

You are here: [Home](#) > [Publications & Resources](#) > Protect yourself against cyber-attacks

Protect yourself against cyber-attacks

A cyber-attack is an attempt by an individual or group to obtain unauthorized access to a computer network or system. It may be executed for financial gain, to obtain data, or to damage the reputation of an individual or entity. Cyber-attacks are a growing concern in the financial services sector. In 2015, 8.5 million Canadian consumers were affected by cybercrime ([Norton Cyber Security Insights Report 2016](#)) .

The financial services industry is shifting toward online products that make it easier for people to do business. But portals, online applications and mobile apps increase the ways in which cyber-attacks can occur against consumers.

FSCO's regulated sectors, such as insurance providers, mortgage brokerages and pension plans, have a responsibility to protect information and provide a safe online environment for consumers. This includes implementing policies and processes that help prevent cybercrime and lay out the steps to take if a cyber-attack takes place.

However, criminals are finding new ways to steal confidential information even from those who are diligent in protecting their online profile. If you deal with any financial service organization online, it is important to be aware of the risks involved and the steps you can take to protect yourself.

What do cyber-attacks look like?

Some cyber-attacks may seem obvious to you, such as suspicious emails, but others can be hard to detect. Some of the most common ways criminals try to steal your information include:

Hacking: cyber criminals gain access to your device or an organization's information technology systems to steal your information

Malware: viruses, spyware or adware are placed on your device to steal your information

Pharming: cyber criminals redirect an organization's legitimate website to a similar-looking website that captures the information you enter

Phishing: fake emails, text messages and websites asking for your information, such as your social insurance number (SIN)

Spam: mass distribution of unwanted messages to you or from you to your contact list

Wi-Fi Eavesdropping: captures your online activity over an unsecure Wi-Fi network

How can you reduce the risks of a cyber-attack?

Practicing regular reviews of your online profile can reduce your exposure to cyber-attacks. Simple steps you can take – such as using strong passwords, changing passwords regularly for each of your devices and services, and updating software to the latest version – may address up to 80 per cent of the risk of compromises due to cyber-attacks (Insurance Institute, 2015). Other things you can do include:

- Start a discussion with your financial service providers so you understand how your information is kept safe: [Questions to Ask your Financial Service Providers about Cyber](#)

Security  Size: ## kb

- Avoid using public Wi-Fi when dealing with financial service providers and opt for an encrypted or secure connection. Turn off Wi-Fi and Bluetooth settings when you are not using them.
- If you receive an email from a financial service provider asking for information, give them a call (on a number not given in the email) to confirm it is legitimate. When in doubt, delete it.
- Use safe payment options, such as credit cards, when making purchases online. Avoid using money transfers – this is not a common practice in the financial services industry.
- Find other tips and resources on Public Safety Canada's website – [Get Cyber Safe](#) .

Watch this two-minute video for seven ways to reduce the risk of a cyber-attack

Deceptive transcript: Seven ways to reduce the risk of a cyber-attack 

What should you do if you suspect you've been a victim of a cyber-attack?

If you suspect you've been a victim of a cyber-attack, contact your local law enforcement agency immediately. You should also inform your financial service providers so they can monitor your accounts for suspicious activity or lock your account. They may also advise you to change your password. For more information, visit the [Canadian Anti-Fraud Centre \(CAFC\)](#) .