Hot **off the press!**

Has there been a rise in cybersecurity related issues worldwide? This month's newsletter will touch on recent topics and advice from our cyber security professional, Simmer Principio.

A lot of cybersecurity headlines are reaching our desks lately, but does that mean we have to be on high alert? Luckily, we can continue to apply the same cybersecurity standards to protect ourselves. Here are some of the hot topics We're been seeing and tips to keep up our security habits.

Silicon Valley Bank and other bank failures

The US's biggest bank failure in decades occurred in March, putting many worldwide into a panic. Customers of Silicon Valley Bank were frantically pulling their money out, which trickled over to other banks as well. This led to a classic run on the banks.

But what does this situation have to do with cybersecurity? Simmer Principio, Cyber Security Analyst at E-Tech, has weighed in with important reminders as we watch the story unfold. "We advise that everyone stay cyber smart and remember to think before responding to or acting on any email, text message or phone call you may receive relating to the (banking crisis)."

These situations also make executives more vulnerable to Business Email Compromise (BEC) attacks. A BEC attack is a phishing attack where an attacker strikes up a typical business conversation with someone who has high-level access to financial information. They do this in hopes of obtaining money.

Simmer advises getting into the habit of speaking with someone before doing large transactions and verifying the source of the request. Today, many people shift thousands of dollars per month through Zelle, Cash App and other digital financial transaction mechanisms with little thought.

ChatGPT and other AI tools

ChatGPT and other AI writing tools (such as Jasper.ai and Copy.ai) use artificial intelligence algorithms to assist humans in writing and creating. These tools can be used in various ways; however, cybersecurity insiders worry that hackers will be the ones getting the most use out of AI.

Hackers are always trying to get ahead of the game, and cybersecurity experts are trying to keep up. Hackers use AI tools to help build more realistic phishing attacks, write dangerous code and find ways to access organizations' secured systems.

But even with access to AI tools, hackers still have their work cut out for them.

Simmer Principio suggests that businesses and organizations must follow a multi-faceted cybersecurity approach. The basics are still essential and effective in stopping attacks. Creating a strong, unique password is the first step in securing data, followed by using multi-factor authentication tools and staying alert to the emails in your inbox.

Tax season doesn't have to be scam season

CRA & IRS Tax Tip:
The CRA or IRS will never:

- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer. Generally, the CRA or IRS will first mail a notice of assessment or bill to taxpayers who owe taxes.
- 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.

Cybersecurity roles — Incident responder

Have you ever wondered what your friendly cybersecurity team is up to? We'll share a cybersecurity job role each month to give you an inside look!

Incident Responder
An incident responder's job is to quickly use their available forensic tools to address cybersecurity incidents. With the rise in cybercrime and a gap in the cybersecurity job field, the incident responder role is critical and in high demand. Typical incidents a responder must be prepared for include phishing attacks, malware and internet-facing vulnerabilities.Incident responders need to respond to the incident and be part of the discussion on how to prevent attacks, mitigate attacks, recover data and brief the necessary team members on lessons learned for the next attack. Incident response plays a critical role in securing organizations.