



The Art of Fraud Prevention

A guide to keeping your business and customers safe



by Diane Amato, for RBC



This is your business.

You've worked hard to build it, and you pour your blood, sweat and tears into running it. No one has the right to steal your money, data or clients from you. For as hard you've worked to build your business, you need to work just as hard to protect it.

Let's face it, talking about fraud — and its potential impact on your business and your bottom line — is heavy stuff. It's easy to put it to a distant back burner for future thought. But for all the doomsday news about how hackers, fraudsters and crooked bookkeepers can thwart the success of your business, there are tough consequences that can come from not dealing with the realities of business fraud.

What's Inside

Why You Should Keep Fraud Prevention on Your Radar	3
Cybercrime and Your Business	
Criminal Threats and What to Do About Them	4
Payments Fraud	
Everything Old Is New Again	6
Social Engineering	
When Being Polite Can Cost You	8
Cheque Fraud	
It's Still a Thing	10
Internal Fraud	
How to Protect Your Business From the Inside Out	12
10 Ways to Protect Your Business From Fraud	14





Why You Should Keep Fraud Prevention on Your Radar

1 Preventing fraud is possible.

And in many cases it's easy. If you're running a large corporation, you may need sophisticated systems to fully protect your information. But if your company is small to mid-sized, keeping your finances and your information safe usually comes down to simple controls and policies that limit your exposure. Check out [10 Ways to Protect Your Business from Fraud](#) for tips you can easily implement.

2 Detecting fraud — and possible attacks on your business — can protect your company's money and reputation.

Depending on the size of your business, the funds, client data and company information that you can keep from leaking out can work out to thousands — if not millions — of dollars in immediate cash or revenue down the road. Whether it's [cybercrime](#), [payments fraud](#), [cheque fraud](#) or an [internal scam](#), if your business is a victim, you could quite literally lose it all. Reason enough? We think so.

3 Fraudsters are getting smarter and more sophisticated.

You work hard in your business every day. At the same time, fraudsters are working hard to get your business information and money. They're committed to their craft and are always coming up with new ways to dupe, swindle and steal. To see just how innovative fraudsters can be, read [Social Engineering: When Being Polite Can Cost You](#). Staying vigilant and [being aware of the latest scams](#) can help you keep up on their techniques in order to avoid becoming a victim.

4 It's not always top of mind.

When you're alert to the risks of fraud and suspicious of things that are out of the ordinary, you're in a much better position to fend off a fraudulent attack on your business. For more about the impact of letting your guard down, take a look at [Cybercrime and Your Business: Criminal Threats and What to Do About Them](#).

Because fraud is likely not the first thing you think of every morning, it's a good idea to tune in to news, helpful posts and the [latest reports](#). You can get started with the [Alerts from RBC](#) that cover the most up-to-date information about privacy, fraud and other security-related issues that you should be aware of.





Cybercrime and Your Business

Criminal Threats and What to Do About Them

Cybercrime’s broad definition is that it’s any crime that involves a computer — from spreading a virus, stealing funds, to identity theft and stealing client data.

And while there are many different variations of Cybercrime, there are three especially prominent types business owners should be aware of.

Cybercrime has become the number one money-making criminal activity around the world, costing businesses \$400B annually¹.

Phishing

Phishing is a very common online scam where an email is sent, attempting to trick the recipient into giving up personal, business or financial information. Typically, a phishing email will explain an urgent situation (“Our audit department has detected a problem with your

TIP

Employees are trained to be helpful and provide good customer service, which can also make them targets for phishing attacks. Train them to also be cautious about clicking links in emails and downloading attachments.



account”) with a time limit to act (“You have 24 hours to verify your account”) and a link to click where you’ll be asked to enter your confidential information (“to fix the “problem”). The fraudster then gets access to your passwords, account numbers, client base, or even your computer systems. Remember, legitimate organizations will never ask for information to be sent in this manner.

