Green Private Wealth of Harbourfront Wealth Management is a discretionary portfolio management group focused on helping investors achieve their goals through building wealth and managing their risks.

Cyber Security

We wanted to send an email to address concerns we have had recently over Cyber Security to keep our clients safe. Please read through and if you have any questions reach out.

Hackers, scammers, and fraudsters have one thing in common with each other; their full-time job.

That job is to get your personal information. They personalize scams to victims by referencing familiar things that people can relate to. Once they have your access that's when the "fun" begins for them the headache starts for you.

You may not know you are giving out to your sensitive information such as login credentials, credit card information, or bank account details just by simply clicking on an attachment or opening a link on what looks like a legitimate website.

To avoid these phishing schemes please familiarize yourself and use extra caution, if it's too good to be true or offering free money – it's a scam. Please remember the following:

- We will not ask you to provide sensitive personal information (like user names, passwords, bank account numbers or SIN) over email.
- Do not try to open any shared document that you're not expecting to receive from us.
- Do not click on links or attachments from us that you do not recognize or are not expecting. Be especially wary of .zip or other compressed or executable file types.
- If you get an email saying your account is locked out, go directly to the website, and try. Do not use the link that was sent.

Best Practice

- Use strong and unique passwords for each account: Create complex passwords that are difficult to guess and avoid using the same password for multiple accounts.
- To determine if the sender is legitimate hover over the from name and the email address will pop up. Legitimate emails from us will have the @greenprivatewealth.com domain in it. If it is anything different, then it is a scam, and you should call us.
- Ensure you add our email addresses to your safe sender list. This will allow your email program to flag phishing emails using our names.

Canada Revenue Agency (CRA)

The CRA is moving more and more with online communication. The CRA will notify you via email regarding any mail communications available to you, the most recent one being your Notice of Assessment (NOA) being available and instructing you to log into My CRA Account.

CRA emails will not ask you to click any links, ask for personal information, request payment by a prepaid credit card or gift card, use aggressive language or tone and they will not threaten to call the police in any emails. Safe and secured CRA emails will direct the user to log into their "my account" for any communications. These emails are not a scam.

Common Scams and Frauds Examples

- **Investment Opportunities** – This will usually come from someone else whose account has been scammed that you know and trust. They are now trying to scam you as well. Trying to trick you into investing money into stocks that are fake and made up.
- **Grandparent Scam** – A person calling pretending to be your grandchild and saying that they are in trouble with the police and need bail money. They will say they do not want you to tell the parents, they are a little sick right now that's why they sound different, will request small amount of money at first then continue to ask for more. You may even speak to a "police officer."
- **Social Media platforms** – with the rise of new technology, scams are also becoming more advanced. If you are selling a product online and someone gives you a cheque and makes a "mistake" in the amount and says "you keep the extra $50 for your trouble but if you could please cash the cheque and send me back a $100.00 – this is a fraudulent cheque and will get returned by your bank.

Types and Descriptions

- **Phishing** – In this type of attack, hackers impersonate a real company to obtain your login credentials. You may receive an e-mail asking you to verify your account details with a link that takes you to an imposter login screen that delivers your information directly to the attackers.
- **Spear Phishing** – Spear phishing is a more sophisticated phishing attack that includes customized information that makes the attacker seem like a legitimate source. They may use your name and phone number in the e-mail to trick you into thinking they have a connection to you, making you more likely to click a link or attachment that they provide.
- **Whaling** – Whaling is a popular ploy aimed at getting you to transfer money or send sensitive information to an attacker via email by impersonating a real company executive. Using a fake domain that appears similar to you, they look like normal emails from a high-level official of the company, typically the CEO or CFO, and ask you for sensitive information (including user names and passwords).
- **Shared Document Phishing** – You may receive an e-mail that appears to come from file-sharing sites like Dropbox or Google Drive alerting you that a document has been shared with you. The link provided in these e-mails will take you to a fake login page that mimics the real login page and will steal your account credentials.

Please never hesitate to call us in Burlington (905) 634-3975 or Woodstock at (519) 539-8212 if you have any suspected suspicion we are here to help! We would always rather you ask and make sure!

GREEN PRIVATE WEALTH
HARBOURFRONT WEALTH MANAGEMENT

112 Springbank Ave. N., Woodstock, ON N4S 7P8 (519) 539.8212
200-5045 South Service Road, Burlington, ON L7L 5Y7 (905) 634.3975

greenprivatewealth.com