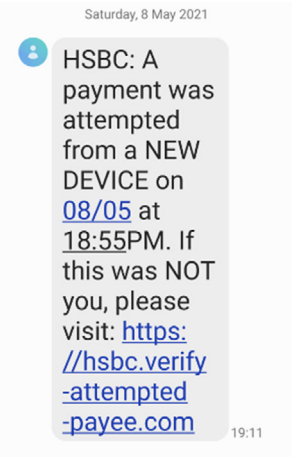
Fraud Alert

tiaa

Smishing Texts from Banks

As many of us now use on-line banking to make payments from our bank accounts, fraudsters are taking advantage.

Text messages are being received purporting to be from banks stating that a payment was made from a new device, and to click on a link if it wasn't you. On the right is an example of smishing (text message scam), purporting to be from HSBC, but any bank could be named in the text message. If you click on the link you will likely be asked for personal and financial information that could be used for fraudulent purposes by the scammers.



The National Cyber Security Centre (NCSC) website provides advice for dealing with suspicious text messages, as well as phone calls and emails, as spotting scams is becoming increasingly difficult. Full details are at:
https://www.ncsc.gov.uk/guidance/suspicious-email-actions

If the receive a message similar to the one above, don't assume that the sender is who you think it is.

The NCSC advise that suspicious text messages should be forwarded to 7726. This free-of-charge short code enables your provider to investigate the origin of the text and take action.

Status: Action Required

The alert provides information and advice to employees about fraud and economic crime and the risks associated with it.

If you have fallen victim to fraud or cyber-crime you should report it to Action Fraud by calling 0300 123 2040, or visit: https://reporting.actionfraud.police.uk/

If you have given your bank details and think you may have lost money to a scam, contact your bank immediately on a known telephone number.

How to protect yourself from fraud

- If you do not have an account with the bank that is sending you the text, delete the message.
- If you do have an account, think whether it could be genuine or not. Advice on bank websites is that any genuine message may contain a link to the bank websites but will NEVER link to pages asking for any financial or personal details such as your PIN or password.
- Use a trusted source to check - contact your bank directly on the usual number to check for account texts. Never use contact details in the message.
- Most banks have advice on scam texts and emails on their own websites, with further helpful guidance for their customers.

For further discussion and support, including fraud awareness training services, contact:

Melanie Alflatt, Director of Fraud and Security ■ Email: **fraud@tiaa.co.uk**

www.tiaa.co.uk
0845 300 3333