






How to spot suspicious calls, texts, and emails

Fraudsters often try to manipulate their victims into taking fear-based actions. For example, a spurious bank call-back service which pretends to alert the victim to bank account fraud, then requests detailed account information on response. Attackers may also impersonate a senior employee requiring urgent assistance. They may pretend to be in a rush, in an attempt to take control of the situation.

What to look out for

Fraudsters may use one or more of the following tactics to try to target your organisation:

Warning signs	What you should do
 <p>You receive a call from a seemingly legitimate number and the caller tries to get you to divulge sensitive information, like the code from your Security Device.</p>	<p>End the call and call back using a verified phone number to confirm the call is genuine. HSBC will never ask you to provide the code generated by your Security Device.</p>
 <p>Over-friendly or intimidating people claiming urgency, even threatening to complain or citing familiar names and details to pressure you into disclosing bank or personal information.</p>	<p>Trust your instincts. Do not provide any information. Report the call through your organisation's internal processes.</p>
 <p>Requests that are unusual or that require you to 'cut corners' or make exceptions to established procedures.</p>	<p>Ask questions to help you verify whether the request is genuine or not. Engage your manager or HSBCnet System Administrator for a second opinion before taking any further action.</p>
 <p>You receive an email that appears to be from a colleague within your organisation. When you reply, the email address of the recipient changes to an external party.</p>	<p>Do not reply, click on any links or open any attachments. Report the email to your HSBCnet System Administrator and forward the email to hsbcnet.phishing@hsbc.com. Then delete the email from your inbox.</p>
 <p>An unexpected text is sent to your mobile phone claiming to be from HSBC asking you to click a link to take urgent action.</p>	<p>Don't click any links in texts you weren't expecting to receive. Don't reply using the contact information provided in the text. Verify the text using known HSBC contacts.</p>

Stay vigilant

If you are ever doubtful about your HSBCnet activities or the authenticity of incoming telephone calls, texts or emails purporting to be from HSBC, please call your local HSBCnet Support Centre or your HSBC representative for further verification.