



ēducaloi

Information Empowers

PREVENTING ONLINE FRAUD

A Guide for Seniors



Éducaloi is an independent non-profit organization whose mission is to explain the law in Quebec using everyday language and to develop the legal skills of the population of Quebec.

Important notice

The law changes. The information in this guide is up to date to March 2024. Visit the Éducaloi website (educaloi.qc.ca) to check whether there is a more recent version of this guide.

This guide is meant as legal information, not legal advice. If you need advice on a specific situation, consult a lawyer or notary.

This guide only applies in Quebec. Anyone can reproduce this guide for non-commercial reasons. However, it cannot be modified in any way. This guide is the property of Éducaloi. © Éducaloi, 2024.

Table of Contents

PROTECT YOUR BANKING INFORMATION AND PERSONAL DATA

André's story	4
What about identity theft?	6
How to avoid what happened to André	7
What to do immediately if you're a victim	9

PROTECT YOURSELF FROM ROMANCE SCAMS

Suzanne's story	10
What about grandparent scams?	11
How to avoid what happened to Suzanne	12

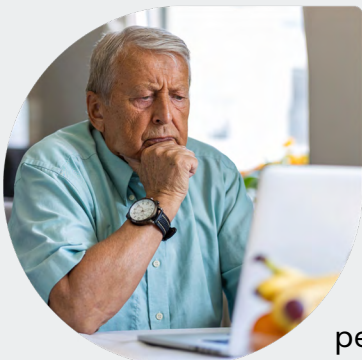
PROTECT YOUR INVESTMENTS

Amir's story	13
Transferring savings abroad	14
What about RRSP scams?	14
How to avoid what happened to Amir	15
What about cryptocurrencies?	16

LEGAL ACTION IN CASE OF FRAUD 17

OTHER USEFUL ACTIONS 18

Protect Your Banking Information and Personal Data



Story based on true events

André's story

André received an email from a delivery company regarding a parcel he'd recently ordered. He was asked to confirm his personal information so that the parcel could be shipped.

After clicking on the link provided, André entered his address and telephone number on the form that appeared on the screen. He also provided his credit card information.

André hoped his parcel would arrive soon.

A few days later, he checked his credit card statement. A series of transactions he knew nothing about had been made with his card. Three luxury items were ordered for a total of \$4,700.



OTHER PRETEXTS FOR CONTACTING YOU

Not all scammers pass themselves off as delivery companies like in André's story. They can also make you think they are

- your telephone company or Internet provider,
- an e-commerce site,
- your bank or credit union, or
- a government agency, such as the Canada Revenue Agency.

Fraud strategy

A strategy commonly used by scammers is to **send you an email pretending to be a well-known company.**

The pretext could be, for example

- to confirm an order,
- to prevent your account from being suspended or automatically upgraded to a premium account, or
- to reimburse you for a billing error.

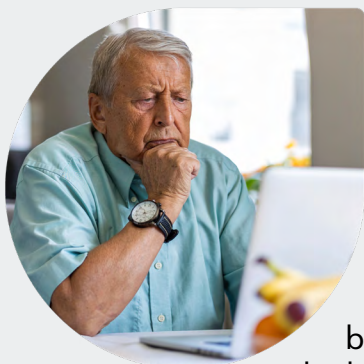
When you click on the link you've received, you're directed to **a site that looks completely legitimate.**

You're asked to **re-enter your credit card information** or your banking information.

Once this information has been obtained, the scammers use it to make payments or large purchases.



Protect Your Banking Information and Personal Data



What about identity theft?

After the mishap with his credit card, André looked for information everywhere: on the Internet, by contacting his bank and by talking to people he knows. Even though he'd lost a lot of money to the scammers, he discovered it could've been a lot worse.

He already knew that you should never share your social insurance number (SIN) on websites that do not legitimately require it. However, he didn't know that the same applies to your date of birth and driver's licence number.

By talking to other people, he learned that a childhood friend of his had her identity stolen that way.

By cross-referencing his friend's date of birth with other personal data, some crooks were able to open an account with Hydro-Québec, and obtain a driver's licence and health insurance card in her name.

With these identity documents, they were ultimately able to borrow a large sum of money from a bank by mortgaging her condo.

Fraud strategy

Scammers try to get as much personal information as possible, not just credit card numbers or banking information.

With enough personal information, some crooks **manage to obtain identity documents in their victims' names** and then impersonate them.

Once this happens, scammers can carry out major transactions, such as selling their victim's house, borrowing large sums of money in their name, or receiving social or pension benefits in their place. This is called "identity theft."



