CYBER LIABILITY

How to protect yourself from COVID-19 technology scams

VICTOR

During these unprecedented times, millions of Canadians are practicing physical (social) distancing and working from home. These practices are currently the "new normal" in an effort to keep safe from COVID-19.

However, in working from home, we have become more vulnerable to COVID-19 technology scams. This pandemic has created a perfect environment for cyberscammers and cybercriminals who are looking to take advantage of our emotions (fear, concern, sympathy) for their own personal or monetary gain. Whether we are on our computers, laptops, tablets or mobile phones, we need to be on our guard.

Here are five examples of COVID-19 technology scams that you could encounter along with tips on ways to protect yourself from these scams before they occur.

Phishing Email

Scam 1

You receive an email with the subject heading: "COVID-19 update" and/or "urgent" with a link that directs you to a supposed Microsoft login page, which then prompts you to sign in to access critical information. This is a phishing email scam. The scammer wants to harvest your password and steal your money and identity. Such a scam can appear like it is coming from a recognized public health authority (i.e., Health Canada), government office (i.e., Government of Canada), or even from a colleague, friend or family member.

Tip

Important information that is sent by email in the form of only an attachment and has little or no message in the body of the email is likely a scam. If a public health organization wants you to be aware of important COVID-19 information, they will simply tell you in the body of the email or send you a letter by regular mail.

Do not "click" on a link without first ensuring it is a valid address. Scammers are more and more sophisticated and can create convincing emails that trick us into taking action. Be wary of any emails or texts that you were not expecting to receive, especially those containing links and attachments from unknown or suspicious senders. If you are unsure if the email or text was sent by an individual or known company, contact that individual or company directly to verify that the message is real.

Hacker

Scam 2

You browse the Internet while on your company's network and visit a non-recognized website supposedly containing COVID-19 information. You click on a link to this information, which then causes your company network to be infected with a ransomware virus—ultimately making your company's network and data inaccessible. The virus also causes your company network and systems to crash. Now, no one at your company is able to access their computer and systems and you are faced with ransom demands.

Tip

Be careful when surfing the Internet and ensure that websites are legitimate and trusted sources. Pay attention to the domain name. Scammers may mimic known companies with small changes to the company's official name (i.e., Ontari00.com) to trick you. So double check the website address bar to ensure accuracy first before visiting a website. Also, before you enter any private information, ensure the website address is secure and uses encryption. You can do this by checking that the URL starts with "https" (and ends with "s") versus unsecured websites, which start with "http" (which is unsecure). Never enter personal information on websites that are unsecured. Some browsers such as Google, Mozilla or Internet Explorer, may warn you of suspicious or unsecured websites. Look for grammar or spelling errors, which could be clues that a website was created quickly and is fraudulent. Legitimate companies have professional websites with grammatically sound content.

To mitigate potential attacks to your computer network, also ensure you have intrusion detection, anti-virus and anti-theft software in place and practice regular backup protocols. Only use a secure Wi-Fi with security protection software in place. Don't use open or publicly accessible Wi-Fi when working on your laptop or any other technology device.

Scam 3

You receive a text message on your mobile phone from what appears to be an emergency response COVID-19 support agency purporting to have sent you relief funds to assist you during this financial crisis. This is a texting scam called “smishing.”

Tip

Prime Minister Justin Trudeau issued a warning about texting scams that attempt to lure unsuspecting Canadians with messages about COVID-19 support (see CBC news: “Trudeau warns of COVID-19 text scam exploiting new emergency benefit program”). Protect yourself, and be wary of text messages from unknown or suspicious senders. In fact, don’t click on any link unless you have a reasonable basis to trust it, or it is a well-known website of an established organization (i.e., Government of Canada, World Health Organization, etc.).

