Canaccord Genuity
Wealth Management

Helping Seniors with Cybersecurity

Seniors comprise a growing share of our population: Canadians are living longer than ever and, at the same time, having fewer children than decades ago. As the number of seniors continues to grow, they have increasingly become a target for fraud. Alongside our greater reliance on technology, the habits of a typical senior citizen can often make them vulnerable to fraudsters, especially through mobile phones or internet channels. According to a recent poll, while 42 percent of seniors own a smart phone, only 26 percent feel "very confident" when using computers and mobile devices.[1] Complicating matters is that fraudsters continue to improve the sophistication with which they target individuals, developing new and evolving scams. Yet, the outcome is most often the same: a significant amount of money is lost by victims to these fraudulent activities. According to the latest statistics, senior citizens lose more than $20 million to fraud each year.[2]

How can we protect seniors from fraud? As a starting point, having conversations with elderly loved ones, as well as building a system of checks and balances to help protect them may be good ways to help safeguard their well-being. Here are some suggestions on where to begin:

1. **Have conversations with seniors to educate them about scams.** Talk regularly with seniors. Discussing the different types of fraud and evolving scams can help to educate loved ones about how easy it may be to become a victim of fraud. Keep in mind that with our increasing reliance on mobile devices, it may be harder for a senior to spot fraud on a smart phone than on a device such as a desktop computer due to the mobile's smaller screen and simplified user experience. Often, people can be less inclined to phones. As you engage in these discussions, it may be helpful to talk about the ways in which an individual may be targeted. Here are just a handful of situations:

a. **Phishing** – Phishing uses email or texts to trick a recipient into revealing sensitive personal information, such as birthdate, address, social insurance number and financial information, such as credit card or bank account numbers. This information is often used in identity theft, when a scammer takes on the victim's identity to commit fraud. Often, the fraudster does this by masquerading as others through an email, such as impersonating a financial services company or retailer. However, increasingly "voice phishing," or "vishing," is being conducted over the phone. For example, some vishing calls make false claims of fraudulent activity on a victim's bank account or credit card to direct a victim to enter sensitive information to resolve a supposed situation.

b. **Social media scams** – Victims can be convinced to enter an online relationship through email messages or fabricated profiles on social media or dating sites. Eventually the scammer asks the victim to send funds for things such as money for travel, a medical emergency or family assistance, or for other activities such as a business venture or investment. Romance scams commonly occur over a longer time period to build trust with victims. Some have even led to in-person meetings before the scammer solicits financial assistance.

c. **Government imposter scams** – Individuals claiming to be from the Canada Revenue Agency call victims and state that there is a compromised social insurance number, an outstanding case against the individual or that taxes or unpaid balances are owed. Oftentimes, the victim will be threatened with arrest or a fine if they do not help to resolve the situation through immediate payment.

d. **Bank investigator scams** – Callers claim to be an employee of a financial institution and ask for the individual to verify their credit card details as part of an investigation of fraudulent activity on their account. Once this information is provided, the victim's credit card is compromised.

2. Teach good digital and telephone "hygiene."

Teaching seniors to practice good habits, both online and on their phones, may help to provide an element of protection. As a starting point, here are some basic practices that can help to improve security:

a. **Password and account security practices** – Passwords for online accounts should be difficult to guess and consist of letters, numbers and symbols. Passwords should also be changed on a regular basis to avoid being compromised. It is never advisable to reuse the same login/password across multiple sites. However, with dozens of logins and complex passwords to manage, remembering these details may be difficult for many seniors. To address this situation, the use of a password manager may help to generate, store, encrypt and auto-fill passwords, with the senior needing to only remember one password. Some sites allow the user to enable multi-factor authentication, which requires proof of identity beyond a userID/password combination, providing an additional layer of security. Enabling this feature may help to better protect loved ones.