How to avoid what happened to André

Carefully read **emails that ask you to update your account or subscription information** and deal with them accordingly:

- **Compare the email address the message was sent from and the address on the company's legitimate website.**

Is there a small difference that could point to fraud?

For example: info@companyname.s.com instead of info@companyname.com?

- **Avoid clicking on a link in an email of this kind.**

Legitimate companies generally do not ask you to click on a link in an email to enter personal information.

- If you think you need to update your personal information or modify one of your accounts, **go to the company's website directly via your browser.** Do not use the link provided in the email.
- If you receive a fraudulent message, **simply delete it**, without responding to it.



DID YOU KNOW?

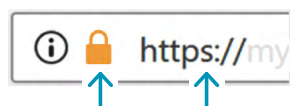
Each day, more than six billion emails are sent all over the world in order to extract banking information or personal data from their recipients.

Protect Your Banking Information and Personal Data

There's more...

- **Only enter your credit card number** to make **a payment on sites of well-established companies.**

Make sure you're using a **secure connection** when you enter your card number or personal information:



There should be a closed padlock icon at the beginning of the browser's address bar, as well as an **"s" after the "http."**

- **Refuse to provide your ID numbers**, like your social insurance number (SIN), your driver's licence number and your health insurance card number on sites that do not require them.
- **Avoid giving your date of birth or your address** when you don't think it's necessary.
- Regularly **verify your bank statements** to detect any unusual transactions.
- **Use a different password** for each of your online accounts.
- **Verify your credit report every year**, via the Equifax or TransUnion websites. Activate a security alert or a lock in your report if you have any suspicions.

What to do immediately if you're a victim

Did you **provide your credit card number** after clicking on a link received in an email?

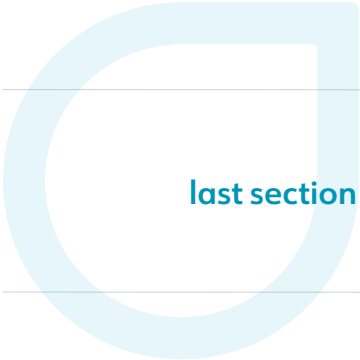
- Contact your credit card company **to have your card locked** and order a new one.
- If there were any unauthorized purchases since the incident, **check** with your credit card issuer **if you have the right to recover the money** lost to fraud. In some cases, the credit card company covers such losses.

Did you **give your banking information** on a site that you now think may be suspicious?

- **Change your password** and **immediately contact your bank** to inform them of the situation.

Do you have **reasons to believe** that you're a victim of **identity theft**?

- **Call your credit card issuer** to change your card(s).
- **Contact your bank** to change your login information and verify that your address and telephone number have not been modified in their system.
- **Contact Equifax or TransUnion** to activate a security alert or security lock on your credit record.
- Depending on your level of suspicion, you could contact **the police, public agencies** and all **your other service providers** to verify the information in your file.



Consult the
last section in this guide on other useful actions to take
in the event of fraud.

Protect Yourself from Romance Scams



Story based on true events

Suzanne's story

A widow for many years, Suzanne joined a dating site a few months ago.

Over a few weeks, she developed a special relationship with a man her age who is also widowed.

Suzanne talked to this man both about her everyday life as well as various subjects of interest to her. Gradually, she started to talk about plans for the both of them.

One day, Suzanne's correspondent told her he was in a difficult situation and asked her to send him money.

Suzanne believed they had a trusting relationship and wanted to help. She sent him the money he needed to get through his difficulties. In the following months, she sent her new romantic partner significant sums of money on several occasions.

But one day, the man abruptly ended the conversation when Suzanne explained to him that she was no longer able to send him money. He stopped responding to her messages and disappeared, along with the money she'd already sent...



OTHER PRETEXTS FOR CONTACTING YOU

To achieve their goals, scammers **manipulate your feelings**. But scammers have more than one trick up their sleeve... They can **also pretend they're a relative** to build a sense of trust.

What about grandparent scams?

These scams target grandparents. A crook could, for example, write a message to Suzanne on social media, pretending to be one of her grandchildren and claiming to be in trouble.

In his message, the fake grandson could explain, for example, that he's been arrested by the police and needs bail money. Or he could say that he's travelling overseas and his wallet was stolen.

If Suzanne responds, and sends money to help him, she's fallen into the scammer's trap.



How to avoid what happened to Suzanne

Romance scams are extremely common. They affect all genders, all ages, and all social classes—including those who never thought they'd fall for it.

Recognizing romance scams

It's **suspicious** if the person you're corresponding with on a dating site

- always finds an excuse not to **meet you in person or talk via video call**.
- **quickly suggests continuing the conversation elsewhere** than on the dating site, for example on Whatsapp or Messenger (a classic fraud strategy since dating sites regularly delete fake profiles from their platform), or
- **asks you for money**.



