Be Cyber Aware

RBC Fraud Prevention and Cyber Safety Book

RBC

Learn how to protect your digital assets, safeguarding yourself, your family and your business.

Education - the best defense against fraud.

With the rise of cyber crime around the globe, it's never been more important to ensure you educate yourself and your family on how to stay cyber safe. With the rapid evolution of technologies, such as generative AI, cyber criminals can defraud you of your digital assets through unexpected ways.

This guide will help you learn how to protect yourself, your family and your digital assets.

What's Inside

Banking Safely and Securely with RBC

With the RBC Digital Banking Security Guarantee, you're fully protected against any transactions you didn't make or approve or provide authorization for. Should something ever happen, we will fully reimburse you for any unauthorized transactions made through the RBC Mobile app or RBC Online Banking.

Safeguarding the security of our systems and the confidentiality of our clients' information is always a top priority. To ensure our clients have a safe and secure online banking experience, we encourage you to enable the following security features on all your online accounts:

Two- or multi-factor authentication (when possible)

Enabling two- or multi-factor authentication adds an extra layer of security because you verify your identity in two or more ways: a strong password and either a numeric code or some sort of biometric like a fingerprint.

Auto-deposit for e-transfers

With Interac e-Transfer Auto-deposit, there's no need to log into your Online Banking or answer a security question to receive an e-Transfer. Once you register your e-mail or mobile phone number, anytime someone sends you money, the funds will be automatically deposited into the specified account. This service eliminates the need for a security question and answer in every transaction lessening the risk that someone unintended could intercept the funds.

What You Can Do

Clients also play an important role in protecting and safeguarding their systems and accounts. We regularly educate our clients about best practices like installing software updates, protecting your passwords and email accounts and being aware of phishing scams.

1. Use strong security questions

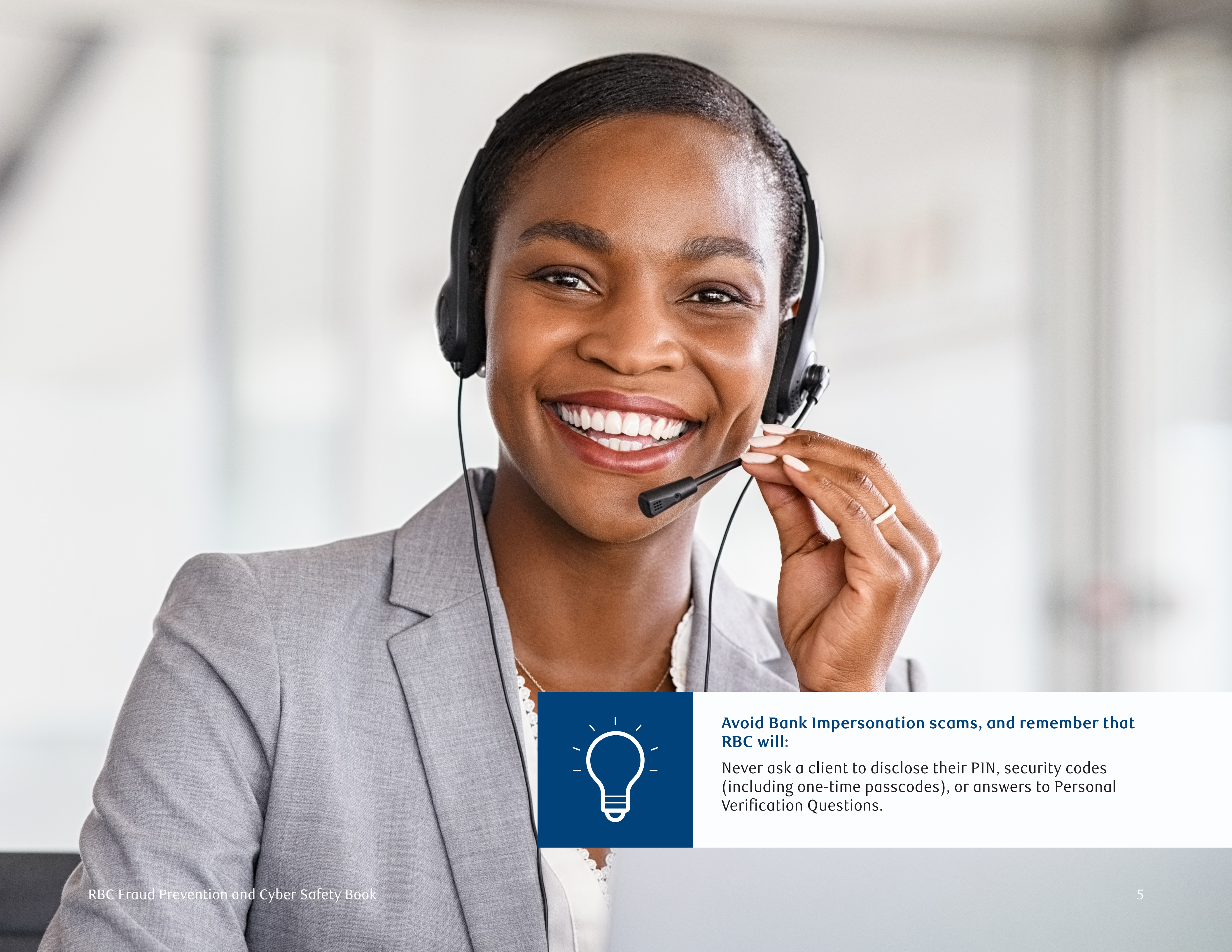
If you choose not to enable auto-deposit, when sending money through Interac e-Transfer, ensure that your security questions are difficult to guess and avoid answers that can easily be found online or through your social media pages, like your pet's name, or your favourite vacation destination. Never send the answer to the security question in the message you add to the transfer.