b. **Never share personal information** – Remind seniors that every time a user clicks on a new website or answers a seemingly innocuous quiz or question online, their data is being collected. Information broadcast on websites or social media can easily be accessed by unscrupulous individuals. As such, seniors should be reminded to never disclose sensitive personal information and always enable privacy settings on social media sites.

c. **Validate the source** – "Spoofing," when someone pretends to be someone they aren't, has become more sophisticated with individuals being targeted not just by email, but also via phone calls and texts. However, there may be subtle indications that a source could be a fake: an email/text doesn't address the individual directly ("dear customer") or contains spelling or grammar errors. If the senior answers a questionable phone call, remind them that they shouldn't be afraid to ask for identification and call the (supposed) source back using the general information number listed on an official website. A phone call inquiry using a general number on a company website can help to verify if an email or text is credible.

If a senior believes that they are being targeted with a scam or potential fraud, consider suggesting ways to safely respond:

a. **Phone calls** – Hang up immediately. Block the number so that they are unable to call again.

b. **Email** – Do not open unknown attachments or click on links when uncertain of their origin. Never reply to suspicious emails. Mark the email as spam or junk. When in doubt, call the organization directly using the phone number posted on a general website. Remember that reputable institutions will never ask to verify account information or sensitive personal data online.

c. **Text** – Block the incoming number. Never reply or click on links within the text.

d. **Social media** – Report the violation to the social media site. Block the user.

3. **Consider preventative measures to help limit the exposure.** There may be actions that can be taken in advance to limit a senior's exposure to fraudulent activity.

   a. **Block unwanted calls on mobile phones** – Many smartphone devices allow the owner to silence unknown callers. There may also be third-party applications that can block robocalls or unwelcome callers.

   b. **Keep an inventory of devices** – By creating a list of all of the devices owned by the individual, it may be easier to understand potential areas of compromise. For instance, computers and smart phones may have security breaches and can be prime targets for hackers if the software is not up to date.

   c. **Dispose of unused hardware** – Consider disposing of devices that aren't used regularly and ensure that any information stored on those devices has been permanently deleted before disposal.

4. **Continue to advocate by being on guard and helping to monitor activities.** Watch for signs of fraud that may help to uncover potential abuse. Remember, in some cases, fraudsters can target certain individuals on a recurring basis. Keep an eye on the spending activity of the senior by reviewing bank and credit card statements where possible. There may be tools that can help to monitor financial transactions, such as certain personal finance applications, to identify unusual financial activity.

If you live too far away to check in regularly, consider the support of others, such as a care manager or independent agency to oversee caregiving. If you suspect fraud, report it to the relevant financial institution, the local police and the Canadian Anti-Fraud Centre.

WE ARE HERE TO ASSIST

If we can act as an impartial third party to support family conversations around fraud or provide resources to help seniors in managing their finances, please let us know. For more information, please consult the Government of Canada website: https://www.ic.gc.ca/eic/site/Oca-bc.nsf/eng/ca03025.html. This website contains resources to support these conversations, including a list of red flags that may be useful for seniors to identify areas to watch for when protecting against fraud: https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04333.html#sec14. The Canadian Anti-Fraud Centre also has resources that may be of use: https://www.antifraudcentre-centreantifraude.ca/.

1.https://www.pewresearch.org/internet/2017/05/17/technology-use-among-seniors/ 2. https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04334.html

CANACCORD GENUITY WEALTH MANAGEMENT IS A DIVISION OF CANACCORD GENUITY CORP., MEMBER-CANADIAN INVESTOR PROTECTION FUND AND THE INVESTMENT INDUSTRY REGULATORY ORGANIZATION OF CANADA

This document is for general information only, not intended to provide tax, legal or financial advice, and under no circumstances should be interpreted as a solicitation to act as a securities broker or dealer in any jurisdiction. All views are intended for general circulation only and do not have any regard to the specific investment objectives, financial situation or general needs of any particular person, organization or institution. All investors should consult with a qualified investment advisor or tax professional before making any investment decisions.

Tax & Estate advice offered through Canaccord Genuity Wealth and Estate Planning Services.