Malware

Malware is designed to creep into your computer and wreak havoc on your systems. Whether it corrupts your files, messes up your applications, spies on your activity or copies your data, malware is often a means to an end — it’s used as a way in to steal money or information. Common signs that may indicate a computer has malware include decreased computing speed, missing or deleted security software and increased computer crashes or freezes. There are several ways to protect your business against a malware attack, including installing up-to-date anti-virus software, removing old applications, and never providing confidential information or signing in IDs or passwords when responding to an unsolicited email or text.

Ransomware

Ransomware is one of many types of malware, and is worth calling out here as it’s on the rise and especially damaging to businesses. That’s because once it gets in, ransomware typically copies everything on your computer and locks you out. It then holds your data hostage until a ransom is paid. Ransomware can be crippling to your business, and it can take weeks — or longer — to recover from a ransomware attack. During that time, it may be impossible to run your



business. The same malware prevention tips apply to ransomware attacks — but beyond being vigilant about your software and email practices, it's important to back up your data on a regular basis so that if you are a victim of a ransomware attack, you can get back to business sooner.

Besides these very real hazards, there is one thing that is especially dangerous to a business: an owner who thinks they are immune to such attacks.

Protecting Your Business

The reality is, all businesses are at risk. To avoid falling victim to Cybercrime, take note of these tips that can protect your business:

1 Hire an expert.

If your business is low-tech and doesn't run sophisticated systems, you may believe that you are impervious to cyber fraud. But even if you and your employees just use email to communicate, you're at risk. If you make purchases online, you're potentially a target. If you're not computer savvy, hire a trusted supplier who is — someone who can make sure your systems are up-to-date and that you have the right anti-virus software installed.

2 Educate your employees.

Your employees are likely lovely people you would trust to watch your children. But while they might not have bad intentions, everyone is human, and mistakes can be made — whether it's logging in to work from a coffee shop (and exposing your data to an insecure network) or clicking on a malicious pop-up. With **90% of all cyber security breaches a result of human error**, even your most loyal employees could be your weak link.

3 Remember you're a potential target.

If you think only retail or tech giants get hacked, think again. There are many opportunities for hackers to get money and information from even small businesses — whether it's re-directing a wire transfer you're sending to a vendor or using your

data to hack one of your customers or vendors. Fraudsters can spot opportunities regardless of the size of your operation.

4 Stay vigilant.

Cyber thieves are smart. Really smart... not to mention extremely sophisticated — and will take any opportunity to target a vulnerable business. When they infiltrate your systems they can monitor your email correspondence so they know your habits, contacts, writing style and travel schedules. This tactic can allow them to easily pose as someone you trust and convince you to re-direct a transfer to a new bank account.

5 Make your passwords stronger.

If you're going with a single word with a couple of numbers, your passwords just aren't strong enough. To make your password stronger use letters, numbers and special characters. You should not use the same password across systems and they should also be changed regularly to keep hackers at bay.

Today's cybercriminals are patient and sophisticated and look at what they do as a career versus a crime. They have access to funding and therefore have no reason to let up on their cyber attacks. To safeguard your computer systems, it's important to stay vigilant and implement controls. To help you get started, review these [10 Ways to Protect Your Business from Fraud](#).

TIP

Longer passwords with more characters can be more secure than short, easy-to-remember ones. That's because fraudsters, or the programs they use to guess your password, will have to work harder.





Payments Fraud

Everything Old Is New Again

Wire fraud has been around for over 100 years. And while it started out as intercepting telegraph wires, payment fraud has had a long and dramatic evolution to its current state, which includes wire, email and cheque fraud. Here's a look at what wire and email fraud looks like today, and how you can protect your business from both. You can learn more about preventing cheque fraud in [Cheque Fraud: It's Still a Thing](#).

While intercepting or re-directing a payment can happen through a variety of clever tactics, payments fraud generally comes about when a criminal lies about a situation in order to convince you (or your employees) to send money through a payment or transfer of some kind.

The largest emerging threat on the payments fraud landscape right now is a scam called Business Email Compromise. Here's what you need to know:

How Does it Work?

Say you're the business owner or CEO/ CFO of a business (basically, someone with authority to send large amounts of money). A fraudster would get their hands on your email or other online credentials, then posing as you, send instructions to someone in your company to send a payment to a particular account.

