TIP SHEET 4

PHISHING

connect smart week
10 - 14 OCTOBER 2016

Phishing is the practice of sending an email or text message pretending to be someone from a real company or government agency. The aim of the cybercriminal is to trick individuals to give away personal information such as passwords or credit card numbers. It may seek these details with some urgency in order to speed up a response. For example, you may be asked to click on a link which asks you to log into your bank account.

Whaling is a kind of phishing where hackers target the "big phish" – specifically managers and senior executives. These high profile targets typically have access to more information and as a consequence the payoff may be bigger. Whaling can be used to try and fast track executive sign-off on a payment.

If, for example, an employee receives an email claiming to be from a manager asking for a payment to be made or to send personal information, they should not complete the request until it is confirmed as a genuine request. Never bypass standard payment approval processes within your organisation in response to an unexpected email or phone call.

Employees should also be careful about how much information they provide over the phone to contacts they have not dealt with before – this information could be used to carry out phishing or whaling scams.

SIMPLE STEPS TO DEAL WITH PHISHING

1. Know how to recognise valid emails: Is the email from someone you know or have received an email from before? Is it something you were expecting? Does it look strange (e.g. unusual spelling or other errors in the email address or domain name)? Has it passed the anti-virus test?

If you think there's a possibility that an email is not genuine – forward it to your IT team or manager. Do not respond to it. Signs that it may be a phishing email include:

- Emails signed with a generic signature block, such as "Customer Service"rather than an individual's name, title and other details
- The email address or domain name do not match the "from" name, for example the email purports to be from "John Smith" or "The Smith Company" but the email address bears no relationship, such as: phishingagogo@theftonline.com
- Emails purporting to be from a business or a government agency but sent from generic mail services such as Gmail or with an unrelated email address
- Emails from organisations with which you have had no prior relationship
- Emails with offers that are "too good to be true"
- Emails asking for information e.g. passwords or logins

2. Think before you click: Employees should not open suspicious links in emails, tweets, social media posts, online ads, messages or attachments – even if they think they know the source.

Before clicking a link users should hover their mouse over the link to see if the link will lead to the correct destination – the website address underneath the link should show up. Some links may look genuine – but lead you to a different, possibly fake or scam, destination or result in the downloading of a virus or malware onto the computer and into the workplace network.

Banks will never send an email which has a link or an attachment to their Internet banking site. You should always manually type the bank's website address into the address bar rather than following a link.

3. Verify the email: If you are unsure about whether an email is from a legitimate company or government department, try calling the organisation that appears to have sent the email. Get the contact details from a previous account statement or invoice, or look it up online. Do not use any of the details or links provided in the suspicious email until you have verified that the email is genuine.