Global service
built around you

North

Phishing awareness: useful hints and tips to help stop you from becoming a victim!

The threat around phishing emails remains high. Even more so since COVID-19 resulted in employees adapting to work remotely from their homes or through a hybrid approach, with time divided between homes and offices. The current conflict situation involving Russia and Ukraine has further heightened the cyber threat level of associated activities.

Hackers quickly identified the opportunity to take advantage of this unprecedented situation and raised their game around attempts to hack organisations. Employees within any organisation remain its greatest asset, but they can also be its greatest security threat due to their inherent trusting nature. Its far easier to hack a human rather than attacking sophisticated system-based controls that may be in place.

The number of Phishing emails has increased by approximately 400%* globally over the past 18 months with employees remaining a prime target, predominantly by being tricked into clicking a link, opening a malicious attachment, providing personal or commercial data or unknowingly sending payments to a fraudulent recipient.

Phishing emails are effective because they are quick, cheap and easy to send and can reach millions of mailboxes within seconds. One click or response makes it worthwhile for the hackers.

Here are some useful hints and tips to watch out for when receiving an email to help you stop becoming the victim of a successful phishing attack:

- Always assess the **context** of an email, do you know the sender and were you expecting an email from them or is it completely out of the blue or making an unusual request?
- If your organisation utilises spam filter warnings within the email subject or use warning banners to advise that an email has been sent externally to your organisation, be suspicious if the email is portraying to be from a work colleague internally but is marked as external.
- Is the sender hassling you to do something or to take an action? Never feel rushed into taking an action, it's a common tactic to hurry you into making a mistake.
- Is there an incentive to open an attachment? For example, something nice if you comply such as a gift voucher or something nasty if you don't i.e., a fake speeding ticket or fake legal summons using fear in the hope to convince you to click a link or open an attachment.
- Does the domain name/ email address look correct? Hover your mouse over the email address or right mouse click to check the email properties. Does the spelling of the email address look correct or have letters been replaced to fake a domain name such as use of 'rn' to look like an 'm'?
- Is the email addressed to you personally or is it just generic i.e. Dear Sir or Madam? Does its structure look genuine? Many Phishing emails are not personalised, is something just not right? Trust your instinct and report/ always ask for help if unsure.
- An email contains a request for money/ change of bank details held on file or to provide personal details. Please be wary of unexpected requests.
- Remember genuine email accounts can also be hacked. Please be wary of the content of an email if the style of a message from a contact that you know suddenly changes i.e., the way they address you or their grammar/ use of language changes or they ask you something odd and unexpected such as clicking a link or opening a strange and unexpected attachment.
- If unsure of the legitimacy of an email portraying to be from a contact, verify its authenticity by contacting them directly via independently verified contact details not from the details displayed within the email just received! Pick up the phone and verify.

Think before you click, always assess the content and context of an email, don't feel rushed into taking an action, if in doubt pick up the phone to verify a request with the sender, report all suspicious email to your organisation's IT team through the relevant channels.

For more information, please visit www.nepia.com

* percentage average across multiple sources/ publications