2. Use a secure internet connection

Steer clear of public Wi-Fi, especially if you're logging into any accounts with private or sensitive information, like your bank account.

3. Use strong, complex passwords

A strong password is critical to protecting your online accounts. Passwords are often the first defence against cyber criminals. They protect personal information, like your bank accounts, health data, or private documents from falling into the wrong hands.



Avoid Bank Impersonation scams, and remember that RBC will:

Never ask a client to disclose their PIN, security codes (including one-time passcodes), or answers to Personal Verification Questions.

Fraud Prevention and Cyber Safety

Protecting yourself and your family in the digital world

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

And while there are many different variations of Cybercrime, here are some prominent types you should be aware of along with ways of countering them.

Password Compromise

A common way scammers get access to your information or break into your online accounts is by guessing your password. By using multiple computers, making billions of guesses per second, criminals can guess even relatively complicated passwords in a matter of hours.
Many of us like to use simple, easy to remember passwords such as the word "password" or the digits "1234". Unfortunately, scammers know this and therefore it's like handing out your house keys and address to strangers.

What You Can Do:

☐ Never share your passwords with anyone.
☐ Don't use your Online Banking password for anything else. While it's best not to re-use any passwords at any time, it's especially important to use extra caution when it comes to sensitive information such as your bank account.
☐ The longer, the better. Experts suggest creating passwords that are at least 12 characters long, ideally 16.
☐ Reset your passwords regularly.
☐ Use multi-factor authentication. While passwords are more secure than no protection, your data is far safer if you combine a password with multi-factor authentication (MFA).

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 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.

What You Can Do:

☐ Never write personal information in an email, this includes account numbers, birthdays, social insurance numbers and other sensitive data.
☐ Don't open attachments or click on links if you don't know the source. If you receive an email with a suspicious attachment, simply ignore the email and delete it.
☐ Be aware of fake email addresses and websites. If an email sounds strange or is written with typos and incorrect grammar — yet claims to be from a legitimate company — it's best to ignore and delete it. Many scammers create email addresses and websites that look authentic but aren't real at all.
☐ Keep your email address safe. Your email address is personal — avoid posting it on public forums or entering it on sites you don't trust. And just because someone at a store asks for it doesn't mean you have to give it out.

Vishing

If you receive a call from someone claiming to be from a reputable source who wants you to share your personal and banking information, it could be a "vishing" scam, a term derived from "voice" and "phishing."

What You Can Do:

☐ Don't pick up if you don't recognize the phone number.
☐ Never give away personal information to someone you don't know.
☐ Beware of grandchild impersonation. This is one of the most prevalent scams around today and has tricked older Canadians out of nearly $10 million last year. If anyone calls claiming to be your grandchild — especially if they're asking you for money, a credit card or a gift card to help with an emergency — don't fall for it. Hang up and call your family directly.

Smishing

Have you ever received a text message from a number you don't recognize asking you to do something, like provide your private or financial information? It could be a smishing scam.

Smishing, a form of phishing, is when a cyber criminal tries to trick you into providing your personal information via SMS (Short Message Service) or a text. The name comes from combining SMS and 'phishing'.