DID YOU KNOW?

In 2021, reports of romance scams totalled more than *\$60 million* in Canada.

Recognizing grandparent scams

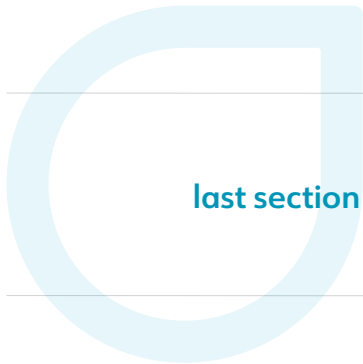
- If one of your loved ones contacts you because they urgently need money without being able to talk to you on the phone, **do not respond to the message you received**.
- **Recontact your loved one**, using another email address, another social media profile or another phone number that you usually use for them, to confirm their identity.
- **Ask them personal questions** that only they could answer.
- If it's not possible to recontact your loved one, **call other members of your family** to validate the story and the identity of the person who wrote you.

Protect Yourself from Romance Scams

There's more...

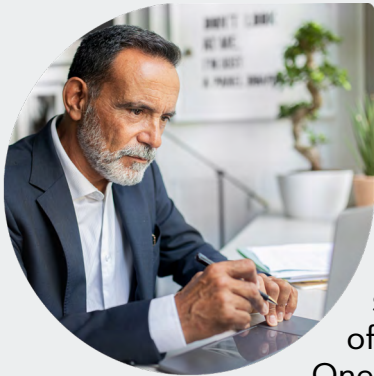
- Configure the parameters of your **social media** accounts. Your posts should **only be visible to people you know**.

Otherwise, scammers can access photos and information you post about yourself and your family. Criminals then use this to impersonate one of your loved ones.



Consult the
last section in this guide on other useful actions to take
in the event of fraud.

Protect Your Investments



Story based on true events

Amir's story

For some time now, Amir has been interested in opportunities to invest in the stock market. He is a member of a Facebook investment group.

One morning, he received a message from an investment advisor who was a member of this Facebook group. The advisor was promoting some investments that she considered very promising.

Amir agreed to have the advisor send him a link by email to the site she was recommending he use to invest.

This did not commit him to anything. After comparing the transaction fees with those charged by the bank, Amir chose the site she recommended.

He started by investing a small sum to test the waters. After three weeks, the returns were exceptional, so he decided to invest most of his savings.

Two months later, disaster struck: Amir searched high and low, but the site had disappeared. And so had the advisor, along with all his savings...



OTHER FORMS OF INVESTMENT FRAUD

Investment fraud can take other forms. Some scammers may invite you to transfer your savings abroad or to reinvest the money in your RRSP. Others may take advantage of the lack of regulation in the cryptocurrency market. For more information, see the following pages.

Protect Your Investments

Transferring savings abroad

You could be advised to invest in countries where taxes on your investment earnings are practically nil.

Be careful! You can certainly invest abroad, but **you must declare your foreign investment income in Canada** and pay Canadian income tax!

If an advisor has no qualms about suggesting that you skirt the law to avoid paying taxes, perhaps this person won't have any qualms about disappearing with your money!

Keep in mind that if you transfer your savings abroad, your money and your scammer can more easily become untraceable. You're making their job easier.



DID YOU KNOW?

Individuals and sites located abroad that offer investment services must **also be registered with the Autorité des marchés financiers of Quebec (AMF).**

What about RRSP scams?

Scammers **regularly target seniors** who have money saved in their Registered Retirement Savings Plan (RRSP) or in their Registered Retirement Income Fund (RRIF).

These crooks appeal to you by suggesting that you take your savings out of your RRSP or RRIF with **promises of greater returns** than what you've accumulated so far.

A fraud technique is to **promise you that the withdrawal from your RRSP/RRIF will be tax free.** The reason given is that the new investment is itself tax exempt.

In reality, the scammer will **disappear with your money.** What's more, you could be required to **pay the tax on the withdrawal** you made by the Canada Revenue Agency and Revenu Québec.

How to avoid what happened to Amir

Only deal with websites and investment specialists who are registered with the **Autorité des marchés financiers** of Quebec (AMF).

Only registered individuals and websites are **regulated**. This significantly reduces the risk of fraud.

You can also be **compensated by a fund** in the event of fraud, under certain conditions and up to a maximum amount. This fund is only available to you if you dealt with an individual or site registered with the AMF.

Verifying registration is simple: visit www.lautorite.qc.ca/en/general-public/registers or call 1-877-525-0337.



DID YOU KNOW?

The **Autorité des marchés financiers** is a government agency that regulates the financial sector in Quebec. One of its roles is to protect individuals who invest.

