# *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

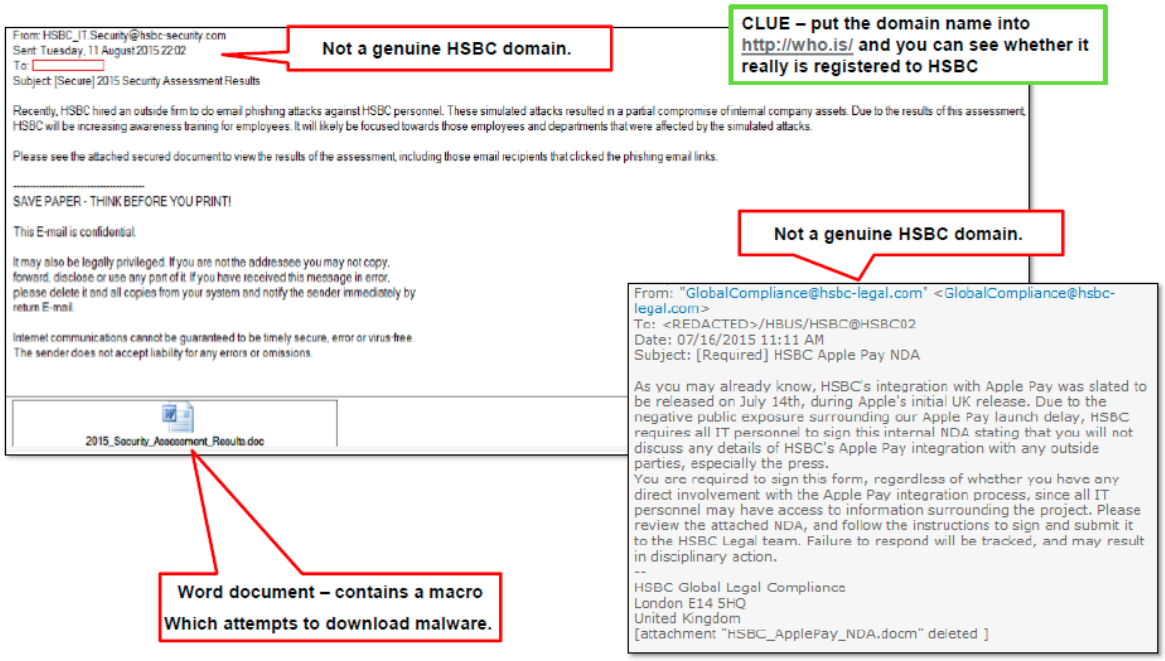
*Learn to spot suspicious emails, there are several tell-tale signs:*

- 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.

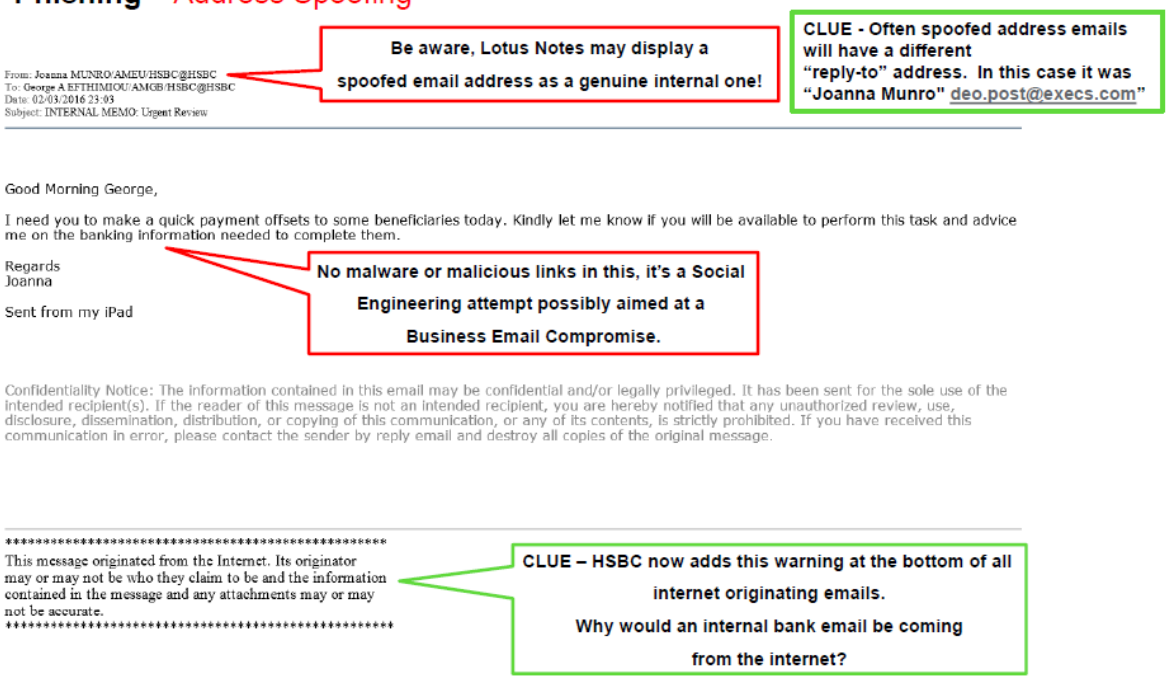
*If unsure, don't click on it!*

*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?
## Spear Phishing Emails –Examples