What You Can Do:

☐ Don't click on links sent by numbers you don't recognize.
☐ Avoid acting out of a sense of urgency or emotion.
☐ If the number isn't legitimate, delete the text message from your phone.

Social Engineering

Social engineering is the art of manipulating people so they give up confidential information. Cyber Criminals often use this tactic, which plays on human emotions, to trick their victims into giving them your passwords or bank information or access to your computer to secretly install malicious software.

What You Can Do:

☐ Never providing confidential information or signing in IDs or passwords when responding to an unsolicited email or text.
☐ Avoid acting out of a sense of urgency or emotion.

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.

What You Can Do:

☐ Installing up-to-date anti-virus software.
☐ Removing old applications.
☐ 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.

What You Can Do:

☐ 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.

Identity Theft

Identity theft happens when someone accesses your personal information (such as your name, date of birth and SIN) and uses it to make financial transactions in your name. This could involve accessing your accounts, opening new credit cards, applying for loans or mortgages or writing cheques in your name.

Thieves can get this information anywhere – such as your mailbox, by email, over the phone, from statements you've thrown into the trash, or even from your old computer hard drive.

What You Can Do:

☐ Review your bank account statements regularly; if you see unknown purchases, that could be a sign that your identity has been stolen.
☐ Never share personal information in an email, this includes account numbers, birthdays, social insurance numbers and other sensitive data.
☐ Immediately report lost or stolen credit or debit cards.

Social Media

As social media has gained in reach and popularity among all ages, it has also gained momentum with fraudsters for scams.

While it's relatively easy for scammers to connect with users, staying safe is also easy — as long as you know what to watch for and how to manage your settings.

What You Can Do:

☐ Don't accept friend requests from people you don't know.
☐ Avoid posting or DMing sensitive information like your phone number, address, and even travel information when leaving for vacation.
☐ Max out your privacy settings. Privacy settings are customizable, and it's best to choose options that offer the highest level of security.
☐ Turn off geotagging/location in the device's settings. Geotagging gives cybercriminals, fraudsters and other bad actors the ability to see where you — or your children — are at any given moment.
☐ Watch out for false investments opportunities, especially ones leveraging high-profile endorsers.

Fake Websites

Online scams are nothing new, but they're not going away. Scammers set up fake retailer websites that look like real online retail stores in these cases. The thing is, you won't receive the goods you paid for.

What You Can Do:

☐ Buy from companies or individuals you know by reputation or from past experience.
☐ Make sure you're still on a reputable website when you go to check out and haven't been redirected to a new page.
☐ Be more cautious with sellers located far away or that don't have many reviews.
☐ Regularly check your credit card statements for frequent or unknown charges.

Data Protection

From the in-person checkout at a retail store to an app download, you are constantly asked for your personal data. But you don't have to give it away. It's okay not to share your postal code, email and phone number. It's also wise to think twice why a website or app asks for your info. Your data is precious — it's worth treating it that way.

What You Can Do:

☐ Decline or unsubscribe, these actions reduce the number of people and organizations that store your contact information.
☐ Use Multi-Factor Authentication, as it makes it harder for cyber criminals to steal your information.
☐ Beware of public Wi-Fi.
☐ Keep social media private.

□ Don’t let sites save your information, especially payment information such as credit and debit card credentials.
□ Get familiar with privacy settings.

VPN: Virtual Private Network

A VPN is a Virtual Private Network. When you use a VPN on your device, it securely connects you to an online network. Using a VPN can be one part of keeping information more private each time you use your devices.

What You Can Do:

□ Sign up for a VPN. Download VPN to your device, log in with your created account, and then choose a server from the list of Canadian servers.

Multi-factor Authentication

Sometimes Multi-factor Authentication (MFA) is automatically turned on – but sometimes the choice to use it is yours.

What You Can Do:

□ Use MFA when it’s an option. Most popular platforms offer MFA and you can activate it within your settings.
□ The RBC Mobile app now has 2-Step Verification for added security and protection. 2-Step Verification means we’ll send a message to your chosen trusted device whenever someone tries to sign in from another device. Then, if the person trying to sign in is not you, you can stop them from accessing your account.
□ Turn on Account Alerts to monitor unusual transaction activity.

Public Wifi

Public Wi-Fi is less secure than your private network because you don’t know who set it up or who else is connecting to it.

