Someone hacked your email!

Emergency Guide

Compromised Email Account



Dany Chouinard
Nicolas Lamoureux

First Edition Canada
2025

Introduction - Why this guide exists and how to use it

Hello, we are here to help you.

This guide was created by two experts who understand exactly what you're going through right now. I'm Nicolas Lamoureux,As an architect of change and transformation, I facilitate governance and simplify digital technology for organizations and my colleague Dany Chouinard is Senior Architect & Expert Manager in Cybersecurity, Technology leader. Together, we regularly help friends or family, with small businesses like you, to get through this difficult time.

We know you're probably feeling overwhelmed, worried, and maybe even angry. This is completely normal. Having your email account hacked is like someone breaking into your home and rummaging through your personal belongings. This violation of your professional space creates enormous stress, especially when your livelihood depends on the trust of your customers.

Why is this guide free? Because we believe that all entrepreneurs AND all citizens deserve access to the right information to protect their personal and financial information, regardless of their budget. We've seen too many small business owners lose customers or close their doors due to a security incident that could have been handled properly, and too many citizens lose their life savings or have their identities stolen.

This guide is aimed at both entrepreneurs and individuals. Whether you're a small business owner concerned about your customers or a private citizen whose personal email has been hacked, the security steps are essentially the same. The main difference: If you're not a business owner, you can skip the sections specific to customers and business communication, but all the other steps (bank security, device wipes, new passwords, etc.) apply perfectly to your personal situation.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Adaptation for individuals: Mentally replace "clients" with "family and friends," "business" with "personal finances," and "professional reputation" with "personal security." The approach and tools remain the same.

How to use this guide: Each section is designed to guide you step by step without overwhelming you. We use simple language, without technical jargon. When you complete a step, check it off the list—this will give you a sense of accomplishment and allow you to see your progress.

Follow the order of priorities: some actions are urgent (today), others can wait a few days.

Remember: You're not alone in this situation. Thousands of entrepreneurs experience the same thing every year, and the vast majority emerge stronger than before. This guide will give you the tools to not only resolve the current crisis, but also better protect your business in the future.

Nicolas Lamoureux: https://www.linkedin.com/in/nicolaslamoureuxqc/

Dany Chouinard: https://www.linkedin.com/in/danychouinard/

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

IMMEDIATE Actions (To be done today)

Take a deep breath. Yes, this is a crisis, but you will get through it.

We know your first reaction is probably panic. It's human. But here's the good news: By acting quickly and methodically today, you'll turn this crisis into an opportunity to strengthen your business's security. Thousands of entrepreneurs before you have experienced the exact same situation and not only survived, but grew stronger.

Your new temporary reality: For the next few days, you're going to function differently. This isn't permanent; it's just time to get everything back in order. Think of it like a home renovation—it's disruptive in the moment, but the end result will be better than before.

Why start with finances: Your money is the lifeblood of your business. Securing your finances first gives you the peace of mind you need to handle everything else with confidence. It's like putting a Band-Aid on a wound before cleaning—you stop the bleeding first.

FINANCIAL SECURITY - ABSOLUTE PRIORITY

Stop Interac payments

- Log in to your bank account online OR go to a branch
- Cancel all scheduled automatic Interac e-Transfers
- Change your online banking password
- Enable SMS notifications for all activity on your accounts

Important: Do NOT make any further online purchases until you receive the new card.

Cancel your credit card

This action will potentially save you thousands of dollars. Hackers often use stolen information within hours. By acting now, you're taking the wind out of their sails.

- **Call IMMEDIATELY** your bank (number on the back of your card)
- **Say exactly this:**"My credit card must be canceled immediately - my email account has been hacked."
- **Request a new card** with a new number
- **Also ask** that all transactions of the last 48 hours are verified

What you will feel:A huge relief after that call. It's normal - you've just regained control of the situation.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Credit Report Lock - The Ultimate Protection

Nuclear weapons against identity theft.

A credit lock goes even further than a fraud alert. It's like putting a tamper-evident lock on your credit report—no one can open a new account in your name, even with all your personal information.

How it works: Your file becomes completely inaccessible for any new credit applications. Banks cannot even consult it without your express permission.

To lock your file:

Equifax Canada :

- Call: 1-800-465-7166
- Say: "I want to lock my credit report"
- Cost: Free
- You will receive a PIN code to keep safe

TransUnion Canada :

- Call: 1-877-713-3393
- Same process as Equifax
- Also free

IMPORTANT - Don't forget: You will need to temporarily unlock your file when you need to:

- Apply for a credit card
- Renew your mortgage
- Financing a vehicle
- Rent an apartment (credit check)
- Subscribe to certain services (telephone, internet)

Practical tip: Mark your calendar with important dates (mortgage renewal, etc.) to remind you to temporarily unlock.

Unlock time: 15 minutes by phone, effective immediately.

This protection gives you: Absolute peace of mind - it is now impossible to open an account in your name without your active participation.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

REPORT TO THE POLICE



The pirates' greatest success? Your silence.

Cybercriminals are counting on one thing: that you keep this attack a secret out of shame or fear of damaging your reputation. This is exactly what allows them to continue operating in the shadows and preying on other entrepreneurs like you. By breaking this silence, you become a hero to all the small business owners who could be their next victims.

Your responsibility to your customers: Your customers trust you with their personal information and payments. By officially reporting this fraud, you show them that you take this responsibility seriously. You transform a moment of vulnerability into a demonstration of leadership and integrity.

But above all, you shed light on criminals who operate in the shadows. Every police report helps investigators identify patterns, trace networks, and protect other victims. Your action today could literally save another entrepreneur's business next week. It's an act of entrepreneurial solidarity.

File a formal complaint

- **Call:** Your city's police service
- **Canadian Anti-Fraud Centre (CAFC) :** 1-888-495-8501
- **Say:**"I want to file a complaint for computer fraud and identity theft."

Important : Ask for your **police report number** - you will need it for insurance and banking.

What you will feel after: A sense of pride and empowerment. You've gone from victim to agent of change.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

URGENT CONTACT WITH YOUR CUSTOMERS

This is when you turn a crisis into a competitive advantage.

Most entrepreneurs who experience this situation hide the problem for fear of losing customers. A big mistake. By proactively reaching out to your customers, you demonstrate a level of professionalism and transparency that your competitors likely never have. You won't lose customers—you'll gain their respect and loyalty.

Your social responsibility: By calling your customers, you're not only protecting your business, you're protecting Canadian families from fraud. These criminals often use your contact list to target your customers. Your call could prevent a grandmother from having her savings stolen or a young family from losing their vacation money.

The message you send: "I take care of my customers even when it costs me time and effort." That's the kind of attitude that builds lifelong customer loyalty and generates positive word of mouth.

Prepare your customer list

Think of it as a crisis marketing campaign—but better, because it's authentic.

- Take out your address book/phone contacts
- Prepare a list of ALL your clients from the last 2 years
- Include their name, phone number and services provided

Call script for your clients

"Hello [customer name], this is [your name]. I'm calling to inform you of an urgent situation. My email account has been hacked by criminals. If you have received emails from me requesting payments or personal information in the last few days, DO NOT REPLY and delete them immediately.

For your safety:

- Stop sending Interac e-Transfers to my old email address
- Do not give any personal information by email.
- I filed a police report (give the number if you have it)
- For our future communications, call me directly at [your phone number]
- I recommend that you use an antivirus program on your computers as soon as possible to ensure that hackers haven't sent viruses to you as well."

Guaranteed result: Your customers will hang up thinking, "Wow, this is someone I can trust."

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Actions WITHIN 48 HOURS

SECURE YOUR DEVICES

Why this step is crucial: Hackers may have installed "bugs" (spyware) on your devices to steal your future passwords. It's like bugging your office—you need to detect and remove them before you can resume normal activities.

Change of mentality: You are now becoming someone who takes security seriously. This habit will protect you for the rest of your entrepreneurial life and impress your business clients.

Scan all your computers and devices

On Windows (detailed steps):

1. **Download Malwarebytes (free):**
    - Open your browser (Chrome, Firefox, Edge)
    - Type exactly:**malwarebytes.com**
    - Click on "Free Download"
    - **IMPORTANT :**Never download from Google - go directly to the official website
    - Click on the downloaded file (at the bottom of your screen or in "Downloads")
    - Follow the installation steps (always click "Next")
2. **Perform the scan:**
    - Once installed, open Malwarebytes
    - Click on "Scan Now" (big blue button)
    - **Go have a coffee**- it takes 30-60 minutes
    - If threats are found, click "Remove Selected"
3. **Download a permanent antivirus:**
    - Go to**bitdefender.com**
    - Choose "Bitdefender Antivirus Free Edition"
    - Install the same way as Malwarebytes
    - Run a full scan

On Mac (detailed steps):

1. **Download CleanMyMac :**
    - Go to**cleanmymac.com**
    - Click "Download for free"
    - Open the downloaded .dmg file
    - Drag the CleanMyMac icon into the Applications folder
    - Open CleanMyMac from Applications
    - Click on "Malware" then "Scan"

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

On phone/tablet:

iPhone/iPad :

- Tap “Settings” (grey icon with gears)
- Tap "General"
- Tap "Software Update"
- If an update appears, tap "Download and install"
- **Plug in your device**- it can take 1 hour

Android :

- Open "Google Play Store" (colored icon)
- Type "Bitdefender Mobile Security" in the search bar
- Press "Install"
- Once installed, open the app
- Tap "Scan Now"

What you might see: Don't panic if the software finds something. This is normal and that's exactly why we're doing this step. Let the programs clean it up automatically.

Total time required: Allow 2-3 hours to complete, but you can go about your business while the scans are running.



Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

CREATE A NEW EMAIL ACCOUNT

Your digital renaissance starts here.

Creating a new email is like moving into a new house after a burglary. You're starting from scratch, but this time with a state-of-the-art security system. This new email will become the secure heart of your business.

Change of perspective: You don't "lose" your old email—you abandon it like abandoning a wrecked car. Your new email will be much better protected and will present a more professional image.

Create a new professional email address

Choose a name that inspires confidence:

Recommended options:

- **Gmail :** nomprenom.entreprise2025@gmail.com
- **Outlook :** votrenom.pro2025@outlook.com

Concrete examples:

- marie.tremblay.comptable2025@gmail.com
- jean.martin.plombier2025@outlook.com
- sophie.roy.consultante2025@gmail.com

Why add “2025”? It shows that you are up to date, modern, and it prevents your name from already being taken.

Creation steps (Gmail - 10 minutes):

1. **Go to gmail.com**
2. **Click "Create an account"**then "Personal use"
3. **Fill in your information:**
    - First and last name
    - Username: yourname.company2025
    - Password: Use your password manager!
4. **Add your phone number**(mandatory for safety)
5. **Gmail will send you a code by SMS**- enter it
6. **Accept the terms**

Similar steps for Outlook.com

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Security configuration (CRUCIAL - don't skip this step!)

Two-Factor Authentication (2FA) - Your Digital Bodyguard:

How it works: Even if a hacker guesses your password, they won't be able to get in without your phone. It's like having two different keys to open your safe.

Enabling 2FA on Gmail:

1. **Click on your photo**(upper right corner)
2. **Click "Manage your Google Account"**
3. **In the left menu, click "Security"**
4. **Search for "2-Step Verification"**and click on it
5. **Click "Start"**
6. **Enter your password**
7. **Add your phone number**
8. **Google sends you a code**- enter it
9. **Click "Activate"**

Recovery Configuration:

- **Use your phone number** as the primary recovery method
- **NEVER your old email compromised**- it would be like giving a key to your new house to your burglar!
- **Add a secondary recovery email**(perhaps that of a trusted relative)

Test final : Log out and log back in to verify everything is working. You should receive a code via SMS.

What you just accomplished: You now have an email account that's more secure than 90% of businesses. Congratulations!

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Change ALL your passwords

The brutal reality: If hackers have access to your email, they can likely guess or retrieve your other passwords. Now's the time to clean house and start fresh.

Why ALL passwords: Imagine your set of keys fell into the hands of a burglar. Even if they only used one key, you'd change all the locks, right? It's exactly the same logic here.

Why a different password everywhere: If you use the same password on 10 sites and just one site gets hacked, criminals can instantly access your other 9 accounts—it's like using the same key for your house, car, office, and safe.

Immediately change passwords for:

- All your other email accounts (Gmail, Outlook, etc.)
- Online Bank Accounts
- Social networks (Facebook, LinkedIn, etc.)
- Services de stockage (Google Drive, Dropbox, etc.)
- Billing/Accounting Accounts
- Any service related to your business

Absolute safety rules to be applied immediately:

A different password everywhere: If you use the same password on 10 sites and just one site gets hacked, criminals can instantly access your other 9 accounts—it's like using the same key for your house, car, office, and safe.

Enable two-factor authentication (MFA) wherever it's offered: As soon as you see "Enable 2-Step Verification" or "MFA" on a site, enable it immediately - it's free and makes your account 99% more secure.

Change ALL your recovery addresses: On each account, go to the security settings and replace your old, compromised email with your new, secure address - otherwise hackers can still regain access to your accounts "through the back door."

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

STOP ! **Before we begin, let me save you hours of frustration.**

The problem : Creating 15-20 different and complex passwords and then remembering them is an impossible task for a normal human brain.

The magic solution: A password manager

Think of it as an ultra-secure digital vault:

1. **You only have one key to remember**(your master password)
2. **The vault automatically creates unguessable passwords**(like "X9#mK7@pL2$vN4!78dtfa74!*&")
3. **It automatically fills in your information** when you visit a website
4. **It works on all your devices**- computer, phone, tablet

How it works in practice:

Step 1: You go to**1password.com**or**bitwarden.com** (free)

Step 2: You create ONE super strong master password

The "Oh! Canada passwords" technique

Strong AND easy to remember!

The secret: Use lyrics from Canadian songs you know by heart, then transform them with a few simple rules. The result: ultra-secure passwords that your brain naturally remembers!

Why it's great: Your password manager will automatically generate passwords, but you still need a VERY strong master password to access it. This technique allows you to create that perfect master password.

Concrete examples with Canadian classics:

1. **"Ahead by a Century"** - The Tragically Hip
    - **Transformation:** Replace letters with numbers and add symbols.
    - **Result:** 4h3ad_ByA_C3ntury!
    - **Why it's strong:** 16 characters with a mix of uppercase and lowercase letters, numbers, and symbols.
    - **Why it's easy:** It's a classic from one of Canada's most beloved bands that you know by heart.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

2. **"If I Had $1,000,000"** - Barenaked Ladies
    - **Full lyrics:** "If I had a million dollars..."
    - **Transformation:** Use a mix of substitutions and numbers.
    - **Result:** 1f!H@d@m1ll1on$
    - **Why it's strong:** 13 characters with a combination of letters, numbers, and symbols that is not a simple substitution.
    - **Why it's easy:** The structure and substitutions are directly linked to the song title, making it very easy to remember.

3. **"Hallelujah"** - Leonard Cohen
    - **Transformation:** Add symbols and numbers to a classic phrase.
    - **Result:** H@ll3luJ@h
    - **Why it's strong:** A clever combination of symbols and numbers for common letters, making it hard to guess.
    - **Why it's easy:** This is one of the most famous Canadian songs worldwide, and the word is already burned into your memory.

Your simple transformation rules (example):

- Replace "e" with "3"
- Replace "i" with "1"
- Add a "!" at the end
- Replace "and" with "&"
- Use "$" for important "s"

Create yours now:

- **Choose a Canadian song** that you hum in the shower.
- **Take a sentence** of 4–12 words.
- **Apply 2–3 simple transformations.**
- **Test it**—can you type it 3 times in a row?

Magical result: A 25+ character password that's impossible to crack, but one you'll never forget because it's part of your Canadian cultural DNA!

Cultural bonus: Every time you type your password, you're supporting Canadian music in your head. It's patriotic cybersecurity!

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

A password manager (suite)

Step 3 : The manager automatically generates passwords like "M8#kP9@vL3$nQ7!" distinct for each site

Step 4: When you visit your bank, it automatically types in this complicated password

Result : You have military-grade passwords everywhere, but you only remember one simple password!

Quick installation (5 minutes):

1. Go to **bitwarden.com** (thanks and excellent)
2. Click "Start"
3. Create your account with a strong master password
4. Download the extension for your browser
5. Download the app on your phone

Now change your passwords one by one:

1. Go to the website (eg your bank)
2. Click "Forgot Password"
3. When asked for a new password, let Bitwarden generate one automatically
4. Bitwarden automatically saves the new password

Time required: 2-3 hours to do everything, but it's an investment that will save you hours every month for the rest of your life!

What you will feel after: An incredible feeling of control and security. Never again will you say "What was my password again?"

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Actions this week

LEGAL OBLIGATIONS - ALBERTA PIPA

Another layer of protection - and you're getting the hang of this!

If you're operating in Alberta, there's good news: you're already thinking like a privacy-conscious entrepreneur! Alberta has its own **Personal Information Protection Act (PIPA)** that works alongside the federal rules, but don't worry - you're building the right mindset and habits.

Mindset shift: You're not drowning in regulations - you're becoming an expert in a system designed to protect both you and your customers. Alberta's approach shows the province takes privacy seriously, which means your clients can trust you more when you follow the rules properly.

Why Alberta PIPA matters for your situation

The practical reality: Alberta's PIPA regulates how private sector organizations collect, use, and disclose personal information Government of AlbertaOipc, and if customer data was compromised in your email hack, this law likely applies to you.

The reassuring part: Organizations must develop policies that are "reasonable" - meaning what a reasonable person would consider appropriate in the circumstances Personal Information Protection Act – Overview | Alberta.ca. You're already being reasonable by following this guide!

What Alberta PIPA requires (simplified version)

Your potential obligations include:

- **Reporting privacy breaches** to the Office of the Information and Privacy Commissioner (OIPC) of Alberta
- **Notifying affected individuals** when the Commissioner determines it's necessary
- **Implementing appropriate security measures** for the sensitivity level of your data
- **Maintaining reasonable policies** for protecting personal information

Key difference from other provinces: The Commissioner may issue a decision requiring an organization to notify affected individuals, but organizations can also notify on their own initiative Breach Notification Requirements | OIPC of Alberta - which means being proactive (like you're doing) is always appreciated.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

The enforcement approach (stay calm!)

Penalties for non-compliance: Up to $10,000 for individuals, up to $100,000 for organizations.

Perspective check: Since 2012-2013, at least 80% of organizations have voluntarily notified affected individuals Breach Notification Requirements | OIPC of Alberta - this shows most businesses act in good faith, just like you're doing.

Your simple next steps

We're still not lawyers - but here's where to get the official information:

Action steps:

1. **Visit oipc.ab.ca** (Office of the Information and Privacy Commissioner of Alberta)
2. **Look for "breach notification" guidance**
3. **Consider consulting a privacy lawyer** familiar with Alberta PIPA if you have significant customer data exposure

Encouraging news: Alberta's system is designed to be reasonable and practical. By following this guide and acting transparently with your customers, you're already demonstrating the "reasonable person" standard the law requires.

Bottom line: You're building trust with Alberta customers by showing you understand and respect their privacy rights under provincial law!

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

LEGAL OBLIGATIONS - BRITISH COLUMBIA PIPA

West Coast privacy protection - you've got this!

British Columbia has its own **Personal Information Protection Act (PIPA)**, and here's some actual good news: BC's approach to breach notification is currently more flexible than other provinces! But that doesn't mean ignoring it - it means you have more control over how to handle your situation professionally.

Mindset adjustment: Think of BC PIPA as giving you the framework to be a privacy leader in your industry. You get to choose how to exceed your customers' expectations rather than just meet minimum requirements.

Why BC PIPA is relevant to your recovery

The current reality: BC's Personal Information Protection Act is the cornerstone of data protection in the province, regulating how organizations collect, use, and disclose personal information Understanding British Columbia's Personal Information Protection Act (PIPA) - Centraleyes, so if you handle BC customer data, this law provides your guidelines.

The flexibility factor: BC PIPA does not currently require private organizations to notify affected individuals or the BC OIPC when a privacy breach has occurred - the decision to do so is voluntary British Columbia's Privacy Regulator Issues New Privacy Breach Guidance: Here's What You Need to Know - McMillan LLP.

What this means for your situation

Your opportunities under BC PIPA:

- **Voluntary breach reporting** to the Office of the Information and Privacy Commissioner for BC (OIPC)
- **Proactive customer notification** (which builds trust even when not required)
- **Implementing strong security measures** appropriate to your data sensitivity
- **Developing robust privacy policies** that show your commitment

Strategic advantage: Since notification isn't mandatory, when you DO notify customers proactively (like this guide recommends), you stand out as exceptionally trustworthy and transparent.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

The enforcement landscape (breathe easy!)

Potential penalties: Up to $10,000 for individuals, up to $100,000 for organizations found in breach.

Practical perspective: It is important to seek legal advice to develop a breach response strategy British Columbia’s Privacy Regulator Issues New Privacy Breach Guidance: Here’s What You Need to Know - McMillan LLP, but BC's current voluntary approach means you have room to craft a response that works for your business size and situation.

Your strategic approach

Since we're not providing legal advice, here's where to get BC-specific guidance:

Next steps:

1. **Visit oipc.bc.ca** (Office of the Information and Privacy Commissioner for BC)
2. **Review their privacy breach guidance**
3. **Consider this an opportunity** to exceed customer expectations voluntarily
4. **Consult a BC privacy lawyer** if you're handling significant amounts of sensitive data

The BC advantage: You get to be the entrepreneur who goes above and beyond legal minimums. Your voluntary transparency and proactive security measures will make you stand out in the BC market.

Final thought: BC customers will remember and respect a business owner who communicated openly about a security incident even when they didn't legally have to. That's the kind of reputation that builds lasting success!

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

LEGAL OBLIGATIONS - QUEBEC LAW 25

Take a breath - we'll navigate this together, step by step.

This section may seem intimidating, but that's normal. Many business owners learn about these obligations for the first time during an incident like yours. The important thing is that you're now aware and can act with full knowledge.

Change of mentality: Instead of seeing this as an additional threat, see it as an opportunity to comply and show your customers that you take their data seriously. This can become a competitive advantage.

Why this information is important to you

The reality: As a Quebec entrepreneur, you may have legal obligations following a hack into your email account, especially if your customers' personal information has been compromised. Better to know now than later!

The good news: By following this guide so far, you've already taken several steps toward compliance.

What Quebec Law 25 says (in simple terms)

Law 25 establishes rules that companies must follow to protect their customers' personal information and respond appropriately if problems arise.

Your potential obligations could include:

- **Quickly assess the situation** and take steps to protect your customers
- **Determine the risk level** for the people concerned
- **Notify the authorities**(Access to Information Commission) in certain cases
- **Inform your customers** if their data has been compromised
- **Document the incident** in a register

Important to remember: These obligations depend on your specific situation – the type of information compromised, the number of customers affected, the nature of your business.

Why you shouldn't panic

Sanctions can seem daunting(fines that can reach several million), but they target companies that completely ignore their obligations or act in bad faith. You are doing the right thing!

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Your next step (simple and clear)

We cannot give you legal advice - **we are not lawyers**. But we can guide you to the right resources:

Recommended immediate action:

1. **Visit quebec.ca** and search for "Law 25" for official information
2. **Visit cai.gouv.qc.ca**(Access to Information Commission)
3. **If you have any doubts, talk to a lawyer** specialized in data protection

Reassuring perspective: Most small businesses that act in good faith and take appropriate measures do not have major problems with these obligations. The important thing is to be aware of them and act correctly.

You are not alone: Thousands of Quebec entrepreneurs are navigating these same obligations. Government resources are there to help you, not punish you.

Final result: By informing yourself now, you are turning a potentially stressful legal obligation into a demonstration of your professionalism and respect for your clients.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

LEGAL OBLIGATIONS - CANADIAN FEDERAL LAW

A second layer of protection - but no extra stress!

If you thought Quebec's Bill 25 was the only one to consider, there's also a Canadian federal law that might apply to your situation. But take a deep breath—you're not drowning in legal paperwork, you're becoming a compliance expert!

Change of perspective: Instead of seeing this as a complication, consider that Canada has several layers of protection in place for you AND your customers. It's a system designed to support you, not punish you.

Why this information concerns you too

The simple reality: If your business processes personal data of customers (even just their names and emails), the **Personal Information Protection and Electronic Documents Act (PIPEDA)** might also apply to your situation.

The good news: The principles are very similar to those of Law 25 - you are not learning a completely different system!

What the Federal Law Says (Simple Version)

Basically, this law says the same thing as Bill 25, but on a Canadian scale:

Your potential obligations include:

- **Quickly assess whether the incident poses a "risk of serious harm"**for your customers
- **Notify the Privacy Commissioner of Canada** in some cases
- **Inform the people concerned** if their data has been compromised
- **Keep a detailed record** of all security incidents
- **Maintain appropriate security measures** to protect data

Risk assessment factors:

- The sensitivity of the information (a social security number vs. an email address)
- The likelihood that this information will be used maliciously

Sanctions (to give you an idea)

Possible fines: Up to $100,000 for failure to comply with notification obligations.

Reassuring perspective: These sanctions target companies that willfully ignore their obligations, not those that make appropriate good faith efforts like you are doing.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

How to navigate those laws

Your simple approach:

1. **Check out both**- provincial AND federal bonds
2. **Follow the strictest requirements** between the two
3. **I document everything** what you are doing (you are already on the right track!)

Your practical action (don't panic!)

We are still not lawyers - we guide you to the right resources:

Next simple steps:

1. **Visit priv.gc.ca** (website of the Privacy Commissioner of Canada)
2. **Search for "security breach"**in their resources
3. **If necessary, consult a lawyer** who knows BOTH provincial and federal laws

Practical tip: Often, by complying with the requirements of Act 25 (which are generally more detailed), you automatically comply with a good part of the federal requirements.

What you need to remember: You're not juggling conflicting systems—you're following layers of protection that complement each other. By acting in good faith and being well-informed, you're on the right track.

Final result: You become an entrepreneur who understands and respects all the rules of the game, which gives you a huge advantage over your competitors who ignore these obligations!

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

OFFICIAL COMMUNICATION

It's time to turn your transparency into a competitive advantage.

This step may seem counterintuitive, but it's brilliant: instead of hiding the problem, you'll make it a public demonstration of your professionalism. Your competitors hide their problems; you show how you handle them. This difference will leave a lasting impression on your customers.

Change of mentality: You go from "I hope no one finds out" to "I'm showing everyone how a real professional handles a crisis." That's the difference between an amateur and a mature entrepreneur.

Why this communication makes you stronger:

- Your customers see that you have their interests at heart
- You get ahead of the rumors and control the narrative
- You demonstrate your integrity and transparency
- You educate your contacts about cybersecurity (they will thank you)

Send an official email to all your contacts

Perfect timing: Send this email when you've completed all the previous steps. Your customers will receive a message from someone who has the situation under control, not someone panicking.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Object :URGENT - Change of email address following hacking

Message type :

“Dear customers and partners,

I am informing you that my email account [old address] has been compromised by cybercriminals. I am contacting you immediately for the sake of transparency and to protect your interests.

Actions I took: ✓ Report filed with the Quebec police (report #[number]) ✓ New ultra-secure email account created with two-factor authentication ✓ All my systems have been cleaned by professional software ✓ All my banking information has been secured

For your protection:

- Do not open emails from my old address [old email]
- Use only my new address: [new address]
- If you have any doubts about the authenticity of an email, please call me at [phone number]
- I highly recommend installing an antivirus on your devices as a precaution.

What this means for you: Absolutely nothing in our services. My commitment to quality and safety remains unchanged - it's even strengthened.

This experience has allowed me to significantly strengthen the security of my company. Your information and our future communications will be better protected than ever before.

I apologize for the inconvenience and thank you for your understanding and continued trust.

Sincerely, [Your Name] [New Email] [Phone Number]

P.S. If this situation concerns you for your own business, please feel free to ask me for advice - I would be happy to share what I have learned."

The genius of this message: You end up in a position of strength, as an expert who can now help others. You turn a weakness into expertise!

Expected reactions: 90% of your customers will respect you more after this message. Many will even thank you for your transparency and ask for safety advice.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Update your business accounts

Your professional rebirth - the perfect opportunity to refresh your image.

Don't think of this step as a chore; think of it as a free rebranding campaign! It's the perfect excuse to modernize your professional presence and show that your business is constantly evolving. Your competitors make these updates once a decade—you're doing it now because you're proactive.

Change of mentality: Instead of enduring this update, you're leading it. You're taking this opportunity to enhance your brand image and showcase your dynamism.

Action plan by priority:

1. Professional Social Networks (Day 1-2)

- **LinkedIn :**
  - Edit your "Contact Information" section
  - Add a note in your summary: "Following the strengthening of my cybersecurity, my new professional email is [new address]"
  - **Bonus :**Share a post about the importance of cybersecurity for SMEs - you'll look like an expert!
- **Facebook Business:**
  - Update the "About" section
  - Change contact information
  - Post a reassuring update to your followers

2. Business Directories (Day 3-4)

- **Quebec Yellow Pages**
- **Google My Business**(super important for local SEO)
- **Quebec Business Directory**
- **Chambers of Commerce**(if you are a member)

Pro trick: While you're there, double-check that all your information is correct and up-to-date. Take the opportunity to add new photos or update your description!

3. Business Cards - Your New Look (Day 5)

Why it's great: You'll get brand new, freshly printed cards with your new secure email. It looks ultra-professional and modern!

Suggestions for improvement:

- Add a small security symbol (🔒) near your email
- Put "Secure Email" in small print under your address
- Take the opportunity to modernize the design if it was due!

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

4. Invoices and official documents (Day 6-7)

Models to update:

- **Invoice headers**
- **Quotes and submissions**
- **Standard contracts**
- **Electronic signatures**
- **Recurring Email Templates**

Psychological tip: Add a small line at the bottom of your invoices: "Secure Communications - Your Privacy is Our Priority." Your customers will notice your attention to security!

Efficient organization: Create a "New 2025 Templates" folder and save all your new templates in the same location. Delete the old ones to avoid mistakes.

What your customers will notice: Your consistency and attention to detail. They'll see that you don't do things by halves and that you take your business seriously.

Estimated total time: 3-4 hours spread over a week, but you can do a little each day during your breaks.

Final result: A refreshed and consistent professional presence that inspires confidence and demonstrates your constant evolution!

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

SURVEILLANCE AND PROTECTION

You now become a detective of your own financial security.

This step transforms your relationship with money and safety. You go from "I hope everything is okay" to "I actively look out for my interests." It's the difference between driving with your eyes closed and driving with all your senses on alert. This new habit will protect you for life.

Change of mentality: You're no longer a potential victim—you're a vigilant guardian of your finances. This active monitoring will even help you discover savings and optimize your spending!

Monitor your bank accounts

Your new morning routine - as important as your coffee!

Why 2 intensive weeks: Criminals often use stolen information within 14 days of the hack. After this period, the risk decreases drastically. This is your "high alert period."

Daily routine (5 minutes each morning):

1. **Open your banking apps**or go to the websites
2. **Check ALL your accounts:**
    - Checking account
    - Savings account
    - Credit cards
    - Line of credit
    - Any other financial product
3. **Search specifically for:**
    - Transactions you don't recognize
    - Strange amounts (even small ones - hackers often test with $1-5)
    - Unusual transfers
    - New Interac e-Transfer recipients

Configure automatic alerts:

At most banks:

1. **Log in to your online account**
2. **Search for “Alerts” or “Notifications”**in the menu
3. **Activate:**
    - Alert for ANY transaction (even $1)
    - Interac e-Transfer Alert
    - Alert for pre-authorized payments
    - Alert for account logins
4. **Choose :**SMS AND email (your new secure email)

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

If you see something suspicious:

- **DON'T PANIC**- that's exactly why you're watching!
- **Call immediately** the number on the back of your card
- **Say:** "I have a suspicious transaction following an email hack."
- **Have on hand:** Date, amount, and description of the transaction

Monitor your credit

Your credit report - the complete picture of your financial health.

Why it's crucial: Criminals sometimes use your information to open accounts in your name (credit cards, loans, cell phones). You might not know it for months!

Get your report for free:

Option 1 - Equifax Canada :

1. **Go to equifax.ca**
2. **Click "Free Credit Report"**
3. **Fill out the form**(they will verify your identity with personal questions)
4. **You will receive the report by mail** in 5-10 days

Option 2 - TransUnion Canada :

1. **Go to transunion.ca**
2. **Click "Free Credit Report"**
3. **Same process as Equifax**

What to look for in your report:

- **New accounts** that you have not opened
- **Addresses** that you have never inhabited
- **Employers** which are not yours
- **Credit applications** that you have not done

Place a fraud alert (highly recommended):

How it works: A special note is added to your file. When someone applies for credit in your name, the bank MUST call you to confirm it's you.

To activate it:

- **Call Equifax:** 1-800-465-7166
- **Say:**“I want to place a fraud alert on my file following a hack.”
- **Duration :**The alert remains active for 6 years (free!)
- **Effect :**Automatic protection with no effort on your part

What you will feel: A huge relief to know that you now have an alarm system over your entire financial life.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Investment time: 30 minutes to set everything up, then 5 minutes a day for 2 weeks. After that, you can reduce to 2-3 times a week.

Result : You sleep soundly knowing that nothing can happen to you without you knowing about it immediately!



Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

FUTURE PREVENTION

PERMANENT SECURITY MEASURES

Congratulations! You are now more armored than 95% of entrepreneurs.

This crisis you've just gone through will make you a stronger, wiser, and more respected entrepreneur. You now have cybersecurity expertise that your competitors don't. Use it as a competitive advantage!

Your new identity: You are no longer someone who "hopes not to get into trouble" - you are someone who is actively preparing for success and security.

Regular Backups - Your Digital Insurance Policy

The golden rule: If you cannot afford to lose this information, it should be backed up in 2 different places.

- **Back up your important data** on an external hard drive (disconnected from the internet when not in use)
- **Recommended cloud service:**iDrive.com (military-grade encryption, affordable)
- **Frequency :**Once a week for important documents, daily for critical data

Continuing Education - Your expert continuing education

You're now a security expert - keep learning!

