Do Not Get Spoofed By Number Scams

1. INTRODUCTION

Many phone handsets now let you see the number of the person calling before you answer.

This feature - known as 'Caller ID' or 'Calling Line Identity' (CLI) - is a handy way of screening the calls you want to answer from the ones you don't.

However, there have been growing instances of nuisance callers and criminals deliberately changing the Caller ID, a practice known as 'spoofing'.

2. Why Do They Do This?

Sometimes there's a good reason for a caller to modify the Caller ID (for example, a caller who wishes to leave an 0800 number for you to call back if you want).

However, with spoofing callers deliberately change the telephone number and/or name relayed as the Caller ID information.

They do this to either hide their identity or to try to mimic the number of a real company or person who has nothing to do with the real caller.

For example, identity thieves who want to steal sensitive information such as your bank account or login details, sometimes use spoofing to pretend they're calling from your bank or credit card company.

3. What Is Being Done?

Calls with spoofed numbers can and do come from all over the world and account for a significant and growing proportion of nuisance calls.

That's why Ofcom is working with the international regulators - as well as the telecoms industry - to find solutions to the problem.

Voice over IP (VoIP) technology - the type of technology used to make internet calls - is often used in spoofing. The Internet Engineering Task Force (IETF), which helps to develop internet standards, has created a group specifically to tackle this issue.

4. What Should I Do?

Identity thieves and other fraudsters often pose as representatives of banks, credit card companies, creditors, or government departments to get people to reveal their account numbers and other sensitive information.

Never give out your personal information in response to an incoming call, or rely upon the Caller ID as the sole means of identification, particularly if the caller asks you to carry out an action which might have financial consequences.

If someone rings you asking for this information, don't provide it. Instead, hang up and call the phone number on your account statement, in the phone book, or on the company's or government department's website to check whether the call was genuine. Wait at least five minutes before making the call - this ensures the line has cleared and you're not still speaking to the fraudster or an accomplice.

To report it to the police, call 101 or 999 if the crime is in progress action.

5. I Think I Have Been a Victim of Caller ID Spoofing

Tell Action Fraud
If you have been targeted by a scam, or know someone who has then call Action Fraud on 0300 123 2040 or visit www.actionfraud.police.uk

Action Fraud is the UK's national reporting centre for fraud and internet crime. However, if debit cards, online banking or cheques are involved in the scam your first step should to contact your bank or credit card company.

Tell Trading Standards
If you think something may be a scam, phone 03454 04 05 06 and tell the Citizens Advice Consumer Service, who can pass details of the case on to Trading Standards.

The Trading Standards service is responsible for protecting consumers and the community against rogue traders and traders acting unfairly.

Tell Others
Warn family, friends, neighbours, the local Neighbourhood Watch scheme etc. If you get a suspicious circular or are contacted by someone you think may be a scammer, make sure you tip off others.