PHONE SPOOFING SCAMS

WHAT IS IT?

Phone spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Scammers often use neighbour spoofing so it appears that an incoming call is coming from a local number, or spoof a number from a company or a government agency that you may already know and trust. If you answer, they use scam scripts to try to steal your money or valuable personal information, which can be used in fraudulent activity.

WAYS TO PROTECT YOURSELF

- Don't answer calls from unknown numbers. If you answer such a call, hang up immediately.
- If you answer the phone and the caller - or a recording - asks you to hit a button to stop getting the calls, you should just hang up. Scammers often use this trick to identify potential targets.
- Do not respond to any questions, especially those that can be answered with "Yes" or "No."
- Never give out personal information such as account numbers, Social Security numbers, mother's maiden names, passwords or other identifying information in response to unexpected calls or if you are at all suspicious.
- If you get an inquiry from someone who says they represent a company or a government agency, hang up and call the phone number on your account statement, in the phone book, or on the company's or government agency's website to verify the authenticity of the request. You will usually get a written statement in the mail before you get a phone call from a legitimate source, particularly if the caller is asking for a payment.

WAYS TO PROTECT YOURSELF (CONTINUED)

- Use caution if you are being pressured for information immediately.
- If you have a voice mail account with your phone service, be sure to set a password for it. Some voicemail services are preset to allow access if you call in from your own phone number. A hacker could spoof your home phone number and gain access to your voice mail if you do not set a password.
- Talk to your phone company about call blocking tools and check into apps that you can download to your mobile device

HOW IT HAPPENS

Many phones have what is known as caller ID - the number of the person calling is displayed. Although many people find this a useful way of screening the calls they want to answer from the ones they don't, it's not a reliable way of checking who's on the other end of the line. Scammers can change the caller ID displayed on your phone. This is known as 'spoofing'.

They do this either to hide their own identity, or to try and mimic the number of a real company or person. They use spoofing to pretend they are calling from a genuine number e.g. the victims bank or credit card Company, utility provider, or a government department. Their aim is to steal sensitive information like bank account or log in details, in order to gain access to the victims' money.

Calls with spoofed numbers can come from anywhere in the world.

BOILER ROOMS HAVE BEEN KNOWN TO HARASS VICTIMS WHO HAVE REPORTED THEM, SO DON'T FEEL LIKE YOU'RE AT FAULT.

HOW TO REPORT IT

If you have been affected by this report it to Action Fraud by calling 0300 123 2040 or visiting www.actionfraud.police.uk

You can access many of the services provided by Greater Manchester Police online at gmp.police.uk. For emergencies only call 999, or 101 if it's less urgent.

TAKE FIVE TO STOP FRAUD

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

GREATER MANCHESTER POLICE