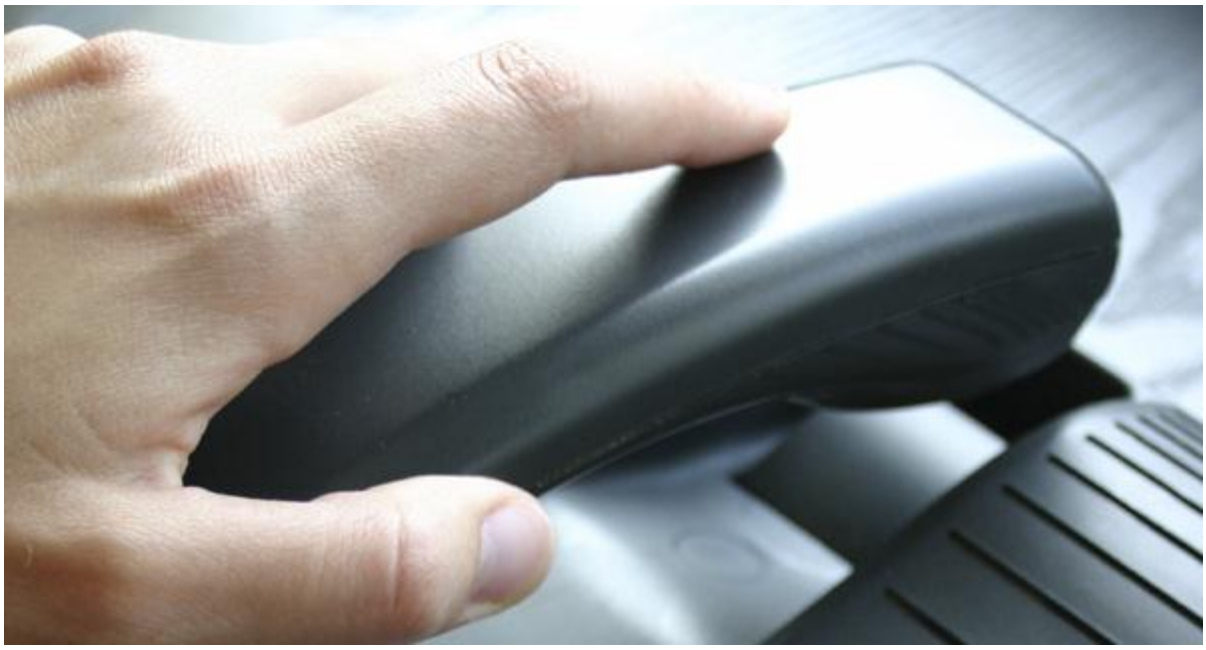
ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Action Fraud is not an emergency service dial 999 if you are in immediate danger.

Alert: watch out for new “number spoofing” scam



Fraudsters are using a new scam to make the people they are phoning believe they are speaking to a trusted organisation by fooling their phones into displaying any number they choose.

The scam, known as ‘number spoofing’, works by fraudsters cloning the telephone number of the organisation they want to impersonate and then make it appear on the victim’s caller ID display when they telephone them on a landline.

The fraudsters will then gain the person’s trust by highlighting the number to them, claiming that this is proof of their identity, before trying to scam them in various ways.

However, it’s not only individuals who are vulnerable to this type of fraud. The **National Fraud Intelligence Bureau** also warns that spoofing is used in **Mandate Fraud**. Emails and telephone numbers of genuine companies have been spoofed by fraudsters in order to fraudulently initiate transfers (for example, impersonating the company director to the

same company's accountant), or modify existing account details (impersonating a supplier with respect to a genuine invoice, or an employee with respect to pay).

Increasingly common

Financial Fraud Action UK's intelligence unit who issued the alert said the scam has become increasingly common in recent weeks. Whilst the technology needed to spoof someone's number has existed for years, only recently have criminals begun using it to defraud people.

The advice to beat the scam is simple – never assume that someone is who they say they are just because their number matches that of an organisation you know. In fact, if someone tries to draw your attention to the number on your caller ID display, you should immediately become suspicious.

New variation

This scam comes as a new variation on a type of telephone fraud, where fraudsters call people and pose as bank staff, police officers or other trusted organisations to persuade their victim to part with financial and personal details.

Once criminals have their victim's confidence they will try to extract information such as the victim's PIN, online passwords or other sensitive information which will then be used to steal from their bank account.

Read more on the **Financial Fraud Action UK** website.

Please note: Action Fraud is not responsible for the content on external websites.

To report a fraud and receive a police crime reference number, call Action Fraud on 0300 123 2040 or use our online fraud reporting tool.