HSBCnet

Social Engineering

Risks to your business:

- Data loss
- Financial loss
- Fraudelent internet banking redirection

Do you know who you're actually talking to on the other end of the phone? Does an email or text message look genuine? Be vigilant. Thieves now have various clever ways to steal information for fraudulent purposes.

These tactics are known as Social Engineering, and it's on the rise.

How Social Engineering works

Phishing
Emails

Emails may create a sense of fear, urgency or opportunity to encourage recipients to click on a link or open an attachment that then infects their machine with a virus or malware.

This then allows criminals to steal information or money and/or disrupt a computer system.

While many fraudsters act randomly, some target specific groups of employees or customers. This is called spear phishing. One example is CEO fraud, where criminals impersonate senior executives and instruct colleagues to transfer money to them.

Another tactic is payment diversion fraud. Criminals will send an email claiming to be from a supplier. It says its bank details have changed so funds should be transferred to another account instead.

Don't reply to these emails.

Vishing
Phone calls

Fraudsters will often create a sense of panic to get a quick response over the phone. Targeting organisations, they may pretend to be a senior colleague or a customer in a rush or requiring urgent assistance.

Fraudsters may also call you pretending to be from HSBC. They may try to direct you to perform actions which would enable unauthorised payments to be sent to the criminal. This could include providing security codes generated from your token.

Many vishing campaigns are high volume, using auto-dial and broadband calling to contact thousands of potential victims per hour.

If you receive a suspicious call, do not provide any information.

Smishing
SMS texts

'Smishing' texts try to entice their target to click on malicious links, activating trojan viruses which can steal passwords and other high- value data.

Text messages may claim that your bank suspects there has been fraudulent activity on your account, that you are in trouble with tax authorities, or have won some money.

Smishing texts typically request urgent action, which often means clicking on a malicious link that in turn enables data theft. Spam filters stop many phishing emails from reaching inboxes, but no mainstream solution yet exists to prevent texts from reaching their intended target.

Don`t reply to these texts or click any links within them.

If you're suspicious about an incoming phone call, text or email purporting to be from HSBC, please call your HSBC representative for further verification

HSBC

Warning signs	Recommended action
You receive a call from an unknown long distance number or a redirect from the operator	Ask for the caller's identity (eg. Who they are, where they are from and why they need the information). Confirm the caller's identity through your organisation's verification process.
Over-friendly or intimidating people claiming that something is very urgent or important, and even threatening to complain. These people can cite familiar information including the name of your department or manager to pressure you into disclosing information.	**Trust your instincts.** If you receive a suspicious call for bank or staff information, do not provide any information. Report the call through your organisation's internal processes.
Requests that are unusual or that require you to 'cut corners' or make exceptions to established procedures.	If in doubt, 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.
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.	If you think you've received a suspicious email, 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.
An unexpected text is sent to your mobile phone claiming to be from HSBC asking you to click a link to take urgent action	Don't click any links in texts you weren't expecting to receive. Don't reply to the text using the contact information provided in the text. If in doubt, verify the text using known HSBC contacts.

How to keep your business safe:

- Raise awareness of the potential impact of Social Engineering within your organisation and implement a policy for reporting suspected cases.
- Never share financial or company information with people you don't know.
- Don't be rushed into making a quick decision.
- Never click on links in text messages or emails, or open or download attachments, unless you are sure they are safe.
- Be careful about the information you share on social media as this can provide fraudsters with many small pieces of information that make a bigger picture.
- Always call phone numbers you know and have checked. If someone claims to be a colleague, check their name on your organisation's staff directory and call them back on their internal telephone number.
- Forward any suspicious emails to **hsbcnet.phishing@hsbc.com.**

If you suspect you have been the victim of fraud, contact your HSBC representative immediately.