Why Does it Work?

Criminals are detail-oriented and do their research. In an email, a fraudster will include details about team members and current projects — and even confidential projects — making the communication appear totally legitimate.



TIP

Training and education may be your strongest tools in protecting your business from potential fraud. Owners should develop strong security habits in both employees and themselves.





What are Some Common Variations?

Business Email Compromise takes a few different forms. Here are a few examples:

Owner/CEO fraud

This is where a fraudster either hacks into the email of an owner, CEO or other high-ranking executive, or duplicates a domain so it appears an email is coming from the company's highest ranks. They then send a fake email to request a financial transaction while the executive is away on vacation, typically asking to change routing information for an account or to make an out-of-the-ordinary deposit or transfer.

Because the fraudster will have been monitoring email activity and would have done their research, they will often wait for the target to go out of town so that the email recipient can't verify the request face-to-face. They will also include reasons for not following standard policy or for keeping a request secret: *"I plan to make an announcement in the morning. Until then, please don't tell anyone."*

A request for payment from a vendor

A fraudster posing as a vendor will email someone in accounts payable and tell them that their account details have changed — and can they please send payment to this new account number instead? Even if your company's systems aren't hacked, if your vendor's email is compromised, a fraudulent request or redirection of funds can appear legitimate.

A lawyer impersonation

In a similar scam, a "fake" lawyer will request a fund transfer for a large transaction to a fraudulent account to settle a legal dispute or pay an overdue bill. The fraudster will convince their target the transfer is confidential and time-sensitive, so it's less likely that the employee will attempt to confirm they should send the transfer.

What Types of Businesses are at Risk?

Businesses of all sizes have been targeted by Business Email Compromise, and it's a scam that's been reported in 80 countries.

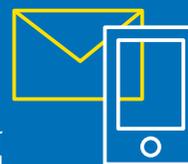
While businesses working with foreign suppliers or those that regularly send wire transfers are the most vulnerable, fraudsters are flexible and can adjust their tactics to use other payment methods. So every business needs to treat email requests for funds with caution.

How Can I Protect My Company?

Business Email Compromise — or other variations of payments fraud — are often caused by human error as well as online systems and accounts that are hacked. There are strategies to boost your online security that can be easily implemented — but the most effective way to safeguard your business may be to train your staff/employees. Ultimately, it takes a person to send a transfer or payment.

TIP

Switch up your communication methods when it comes to verification; for example, if a transfer request arrives via email, use a phone number (you know to be real) to verify the sender.





Social Engineering

When Being Polite Can Cost You

Your business may have all the firewalls, anti-virus software and cyber security experts you need. But that doesn't mean your company is immune to fraud. That's because the human side of business fraud can affect your company just as acutely as even the most sophisticated technical scheme.

Hacking and manipulating human psychology is often referred to as social engineering, and typically manifests in fraudsters tricking employees or business owners into giving away valuable information.

Today's hackers do their research

Because today's hackers do their research, if your business is in their sights they will understand who does what in your company, know your partners and processes, and target specific employees using highly relevant information, offers and questions. Fraudsters may have even contacted someone in your company via a social networking site, starting a conversation and building a rapport. Your employees — particularly those who are polite, friendly, non-confrontational and trusting — may be easily duped into divulging information that can result in financial or business information losses.

Be aware of some of the more common ways scammers gain access to your employees:

Pretexting

This is where a fraudster creates a false reason — or pretext — for getting in touch with an employee, and requests confidential or secure information. It could be someone pretending to be a prospective supplier, a research firm, bank or government agency asking for other employee names, banking information, login

credentials or something seemingly innocuous (such as a child's name, anniversary date or cell phone provider). Any information gathered can be used to complete a profile, allowing a fraudster to pose as an employee and gain access to your accounts, systems or customers.

TIP

Unless you have verified a person's authority to have access to information about an employee, your company, or your company's networks, sharing information may put your business at risk.



Caller ID or email spoofing

It's easier than you might think to fake caller IDs and email addresses. Many people get fooled by phone calls or emails that appear to be coming from a completely legitimate source. Just because a genuine looking ID or email address appears, doesn't mean the person on the other end of the connection is on the up-and-up.

Baiting

Specifically targeting human curiosity, this technique uses the promise of an item — such as a free music download — if the employee enters key information or credentials. The bait can also take a physical form. Be wary of USBs left around the office or parking lots — curious employees may plug them in and unwittingly infect your systems.



Tailgating

We've all done it at one point in our lives — let someone in behind us — whether it's into an apartment building or office space. Posing as a delivery or service person, a fraudster can easily gain access to unauthorized spaces if they find an unsuspecting person willing to hold the door for them as they enter your office. From stealing a laptop to entering your server room, picking up invoices (with client or vendor information) to plugging a malicious device into an unattended workstation, tailgaters can steal property or data in many ways.

Even if you have sophisticated anti-virus systems in place, your fraud prevention controls need to extend beyond cyber security to the human side of your business. Given the advanced and well-researched nature of fraud tactics, you and your employees can easily fall victim to social engineering scams, and put your company's account numbers, passwords, customers and other information at risk.

Protecting against social engineering scams comes down to employee training and awareness, as well as an investment in online detection services that can sniff out fake email addresses, malicious websites and hovering viruses.

Get more tips on how to implement the right controls in your company: [10 Ways to Protect Your Business from Fraud](#).

Cheque Fraud

It's Still a Thing



Writing a cheque is one of the oldest ways to pay (some make the case that cheques have been around since the Roman times). And even with the advancement of payments technology and the many electronic options available, cheques are still used by many businesses. In fact, while they have been declining at a rate of about 5% per year over the last 10 years, Canadian banks still process **over 1 billion** cheques annually.

When you consider that kind of volume, it doesn't come as much of a surprise that cheque fraud is still a thing.

*In fact, cheque fraud is a **BIG THING**, costing businesses more than any other type of fraud in recent years².*

(While not as frequent as some of the more common forms of fraud, losses per incident can be higher).

Since it's estimated that cheques will be in use until at least 2050³, this form of fraud is something business owners shouldn't lose sight of.

Why is cheque fraud still happening?

Given that cheque fraud has been around nearly as long as cheques, shouldn't we have solved the problem by now? Well, there are a few reasons it's still an issue:

1 Technology.

True, the payments industry has advanced. Ink, paper and watermarks have improved to make cheques more difficult to copy. The thing is, fraudsters have been making their own strides, and a cheque is still a relatively easy (and inexpensive) thing to create, duplicate or manipulate. While technology is working to make cheques more difficult to falsify, high-tech fraudsters are also improving their technology to create realistic counterfeit cheques — as well as the fake ID they can use to cash them in.

2 Low cost of entry.

All a fraudster really needs is some high quality paper, a printer, scanner, and an affinity for Photoshop to create a fake cheque. Unfortunately, low overhead makes this an easy career to launch.

3 Easy to intercept.

Because cheques are physical things, they can be intercepted at any point in the delivery process — whether it's by employees, mail carriers or couriers, or thieves who go through mailboxes, dumpsters or recycling bins.



How can businesses protect against cheque fraud?

The good news is, when it comes to cheque fraud, the right controls can generally protect your business. It's just a matter of implementing the policies, services and routines that will make a real difference on the security of your financial transactions. Here are the most effective business practices:

Use electronic forms of payment.

Whether that's e-Transfers, direct payments or wire transfers, removing the physical element of a payment can reduce the risk of cheque fraud from your business.

Check your account balances daily.

That way, you can quickly spot a fraudulent cheque transaction and alert your bank. Keep in mind, too, that there are federally-imposed time limits as to when a cheque can be returned to the depositor's bank after it has been debited from your account.

TIP

Because different banks have different polices and conditions, the sooner you spot something out of the ordinary, the better your chances of recovering lost funds.



Use automated fraud detection services.

Services such as Payee Match, Positive Pay or Reverse Pay can help spot inconsistencies or anomalies faster and help you easily reconcile your cheque transactions.

Lock down your cheque supply.

Don't leave cheques lying around on desks or unsecured. Always store your cheques, deposit slips, bank statements and other documents in a secure location.

Shred cancelled cheques and old statements.

Don't give fraudsters a blueprint to copy account numbers and cheque information.

Require double signatures.

Having two company officers sign each cheque, or cheques above a certain amount, can help reduce the risk that someone will write a cheque to themselves or a fictitious company.

Have different accounts for different functions.

By segregating your accounts — and the cheques you write from them — it's easier to balance your cheque book and spot inconsistencies.

Yes, cheque fraud is still a (big) thing, but it is preventable. Take these tips to heart, educate your staff, and your business will be in a safer spot.

Internal Fraud

How to Protect Your Business from the Inside Out



Whether it's stealing cash from the register, manipulating cheques, skimming office supplies or embezzling millions, internal fraud can take many forms. For those businesses affected, it can be emotionally difficult as well as financially challenging to accept, as in some cases it's a once-trusted employee who's behind the theft.

While internal fraud can be heart-breaking and potentially crippling for business owners, it is something that can generally be caught with the right controls in place.

Often it's a matter of creating strong policies, staying diligent with employee onboarding and exit strategies, and avoiding giving too much authority to any one person.

Consider these techniques to prevent internal fraud in your company

Have the right hiring processes in place.

This involves comprehensive screening, thorough reference checks, and impartial background checks, and reviews. It's also a good idea to do some additional digging if someone is going to be given access to financial transactions.

Implement an exit strategy.

Ensure that when an employee leaves your company that you deactivate their online and internal access. You don't want an ex-employee having access to their email — or other company info — from home.

Do a regular review with reporting managers.

Jobs can change and evolve over time. Simply asking: "Does Christine still need to make wire transfers?" will help manage who has authority to do what.

Manage financial limits appropriately.

When you're setting up access limits — whether it's to make transfers, sign invoices or write cheques — many business owners just default to the maximum. As a result, far too many junior level employees have access to transfer large amounts of money. Assign limits that are appropriate to the level of the employee and your business needs, and review them regularly.



Do a regular check of employee log-ins against an HR list.

If your company is growing quickly, or employs people who work remotely, you won't always have a great handle on who is working for you. Checking who is logging in to your system against an up-to-date employee list from HR will help confirm that everyone who has access to your data is an active employee.

Segregate cash duties.

If you own a retail business, make each employee responsible for their own cash drawer so there's less opportunity to hide a theft. It's also a good idea to separate cash responsibilities: for instance, the employee who is responsible for reconciling receipts shouldn't also handle or receive cash.

Ensure at least two people are required to approve a transaction.

Implementing a dual control policy when managing financial transactions is one of the best ways to tackle internal fraud. Too many times, internal theft is the result of a bookkeeper, Accounts Payable clerk — or even the CFO — having the freedom to move money around unchecked. Even if you trust an individual implicitly, you don't want to give total control to any

one person. If you get any pushback from your staff, remind them that a dual control policy will also help protect them should they make a mistake or get a virus on their computer — an error could be caught before costing the company a significant amount of money.

If it happens to you, report it.

Many times, business owners are too embarrassed to report internal fraud, believing that they should have been aware of what was going on within their own company. But fraudsters are smart, sneaky and manipulative, so it's often not easy to spot malicious intentions or activity. Reporting the fraud may help you recoup losses — or at the very least, protect another unsuspecting company from hiring the thief.

Just about every business is vulnerable to internal fraud at some point. The best way to bolster your company's defences is to run a buttoned-down operation with strict controls and policies in place that make it virtually impossible for anyone to steal from you.

TIP

Even if you trust an individual implicitly, you don't want to give total control to any one person.



10 Ways to Protect Your Business from Fraud

There are many different types of business fraud out there — from cybercrime to internal theft, payments fraud and social engineering. While the methods for defrauding businesses can vary, generally the ways to prevent it from affecting your business are the same.

