microsoft or BT , and tell you there is a fault on your computer or Broadband. They then probably will ask you to download remote access software to gain access to your computer, or else install Malware on your computer.
- Impersonation Scams - Typically these may claim to come from your “Bank Fraud Department” telling you that your account or bank cards have been compromised and you need to transfer money to another so-called Safe Account, from where it vanishes. Similarly calls may come from fraudsters masquerading as a Police Officer, Utility Provider, HMRC or DVLA.
- Prize Draw Scams – “You have won the Lottery or a Prize Draw!” Sounds good but is it? You may think you never entered the competition but they will convince you that you have, then ask for your bank details so you can “receive” the prize
- Financial Scams – you are called with tempting offers for investing your money in funds, schemes or perhaps in Bitcoins with the promise of huge returns. Since 2019, it has been illegal to make cold calls to sell Pension schemes, so any calls about Pension Schemes will be scams. This scheme may be extended in the future to ban an unsolicited financial cold call.

How can you stay safe?

- Never give out your financial information over the phone, and just hang up if you are unsure about the caller's identity
- Register for "TPS" - Telephone Preference Service - this prevents bona fide companies calling you so you will then know that any cold call is a fake.
- Scammers will often keep the phone line open after the call so even when you think you are calling a legitimate number you are still speaking to the fraudster. Wait for up to 15 minutes or make the call using a different phone line or mobile

Please feel free to share these messages with any vulnerable friends, relatives or neighbours.

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

Take Five To Stop Fraud

- **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

If you think your bank account or personal banking details have been used fraudulently, then use the short phone number **- 159** - to contact the Fraud Prevention Department of most major UK banks.

For further information visit:
https://www.actionfraud.police.uk/

https://takefive-stopfraud.org.uk/