Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

SPOTTING MALICIOUS EMAIL MESSAGES

OCTOBER 2018

ITSAP.00.100

Who receives malicious e-mails?

Organizations and their networks are frequently targeted by a wide variety of threat actors looking to steal information. Cyber intruders are technologically savvy, vulnerability conscious, and aggressively agile; a successful intrusion can quickly lead to the loss of data integrity and confidentiality. Employees are privy to important and sensitive information, and as a result, often receive malicious e-mails that are intended to provide cyber intruders access to this information. Everyone needs to be aware of the threats and take care to ensure that organizational information is protected and secure.

Phishing vs. spear phishing

Phishing is the act of sending mass e-mails that appear to be from a legitimate source, but contain infected attachments or malicious links. The e-mails are written to trick receivers into opening attachments or clicking on links that permit threat actors to obtain personal credentials or gain access to a computer system and its information.

Spear phishing, although similar to phishing, is a tactic threat actors use to send socially-engineered e-mails to specifically target individuals or groups based on their personal characteristics, interests or lines of work. The messages appear to be sent by a credible source on subjects that are relevant to the recipient. A greater effort is required to create spear-phishing e-mails, but threat actors are willing to make the effort because receivers are more likely to open the infected attachments or click on the malicious links.

Why is spear phishing so effective?

Spear phishing is effective because phishers create e-mails that seem genuine: they contain company logos or trademark information, the subject line is relevant, the message is pertinent. Given receivers' desire to trust, it is easy for them to believe that these e-mails are legitimate and click on the links or open the attachments.

Malicious software can be contained in attachments such as PDFs, photos, office documents, as well as Web links that seem legitimate. Spear phishing can create an opportunity for cyber compromises in any organization.

AWARENESS SERIES

SPOTTING MALICIOUS EMAIL MESSAGES

OCTOBER 2018

ITSAP.00.100

No one is immune

Everyone can be a target of phishing and spear-phishing e-mails. However, those more commonly targeted include the following individuals:

- Senior executives and their assistants
- Help desk staff, system administrators
- Users who have access to sensitive information
- Users with remote access
- Users whose jobs involve interacting with members of the public

How to detect spear-phishing e-mails

While spear-phishing e-mails can be hard to identify, there are a number of proactive ways to avoid falling prey to them and triggering a cyber-incident. Before opening attachments or links embedded within an e-mail, take the following steps:

- Make sure you know the sender of an e-mail and that its tone is consistent with the sender.
- Make sure that the Web address or attachment is relevant to the content of the e-mail.
- Make sure that the sender's e-mail address has a valid username and domain name. A suspicious e-mail address could be similar to the one below:
  "John Doe <ohndoe.%nklo17er@gkmail.com>".

How to handle malicious e-mails

It is crucial to maintain a high level of cyber awareness and scrutinize all e-mails before opening them. If you have received a suspicious e-mail or suspect malicious activity, report the incident to your IT Service Desk and/or your Organization's Security Team and follow their instructions.

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Come visit us at Canadian Centre for Cyber Security (CCCS) **cyber.gc.ca**