Registers of Scotland
ros.gov.uk

Security and Information Assurance

PHISHING EMAIL ADVICE

Registers of Scotland
Departmental Security Group
Policies and Procedures

Department	Security and Information Assurance (SIA)
Topic	Phishing email advice
Number	SIA17
Date	21 April 2014

Phishing emails are on the increase so there is every chance that you will receive one from time to time.

A phishing email is where the sender tries to trick you into opening up an attachment or an embedded link in an email. Their purpose is usually criminal, with the objective to steal sensitive personal information from you such as bank, email, social networking credentials to carry out harm against you.

Individuals need to be on their guard for phishing emails both in the office, at home or on their smart phone and take steps to avoid being a victim of one of these.

Our office email defences do offer some protection to prevent delivery of phishing emails to office email accounts however some evade these defences and get delivered to staff.

We have seen an increase in two types of phishing emails.

1) Where the email pretends to be from a trusted organisation such as a bank. For example where the email states that you need to urgently sign into your account to resolve a problem. The link in the email will take you to a website that looks exactly like the real one but is actually a fake designed to trick you into entering personal and sensitive information about your account.

2) Where the email pretends to be from a friend or family member. This email generally looks suspicious and will have a strange link but as it pretends to be from some you know well, the tendency is to trust it and click on the link. In this instance this action will likely download malware onto your equipment which in turn, unknown to you, will send your sensitive personal information such as bank, email, social networking credentials to the criminal each time you access these sites.

Tips to spot a Phishing email

Fake emails often (but not always) display some of the following characteristics:

- Bad spelling and grammar.
- The email does not use your proper name, but uses a non-specific greeting such as “Dear customer.”
- The sender’s email address is different from the trusted organisation’s website address.
- A sense of urgency; for example the threat that unless you act immediately your account may be closed.
- A suspect looking email from a family member or friend which contains a strange link.
- Roll your mouse pointer over the link to reveal its true destination, displayed in the bottom left corner of your screen. Beware if this is different from what is displayed in the text of the link.

Remember, organisations such as banks will never email you to request your personal information such as username, password or bank details.

If in any doubt regarding the authenticity of a particular office email you should either contact the Service Desk on ext 3166 or phone the organisation direct.

If you are sure that an email is a phishing scam then you should delete it from your mailbox.

Where to get more information

More information on phishing and how to avoid being a victim can be found on.

https://www.getsafeonline.org/index.php/protecting-yourself/spam-and-scam-email/

The following sites are one of many sites that provide information on the latest phishing scam emails

http://www.millersmiles.co.uk/

http://www.hoax-slayer.com/