What You Can Do:

□ Avoid logging into any accounts that hold private or sensitive information.
□ Use a secure and encrypted VPN.
□ Be aware of who is around you and who may be looking over your shoulder.

Phone Settings

Smartphones are smart, but they’re not always secure. When it comes to keeping your smartphone secure, there are two things to consider: protecting the device from loss or theft and protecting the data you’ve stored on it.

What You Can Do:

□ Turn off Bluetooth when you’re not using it.
□ Don’t install - or make sure you uninstall - those nosey apps or any apps you’re no longer using.
□ Turn on the “Find my Mobile” tool so you can locate missing devices and protect data.
□ Enable multi-factor authentication for the sites you visit.

Did you know?

The Canadian Anti-Fraud Centre estimates over 70% of fraud consist of cyber scams.

Cyber Scams

A snapshot of the most common types of scams

Bottom line, scams are on the rise. But some are more popular than others.

Email Scams (Phishing)

55% of respondents experienced a fraud attempt via emails that appear to come from a legitimate source and direct you to a fake website[1].

Phone Scams (Vishing)

In 47% of cases, fraud was reported via a phone call where a fraudster tried to trick them into sharing sensitive information[1].

Text Message Scams (Smishing)

40% of respondents received fraudulent text messages in attempts to trick them into giving away sensitive information[1].

The most effective phishing, vishing and smishing tactics leverage current events (such as Ukrainian relief efforts and COVID-19) or create messages that appear to be coming from trusted organizations, or even people you know.

Here are the most common scams and how to defend against them.

1. Government (federal, provincial, and municipal):

Fake emails, calls and texts from scammers impersonating the Canada Revenue Agency, demanding immediate payment with the threat of arrest or imprisonment.

2. Delivery agencies:

Canada Post and UPS are two of the most commonly impersonated delivery organizations where fraudsters will request payment or information before a delivery can be made.

3. Retail:

For instance, a scammer will impersonate Amazon and reach out to you, claiming there is an issue with a recent order and that you're eligible for a refund. The catch is that to receive your refund, you'll either have to follow a link to another website or provide them with personal information.

4. Health:

Scams related to COVID-19 or other viruses, vaccines and test kits are still circulating.

5. Finance:

You may receive an email that you are locked out of your bank account and must enter your login credentials to unlock it and access your money.

Tip:

Being aware of online scams and knowing what to look for is the key to protecting yourself against cyber criminals. Visit **rbc.com/scamalerts** to view cyber scams currently affecting RBC clients.

Fraudsters are getting more and more creative and it's becoming harder than ever to tell if something's a scam. Fact is, that if you aren't vigilant, it gets very difficult. Your best defense is to take active measures to protect yourself – set up alerts, enable multi-factor authentication, maintain unique passwords, especially for banking. And remember, never share any of your personal financial information.

Kevin Purkiss, Vice President, Fraud Management

Common Scams

Email

Your payment is waiting.
Click to accept: tiny.cc/ylayuz

Text Message

We regret to inform you that our driver couldn't secure a signature for your package. Act promptly to avoid additional delays by completing the rescheduling process. for further assistance, please view: serv1postcanada.imfo

Email

Reset your password:
Click to accept: tiny.cc/ylayuzt

Text Message

Your Netflx membership is on hold. We're having some trouble with your current billing information. To using your account as normally, please follow the instructions by clicking on the link below: Netfix-reactivatemyacount.com

Plan and Manage

Cyber Security Incident Management

Companies of all sizes often make prevention their sole focus when in reality, it's not a matter of if your company will be impacted by a cyber security incident, but when. Mitigating a cyber crisis often comes down to properly managing a cyber incident before, during, and after it unfolds. This starts with a broad view of cyber crisis management and effective planning. Creating a cyber security plan for your business is the first step you can take to help mitigate your cyber risk. While there isn't one plan that will work for every business there are basic security principles that any business can follow, regardless of size.

Building a Cyber Security Crisis Plan

The single most important factor in being able to successfully manage a cyber security crisis is having a plan in place. Planning for a crisis may seem defeatist, but in an evolving digital environment, planning for one is simply another part of having a strong risk management and incident response strategy.

You can enlist your security firm and/or any cyber security personnel within your company to help develop and test the plan, but it must be developed in partnership with the executive and business teams, as cyber security crises are, at their core, a business problem.

A good cyber security crisis plan will have these essential components:

A crisis management team

We often think of cyber as the domain of IT employees, but you'll need a broad selection of skillsets to manage the crisis. Depending on the size of your company, the team may include representation from IT, legal, communications, and operations.