If you are unsure if the website you are visiting is linked to an established or well-recognized organization, conduct research. Copy the link or website address of the organization in question directly into your web browser to ensure it is legitimate. If you were not expecting the text message, it is most likely not real and is an attempt to infect your mobile phone or device with a virus—again making your phone or device inaccessible. The text message could also be an attempt to access unauthorized sensitive information. Don’t reply to the text message and delete it immediately.

Scam 4

You receive a call on your phone, supposedly from your local municipal government soliciting donations to help combat the COVID-19 crisis. As a business, you may also get calls from scammers trying to exploit your vulnerability due to the financial fallout of the crisis by offering you first aid supplies or a bailout loan.

Tip

This is a form of social engineering fraud or scam called “vishing“ and it is a fraud tactic that tricks individuals into revealing financial or personal information. In fact, this occurred when fraudsters impersonated City of Brandon employees seeking donations (see CBC news article: “Fraudsters pretending to represent city staff in COVID-19 phone scam: Brandon police”). Do not reveal any personal or financial information to unsolicited callers. Hang up and call the organization or charity directly to verify the validity of the call before providing any information. Taking this extra verification step will help to protect you from financial loss.

In addition, ensure your employees are aware of these scams so they can avoid them. If you’ve fallen victim to such a scam, however, contact the Canadian Anti-Fraud Centre or your local police. If you have a cyber liability policy in place, report this phone scam to your insurance company.

Man-in-the-Middle

Scam 5

Due to the COVID-19 crisis, you are now working from home and decide to respond to pressing client matters using your personal email in order to save time. Since your personal email is not encrypted, a hacker is able to access your emails and becomes privy to sensitive and confidential information. The hacker is then able to use this information to perpetrate identity theft against your clients. As a result, you are faced with a potential third party liability claim. Not only that, but your insurance company will not pay your claim as you were not using your company's secure network while working.

Tip

Only use secure corporate protected networks when working from home. Avoid using personal emails as they are outside your information technology department's control, without the same stringent security protocols. Companies will customarily use VPNs, Two Factor Authentication (2FA) and/or Multi Factor Authentication (MFA) alongside additional security in order to access their networks securely.

Personal emails may not only expose you to "man-in-the-middle" scammers, but could unknowingly expose sensitive information in your emails that may be readily accessible to untrustworthy individuals ("bad actors") and/or scammers. You may also be violating company policy by using your personal email and find yourself without insurance should a claim arise. Finally, in all circumstances, ensure that your user name and password(s) are not easy to figure out by a hacker. Update your passwords regularly and use passwords and user names that consist of a complex combination of letters, numbers and symbols. Avoid using common names and numbers (e.g., your name, birthday, 123, etc.).

Additional tips when working from home during COVID-19

- ✓ Don’t copy work-related information to personal technology devices (e.g., personal phone, home computer, personal online storage, etc.).
- ✓ Mute or shut down any digital assistants such as Alexa, Google Home, etc., since they are constantly recording nearby conversations.
- ✓ Protect your privacy while video conferencing using platforms like Zoom or Skype by making the meeting private to avoid “bad actors” from barging in. Also, limit sharing capabilities to protect sensitive information.
- ✓ Don’t let family members or friends use your company-provided equipment (e.g., laptop, mobile phone, etc.).
- ✓ Don’t use personal email, file sharing sites, social media or other systems that are not approved and secured by your company.
- ✓ Conduct regular security audits and tests on your computer and systems.
- ✓ Implement a plan in case of a technology scam or cyberattack.
- ✓ If you own or lead a business, make sure your company has cyber liability coverage in place.

For more information, visit victorinsurance.ca or view the following additional resources:

- Victor (formerly ENCON) Cyber Insurance
- COVID-19 Resources
- Infographic: "Typical day in the life of a business owner"
- Animated video: "A day in the life of a business owner in a cyberworld"

#COVID-19 #TechnologyScams #TheThreatIsReal #StaySafe

This publication has been prepared for general information use. It should not be relied upon as legal advice or legal opinion with respect to any specific factual circumstances. Program availability and coverage are subject to individual underwriting criteria.