Digital Safety and Scams: Business Edition

How to protect your business, your data, and your bottom line in a connected world

Table of Contents

Why Cyber Security Matters

In today's digital-first economy, businesses of all sizes rely on the internet to serve customers, manage operations, and nurture growth. But that connectivity comes with risk, particularly for small businesses, who may not have the same resources as larger organizations to guard against scams and cyber threats.

The good news is, you don't need to be a tech expert to take action. This guide covers essential cyber hygiene practices, how to spot scams that target businesses, and what to do if your business is affected by fraud or a cyber incident.

Cyber Security Basics: Business Protection Checklist

Strong cyber habits can help protect your systems, data, customers, and reputation. These proactive measures are key to minimizing risk.

☐ **Install security tools for your systems and keep systems and software up-to-date**
The right anti-virus and anti-malware tools can help guard against malicious attacks. Applying updates and patches regularly can help close security gaps and improve system resilience.

☐ **Install a Domain Name System (DNS) firewall**
Firewall software can protect your business network from malicious internet traffic, as firewalls scan network traffic and block unwanted traffic from affecting your network. The Government of Canada's Get Cyber Safe website explains how firewalls provide an extra layer of protection for your devices.

☐ **Create strong, unique passwords and passphrases – and ensure your employees do the same**
Requiring login credentials for all employees and accounts can prevent unauthorized access. Update passwords on a routine basis and never share your credentials with others.

☐ **Back up data regularly**
Consider using secure, off-site storage and maintain both cloud and physical backups. This ensures you can recover critical information should your business be a target of a ransomware or malware attack.

☐ **Use a VPN for remote access**
Virtual private networks (VPNs) encrypt data and secure employee access to your business network.

☐ **Limit data sharing and access**
Restrict employee access based on role to strengthen control over your data. Regularly review who has access to systems and remove access for employees who leave or change roles. Also, disable file-sharing features to reduce exposure.

☐ **Educate your employees**
Employees are often a company's weakest link when it comes to cyber security. Provide practical, on-going cyber awareness training so they can recognize scams and respond appropriately.

☐ **Implement formal cyber policies**
Clear guidelines help ensure employees understand their responsibilities – and know what to do in a crisis.

Spotting Common Scams

Businesses are attractive targets for scammers because they handle valuable data, process large transactions, and involve multiple employees – each a potential entry point for fraud. Knowing the red flags can help your team avoid serious financial and operational consequences.

Social Engineering Scams

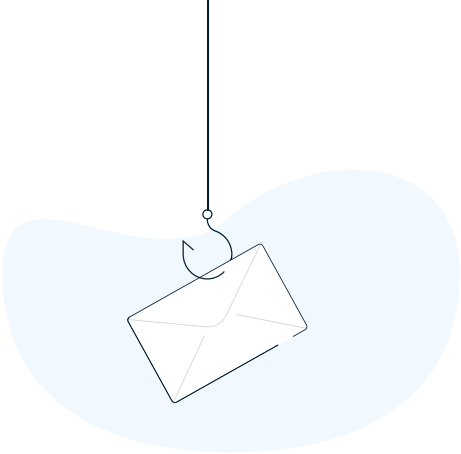
Social engineering scams target the human side of your business – your employees. In these scams, scammers manipulate staff into sharing confidential information or performing an unauthorized action, often by posing as a colleague, vendor, or customer in urgent situations.

Training your team to pause, verify unusual requests, and follow escalation procedures is key to preventing these attacks.

Email Scams (Phishing)

Phishing emails often appear to come from legitimate sources, like suppliers or company leadership. They typically include an urgent request to click a link or download an attachment with the purpose of installing malware or accessing sensitive credentials.

While these scams have become increasingly sophisticated, there are ways to spot them: small inconsistencies in the sender's address, language, or URL can help your team detect a fake.



Ransomware

Ransomware is one of the most damaging cyber threats for businesses. It encrypts your data and demands payment to unlock it. Attacks often begin with a phishing email or an infected file. Keep in mind that even if you pay the ransom, there are no guarantees that the scammer will unencrypt your files or sell the data online.

Regular backups, security software, and employee training are your best defence – and can reduce downtime if you're hit.

Phone Scams (Vishing and Smishing)

Phone scams use voice calls or texts to impersonate vendors, banks, or even government agencies. These scams often rely on urgency or fear to extract sensitive information like account credentials or payment approvals.

Be sure to remind staff to verify all requests independently (i.e., by calling back through a trusted number) before acting.

Bank Impersonation Scams

These scams often begin with a call, text, or email pretending to be from your bank. They may contact staff about a "security breach" or "account issue," requesting login information, one-time passcodes, or even fund transfers to rectify a situation.

These interactions can feel very legitimate and have been successful in tricking employees, especially those with limited cyber security training.

It's worth reinforcing to your team that if they're ever unsure, the safest step is to hang up and call the bank directly using a known number.

AI-Powered Scams

Artificial intelligence allows fraudsters to craft more convincing scams – like cloning voices, writing flawless emails, or creating deepfake video calls. Businesses around the world have fallen victim to fake vendor requests, CEO impersonation scams, and even chatbot scams – all enhanced with AI.

Staying cautious and verifying the identity of the person on the other end of the communication is more important than ever.