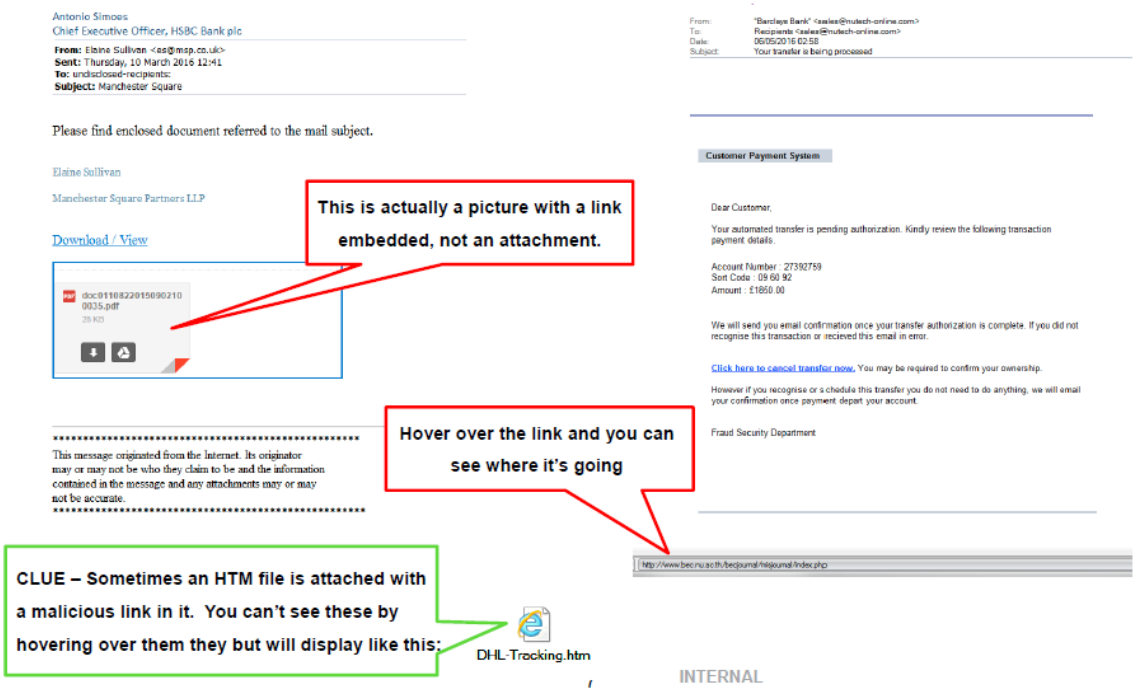



# What are the signs to spot a suspicious e-mail?
## Phishing – Address Spoofing



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

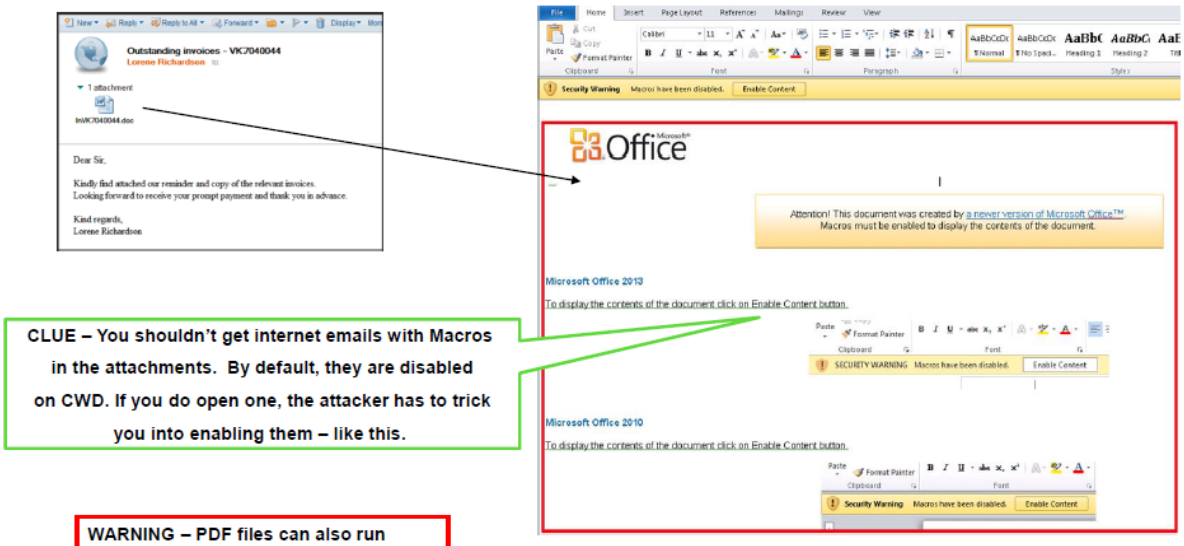
## Malicious Links – watch what you click






# 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.