#MulletOver
Tell tale sign that it's a scam!
Your bank, or any other official organisation, won't ask you to share personal information over email or text. If you need to check that it's a genuine message, call them directly.
ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk
Cyber Aware
TAKE FIVE TO STOP FRAUD

Many scam messages share common tell tale signs. Asking you to "verify" personal or financial details is one of them.

Could you spot the tell tale signs of a phish? 🎣 Find out more here: https://www.actionfraud.police.uk/mulletover #MulletOver

What is phishing and how does it work?
You wouldn't let a thief enter your home, but what if the thief was masquerading as someone familiar, such as a postman, and tricked you into opening the door? Phishing works in a similar way - criminals use legitimate-looking messages and websites to trick people into opening the doors to their personal data, giving up logins, passwords or even payment details. That information can then be used to commit fraud and cyber crime.

How big is the problem?
Phishing attacks are a common security challenge that both individuals and businesses across the UK face on a regular basis.
The National Cyber Security Centre's Suspicious Email Reporting Service (SERS) received over 1.7M reports from the public between April and August 2020, with the most commonly faked brands being TV Licensing, HMRC and GOV.UK.

How can you protect yourself from phishing scams?
Many of the phishing scams that get reported to us have one thing in common, they started with a message out of the blue. Whether it's an email asking you to "verify" account information, or a text message claiming to be from your

bank, the goal of a phishing attack is usually the same - to trick you into revealing personal and financial information.

Criminals are experts at impersonation and they’re constantly getting better at creating fake emails and texts that look like the real thing. Here’s some simple advice you can follow when it comes to dealing with phishing scams:

1 - *Remember, your bank, or any other official organisation, won’t ask you to share personal information over email or text. If you need to check that it’s a genuine message, call them directly. Don't use the numbers/emails in the email, but visit the official website instead.*

2 - *If you have received an email which you’re not quite sure about, forward it to the Suspicious Email Reporting Service (SERS): report@phishing.gov.uk. If it turns out to be a malicious, your report will help other people from falling victim to it.*

3 *- Received a text message you’re not quite sure about? Maybe it’s asking you to “verify” personal or financial details, such as a banking password? You can report suspicious text messages by forwarding them to 7726.*

4 ***-*** *If you’ve lost money or provided personal information as a result of a phishing email, notify your bank immediately and report it to*
Action Fraud: www.actionfraud.police.uk

For more simple tips on how to protect yourself online, visit:
www.actionfraud.police.uk/cybercrime

+++