Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

Spotting Malicious Email Messages

April 2022

ITSAP.00.100 V.3

Organizations and their networks are frequently targeted by threat actors who are looking to steal information. Threat actors are technology savvy, vulnerability conscious, and aggressively agile; a successful intrusion can quickly lead to data and privacy breaches. As an employee, you may have access to sensitive company information, and you should be wary of malicious emails, which threat actors use to infect devices and systems and access information. By learning about malicious emails and phishing attacks, you can help protect and secure your organization's information.

Phishing attacks

Phishing is the act of sending communications that appear to be legitimate but are fraudulent. Phishing emails often contain malicious attachments or links to malicious websites. Threat actors carry out phishing attacks to trick you into disclosing sensitive information, such as credit card numbers, social insurance numbers, or banking credentials.

Phishing attacks can take the form of emails, texts, or phone calls, but this document focuses on malicious emails.

While some phishing emails may be generic, threat actors can also carefully craft emails that look more convincing or legitimate :

- **Spear-phishing email** : A threat actor sends emails to specific targets, such as an individual, a group, or a company. A spear-phishing email is crafted using the recipient's personal or professional characteristics and interests. Threat actors often use publicly available information from the individual's social media accounts. Spear-phishing emails require more effort from threat actors, but recipients are more likely to respond to the email, open attachments, or click on links.
- **Whaling email :** A threat actor sends emails to high-profile individuals or senior executives at a company. Threat actors create targeted and convincing emails by using personal information about the individual or the company they work for. Threat actors may use publicly available information from the company's website or social media accounts.

An effective method of attack

Phishing attacks are effective because threat actors can be highly skilled at creating emails that look legitimate. These emails contain company logos or trademark information. The subject lines are relevant, and the messages are pertinent.

Given our desire to trust (and the number of emails we receive daily), it can be easy to believe the content we read in these emails, click on embedded links, or open attachments. However, the attachments may contain malicious software, and the links may direct you to malicious websites. Even if an email comes from someone you know, you should always think twice before clicking links or opening attachments.

No one is immune

Although anyone can be the target of phishing and spear-phishing emails, the following individuals are more commonly targeted :

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

Beware of quishing—a phishing attack using malicious "quick response" (QR) codes in emails that re-directs you to phishing websites when the QR code is scanned. Check the website URL to make sure it is the intended site.

AWARENESS SERIES

Cat. No. D97-1/00-100-2021E-PDF
ISBN 978-0-660-38743-7

Identifying malicious emails

Malicious emails can be difficult to identify, but there are some steps you should take to determine whether emails are legitimate or fake :

- Check that the sender's email address has a valid username and domain name. A suspicious email address could be similar to the one below: **"John Doe <johndoe.%nklo17er@gkmail.com>".**
- Verify that you know the sender of an email and that its tone is consistent with the sender.
- Look for grammatical errors or typos in the body of the message. Companies want to maintain a high degree of professionalism and generally do not send out emails that contain these types of errors.
- Consider the tone of the email or what is being offered. If the email is threatening or sounds too good to be true, then it is probably a phishing email.
- Pay attention to what is being requested. Most companies do not ask for sensitive or personal information in an email.

Handling malicious emails

Handle suspicious emails with care. When in doubt, avoid opening suspicious emails and contact the sender by another means (e.g. phone call) to confirm they contacted you.

Do not click on links, attachments or QR codes provided in emails. If you are being asked to log in to an account for an unsolicited reason, do not click the link. Do not open attached files and avoid scanning QR codes. Instead, visit the company's website by manually entering the URL in your web browser or search for the website through a search engine.

Report suspicious emails. If you receive a suspicious email or suspect malicious activity on a work device or a work account, report the incident to your organization's IT and security teams. Follow their instructions and avoid forwarding the email to coworkers. You can also report phishing emails to us (**cyber.gc.ca**) or the Canadian Anti-Fraud Centre (**antifraudcentre-centreantifraude.ca**).

If you receive an offensive, abusive, or potentially criminal message, inform your local police. Save the message as authorities may ask you to provide a copy to help with any subsequent investigations. **Do not send the message to anyone else.**

Interacting with a malicious email

If you accidently interact with a malicious email, remain calm and begin by taking the following actions :

- Stop using your device.
- Disable Wi-Fi or disconnect network cables so the device cannot communicate with the Internet.
- Power off the device.
- Contact your IT security department if you are using a corporate device. They can disable accounts and other device features.
- Change your password, passphrase, or PIN using a different device.
- Scan the device using anti-malware software if possible.
- Restore network connections only when you believe you have a clean system.
- Perform any available updates and security patches on your device.
- Monitor your accounts regularly for suspicious activity.

Additional publications

To learn more about phishing attacks or other cyber security topics, visit our website.

You can find additional guidance and resources, including the following related publications :

- Have You Been Hacked? (ITSAP.00.015)
- Protect Your Organization from Malware (ITSAP.00.057)
- Don't Take the Bait: Recognize and Avoid Phishing Attacks (ITSAP.00.101)
- How to Protect Your Organization from Malicious Macros (ITSAP.00.200)
- Cyber Security Tips for Remote Work (ITSAP.10.116)
- Best Practices for Passphrases and Passwords (ITSAP.30.032)
- Implementation guidance: email domain protection (ITSP.40.0645 v1.1)
- Security Considerations for QR Codes (ITASP.00.141)

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 (Cyber Centre) at **cyber.gc.ca**