For the love of money

As tax season approaches, we should be aware of potential scams that could impact us. Filing taxes or doing any government task can be a stressful experience, and it can also be the perfect opportunity for scammers to take advantage of unsuspecting citizens. Phishing emails and fraudulent payment demands tend to increase during this time, and with a large amount of money being moved around, hackers know there's something out there for them. Brush up on their tactics and continue to stay safe this tax season.

CRA/IRS Impersonation tactics

Phishing and smishing messages

Scammers will send phishing emails or text messages (smishing) that claim to be from the CRA/IRS. These messages may state that you have an unpaid balance, need to update your taxpayer information immediately or need to collect a refund. These messages often contain links. The link leads you to a copycat site where you enter information such as name, date of birth, and ID number. The attacker can then use that information to steal your identity.

Social engineering scare tactics

Scammers play on your fears by dropping lines like "Pay now or go to jail!" It's the classic fear factor. They know that when fear kicks in, people often act without thinking.

- **Urgency:** Hackers love to create a sense of urgency. If a message pushes you to act immediately or threatens serious consequences, slow down. Scammers thrive on quick reactions.
- **Unexpected requests:** Be cautious of unexpected emails or texts, especially those asking for personal or financial information. Legitimate organizations won't randomly ask you to provide sensitive details.
- **Check the source:** If something feels off, double-check the sender. Hover over links (don't click them!) to see where the link will take you. Hackers use link masking to hide the actual URL of the link. Most browsers will display the true link when you hover the mouse pointer over it.

How to protect yourself

By following these two simple rules, you can safeguard yourself against tax scams.

1. **Don't trust emails or texts claiming to be from the CRA/IRS:** The CRA/IRS does not communicate through email or text messages for personal or financial information. If you receive a message like this, delete it immediately.
2. **Bookmark the official CRA/IRS website:** When working on your taxes, always access the official CRA/IRS website through a secure bookmark. Refrain from clicking on any links in unsolicited messages, as they could lead to fake login pages designed to steal your personal data.

More than CRA/IRS impersonation emails

CRA/IRS impersonanation is a major way hackers try to steal your data, but it's not the only way. This time of year, online tax filing companies are upping their marketing game. Phishy tax related emails are landing in our inbox daily. Avoid clicking links in any tax service-related email offering discounts and "too good to be true" deals. It is always best to go directly to the offical website of your choosing to complete your tasks.

Protecting your heart and wallet

Love is in the air, but so are scams, especially the number one Valentine's Day trick: the romance scam. As we approach Valentine's Day, be on the lookout for online charmers who may not have your heart in mind. These scammers initiate online connections, showering you with charm to establish a quick emotional bond.

Then the scammer pretends to be in financial trouble and asks you to send money. They encourage you to take out loans and max out credit cards to "help them out."

Keep an eye out for red flags! Romance scammers aren't what they appear to be, so they'll find excuses not to visit, call or appear on video chat. It's better to be safe than sorry, so don't buy gifts for anyone you haven't met.