Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

CYBER HYGIENE FOR COVID-19

The Cyber Centre has seen an increase in reports of malicious actors using the Coronavirus (COVID-19) in phishing campaigns and malware scams.

The response to COVID-19 is being led by Public Health Agency of Canada (PHAC), with support from public health officials and agencies across Canada. For information about COVID-19 please visit the Government of Canada's COVID-19 Outbreak Update page for the most up to date information.

BEWARE OF FAKES

With public concern around COVID-19 growing, there is an increasing number of phishing attempts referencing the virus. Phishing is the act of sending mass emails that appear to be from a legitimate source, but contain malicious attachments or links. The emails are written to trick receivers into opening attachments or clicking on links that permit threat actors to obtain personal credentials, or gain unauthorized access to a computer system. There have been recent instances where phishing has been used in attempt to impersonate various health agencies.

Malicious cyber actors are quick to take advantage of high profile events, particularly those that cause worry and concern.

WAYS TO PROTECT YOURSELF

Here are some ways that you can Protect your device from malware:

Against Malicious Emails:

- Make sure the address or attachment is relevant to the content of the email.
- Make sure you know the sender of an email.
- Look for typos.
- Use anti-virus or anti-malware software on computers.

Against Malicious Attachments:

- Make sure that the sender's email address has a valid username and domain name.
- Be extra cautious if the email tone is urgent.
- If you were not expecting an attachment, verify with the sender.

Against Malicious Websites:

- Make sure URLs are spelled correctly.
- Directly type the URL in the search bar instead of clicking a provided link.
- If you must click on a hyperlink, hover your mouse over the link to check if it directs to the right website.

4 PRACTICAL WAYS TO MAKE YOURSELF CYBERSAFE

- Use unique passphrases and complex passwords
- Apply updates to your mobile devices, computers, and applications
- Store your data securely and know your backup procedures
- Secure your social media and email accounts

Are You Prepared?

Security IT Actions to Protect Your Organization