Plans tailored to a variety possible scenarios

Once you've identified the most pressing risks, make a plan for each, and identify the capabilities you'll need to manage them. If you don't have a capability in house, consider how you'll develop it or bring it in in the event of a crisis.

A detailed communication plan

Figure out which stakeholders needs to be notified at which stage, and how. Stakeholders include clients, investors, and partners, and you'll also need to determine how you'll capture and share information with law enforcement and regulatory agencies, if applicable. From a reputational standpoint, regular and transparent communication will allow you to control the narrative and avoid speculation.

A regular review cycle

The cyber crime landscape evolves on a daily basis, and with it the types of threats that your business could face. Therefore, your plan should be regularly revised to incorporate any emerging threats, and it should also be tested regularly to ensure that the plan remains feasible.

A client-first approach

Protecting the client should be a priority reflected in your cyber security crisis plan. This means planning for proactive, frequent, and transparent communication with clients about what happened and how it affects them, and responding to inquiries in a timely and accurate manner.

Getting Started

To help you, we have developed a Cyber Security Crisis Management Template, which you can download here. The information provided will help your business prepare in advance of a crisis, mitigate certain risks, and shorten the length of time it takes to get back on track.

Cyber is just one more risk that businesses need to manage in order to ensure that a cyber security crisis doesn't catch them unprepared. Having a crisis plan in place can mitigate the impact from a legal and reputational standpoint, allow you to act quickly, and ultimately protect your client relationships.

Double down on safety
Think of it as having more than one lock on your door.

> *There is no one size-fits-all solution when it comes to protecting yourself and your business. Cybercrime awareness and education must expand, so everyone has a better understanding on how their actions impact their Family Office's security posture. A security system will only be as strong as its weakest link.*

Adam Evans, CISO & SVP, RBC Global Cyber Security

Plan and Manage: The Checklist

Cyber Security Incident Management

Security Focused Technology Decisions

□ Use Security Focused Operating System
□ Install Antivirus software
□ Install Firewall
□ Up to date software patching
□ Turn off unneeded data sharing
□ Systems/data backed-up
□ Systems/data back-ups stored offsite

Office Network(s)

Separate networks:
□ Change default network details
□ Use strong password
□ Hide essential office network
□ Internet of Things (IoT) devices (e.g., cameras, thermostat, AV equipment, appliances, etc.) on separate network
□ Create guest network (if required)

Each device on network:

□ Up to date software
□ Up to date firmware

Remote Access:

□ Avoid public networks
□ Set-up/use virtual private network (VPN)

Mobile Device Security

□ Download and use the RBC Mobile Banking app
□ Disable Wi-Fi & Bluetooth (when not using)
□ Set strong password and/or biometrics to unlock device
□ Install VPN
□ Install updates immediately
□ Uninstall unused or apps that automatically share data
□ Periodically erase network setting to forget previously used insecure networks
□ Factory reset device before return or service
□ Turn on "Find my phone" feature (allows to remotely wipe data on phone if lost/stolen)
□ Disable developer access (Android only)
□ Schedule regular encrypted backups
□ Configure auto-cloud storage to match comfort level of shared data

Compliance & Privacy (periodic review)

□ Device inventory
□ Device usage reporting
□ Network report
□ Print logs
□ Physical security (e.g., secure areas, locked cabinets, locked screens, document shredding, etc.)

Password Management

☐ Unique passwords for each app/service
☐ Use maximum password length
☐ Avoid common words (e.g., password)
☐ Avoid using passwords with obvious sequential attributes (e.g., Summer2023!)
☐ Enable multi-factor authentication where possible
☐ Consider password manager / physical token / FIDO key for added security

Advance Preparedness

☐ Incident Response Plan
☐ Table top/fire drill exercise

Remember, good security posture is not complicated, but it takes effort to turn it into a habit – a habit that could save you and your business a great deal. Because it's not a matter of "if" but "when" you will experience a cyber incident in our increasingly interconnected, digitized world.

Adam Evans, CISO & SVP, RBC Global Cyber Security

Key Takeaways

How to stay ahead

The best way to defend against cyber crime is through awareness and education.

While you may not be able to stay current with every scam around, being aware of the types of threats and risks that exist can help keep you safe.