Protect your business from fraud with these 10 tips:

1 Be suspicious.

If something looks or sounds bizarre, or is in any way out of the ordinary, take extra caution. Do not open emails, strange links, pop-ups or websites from people or companies you don't know or recognize. And keep in mind that offers that seem too good to be true, generally are.

2 Pick up the phone.

If you or your employees receive a strange request asking for business or personal information via email, call to verify it's legitimate. Never trust a phone number provided in the email or text. Whether it's a vendor you work with or a publicly available number for a bank or service provider, it's important to have a conversation to confirm the email is legitimate. Remember, your financial institution will never request personal or confidential information through email.

3 Know your network.

Even if they're not located near your office, build a relationship with your vendors and your partners outside of email. Know their voices, their writing styles, their policies and their schedules. That way, if a particular vendor writes with an odd request,

you can pick up on it immediately. You will also be comfortable with calling them to confirm what's going on.

4 Manage invoice and payment limits appropriately.

Junior employees should have lower access limits when it comes to the amount they can send, approve or pay out. While your days are undoubtedly busy, avoid setting high default limits out of convenience. Set appropriate financial limits and review them regularly.





5 Implement dual controls for payment transactions.

Ensure that at least two people must approve a transaction before it goes through, thereby avoiding giving complete control to any one person. This dual control strategy protects your company. An inadvertent error — or malicious intent to steal funds — that might otherwise cost your business money could be caught by a second set of eyes.

6 Update your software and browser.

Running old, out-of-date software doesn't give your systems the protection you need to safeguard your information. Installing anti-virus software (and updating it regularly), implementing back ups and outsourcing to tech experts can protect your business from cybercrime. It can also help you get your business up and running faster should any of your systems get compromised.

7 Get insurance.

If you fall victim to a crippling ransomware scam, your business may not be able to operate for an indeterminate amount of time (some ransomware attacks can take months to recover from).

Business continuity insurance can protect you if you're unable to do business, protecting your livelihood and that of your employees.

8 Educate your employees.

Make sure your employees are aware of the fraud threats and tactics out there today, and train them on anti-fraud policies and techniques. Consider testing employees randomly with false phishing scams to see if they are adopting the policies you have in place. Keeping fraud on your employees' radar through regular updates and sessions will also go a long way toward protecting your company.

9 Check your accounts regularly.

When you're on top of your banking, you'll be in a position to spot a fraudulent transaction right away. Keep in mind, if your financial institution has a policy to reimburse you from unauthorized transactions, there may be a time limit in place when it comes to reporting the incident. If you suspect fraud, notify your bank right away.

TIP

If you suspect fraud, notify your bank right away.



10 Notify your IT department if you suspect fraud.

Your IT team may be able to stave off a fraudulent attack on your systems, particularly if you notify them immediately. While some damage may be done if an employee clicks a malicious link, your tech team may be able to minimize the impact to the rest of your company.

Get the latest information about privacy, fraud and other security-related issues that you should be aware of. You can get started with the [Alerts from RBC](#) or by visiting [The Canadian Anti-Fraud Centre](#).

As hard as you've worked to build your business, you need to work just as hard to protect it, but you don't have to do it alone. One of the steps is keeping a watch on your business cash flow.

Visit RBC Business to learn more about how we can help you monitor your accounts so you always know where your cash flow stands.



Visit the Discover & Learn portal for more interesting content
discover.rbcroyalbank.com/business

Sources:

1. Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II
- 2-3. 2016 AFP Payments Fraud and Control Survey, Association for Financial Professionals

These articles are intended as general information only and are not to be relied upon as constituting legal, financial or other professional advice. A professional advisor should be consulted regarding your specific situation. Information presented is believed to be factual and up-to-date but we do not guarantee its accuracy and it should not be regarded as a complete analysis of the subjects discussed. All expressions of opinion reflect the judgment of the authors as of the date of publication and are subject to change. No endorsement of any third parties or their advice, opinions, information, products or services is expressly given or implied by Royal Bank of Canada or any of its affiliates.

© / ™ Trademark(s) of Royal Bank of Canada. RBC and Royal Bank are registered trademarks of Royal Bank of Canada.