There's more...

- Beware of **investments with guaranteed exceptional returns**. There's **no such thing**.
An offer that's too good to be true is usually fraudulent.
- **Do not access an investment site via an email** sent to you.
Scammers create perfect replicas of legitimate websites, but with slightly different Internet addresses.
- **No one asked** you questions about **your investment goals and your financial situation**? That's suspicious.
The law requires investment advisors to ask you these questions before recommending investments.
- **Always take time to think about offers**.
Beware of emails offering investment opportunities that are only available for a very limited time. A popular technique among scammers is to force you to act fast.

Protect Your Investments

What about cryptocurrencies?

You may know people who boast about having made record profits in a short period of time by investing in cryptocurrencies.

What you need to know...

If you'd like to invest in cryptocurrencies:

- **The anonymity** of investments in cryptocurrencies **makes things easier for scammers.**
- Don't believe anyone who tells you that cryptocurrencies are investments with guaranteed exceptional returns. There's **always a risk that there will be a downturn in the market, or a crash.**
- **Training workshops and seminars on cryptocurrencies** are a popular way for scammers to make contact with you and gain your trust.
- Beware of **offers to transfer your cryptocurrencies from one platform to another.** It's one of many fraud techniques used to steal your cryptocurrency investments.

What to do...

If you decide to invest:

- Only invest using a site **registered with the Autorité des marchés financiers** of Quebec (AMF). Only these sites are **regulated**. This significantly reduces the risk of fraud.

Verifying registration is simple: visit www.lautorite.qc.ca/en/general-public/registers or call 1-877-525-0337.

Legal Action in Case of Fraud

Fraud is a crime, whatever form it takes. You can take legal action if you're a victim of fraud.

File a complaint with the police

If you file a complaint with the police and they believe they have sufficient grounds to investigate, they will open an investigation. If the police manage to identify those responsible for the fraud, **criminal proceedings** could be launched.

The **difficulty** is that scammers operate under false names, and often from abroad, making it difficult to **find them**.

If the criminal proceedings result in a conviction, the scammers could be sentenced to a **prison term**.

In these types of cases, it's **not necessary to be represented by a lawyer**.

Civil lawsuit

It's also possible for you to personally take legal action against the person responsible for the fraud. This is called "filing a **civil lawsuit**."

However, it's usually **very difficult to correctly identify** your scammer.

If you do manage to find this person, you can ask that they be **required to compensate you** for losses and inconveniences suffered.

You will likely **need a lawyer** to pursue your civil lawsuit.



Given the difficulties of taking legal action against fraud,
your best defence is caution.

Other Useful Actions if You're a Victim of Fraud

In addition to the emergency measures to take in the event of a breach of banking information or personal data (pages 7-9), here are a few other actions you can take if you're a victim of fraud:

Report the fraud to the Canada Anti-Fraud Centre

These reports enable the authorities to better understand the strategies used by scammers and **help to prevent future fraud**. By reporting your story, you're helping to save others from the inconveniences you suffered.

www.antifraudcentre-centreantifraude.ca or 1-888-495-8501

Contact a Centre d'aide aux victimes d'actes criminels (CAVAC – assistance centres for victims of crime)

In case of fraud, the CAVACs can **refer you to the most appropriate resources** for your case, whether legal, financial or psychological.

The CAVACs can also provide you with an **accompaniment service**.

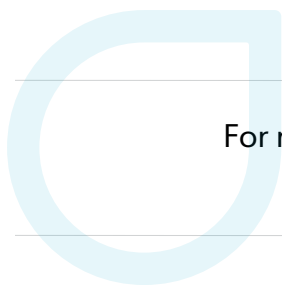
www.cavac.qc.ca/en or 1-866-532-2822

Report the fraud to the Autorité des marchés financiers

If you've been a victim of investment fraud, report it to the AMF and find out if you have access to the **financial services compensation fund**.

www.lautorite.qc.ca/en or 1-877-525-0337

To benefit from the compensation fund, you must have, among other things, invested via an individual or site registered with the AMF.



For more resources to protect yourself from fraud, visit
aineavise.ca/en.



**Do you care about Éducaloi's mission
and activities?**

Make a donation!

[Donate | Éducaloi | Knowledge Empowers](#)

Donations by cheque: Make your cheque payable to "Éducaloï."
C.P.55032, CSP Notre-Dame 11, rue Notre-Dame Ouest Montréal (Québec) H2Y 4A7
educaloi.qc.ca/en

Make the right move with educaloi.qc.ca/en



Facebook @Éducaloi



Instagram @educaloi / @educaloi_en



Twitter @educaloi



LinkedIn @Éducaloi

