



# Cybersecurity and protecting your data

BrokerLink is proud to offer exclusive home and auto insurance premiums to members. Talk to one of our group insurance advisors for all your insurance needs.



## Avoid phishing scams

Phishing scams are becoming an everyday concern for many Canadians. Phishing is a common tactic that cyber criminals use to steal personal and financial information. These scams are continually getting more sophisticated and harder to identify. Phishing messages usually take the form of an email, text message or phone call from a cyber criminal who is pretending to be someone they are not. Individuals are asked to share sensitive information, such as credit card numbers and passwords. Be on the lookout for urgent or threatening language, promises that are too good to be true, typos or bizarre language, and always look at the sender's contact information to determine if you can identify them.

With emails or text messages, you should always be wary of unknown senders by either ignoring them or refusing to click on suspicious links or downloads. If you aren't sure whether a message is legitimate, check on them by contacting the sender through another channel, for example a phone number off a physical document you have or an official website. This is especially important if it involves well-known companies sending you suspicious messages like the Canada Revenue Agency which is a favourite alias for cyber criminals.

Phone calls from "bank reps" or other seemingly official organizations to "verify" financial or other personal information are another way to catch you. Do not provide sensitive personal information over the phone as organisations like your bank usually only gather this data in person or through other secure channels. Always check the phone number of where a call is coming from to help identify whether it is legitimate.

## Keeping your information private online

Sharing information online can be fun, especially on social media where you want to keep your friends and family updated with what's going on in your life. Always be careful how much you're sharing and with whom.

Unfortunately, the more you post the easier it may be for a cyber criminal to use that information to steal your identity or hack your accounts.

To safeguard your accounts, customize your security settings. In your profile settings you can control who can search for your profile, who can follow or contact you, and how much of your profile is visible to the public. Limit the amount of personal information available on your profile, particularly your phone number, address, or any other pieces of sensitive information that a cyber criminal could use against you. Also, be wary of adding people to your friends list that you don't know in real life as these may be cyber criminals looking to trick you.

## How you can protect yourself from threats and keep your information safe:

- Use strong password protection for your computer
- Change passwords regularly and do not share them
- Install and run anti-virus and anti-spyware software
- Install software updates when they are available
- Enable multi-factor authentication

If you are wanting protection and additional peace of mind, consider investing in identity theft insurance for yourself, and cyber insurance if you have a business.



Get a free no-obligation quote today!

1.833.998.3798

atlanticgroups@brokerlink.ca

BrokerLink.ca/municipalities-ns



NOVA SCOTIA  
FEDERATION OF  
MUNICIPALITIES