Smart Advisor Tips Series

FRAUD PREVENTION

March is fraud prevention month, and we want to keep you updated on how to protect yourself from fraud. Our members' safety is our top priority and we want to do everything we can to help prevent you from fraud and scams. Check out our top ten tips for protecting yourself and your finances.

1 Don't Get Caught by a Phish: If you get a voicemail or email from your bank or credit card company that requests you call back, only call the number listed on the back of your card. Never respond directly to the email or call the contact number provided in the message. Chances are, the email or voicemail is a phishing scam and your bank or credit card company will want to know about it. And if you receive a phone call from the government saying you are behind in your taxes and requests that you send money urgently, hang up and call the Canada Revenue Agency directly at 1-800-267-2384. They will investigate the matter on your behalf.

2 Stay Secure while Shopping: There are two very simple signs that you're secure while shopping online. One is the "padlock" icon located at the top of your browser window, and the other is "https" in the address bar. These confirm that the page you are on is secure and that your data will be encrypted.

3 Keep Checking: Check your monthly financial and credit card statements regularly. There are scams that involve frequent transactions being made for only $1 here and there; so small you may not notice them on your balance. Go through your statements and check them closely and carefully for transactions and payments that are out of the ordinary and call your financial institution or credit card provider right away if you spot any.

4 Charity Donations: Donating to charity is great, and we should all be doing our part to help others in need. But never donate to an alleged charity in response to a telephone call; it is impossible to verify the legitimacy of the so-called charity over the phone. Ask the organization to mail an information package, and remember to always check whether or not a charity is registered by calling the Canada Revenue Agency at 1-800-267-2384 or checking its website at www.cra-arc.gc.ca.

5 Password Protection: Avoid obvious passwords like birthdays, addresses, or phone numbers – they are not only easy to guess, but also easy to get with simple searches. Most sites recommend (or even require) a minimum of eight characters and a mix of numb3er5 and le3tt3r5. If your password is ever compromised, make sure to change all accounts that use that password to avoid further privacy risks.

6 Pins are Private: The only person who should know your PIN is you. Never disclose your PIN with anyone, including financial institution employees, law enforcement agencies, or even friends and family members. Do not write down your PIN or store it electronically, instead pick something that is easy for you to remember, but avoid birthdays, addresses, social insurance numbers, and phone numbers. If you suspect your PIN has been compromised, change it immediately at one of our branches or at an ATM with that functionality.

7 It's Probably Too Good to be True: Unfortunately, the world is full of scams, hype, and tricks. If you get a call or email saying you've won a trip, an iPhone, or a large sum of money, with a sense of urgency (Act now! Offer ending soon!), proceed with caution. Chances are it's probably a scam. Usually getting something for nothing comes with a large risk, and this type of fraud can be very dangerous. If you're ever unsure, call us and tell us about the email or call you've received. We can likely point you in the right direction. You can also report fraud to the Canadian Anti-Fraud Centre - http://www.antifraudcentre-centreantifraude.ca/index-eng.htm

8 Work-At-Home "Dream Jobs": Would you like to earn a lot of money in the comfort of your own home and generate thousands in income in your spare time? Ads offering work-at-home opportunities can be found everywhere, from websites to community bulletin boards. It seems like perfect solution for the unemployed or retirees who want to bring in a few extra dollars. But, there's a catch – most of these work-at-home opportunities are scams cleverly designed to leave you with less money than when you began. Most ask that you pay upfront for training and materials and then send useless manuals and instructions that are irrelevant to the job. Also, these scams will ask for your Social Insurance Number, which can be very dangerous. Before accepting an online work-at-home position, thoroughly research the company and be skeptical if you are asked to pay money upfront. And if the offer seems too good to be true, walk away.

9 Keep Your Information Private: Don't disclose personal information about your finances, bank accounts, credit cards, social insurance, and driver's licence numbers to any business that can't prove it's legitimacy. Don't be afraid to request further documentation from the caller so you can verify the validity of the company. And don't be afraid to hang up the phone, delete the email, or close your Internet connection if you don't feel safe and secure.

10 Shred, shred, shred: Shred unwanted personal information, such as bank statements, credit card bills, unwanted receipts, cheques, pre-approved credit applications, and old tax returns.