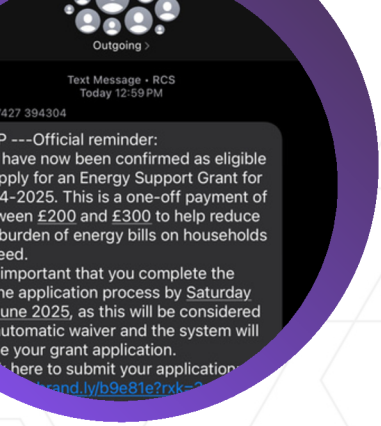

digital. FUTURES

What is Smishing and Vishing?

Phishing isn't limited to emails and fake websites; it also extends to **text messages** and **phone calls**.

- **Smishing** (SMS phishing) is a type of scam where criminals use text messages to trick someone into clicking malicious links or giving away personal information.

You may receive a text message:
"URGENT: Your package delivery is on hold. Click the link to confirm your address: http://fake-delivery-update.com"

Because you recently ordered something online, you might think it's real.

If you click the link, it could:
- Install malware on her phone
- Lead to a fake login page that steals her information
- Ask for credit card details

- **Vishing** (voice phishing) is a type of social-engineering scam where a scammer uses phone calls or voice messages to trick someone into giving away sensitive information, such as passwords, bank details, or personal data.

"Hello, this is your bank's fraud department. We detected suspicious activity in your account. To verify your identity, can you please confirm your account number and the one-time code we just sent?"

The scammer is pretending to be the bank to make you panic and reveal sensitive information. If you give those details, the scammer may then be able to access the account.

Supported by Rural Action Derbyshire in partnership with Digital Support Derbyshire.

How to Protect Against Smishing or Vishing

- **Don't Respond or Click Links** – Avoid replying to suspicious texts (smishing) or clicking on any links, as they may lead to malicious websites or install malware.
- **Verify the Sender** – If the message claims to be from a legitimate company, contact them directly using official contact details (not those in the message) or visit their official website or app instead of using the link.
- **Never Share Personal Information** – Legitimate organisations will never ask for sensitive details like passwords, PINs, or financial information via text or phone calls.
- **Hang Up & Call Back** – If you receive a suspicious call (vishing), don't engage. Hang up and call the company back using their official customer service number.
- **Block & Delete** – Block the sender's number and delete the message or call log to avoid accidentally engaging with it later.
- **Monitor Your Accounts** – If you shared any information, check your bank and online accounts for suspicious activity and update your passwords immediately.

Staying cautious and following these steps can help protect you from falling victim to smishing and vishing scams.

Report & Delete Suspicious Messages - Forward suspicious messages to: **7726** (SPAM) or report calls to your phone service provider and local fraud authorities.

Be extra careful with urgent or threatening messages.

Banks never ask for full passwords, PINs, or one-time codes over the phone.

Don't trust caller ID, it can be spoofed.

Never give personal or financial details to unexpected callers.