

Don't get smished!

Criminals send smishing (SMS based phishing) texts carefully designed to steal your passwords, payment details and personal information.

These text messages may appear to have been sent from businesses, organisations and services you use or by people you know and trust.

By spoofing phone numbers cyber criminals may even be able to get your phone to add scam texts to an existing message thread containing genuine texts you have previously sent and received.

Never click on any included links or respond with personal information or payment details even if you think the message is authentic. Check it using the genuine website or app, or by calling them on a trusted or known phone number.

Contact your bank immediately if you have supplied any payment details. Forward scam text messages to your phone provider on **7726**. Report to Action Fraud via **0300 123 2040** or **actionfraud.police.uk**

Criminals may use information you have unwittingly provided to later call or email you claiming to be your bank's fraud team or the police. Always confirm the caller is genuine by phoning a trusted number (bank letter, etc.) or the **Police on 101**.

If you know how to stay safe from smishing why not pass this guide on to someone else who may not be aware of the risks, to help them stay safe too.

