Cyber

Phishing

Phishing is the "fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords, financial information and credit card numbers."[1]

An example of phishing is receiving a bank email regarding an urgent issue with the account and instructions to click a link to be redirected to an external website and provide personal information to clarify the issue. Although the website may look legitimate, entering personal information as instructed can potentially lead to identity theft and credit fraud. There are also other phishing methods besides email.

Common Types of Phishing[2]

- **Email Phishing:** Generic emails with urgency that requests users to click a link or open and download an attachment.
- **Spear Phishing:** Similar to email phishing, but these emails are targeted to specific individuals, using accurate names, job titles and email addresses.
- **Whaling:** Emails targeted to senior executives with subtler messaging.
- **Smishing and Vishing:** Using either text messages or direct phone conversations to request personal information for an urgent issue.
- **Angler Phishing:** Directing individuals to click a link or download malware by contacting them using social media.

Phishing can also cause malicious damage to networks and systems. For example, an email offering a free screensaver can install the screensaver and also malware, software designed to "disrupt, damage, or gain unauthorized access to a computer system,"[3] which can potentially track web surfing, steal passwords, credit card numbers and private customer information.

How to Avoid Phishing Scams[4]

- Never click links or provide personal information in response to an email or phone call asking for information. Contact the organization directly using a phone number available on the corporate website and use the official website to open log-in pages.
- Never respond to an email, even to unsubscribe or opt out, if there are any doubts about the sender. Doing so will confirm to the sender that they had reached a live and active email account.
- Never open an email attachment if there are any doubts about the sender. File attachments are an easy method of transferring malware.
- Never give out a password. IT personnel do not ask for a password.
- Install reputable anti-virus, anti-spyware and security software and update it regularly.

Aside from security software, it is recommended for corporations to regularly train employees on the topic of phishing. Informed employees are more equipped to recognize and avoid attempted phishing attacks.

For more information, visit cnacanada.ca.

1 Lexico (2019) Retrieved from https://www.lexico.com/en/definition/phishing
2 IT Governance (2019) Retrieved from https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack
3 Lexico (2019) Retrieved from https://www.lexico.com/en/definition/malware
4 Digital Gaurdian (2019) Retrieved from https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams