MARCH 2023 | VOL.3

SPECIAL JOURNAL FOR FRAUD PREVENTION

March, fraud prevention month

See how you can prevent financial fraud.

The more informed you are, the less fraudsters will be able to scam you!

IN MARCH, WE TALK ABOUT PREVENTION

Advice from Otonom Solution

We hear more and more about fraud, data or identity theft. Hardly a month goes by without us receiving an email notifying us of a data leak, hearing on the news that a company has been defrauded or that there has been a massive data theft. It has become so frequent that it unfortunately seems almost trivial.

The month of March, designated as Fraud Prevention Month, reminds us collectively that fraud is anything but trivial and that prevention is everyone's business.

Every year, Otonom Solution's mission is to help its customers and partners with sound advice on payment fraud prevention.

HOW TO PROTECT YOURSELF AGAINST FRAUDERS?

It's Everyone's Business

The advent of new technologies has opened up the world to possibilities that would have been considered impossible not so long ago. However, the very technologies which makes our lives so easy, have also contributed to creating new avenues for scams and attempted fraud.

Businesses of all sizes, as well as individuals, may be subject to attempted fraud. The question is not whether we will face an attempt at fraud, but rather when it will happen.

The best way to guard against fraud is to stay informed and share your knowledge with those around you. In business, we can never insist enough on the notion of prevention.

- Do not assign all tasks to the same person.
- Put policies and standards in place, even if you are a small business with few employees.
- Do not hesitate to invest in fraud prevention training for your employees.
- Review your fraud prevention plan and strategies annually. Fraud evolves, your plan must also evolve.
- Review and test your fraud response plan. Be prepared to react faster.

MAKE SURE YOU HAVE PROCEDURES IN PLACE AND THAT YOUR EMPLOYEES FOLLOW THEM.

MOST FRAUDS ARE HARD TO DETECT BEFORE IT'S TOO LATE.

BE PREVENTIVE BEFORE YOU HAVE TO BE REACTIVE!

HOUSING RENTAL FRAUD

A scam that hurts

Social media offers a great showcase for landlords who wish to put their units up for rent. Put a description, some photos and it's done. The same goes for condos for sale. The visibility is high and the responses are numerous.

Fraudsters saw the opportunity to mount an easy scam. They take the photos and the description of a condo for sale and advertise a condo for rent with a very attractive price on another platform.

The false owner explains, for example, that the condo for rent was occupied by his child during his studies and that he is not ready to sell it immediately. As the visit of the condo must be conducted by the child who has now moved to another city, he asks for a security deposit by bank transfer, specifying that the answer to the security question will only need to be given when the lease is signed.

Potential tenants are delighted with the photos and the price. What they don't know is that the 'autodeposit' feature, offered by some financial institutions, has been activated on the fraudster's side. During the transfer, the potential tenant is notified by a message that the receiver will receive the funds without having to answer the security question, but this can easily go unnoticed in the haste and excitement of having found the perfect rental. Once the money is sent, it's too late. The potential tenant has fallen into the trap and the false owner cuts communications and moves on to the next victim.

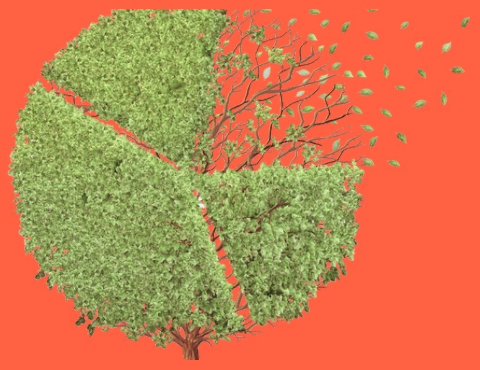
Tips and advice

- Be careful if the photos are incredible and the rent price is really low. When it seems too good to be true...
- Do a web search with the address of the accommodation.
- Security deposits are prohibited in Quebec.

FAKE TEXT OR EMAIL FROM YOUR BOSS

It is increasingly easy to modify the display of a telephone number to make it appear as though it is coming from a recognized agency or from your boss. Same for emails.

Beware of any urgent request to provide confidential documents, to make an urgent payment or to buy gift cards. Take the time to review this request, especially if it is out of the ordinary. We cannot repeat it enough, vigilance can prevent you from being the victim of fraud. Worst case scenario, your boss will see that you take fraud prevention seriously and best-case scenario, you will have saved the company from being defrauded.



AS OF JANUARY 31, 2023

REPORTS OF FRAUD:
6 610
(91 190 IN 2022)

VICTIMS OF FRAUD
3 923
(57 055 IN 2022)

LOST TO FRAUD:
43.6 M$
(531 M$ IN 2022)

Source
Canadian Anti-Fraud Center
https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

SUPPLIER PAYMENT FRAUD

Never two… without three

The scheme is simple, impersonate the supplier in order to modify the bank details for the payment of an invoice, in order to divert it. In addition to assuming the identity of a supplier, the fraudster adds the notion of urgency, so that payment is made quickly, thus reducing the chances of being caught.

How can you protect yourself against this type of fraud? Have a set plan for paying your suppliers and stick to it!

Even if the following points will seem to be self-evident, know that in the midst of a fraud, one can quickly become destabilized. The plan therefore becomes important, so as not to be drawn into a fraud against our will.

- Never change payment details simply by receiving an email or a phone request. Take the time to call the provider, using the contact information on file.
- Never change the address or email of a supplier without first verifying that the request really comes from your supplier.
- Be aware of inconsistencies. For example, a text in dubious English, many mistakes, a change in invoice or email template.
- Any request for an upward invoice adjustment, after receipt thereof, should alert you.
- Ask the opinion of a colleague.
- Take the time BEFORE you lose money.
- When in doubt… there is no doubt. Check with your supplier.

DON'T NEGLECT TRAINING YOUR EMPLOYEES ON RISKS RELATED TO FRAUD.

WE'RE NEVER PREPARED AND EQUIPPED ENOUGH WHEN WE PERFORM FINANCIAL TRANSACTIONS.

YOU DON'T KNOW WHERE TO START?

ASK FOR HELP. MANY TOOLS ARE AVAILABLE AND COMPANIES SPECIALIZE IN THIS KIND OF TRAINING.

THE FAKE TECHNICIAN REINVENTED

A sophisticated scam

The fake computer technician scam has been around for a long time. Almost everyone has already received a call from a stubborn technician in questionable English, who informs us that our computer is infected and that they must intervene immediately.

Although the wind has been taken out of its sails because we talked a lot about it, this scam has evolved. The Canadian Anti-Fraud Center advises us that a variant has emerged in which fraudsters send a fake renewal invoice to an anti-virus subscription. The email includes a phone number to cancel the service or to resolve the non-payment issue. It is by dialing the number that the fake technician comes on the scene and asks you to access your computer remotely to help you with your problem and at the same time try to steal your data.

- Only accept requests for remote support from people or companies you know.
- Do not access any personal information (email, bank account etc.) during a remote support session or when you share your screen.
- **Do not yield under the pressure of the fake technician.**

FUNDS RECOVERED IN 2022 WITH CAFC ASSISTANCE

$2 883 792

Source
Canadian Anti-Fraud Centre
https://www.antifraudcentre-centreantifraude.ca/index-eng.htm

PASSWORD

Do not recycle. Do not use the same password for all your accounts.

Use complex passwords and even passphrases. 8 characters MINIMUM.

Use a password manager.

Mix numbers, uppercase letters, lowercase letters and special characters.

If you need to change your password because of a security breach, don't just add a character. Completely change the password.

Be creative and unpredictable in your choice of password.

QUIZ

TEST YOUR KNOWLEDGE

10 questions about cybersecurity
Government of Canada Quiz

GO

Otonom Solution is a Canadian company duly certified by regulatory authorities and which has been at the heart of your operations since 2008. It offers an innovative secure payment solution that combines various productivity tools and a unique approach for managing multiple accounts and different financial institutions with one single access

4 Place Ville-Marie, 3e étage
Montréal, QC, H3B 2E7
1 855 OTONOM1
info@otonomsolution.com

Writing and graphic design
Caroline Brodeur, CISA

Revision
Jean Salvador
Lyne Sylvain
Sylvie Robitaille

Traduction
Dianne Shea

Communication
Wafia Kanzari

FUND TRANSFER ACCREDITATION BY REVENU QUÉBEC

A license to check

Revenu Québec issues a permit to duly certified money transfer businesses.

Do not trust the nice words that are spoken to you, always verify!

It's simple, easy and free. You will only benefit from doing so!
Otonom Solution is proud to be able to state that it is fully accredited.

Check here

THE CANADIAN ANTI-FRAUD CENTER (CAFC)

A site to keep in your favorites

The Canadian Anti-Fraud Center is jointly managed by the RCMP, The Competition Bureau and the Ontario Provincial Police.

There is a lot of information on the frauds circulating and, on the means to prevent them. The best way to protect yourself is to be informed.

DO YOU THINK YOU HAVE BEEN A VICTIM OF FRAUD?

- Stay calm. Panicking won't help you.
- Gather as much evidence as possible. Documents, emails, text messages, call records, employee testimonials, etc.
- In case of phishing, immediately change your passwords and enable two-factor authentication.
- In the event of fraud by the president (top executive), notify your employees that someone is impersonating you and change your passwords.

IN CASE OF FINANCIAL FRAUD, YOU MUST ALSO CONTACT

- Your financial institution AND/OR YOUR PAYMENT PROVIDER.
- The Canadian Anti-Fraud Center at 1 888 495-8501 or online at www.antifraudcentre-centreantifraude.ca.
- Your local police station to report fraud.