- **Never click on suspicious links** in emails - when in doubt, go directly to the site
- **Always check the sender's address**- fraudsters make subtle mistakes (gmai1.com instead of gmail.com)
- **Beware of urgent requests** money or personal information - real organizations donate time
- **Update regularly** your software and systems - schedule it for the first Monday of the month

Your new reputation: Your customers will start asking you for safety advice. Share your expertise generously!

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

CONCLUSION



You have just accomplished something extraordinary.

By following this guide, you've transformed one of the worst experiences an entrepreneur can have into a demonstration of leadership, transparency, and professionalism. You've protected your customers, secured your business, and gained valuable expertise.

What you have really accomplished:

- You took control of a crisis situation instead of being subjected to it
- You have strengthened your customers' trust through your transparency
- You have developed professional-grade security systems
- You have contributed to the fight against cybercrime
- You have become a reference in security for those around you

Important warning: We do not guarantee the absolute success of this method, as each hacking situation is unique. However, this guide is based on recognized best practices from the cybersecurity industry and proven principles of organizational change management.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Sources and references used:

- **Canadian Centre for Cyber Security:** cyber.gc.ca
- **Centre antifraude du Canada :** antifraudcentre-centreantifraude.ca
- **Malwarebytes Security :** malwarebytes.com
- **Bitdefender Research :** bitdefender.com
- **1Password Security :** 1password.com
- **Bitwarden Security :** bitwarden.com
- **Équifax Canada :** equifax.ca
- **TransUnion Canada :** transunion.ca
- **Commission d'accès à l'information du Québec:** cai.gouv.qc.ca
- **Privacy Commissioner of Canada:** priv.gc.ca
- **Office of the Information and Privacy Commissioner of Alberta:** oipc.ab.ca
- **Office of the Information and Privacy Commissioner for British Columbia:** oipc.bc.ca

Our commitment: We will continue to update this guide as threats and best practices evolve. Your security and business success are important to us.

Final thought: Six months from now, when you look back, you'll realize that this hack was a positive turning point in your entrepreneurial journey. You're now better equipped, more aware, and stronger than before.

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

COMPLETE CHECKLIST -
CHECK EACH STEP COMPLETED

IMMEDIATE ACTIONS (Day 1)

□ **Cancelled credit card** and new order
□ **Secure bank accounts**- Interac transfers cancelled
□ **Bank notifications enabled** (SMS + email)
□ **Bank password changed**
□ **Police report filed** - Report number: _____
□ **Customer list prepared** (last 2 years)
□ **Emergency calls to priority customers** finished

ACTIONS WITHIN 48 HOURS (Day 2-3)

□ **Malwarebytes installed and full scan** done on computer
□ **Permanent antivirus installed** (Bitdefender or equivalent)
□ **Full antivirus scan on phone/tablet**
□ **Password manager installed** (Bitwarden/1Password)
□ **ALL passwords changed** with the manager:
□ Secondary email accounts
□ Social networks
□ Cloud storage services
□ Billing Accounts
□ Other professional services
□ **New email account created** - Address : _____
□ **2-factor authentication enabled** on the new email
□ **Configured recovery methods** (phone only)

ACTIONS IN THE WEEK (Day 4-7)

□ **Official email sent** to all professional contacts
□ **Professional social networks updated** :
□ LinkedIn
□ Facebook Business
□ Other platforms
□ **Updated business directories** :
□ Google My Business
□ Yellow Pages
□ Chambers of Commerce
□ **New business cards ordered**
□ **Updated official documents** :
□ Invoice templates
□ Standard contracts
□ Electronic signatures
□ **Daily bank monitoring activated** (2 weeks)
□ **Credit report requested** :

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

□ Equifax Canada
□ TransUnion Canada
□ **Fraud alert placed** on credit file
□ **Government website consulted** (quebec.ca - Law 25) to know my specific obligations
□ **Professional assessment requested** (lawyer if necessary) for my particular situation
□ **Alberta OIPC website consulted** (oipc.ab.ca) for PIPA requirements
□ **Breach reporting assessment** completed for Alberta obligations
□ **BC OIPC website consulted** (oipc.bc.ca) for PIPA guidance
□ **Voluntary notification strategy** considered for competitive advantage

PERMANENT PREVENTIVE MEASURES

□ **Backup system configured** (external drive + cloud)
□ **Maintenance Schedule** scheduled (1st Monday of the month)
□ **Saved emergency numbers** in phone
□ **Formation continue** in planned cybersecurity

SAVED EMERGENCY NUMBERS

□ **Your bank: _____**
□ **Local Police:**
□ **Centre antifraude du Canada :** 1-888-495-8501
□ **Equifax Canada :** 1-800-465-7166
□ **TransUnion Canada :** 1-877-713-3393

CONGRATULATIONS !

You have completed your transformation into a cyber-secure entrepreneur!

IN CASE OF FUTURE EMERGENCY: If you discover suspicious activity, immediately contact the police and your financial institution.

Last word : Keep this guide safe - it might help a fellow entrepreneur in need. Now your experience can help others!

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux

Copyright 2025 - Dany Chouinard & Nicolas Lamoureux