Digital Self-Defence

How to protect yourself and your loved ones from financial fraud

Over the years, scammers have become increasingly successful at stealing money from unsuspecting individuals. Last year, nearly $160 million was stolen from individuals and businesses in Canada, up from $98 million in 2019, according to the Canadian Anti-Fraud Centre. With more people now staying closer to home, that number is likely to rise.

While everyone is at risk of falling for a scam—who hasn't gotten a call from the "Canada Revenue Agency" demanding a late payment—it's Canadians aged 60 to 79 who tend to get hit most. The Canadian Competition Bureau found that seniors lost $94 million to various financial scams between 2014 and 2017, accounting for about 23% of the $405 million lost during that time period.

With threat actors becoming ever more sophisticated, it's important to know how to protect yourself and your loved ones from falling prey to the ever-growing litany of scams and hacks.

Know the threats

When it comes to protection, knowledge is power. Understanding where threats exist and what they look like can help you spot them—especially on behalf of senior family members who may not be as digitally astute. Here are some of the main ways hackers steal sensitive information.

Phishing

This has been, and continues to be, the most popular online attack. A scammer reaches out via text, email, or phone posing as a reputable company the victim might already have an account with, such as a bank or an ecommerce store, asking them to update their account. The victim clicks on a link that takes them to a page that looks like the actual company's website—in reality the URL is slightly off what it should be—where they then proceed to share personal information that ultimately goes to the hacker.

Social engineering

Social engineering is another strategy that fraudsters are using to get unsuspecting consumers into handing over personal information. While phishing would fall into this category—the term relates to manipulating people into divulging confidential data—many hackers are using social media for this purpose, too. For instance, threat actors are creating fake accounts on Facebook, impersonating that person in a chat and asking their "friend" to hand over personal information. Others are sending notes via Instagram or Facebook asking you to check out a link. When the link's clicked, malware gets installed on your device, allowing the attacker complete access to your personal information.

Digital security

The increased use of technology in our everyday activities—both financial and not—has created a perfect opportunity for cybercriminals to prey on unsuspecting consumers. Many of the smart home devices people now use, whether it's a voice-activated speaker or a digital thermostat, can be easily hacked. After breaking into the device, the threat actor can steal personal information from that person's home network. Mobile phones and computers that don't get regular security updates are vulnerable to attack, too.

PINs and passwords

An ongoing concern is password security. The number of websites and accounts that need a password these days is overwhelming, to say the least. That said, there are no shortcuts to creating secure passwords. If you're using the same one everywhere, or using something like 123456—the most common password of 2020—and the hacker finds out, then all of your accounts become suddenly accessible.

Public networks

Another way you may unwittingly cause your information to be compromised is by using public Wi-Fi—an unsecured Internet connection that people often connect to at restaurants, parks, and stores. Hackers can easily break into these networks and then steal information off of your devices.

How to keep you and your loved ones safe

Whether you're concerned about your own devices and information, or you're looking out for loved ones, there are several ways to fortify your security. The first step, especially with older family members, is to have a conversation about what financial fraud might look like. If they notice unusual activity in their accounts or if they're suddenly getting emails from their bank, they should let you know. Encourage them to reach out to you or someone else they trust if they're unsure about a financial request.

A good rule of thumb is to never give out any personal information in an email, by text, or on the phone, unless it's someone you know and trust. Many companies and governmental bodies will let their customers know the ways in which they will be contacted, so they know not to fall for scams that come through other means of communication. The Canada Revenue Agency, for example, will never ask for information via text or email. Before clicking on anything, check the web address of that link (by hovering your mouse over the link) to see if it looks legitimate.

When it comes to creating passwords, consider using a password manager. These programs, which can be integrated into your web browser and also come in downloadable apps, keep track of your current passwords and suggest more complex ones when you're prompted to create a new password. A password manager can also help you to enable two-factor authentication, which forces you to present two pieces of information—usually a password and a code sent via text—before getting access to an account or website.

Last but not least, update your device's security patches. Every piece of technology, whether it's your tablet, phone, computer, or smart system, needs security updates from time to time. You'll usually get prompted by your device when it's time to do so. When you do update, contact any loved ones to remind them to do the same with their devices as well.

With hackers becoming more savvy, there's no time like the present to fix any gaps in your defences to ensure your finances, and those of your loved ones, are protected.