Cybersecurity Checklist: For Seniors

With the rise of cyber crime around the globe, it's never been more important to ensure you educate yourself and your family on how to stay cyber safe. **This checklist will help you learn how to protect yourself, your family and your digital assets.**

Password Protection

A common way scammers get access to your information or break into your online accounts is by guessing your password. Many of us like to use simple, easy to remember passwords such as the word "password" or the digits "1234".

What you can do:
❑ Never share your passwords with anyone.
❑ Don't use your Online Banking password for anything else. While it's best not to re-use any passwords at any time, it's especially important to use extra caution when it comes to sensitive information such as your bank account.
❑ The longer, the better. Experts suggest creating passwords that are at least 12 characters long, ideally 16.
❑ Reset your passwords regularly.
❑ Use multi-factor authentication. While passwords are more secure than no protection, your data is far safer if you combine a password with multi-factor authentication (MFA).

Banking Safely Online

Being vigilant about your online security is essential to guarding against cyber criminals. And, while RBC is committed to keeping your financial information safe and secure, there are simple steps you can take to proactively protect yourself.

What you can do:
❑ Set Auto-deposit for e-transfers. This service eliminates the need for a security question and answer in every transaction lessening the risk that someone unintended could intercept the funds.
❑ Enable 2-Step Verification on your RBC banking app.
❑ Review your bank account statements regularly; if you see unknown purchases, that could be a sign that your identity has been stolen.
❑ Immediately report lost or stolen credit or debit cards.
❑ Never provide confidential information or sign-in IDs or passwords when responding to an unsolicited email, text message or a phone call.
❑ Avoid acting out of a sense of urgency or emotion.
❑ Turn on Account Alerts to monitor unusual transaction activity.

Email Scams

Email scams are very common online scams where an email is sent, attempting to trick the recipient into giving up personal, business or financial information. Typically, a phishing email will explain an urgent situation ("Your Bank Account has been suspended") with a time limit to act ("You have 24 hours to verify your account") and a link to click where you'll be asked to enter your confidential information ("to fix the "problem"). The fraudster then gets access to your passwords, account numbers, client base, or even your computer systems. Remember, legitimate organizations will never ask for information to be sent in this manner.

What you can do:
❑ Never write personal information in an email, this includes account numbers, birthdays, social insurance numbers and other sensitive data.

❑ Don't open attachments or click on links if you don't know the source. If you receive an email with a suspicious attachment, simply ignore the email and delete it.

❑ Keep your email address safe. Your email address is personal — avoid posting it on public forums or entering it on sites you don't trust. And just because someone at a store asks for it doesn't mean you have to give it out.

Phone and Text Message Scams

Have you ever received a call or text message from a number you don't recognize asking you to do something, like provide your private or financial information? It could be a smishing scam.

What you can do:

❑ Don't pick up if you don't recognize the phone number.

❑ Never give away personal information to someone you don't know.

❑ Beware of grandchild impersonation. This is one of the most prevalent scams around today and has tricked older Canadians out of nearly $10 million last year. If anyone calls claiming to be your grandchild — especially if they're asking you for money, a credit card or a gift card to help with an emergency — don't fall for it. Hang up and call your family directly.

❑ Don't click on links sent by numbers you don't recognize.

❑ Avoid acting out of a sense of urgency or emotion.

❑ If the number isn't legitimate, delete the text message from your phone.

Phone Settings

Smartphones are smart, but they're not always secure. When it comes to keeping your smartphone secure, there are two things to consider: protecting the device from loss or theft and protecting the data you've stored on it.

What you can do:

❑ Turn off Bluetooth when you're not using it.

❑ Don't install - or make sure you uninstall - those nosey apps or any apps you're no longer using.

❑ Turn on the "Find my Mobile" tool so you can locate missing devices and protect data.

❑ Enable multi-factor authentication for the sites you visit.

Fake websites

Scammers set up fake retailer websites that look like real online retail stores in these cases. The thing is, you won't receive the goods you paid for.

What you can do:

❑ Buy from companies or individuals you know by reputation or from past experience.

❑ Make sure you're still on a reputable website when you go to check out and haven't been redirected to a new page.

❑ Be more cautious with sellers located far away or that don't have many reviews.

❑ Regularly check your credit card statements for frequent or unknown charges.

Report Fraud

If you believe your confidential information may have been stolen or obtained by a fraudulent party either online, by telephone or through any other means, call us immediately.

For general inquiries or comments regarding Privacy and Security, please also call us.
1-800-769-2511 (telephone banking)
1-800-769-2555 (online/mobile banking)
1-800-769-2512 (credit cards)
1-800-769-2535 (RBC Express online banking Client Support Centre)