What to do about unsolicited texts, emails and calls

As our devices get smarter, so do scammers.

(NC) In the age of buzzing phones and overflowing inboxes, staying digitally safe has become part of modern living. But as our devices get smarter, so do scammers. Here are a few simple ways to stay one step ahead:

Spot the red flags

If your bank, the government, or a well-known company suddenly reaches out with urgent language, like "act now" or "your account will be suspended", pause before you panic. Scammers thrive on pressure and fear. Requests for highly sensitive information like PINs, passwords or card numbers, are big red flags. No legitimate institution will reach out and ask for these details from you.

What to do in the moment

If a message or call feels wrong, trust your gut. Hang up immediately or simply ignore it. There is no need to engage. Whatever you do, don't click suspicious links or respond with personal details.

When in doubt, go straight to the source, because scammers can make a phone call appear legitimate, even the caller ID. You can keep yourself safe by only calling the official number printed on your bank card or listed on the organization's website, not the one you received a call from. A quick verification can save you from a world of hassle.

If you do spot something suspicious, report it to your bank.

Know what you're liable for

Federally regulated financial institutions can't hold you liable for unauthorized debit card transactions, while credit card issuers can hold you liable for a maximum of $50. However, if you provide your banking information to anyone, including a spouse, a family member or someone claiming to be a law enforcement officer or bank employee, you lose that protection.

Scams involving other modes of payment, such as electronic transfers, are not protected through any federal legislation. It's important to be vigilant and keep your PINs and passwords to yourself.

Protecting yourself from fraud and scams can be empowering. By recognizing the signs and knowing how to respond, you can navigate today's complex digital landscape with more confidence.

Learn more about your rights, how to protect yourself and what steps to take if you suspect a scammer is trying to target you at canada.ca/money.

IDENTITY THEFT

Where are you most vulnerable?

Identity theft is on the rise, and so is the damage that criminals can do with that information if it's compromised.

(NC) Here are some of their favourite places to get access to sensitive information, and where you can consider shoring up your defences:

1. Public or unsecured Wi-Fi networks. Hackers can intercept sensitive information as it moves to and from the cloud. Avoid logging into financial accounts or accounts with personally identifiable information on these networks.

2. Your tax return. Many people don't think of their taxes as a security risk, but the forms contain a great deal of personal information. With most people now filing online, tax forms are a prime target for phishing attacks and other scams designed to get you to hand over personal information to fraudsters. Using a virtual private network (VPN) can help. Services like Telus Online Security's secure VPN create a private, encrypted connection so you can file your taxes online without hackers interfering.

3. Your recycling bin. Scammers don't just use high-tech methods. They can also gain personal information by going through discarded documents. Always destroy anything sensitive before discarding it.

4. Unsafe links. One of fraudsters favourite ways to get your identifying information is by getting you to give it to them. They can make fake login pages for banks, tax services and other sensitive accounts. When you log in, the fraudster gets your username and password. Always be skeptical of unexpected communications that have links to click.

When it comes to identity theft, prevention is the best cure. It's important to stay vigilant and treat any unexpected communication with caution. If you're ever unsure, you can verify the communication by reaching out to your bank via its main login page.

The threats to your identity are real, but you have options to stay protected. Learn how you can better protect your identity and finances during tax season and beyond at telus.com/onlinesecurity.