Fraud Trends

HSBC*net* Online Security Controls

En français | En Español | 繁體中文 | 简体中文 | العربية

HSBC*net*

HSBC

Contents

- Types of Fraud
  - Malware Attacks
  - Business E-mail Compromise
  - Voice Phishing (“Vishing”)
  - Short Message Service (SMS) Phishing (“Smishing”)
- How to avoid becoming a victim
- Additional HSBC*net* internet banking safety

Malware Attacks

- Malware is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems
- Customer's systems are compromised to make fraudulent transactions
- Customers will experience slow computers, unusual screens with requests to input codes and screens stating that the user will need to wait for a certain time before logging back in
- Malware can be inadvertently downloaded through clicking on links within phishing e-mails, compromised websites and by downloading pirated software

Malware Attacks

Examples:

- During logon customers may receive a "***Please Wait***" screen
- Computer may seem to be very slow
- Pop-up screens will request the user to input the security code and screens requesting that the customer pushes the yellow button
  (claims of token validation, security challenge or resynchronisation)
- Screens requesting that a second user logs onto the same computer for validation

Business E-mail Compromise

- A method of defrauding by targeting customers of financial institutions
- Occurs when fraudsters impersonate contractors, suppliers, creditors or even senior management to ask a company to change their payment
- Subsequent legitimate payments are then redirected to the fraudster's account

Why is this type of attack is difficult to detect?

- Attacks occur across financial institutions and are not restricted to any one country or region
- Fraudsters are well prepared before the attack by engaging in some form of reconnaissance (social engineering) to ensure details and names are correctly targeted
- E-mail addresses used to request changes on the payee account are identical or very similar to the original suppliers or vendors e-mail which makes it difficult to detect the fraud
- Fraudsters have been known to hack a creditor's e-mail account in order to send the beneficiary change request and thus appears to be a legitimate request
- Traditional mail services are used to send forged letters which appear to be from the creditor
- Exploits a human behavior/response which cannot be prevented by technology

HSBC

Business E-mail Compromise

Examples:

- E-mails from new or existing vendors who claim that account numbers have changed and request payments now be sent to a new location and account
- Vendors claiming payments must now be directed to a parent company in a different country
- Employees receive an e-mail from their CEO/CFO asking them to make payments but it will later turn out that the CEO/CFO's e-mail has been compromised
- E-mail may come from a domain that looks similar to a legitimate source

Voice Phishing (“Vishing”)

- Vishing is the term used to describe tactics used by fraudsters to “fish” for personal information (such as online banking security credentials) over the phone.
- Fraudsters may contact customers pretending to be from HSBC. They may direct you to perform actions which may enable unauthorised payments to be sent to the criminal. This could include providing security codes generated from your token.

HSBC will never request information over the phone that could be used to make a payment, such as asking you to provide security device codes or requiring you to divulge any of your security details.

HSBC

SMS Phishing (“Smishing”)

- Smishing is a variation of Phishing that uses SMS messages instead of e-mail
- Fraudsters may contact customers using SMS pretending to be from HSBC. They may direct you to perform actions which may enable unauthorized payments to be sent to the criminal. This could include providing security codes generated from your token.

HSBC will never request information that could be used to make a payment, such as asking you to provide security device codes or requiring you to divulge any of your security details

How can you avoid becoming a victim?

- Be suspicious of requests to change beneficiary information – question all changes and validate any change request using additional channels
  (i.e. call back and not reply directly to the e-mail)

- Establish internal control procedures for change requests to beneficiary details

- If unusual screens pop up and/or the computer's response is unusually slow, log out from HSBC*net* completely and scan the computer with the most updated version of virus protection software. If in doubt, contact your IT team and/or HSBC Customer Service Manager or team.

- Engage staff in fraud awareness and education

…How can you prevent becoming a victim?

- Never disclose security details over the phone when receiving unsolicited calls
  (ie username, token information, payment details)

- Whenever you receive an unsolicited call from HSBC, request contact details from the caller and validate the information with your HSBC Customer Service Manager or HSBC Help Desk

- Do not amend payment information unless you are certain it is legitimate

- Report attempted fraud to your bank and review e-mail settings (i.e. change password)

Additional HSBC*net* internet banking safety

- Never press the yellow button on the security device unless you are signing a transaction you have created – HSBC never asks for a yellow button response at logon
- Use Dual Control - for transactions and entitlements (*i.e. a minimum of two individuals are required for all activity*)
- Download Webroot *SecureAnywhere* software at www.hsbcnet.com at no cost to you
- Set signature limits
- Block all logons not coming from an approved list of IP addresses
- Update software no longer supported by vendors (*i.e. Internet Explorer 7*)
- Only access HSBC*net* via the website address at the address bar of your browser
- Never access through hyperlinks embedded in e-mails and do not rely solely on the look and feel of a website when using HSBC*net*

HSBC