

Cybercrime Fact Sheet: Email Scams (Phishing)

Background

The Most Common Attack

- Phishing is a technique used to gain information for purposes of doing damage, using fraudulent e-mail messages that can appear to come from legitimate senders.
- **Phishing** is the most common social engineering based cyber-attack method. It works by using emails to entice a user to click on a **malicious link**, or open an **attachment** that then infects their machine with **malware**.
- That malware then enables the attacker to achieve their end goals of **data or money theft** and/or service disruption or destruction.
- **Cyber Criminals** will use phishing techniques with differing levels of expertise.
- Sophisticated attackers will carefully research their targets, often using **Open Source Intelligence** techniques, and construct elaborate “spear” phishing emails, aimed at small numbers of key people.
- **High volume phishing** campaigns focus on getting to as many potential victims as possible. Even if only a tiny percentage are caught and infected, the attacker may be successful. They use generic email lures such as invoices, parcel delivery notifications, online banking messages etc. in order to appeal to a breadth of victims.
- **“Spear” phishing emails**, employ a convincing story based on knowledge of the victim, which is used to entice them to click on a malicious internet link or attachment. This then delivers malware and infects the victim’s computer.
- The story may be based on known information about the victim’s organisation or it may be gathered through research of **social media** or public website information.
- **Phishing attachments** may be delivered to a victim’s inbox, bypassing security and anti-virus by using Microsoft Office “**macros**”. If the victim runs the macro, it automatically downloads malware.
- **Web links** may take the victim to a legitimate looking but malicious website, which exploits vulnerabilities in the victim’s computer to install **malicious code**.

What do organisations need to do?

- Train staff never to open **attachments** or click on **links** in emails originating from unknown sources.
- Install and update **anti-virus** software.
- Keep software and operating systems **up-to-date** by downloading new releases and security patches as soon as they are available.
- Put **policies** in place that further protect your systems and information by giving staff guidelines for conducting business online.
- **Limit access** to systems and information based on job duties, and split financial responsibilities across two or more employees.
- **Restrict internet access** to trusted websites and limit the use of external media devices.

What are the risks?

- **Malware** delivered by phishing has been implicated in many high profile attacks with huge impact.
- The **Sony** attack in 2014 where confidential emails were stolen as well as the companies PCs rendered unusable, is just one of many examples.
- Increasingly both businesses and individuals are being hit with “**ransomware**” delivered by phishing emails, which encrypts the victim’s files and demands payment to make them accessible again.
- Bank customers are also targeted by “**Dridex**” type malware resulting in internet banking fraud.

Key tips

Learn to spot suspicious emails, there are several tell-tale signs:

- An unexpected e-mail, for example a delivery notification for a parcel you haven’t ordered.
- Unusual greeting or title in the subject box.
- Strange tone or odd language.
- A different e-mail address from a known sender.
- An e-mail with an unusual attachment or asking you to enable “macros”.
- A web link to a strange URL domain.
- Any mail or link asking you to enter passwords.
- Keep your home computer operating systems and software up to date – install the latest security patches as they become available, don’t run out of support versions like Windows XP and make sure you have an up to date decent Anti-Virus product – these days even the built in Microsoft Windows Defender is pretty good.
- Avoid “dodgy” sites and downloading free software / apps from unofficial sources. Some of the more advanced AV packages include reputational alerts that warn you when a site is not trustworthy, these can be useful.
- Be careful and aware of what information is available about you on social media and the internet. You can’t hide everything, but if you know what can be found about you, you can be more aware of it being used in a spear phish email against you. Try googling yourself and see what comes up.

If unsure, don’t click on it!

You can find four example screenshots on the next two pages that illustrate the warning signs to look out for...

What are the signs to spot a suspicious e-mail?

Speare Phishing Emails –Examples

From: HSBC_IT_Security@hsbc-security.com
 Sent: Tuesday, 11 August 2015 22:02
 To: [REDACTED]
 Subject: [Secure] 2015 Security Assessment Results

Not a genuine HSBC domain.

CLUE – put the domain name into <http://who.is/> and you can see whether it really is registered to HSBC

Recently, HSBC hired an outside firm to do email phishing attacks against HSBC personnel. These simulated attacks resulted in a partial compromise of internal company assets. Due to the results of this assessment, HSBC will be increasing awareness training for employees. It will likely be focused towards those employees and departments that were affected by the simulated attacks.

Please see the attached secured document to view the results of the assessment, including those email recipients that clicked the phishing email links.

SAVE PAPER - THINK BEFORE YOU PRINT!

This E-mail is confidential.

It may also be legally privileged. If you are not the addressee you may not copy, forward, disclose or use any part of it. If you have received this message in error, please delete it and all copies from your system and notify the sender immediately by return E-mail.

