COVID-19 AND MALICIOUS WEBSITES

May 2020 ITSAP.00.103

Threat actors are taking advantage of the novel coronavirus (COVID-19) pandemic as an opportunity to register malicious websites disguised as resources related to COVID-19, such as news and public health updates, maps showing the spread of COVID-19, or even pleas to donate money to charitable campaigns and emergency funds. Threat actors use malicious websites to misinform the public, steal sensitive information, and spread malware to damage or compromise systems and devices.

COMMON THREATS

Charity scams: Threat actors are counting on your good will during these uncertain times. A threat actor may pose as a charitable organization in an attempt to steal your banking or credit card information. Before making a donation, verify that the organization is real and a registered charity (e.g. with Canada Revenue Agency).

Phishing: Threat actors send emails or text messages with links to malicious websites to try to steal your personal information. **Some threat actors may pose as government departments, offering benefits such as the Canada Emergency Response Benefit.**

Phony or overpriced products: Scammers may offer to sell vaccines, treatments, medical equipment, personal protective equipment, or even cleaning supplies to make money or steal your financial information, such as your credit card number.

SPOOFED WEBSITES

A threat actor spoofs a website to make it look like a legitimate one, using its logos, fonts, and colours. At first, you might not notice that it's fake, but use the tips below to take a closer look:

- **The website's address:** Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g. .com vs. .net). Some websites use words related to COVID-19 to entice you to click on them. For example: corona19-advisory [.] com or cov19esupport [.] com
- **The website's layout and content:** Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Check the footer of the website because you might just notice that something isn't quite right with the layout.

If a website claims to be a reputable source (e.g. Canada Revenue Agency, Public Health), visit the website by using a search engine or typing the address manually into your browser.

REPORT SCAMMERS

If you spot a fake website, report it to the Canadian Anti-Fraud Centre: **antifraudcentre-centreantifraude.ca**

If you receive a phishing message, report it to the Canadian Centre for Cyber Security: **contact@cyber.gc.ca**

ADDITIONAL PRECAUTIONS

You need to be vigilant about cyber security, especially in times of stress and uncertainty. Be wary of unsolicited links, even if they are sent to you by people you know.

Take the following precautions to protect yourself and your information:

- Verify links before clicking them. Hover your cursor over a link to check if the embedded URL matches the link.
- Type a URL manually into a browser or a search engine instead of clicking links.
- Use trusted sources, such as legitimate government websites, to get up-to-date and fact-based information about COVID-19 (e.g. https://canada.ca/coronovirus).
- Do not respond to solicitations for personal or financial information.
- Install anti-virus software and update it regularly.
- Block pop-up advertisements.
- Use protected domain name system (DNS) services, such as **Canadian Shield**, that actively block known-malicious websites when you try to connect to them.

Need help or have questions? Want to find out more?
Visit the Cyber Centre website at **cyber.gc.ca**

AWARENESS SERIES