Cybersecurity—strategies for staying safe online

RBC Wealth Management

Today's fraudsters are becoming more sophisticated all the time. That is why it is more important than ever to protect your personal information when corresponding online and via email.

Have a plan

If you suspect your accounts may have been breached or hacked, have a plan so you know what to do and who to contact.

1. Change your passwords immediately, and consider setting up new accounts.
2. Get your device professionally serviced and cleaned of viruses, spyware, malware or other harmful programs.
3. Request a copy of your credit bureau reports and review for anything that looks out of the ordinary. Review these reports at least once a year.
4. If you suspect your credit has been compromised, freeze applicable accounts until the matter is resolved.
5. Consider signing up for credit monitoring (fees may apply).
6. If you suspect you are a victim of fraud or theft, contact the authorities immediately. To learn more, visit rbcwealthmanagement.com/cybersecurity.

Stay vigilant

You are the first line of defense in protecting your information and accounts. Stay vigilant about changes or activity happening in your accounts.

1. Review your account activity on a regular basis to get familiar with what is normal. This will make it easy to notice when something unusual happens.
2. Learn the best practices of companies holding your accounts. For example, RBC Wealth Management will never send you an unsolicited email asking you to update or verify your account details or other personal information by clicking a link or calling a phone number provided.
3. Be aware of billing and statement cycles. If statements don't arrive on time, follow up immediately to confirm they have not been fraudulently redirected.

Keep information secure

Identity thieves go to extreme lengths to obtain your personal information. Take action to protect your information.

- Enroll in two-factor authentication for online accounts if the option is available.
- Use strong passwords with a mix of letters, numbers and characters. Change them frequently and store passwords in a secure place. Do not repeat passwords.
- Use encryption when sending confidential information by email, and never store sensitive data in your email folders.
- Never share usernames or passwords.
- Don't share personal information over the phone or via email unless you initiate the contact and know the person you are dealing with.
- Never reveal your PIN to anyone, including employees of RBC Wealth Management. When using an ATM, shield the keypad while you enter your PIN.
- Only carry what you need—leave all other information securely at home.
- If it's optional, don't disclose your information.
- Shred paper that contains personal information.

Keep devices secure

Even if you employ strong passwords and carefully destroy documents containing sensitive information, fraudsters could target you via your computer or mobile device.

1. Update your device regularly using patches, security updates or by downloading new versions of apps.
2. Install an anti-virus system.
3. Do not plug in strange or unknown devices like USB sticks.
4. Don't install unknown apps.
5. Be particularly careful when using public or free WiFi connections.
6. Always log out of your account sessions when you are finished.

Having a trusted contact person is important

At RBC Wealth Management, if we think you may be a victim of fraud, we will contact you. Fast action can help resolve issues more quickly. A trusted contact person is someone you authorize us to contact if we are unable to reach you directly. This person should be someone you trust, such as a family member, friend or professional you depend on, like an accountant, attorney or trustee.

Your trusted contact person will NOT be an authorized party on your accounts, nor will we accept instructions from them that will affect transactions and/or change account information in any way. It's simply another way for us to reach you if we need to.

To add a trusted contact person to your account, contact your financial advisor with their name, address and phone number.

22-04-00750_0408 (04/22)