Internet communications cannot be guaranteed to be timely secure, error or virus free. The sender does not accept liability for any errors or omissions.

2015_Security_Assessment_Results.doc

Word document – contains a macro Which attempts to download malware.

From: "GlobalCompliance@hsbc-legal.com" <GlobalCompliance@hsbc-legal.com>
 To: <REDACTED>/HBUS/HSBC@HSBC02
 Date: 07/16/2015 11:11 AM
 Subject: [Required] HSBC Apple Pay NDA

Not a genuine HSBC domain.

As you may already know, HSBC's integration with Apple Pay was slated to be released on July 14th, during Apple's initial UK release. Due to the negative public exposure surrounding our Apple Pay launch delay, HSBC requires all IT personnel to sign this internal NDA stating that you will not discuss any details of HSBC's Apple Pay integration with any outside parties, especially the press.

You are required to sign this form, regardless of whether you have any direct involvement with the Apple Pay integration process, since all IT personnel may have access to information surrounding the project. Please review the attached NDA, and follow the instructions to sign and submit it to the HSBC Legal team. Failure to respond will be tracked, and may result in disciplinary action.

--
 HSBC Global Legal Compliance
 London E14 5HQ
 United Kingdom
 [attachment: "HSBC_ApplePay_NDA.docm" deleted]

What are the signs to spot a suspicious e-mail?

Phishing – Address Spoofing

From: Joanna MUNRO/AMEU/HSBC@HSBC
 To: George A.EFTHIMIOU/AMGB/HSBC@HSBC
 Date: 02/03/2016 23:03
 Subject: INTERNAL MEMO: Urgent Review

Be aware, Lotus Notes may display a spoofed email address as a genuine internal one!

CLUE - Often spoofed address emails will have a different "reply-to" address. In this case it was "Joanna Munro" deo.post@execs.com

Good Morning George,

I need you to make a quick payment offsets to some beneficiaries today. Kindly let me know if you will be available to perform this task and advice me on the banking information needed to complete them.

Regards
 Joanna

Sent from my iPad

No malware or malicious links in this, it's a Social Engineering attempt possibly aimed at a Business Email Compromise.

Confidentiality Notice: The information contained in this email may be confidential and/or legally privileged. It has been sent for the sole use of the intended recipient(s). If the reader of this message is not an intended recipient, you are hereby notified that any unauthorized review, use, disclosure, dissemination, distribution, or copying of this communication, or any of its contents, is strictly prohibited. If you have received this communication in error, please contact the sender by reply email and destroy all copies of the original message.

 This message originated from the Internet. Its originator may or may not be who they claim to be and the information contained in the message and any attachments may or may not be accurate.

CLUE – HSBC now adds this warning at the bottom of all internet originating emails. Why would an internal bank email be coming from the internet?

What are the signs to spot a suspicious e-mail?

Malicious Links – watch what you click

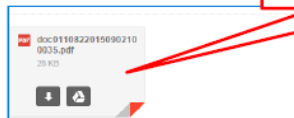
Antonio Simoes
Chief Executive Officer, HSBC Bank plc
From: Elaine Sullivan <es@mnp.co.uk>
Sent: Thursday, 10 March 2016 12:41
To: undisclosed-recipients:
Subject: Manchester Square

From: "Barclays Bank" <barclays@hultech-online.com>
To: Recipients: esullivan@mnp.co.uk
Date: 06/05/2016 02:58
Subject: Your transfer is being processed

Please find enclosed document referred to the mail subject.

Elaine Sullivan
Manchester Square Partners LLP

[Download / View](#)



.....
This message originated from the Internet. Its originator may or may not be who they claim to be and the information contained in the message and any attachments may or may not be accurate.
.....

Hover over the link and you can see where it's going

CLUE – Sometimes an HTM file is attached with a malicious link in it. You can't see these by hovering over them they but will display like this:

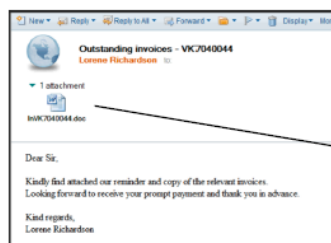


<http://www.bec.ru.ac.th/becjournal/index.php>

INTERNAL

What are the signs to spot a suspicious e-mail?

Attachments – Word/Excel Macros



CLUE – You shouldn't get internet emails with Macros in the attachments. By default, they are disabled on CWD. If you do open one, the attacker has to trick you into enabling them – like this.

WARNING – PDF files can also run malicious scripts. If you open a suspect attachment and get strange errors / messages on your screen – report them.

