Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Malicious Emails

Every day, millions of spam and phishing emails are filtered from email systems but there are always a few that end up in our inboxes.

How do I recognize a malicious Email? There are some telltale signs of a malicious email:

- The sender's address is incorrect (inspect the full address and not the display name).
- The email is not personalized ('Dear Sir or Madam' or 'Dear Cardholder').
- It has embedded links with strange URLs (inspect them carefully - right click, 'copy hyperlink' and paste into a document to view).
- There are spelling or grammatical errors.
- It plays on your emotions, intimidates or threatens you if you do not perform an action
- The content is bizarre, not believable, or offers a deal that is 'too good to be true'.
- It is 'phishing' for information.

How do I prevent from becoming a victim of a malicious email? There are a few safe practices:

- Inspect the components of your email including the sender, subject line and content.
- Do not open any unexpected attachments.
- Do not click on any unverified links.
- Do not click on 'unsubscribe', as it confirms your address is current and correct.
- Do not respond to spam emails, as this will intensify the number that you receive.
- You may wish to 'Disable HTML' and 'Read in Plain Text', or close the preview window to lessen the chance of running a malicious script.
- If unexpected, confirm via separate email or call.
- Delete any suspicious emails, without opening.

What are some other email Best Practices?

- Never divulge personal or confidential information if requested by an unverified source.
- If you must send confidential information through email, encrypt or password protect it
- Do not use company email for personal use.
- Do not access company email from public Wi-Fi
- Always check your 'send to' carefully and do not 'reply to all' unless warranted.
- Use Bcc when sending to large groups or lists
- If you are unsure of the validity of an email, delete it.
- If you are concerned that an email is particularly malicious, notify your IT department so they can investigate.

Despite our best efforts, incidents happen – the most important thing you can do when it does occur is to report it immediately.

What if I have clicked on a link that I believe to have been malicious or contained malware?

1. Follow your company's incident management process. For Provincial Government employees, contact the 7-7000 Service Desk at 250-387-7000 (Option 3) for further direction.
2. If you provided credentials, immediately change your password (to something completely different) from another computer.
3. Report the incident to your supervisor.