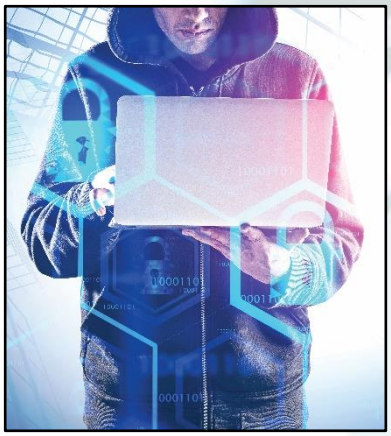
CYBER AWARE

south east
Regional Organised Crime Unit

Don't get caught out!

Newsletter – March 2020

Phishing



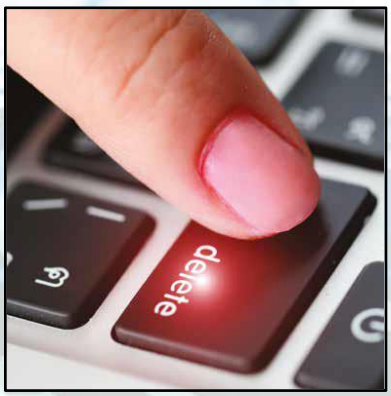
Phishing is the most common form of cyber-attack. It is defined as '*the fraudulent practice of sending e-mails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers*.' Criminals that carry out phishing attacks try to trick you into providing your information so they can use it for their own means. They typically use e-mail, social media platforms, text messaging and phone calls but could use any form of communication to persuade you to share sensitive information.

How does phishing work?

Millions of phishing e-mails are sent every day and use various techniques to persuade you to share information. Many contain a link to a malicious web page on the Internet, which requires you to enter personal data. Some will contain an attachment and will ask you to click on it.

Often, these attachments are designed to install malware onto your computer if you click on them. Some phishing e-mails will also use psychological manipulation (also known as social engineering) to encourage you to click on a link or open an attachment. Many are asking for help or charitable support.

What should I do if I suspect phishing?



Be aware and proactive. If you have any concerns about what you have received via e-mail or any other method of communication, consider the following actions: -

- Check any claims made in the e-mail through another channel, for example, by calling your bank to see if they actually sent you an e-mail or by doing a quick Internet search on some of the wording used in the e-mail.
- Never provide your login or personal details via e-mail and don't respond to a message or click on embedded links from an unknown source.
- If you detect a phishing e-mail, mark the message as spam and delete it. This helps to ensure that similar messages can't reach your inbox in future.

Useful Links

SEROCU: www.serocu.police.uk/individuals

NCSC: www.ncsc.gov.uk

Are you interested in a free cyber awareness presentation? Our Protect & Prepare team can deliver presentations to businesses and other groups (20+ attendees) across Surrey & Sussex. These are approximately 90 minutes in duration and cover a wide range of cyber topics. If you are interested, please e-mail CyberCrimeUnit@surrey.pnn.police.uk.

CYBER AWARE

south east
Regional Organised Crime Unit

Phishing Campaigns

A phishing campaign directed at groups of employees is often referred to as '**Spear Phishing**', and where the activity is directed at high profile employees, it's referred to as '**Whaling**'. Some criminals will spend significant amounts of time researching social media, company documentation and other personal information to design professional phishing e-mails that will maximise their chance of success.

Spoofing

Fraudsters can manipulate the 'From' field in an e-mail to make it appear that the e-mail is from one of your friends, someone in your address book or even yourself. This is called 'spoofing' and the real e-mail address may be concealed in the e-mail code or perhaps not even included in the message at all. Similar tactics can be employed with mobile phone messages and even telephone numbers.

How can I spot a phishing e-mail?

There are some common signs to look for to help you identify a phishing e-mail: -

- Poor grammar, punctuation and spelling.
- Inconsistent design and quality compared to genuine corporate e-mails
- No use of your name, but rather a reference to you as 'friend', 'valued customer' or 'colleague'
- A veiled threat, asking you to act urgently such as 'send these details within 24 hours' or 'click here immediately'
- Unusual sender name, or an incorrect impersonation of someone you know.

If it sounds too good to be true, it probably is. It's most unlikely that someone will want to give you money, or give you access to a secret part of the Internet. Your bank, or any other official source, should never ask you to supply personal information from an e-mail.

Is there anything else I need to know?

If you suspect you have been targeted by a phishing scam, please consider reporting the attempt to Action Fraud and then delete the e-mail.

'If you are going to click on a link or open an attachment – read the e-mail carefully!'

Useful Links

SEROCU: www.serocu.police.uk/individuals

NCSC: www.ncsc.gov.uk

Are you interested in a free cyber awareness presentation? Our Protect & Prepare team can deliver presentations to businesses and other groups (20+ attendees) across Surrey & Sussex. These are approximately 90 minutes in duration and cover a wide range of cyber topics. If you are interested, please e-mail CyberCrimeUnit@surrey.pnn.police.uk.