ROYAL borough of GREENWICH

ALERTS
TRADING STANDARDS
05/02/2026

PHONE SCAMS TAKE SINISTER TWIST AS VICTIMS' VOICES CLONED

Chilling new wave of AI-assisted fraud targets older people and clones their voices

Criminals are using AI technology to clone people's voices and set up unauthorised direct debits over the phone, according to new evidence from National Trading Standards. The advanced voice cloning is part of an organised criminal operation that harvests people's personal data to target victims with a wave of scam and nuisance calls.

The process begins with a so-called 'lifestyle survey' phone call – seemingly harmless, but in fact designed to gather detailed personal, health and financial information. The criminals use this data to develop AI-generated voice clones used to simulate consent for direct debits, deceiving even legitimate businesses and financial providers. These details appear then to be passed or sold to other criminal operations who, with the details, can easily circumvent the banks and set up payments without the victim's knowledge. Victims often do not realise payments are being taken.

How can I protect myself from scam calls?

There are things you can do to protect yourself from scams:

- **Say no:** Ignore a caller that asks you for personal information, such as your PIN, or tells you that your computer has a virus. A genuine organisation will never ask you for these details over the phone, in an email or in writing.

- **Report any scams:** Forward unwanted texts to **7726** for free so your mobile phone provider can flag potential scams.

- **Check the line:** Be aware that scammers can keep your phone line open even after you've hung up. Use a different phone, call someone you know first to check the line is free, or wait at least 10 to 15 minutes between calls to make sure that any scammers have hung up.

- **Use an answerphone:** You can use an answerphone on your landline or voicemail on your mobile to screen your calls.

- **Check your calls:** Get a caller ID device to see who’s calling. But be aware that some scammers appear as a legitimate number, for example, your bank or utility company.

- **Try call blocking:** Some phones have call-blocking features to stop unwanted calls. If yours doesn’t, you can use a separate call blocker. Some blockers come pre-programmed with known nuisance numbers and some allow you to add numbers to that list when you get a nuisance or scam call. You can buy call blockers from various retailers, and some local authorities provide them.

- **Cut the cold calls:** Join the free Telephone Preference Service (Telephone Preference Service (tpsonline.org.uk)). This should cut some of the number of cold calls you receive, though it won’t necessarily block all scammers.

- **Call the company:** If you get a phone call from an organisation asking you for personal information, contact the company directly using a known email or phone number to check the call is legitimate.

- **Avoid links:** If you’ve received a text asking you to follow a link, don’t click on it. If you’d like to check if the text is genuine, contact the company directly either using their official website or phone number and enquire about your account that way.

- **Check bank statements regularly and report anything suspicious**.

WHERE TO REPORT

Protect others by reporting incidents like this.

Report suspicious texts you have received but not acted upon, by forwarding the original message to 7726, which spells SPAM on your keypad.

Report suspicious emails you have received but not acted upon, by forwarding the original message to report@phishing.gov.uk

If you, or anyone you know, have been affected by this fraud or any other scam, report it to Report Fraud by calling 0300 123 2040 or visiting www.reportfraud.police.uk

tradingstandards@royalgreenwich.gov.uk