How to protect yourself & your organisation from phishing attacks

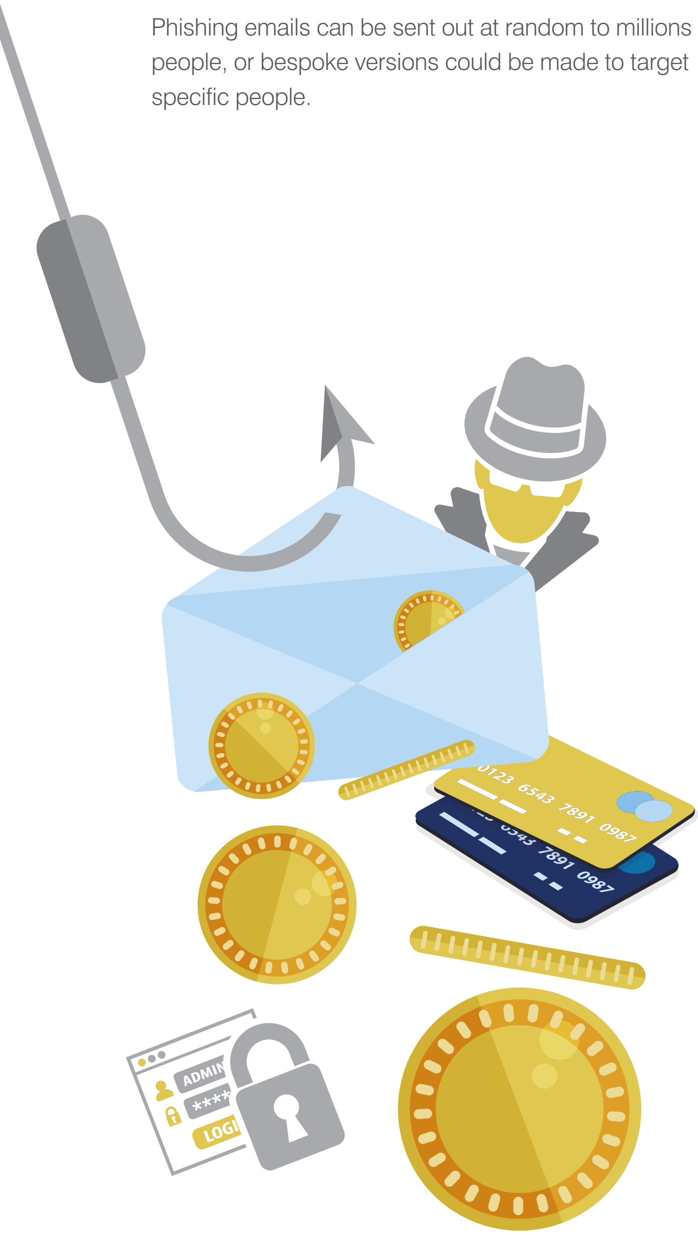
nccgroup

Intelliflo

The act of phishing

Phishing is a method used by cyber criminals to access valuable information, such as usernames and passwords or account details. Senders will typically ask users to click a link to a website designed to harvest credentials, or open an attachment – which is typically malware – that can infect devices.

Phishing emails can be sent out at random to millions of people, or bespoke versions could be made to target specific people.



The act of spear phishing

Spear phishing requires a lot more research on the part of the cyber criminal. It involves them acting as a trusted sender, usually a manager or a client, in order to get the recipient to divulge confidential information or to facilitate transfers of funds to them. Employees are far more likely to send such information, or process payments, to someone that they trust.

Worryingly, phishing and spear phishing attacks are on the rise, increasing by more than a fifth (21%) between 2015 and 2016[1].

And in 2016, 72% of all breaches of UK organisations were as a result of staff falling foul of fraudulent emails[2].

Can you tell the difference between a legitimate email and a phishing email?

It can take as little as one minute and 29 seconds for an organisation to be breached by an attack[3], so knowing how to spot the signs is vital.

[1] http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Annual-Fraud-Indicator-2016.pdf

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

[3] Data gathered from NCC Group's Piranha phishing simulation tool

What to look out for

The most important question to ask yourself when taking note of a new addition to your inbox is: was I expecting this email?

If the answer is no, then think before you click.

Beware of the sender

Cyber criminals can disguise their address to fool you in to thinking they've sent their message from an official domain. Hover over the sender's display name to see what the address actually is.

Check spelling and grammar

Read the email carefully. Emails from official organisations are usually proofread several times before they are sent and rarely contain typos or grammatical errors. If you see any errors, it's likely that you're being phished.

Are you expecting the email?

If a request for a payment is sent to you, or a request for sensitive information, ask yourself if you're expecting such an email?

Nature of the email

If you receive an email urging or hurrying you facilitate a payment or pass on information, consider why this might be. If the email is unexpected and urgent, applying pressure to you, then seek advice from the sender. Cyber criminals will try and prey on your emotions.

Avoid attachments

Does the email have attachments? If so, don't download anything or fill in any forms, especially in emails that claim to be from a bank. It's worth remembering that most large organisations will never ask for personal or sensitive information over email.

Log in manually

Reputable organisations will also never send links to their login pages. If you're asked, via email, to log in to a service, then open your browser and navigate to the website manually rather than use any provided links.

Avoiding the phishermen

While phishing attacks are now more prevalent than ever, there are plenty of ways you can reduce your organisation's risk and potential exposure to attack.

Education is key

User education is vital. If you're not currently doing something to raise user awareness of phishing attacks, consider it; employees who don't know how to spot a phishing attempt could put your organisation at serious risk.

Scan the waters

Many phishing attacks are specifically designed to convince the receiver that the email is from someone they trust inside their organisation. It is therefore important that you make it easy for users to distinguish between emails received from an internal and external source. Microsoft Exchange offers a feature that allows you to implement external email identification[4].

Virus protection

Install and regularly update virus protection across all of your organisation's devices, including computers, tablets and mobile phones.

Patch it up

Always patch software when updates become available. Ideally, all software across all devices should be set to update automatically.

Micro-manage your passwords

Using the same or similar passwords across a range of services can make it easy for hackers to access all of your accounts following a single breach. Consider implementing a password manager, such as KeePass or LastPass, and create strong and varied passwords for each individual account. Make sure that the master password for the manager is a strong passphrase which uses a mix of letters, numbers and symbols.

Implement two-factor authentication

Two-factor authentication (2FA) requires a second credential to be entered when users sign in, especially if the system recognises that they're signing in on new device or from a new location. Even if your password is stolen, malicious parties cannot login without the 2FA. It will not stop every attack on your organisation, but it will reduce the quantity of attacks from hackers looking for a quick win. Verizon also stated in its 2017 Data Breach Investigations Report that 24% of attacks could have been prevented with 2FA[5].

[4] https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016/january/phishing-mitigations-configuring-microsoft-exchange-to-clearly-identify-external-emails/

[5] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Caught in the net?

If you're unfortunate enough to have been fooled by a phishing attempt, you're not the only one.

Contact your organisation's IT department as soon as possible so that they can quarantine the virus or recover stolen information.

And if you've run an executable on your machine, switch it off and unplug your network cable as quickly as possible to stop any spread of the virus to other devices.

If you've given out personal information, such as banking information or credit card details, contact the relevant companies immediately and let them know what has happened.

You can also contact ActionFraud, the UK's national fraud and cyber crime reporting centre. It provides a central point of contact for information about fraud and cyber crime and can help you report fraud if you've fallen victim.

For financial advisers who have any queries, or believe that they have been victim of an attack, NCC Group and Intelliflo have launched a free helpline.

More information is available here.