Be Cyber Aware:

1. Don't pick up the phone if you don't recognize the phone number. If it's really someone you know on the other end of the line, they'll leave a message or send a text explaining the nature of their call.

2. Don't give away personal information to someone you don't know. Even if they claim to be from a trusted company or agency, hang up if they request personal details from you.

3. Don't open attachments if you don't know the source. If you receive an email with a suspicious attachment, simply delete it.

4. Recognize that legitimate companies and financial institutions don't request account updates or login information via text. Confirm any requests received through text by calling the organization's official number.

5. Be aware of fake email addresses and websites. If an email sounds strange or is written with typos and incorrect grammar – yet claims to be from a legitimate company – it's best to ignore and delete it. Many scammers create email addresses and websites that look authentic – but aren't real at all.

6. On social media, only accept friend and follow requests form people you know.

Awareness and education are key to staying safe. Take a moment to get up to speed on the latest threats and tactics to protect yourself and the people you love.

rbc.com/scamalerts

Some telltale signs are that they will tell you not to tell anybody about it. They'll also find unusual ways for you to get money to them. Maybe they'll suggest you put bitcoin into a specific account. Always remember, if it's too good to be true, it probably is!

Kevin Purkiss, Vice President, Fraud Management

Additional Resources

RBC	• Cyber fraud and Best Practices: www.rbc.com/cyber • Stay informed on the latest scams affecting RBC clients at rbc.com/scamalerts
Canadian Anti-Fraud Centre (CAFC)	www.antifraudcentre.ca
Competition Bureau Canada	www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/home
RCMP Scams and Fraud	http://www.rcmp-grc.gc.ca
Canadian Bankers Association	Fraud Prevention: Canadian Bankers Association (cba.ca)

Report cyber fraud to RBC

If you believe you are the victim of a malware attack, or if you think your accounts have been compromised, visit the Report Fraud to RBC web page for contact information and call us immediately. Our dedicated team of experts can guide you through the appropriate measures that may need to be taken.

Glossary

Business Email Compromise	A scam where messages appear to come from a legitimate source such as a CEO or a high-ranking executive and may demand immediate action such as the transfer of funds or information.
Dedicated Payment Device	Independently managed devices used for a single purpose, such as kiosks, retail checkout, and bank ATMs.
Encryption	A way of scrambling data so only authorized users can understand the information. It helps protect the data on your network.
Firewall	A network security device that monitors traffic to or from your network. It allows or blocks traffic based on a defined set of security rules.
Geotagging	The process of adding geographical coordinates or locations to various media, allowing anyone to see where you are.
Guest Wi-Fi Network	An access point on your network separate from the one your primary devices connect to. A guest network allows internet access for devices that may be more susceptible to viruses without letting them connect to your home network.
Malware	Short for "malicious software," malware refers to software developed by cybercriminals to steal information, damage your saved files, or take control of your computer or device.
Multi-Factor Authentication (MFA)	An electronic authentication method that requires a user to present two or more pieces of evidence to gain access to an app or account. It is sometimes referred to as two-factor authentication or 2FA.
Passphrases	Phrases made up of randomly chosen words that are easy for a user to remember yet hard for a hacker to guess (for example, Delay Elephant Buy).
Password Manager	An encrypted database for passwords, which is unlocked using one master password.

Peer-to-Peer (P2P) Payments	Payment systems that allow users to send and receive money from their mobile devices through a linked bank account or credit card.
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
Remote Access Trojans (RAT)	A program used by intruders to take control of a computer for the purpose of performing malicious activities.
Service Set Identifier (SSID)	The technical term for a Wi-Fi network name.
Smishing	A style of phishing that targets your mobile phone. Smishing uses text messages to lure you into clicking links or downloading attachments that will install malware or try to steal your financial or personal information.
Social Engineering	The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
Spear Phishing	A phishing method that specifically targets an individual. Messages may mimic those from friends or family and contain details about you or the organizations you interact with.
Spyware	Spyware is software designed to enter your computer device, gather data about you, and forward it to a third-party. Spyware can be malicious, or it can be legitimate software that monitors your data for commercial purposes like advertising.
Virtual Private Network (VPN)	A group of computers or networks that work together over the internet to secure and encrypt your communications.
Vishing	Short for "voice phishing," vishing involves defrauding people over the phone, enticing them to divulge sensitive information.

For more cybersecurity content visit:
rbc.com/cyber

Sources:
[1] Canadian Anti-Fraud Centre (CAFC), 2023.

This document is intended as general information only and is 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.