Cybersecurity and the Russian invasion of Ukraine

On February 24, 2022, Russian began its invasion of Ukraine. The resulting sanctions have had global impacts, affecting consumers and businesses both in Russia and abroad, most notably for consumers in terms of energy prices. This month's newsletter will highlight some of the main concerns many of us have regarding cybersecurity.

Recent cybersecurity concerns Q&A

What cyber threats are happening due to the Ukraine — Russia war?

There are no credible threats to USA or Canada. Still both governments have reported seeing "preparatory" Russian hacking activity toward businesses but have not concluded whether or not such an attack will occur. Any response from Russia towards these countries would likely be engagement in cyberattacks on critical infrastructure and the businesses supporting said infrastructure. An initial access attack would likely come in a Spearphishing Attachment, Supply Chain Compromise, or Drive-by Compromise.

How can people be protected from cyberattacks related to this issue?

Continue to follow cybersecurity best practices. That includes being cautious of suspicious emails sent by odd senders and domains and thinking before clicking on and downloading anything.

What does all of this mean for you?

Now is the time to put cybersecurity awareness at the forefront of your mind. Update your passwords, and you might even want to look into getting a **password manager** if you don't already have one. Setting up **multi-factor authentication** on your accounts is also an excellent step to take. This adds an additional layer of security to your personal information. Take time to **check all of your devices for updates**, and some will automatically update, some you will have to manually check. Lastly, continue to **listen to your organization's security team** for any information or updates they have. They are constantly monitoring your network and evolving situations.

Where can I go to find valuable and helpful information?

Often we are inundated with a lot of information, and it can be hard to decide the best places to find the facts. We have provided a helpful resource that may be useful if you are interested in doing more research and staying on top of the ongoing situation.

https://www.cisa.gov/shields-up
Cybersecurity and Infrastructure Security Agency — Shields Up. This site is up to date with critical information about cybersecurity-related issues due to the conflict.

https://www.canada.ca/en/revenue-agency/corporate/security/protect-yourself-against-fraud.html
Slam The Scam — This page provides information on how to recognize and report a scam.

Taxpayers — don't fall for these taxing tricks!

Tax Tip: *The IRS/CRA will never:*

- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer.
- Threaten to immediately bring in local police or other law enforcement groups to have the taxpayer arrested for not paying.
- Demand that taxes be paid without giving taxpayers the opportunity to question or appeal the amount owed.
- Call unexpectedly about a tax refund.
- The CRA does not commicate by direct emails, they only send notifications by email.

Taxpayers who receive these phone calls should:

- Record the number and then hang up the phone immediately.
- Report the call to IRS/CRA and local police or other law enforcement.

If you suspect that you may be the victim of a scam or fraud or have been tricked into giving personal or financial information, contact your local police service as soon as possible.

E-TECH **www.etechcloud.ca**