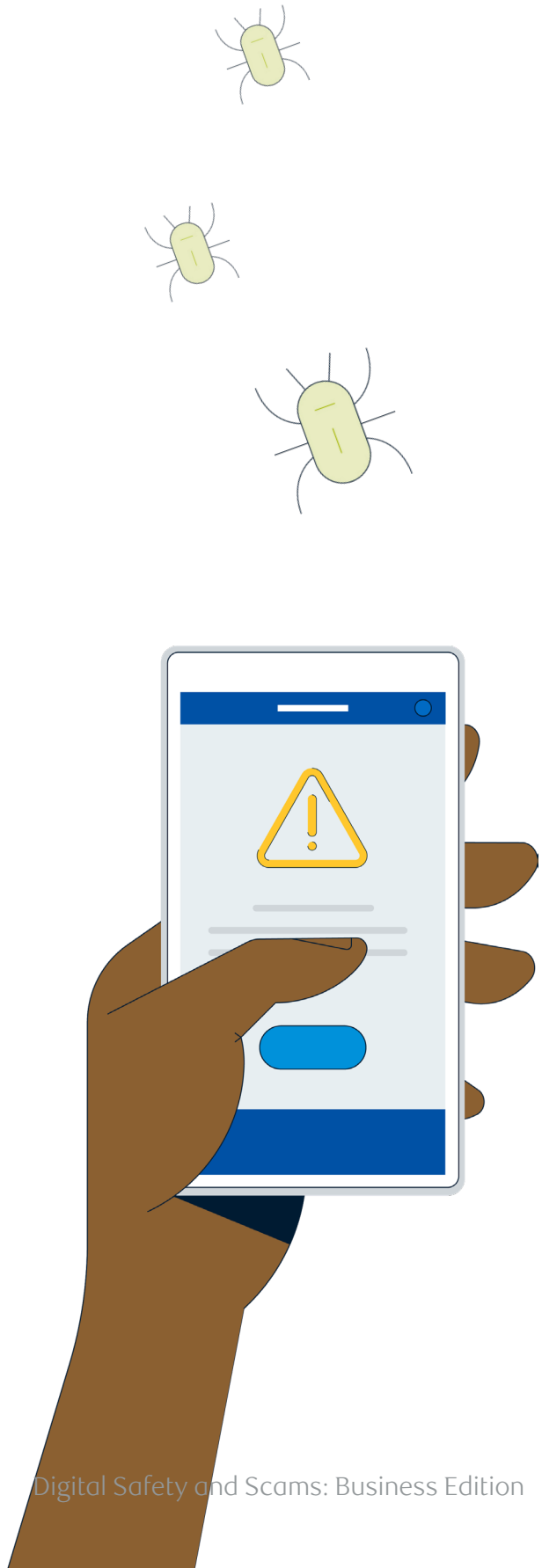
Business Email Compromise and Vendor Email Compromise

Business email compromise (BEC) is a targeted scam where fraudsters hijack or spoof trusted email accounts – often those of executives, suppliers, or internal departments – to request wire transfers, change payment details, or obtain sensitive information. These emails may look completely legitimate and are often timed to match real business activities, like closing a deal or issuing an invoice.

Vendor email compromise (VEC) occurs when a fraudster sends a request that appears to come from an existing supplier. In many cases, they advise of an update to the payment account or beneficiary information on file, to redirect funds into a compromised account. Requests typically include urgency and a request for confidentiality. They are often well-worded, tailored to the business being targeted, and crafted not to raise suspicion.

What makes BEC and VEC so dangerous is that it preys on trust and routine. A well-crafted email can slip past even cautious employees, especially if it appears to come from someone in authority.

Common red flags include urgent payment requests, changes to familiar payment instructions, or unusual language or tone.



Investment and Crypto Scams

Investment and cryptocurrency scams often target individuals through both solicited and unsolicited means. Scammers will lure you in to invest in opportunities (often tied to cryptocurrencies) with a promise of high rates of return in a short amount of time, with little to no risk.

Scammers create fake websites, ads, and might also pose as trusted companies and high-profile individuals – sometimes using deepfake technology to convincingly impersonate someone. They also play the long-game, soliciting via social media platforms, messaging apps, and even dating websites often taking time to build trust. They may share "screen captures" or live "trend graphs" showcasing the progress of the investment. Watch out for red flags such as directions to send e-Transfers to crypto companies, wires, or deposit into Bitcoin ATMs, where the funds are then obtained by the scammer.

Make sure you can directly access your investment account and can independently verify performance. Always do thorough research before investing and remember if an investment opportunity sounds too good to be true, it is likely a scam.

Prevention, Protection, and Recovery

When it comes to cyber incidents, it's not a matter of if your business will be targeted – but when. A well-defined plan can help protect your business from scams, respond quickly, and limit damage.

3 steps to your plan:

1. Create advance procedures

The best way to handle a cyber event is to be ready before it happens. Here are some steps your business can take to prepare.

☐ **Identify key players**
Form a cross-functional crisis management team that includes IT, legal, operations, and communications.

☐ **Map out response plans for likely scenarios**
Think of types of cyber events – like ransomware or data theft – and establish procedures to handle them.

☐ **Develop a clear communication strategy**
Have contact information on hand for your key stakeholders, including clients, partners, regulators, employees, and key technology-based contacts (who may work within or outside your organization), such as your CTO, IT department, and service vendors. Knowing who to contact and how will make for a faster response and transparent communications.

☐ **Test your plan regularly**
As threats evolve, so too should your plan. Revisit, modify, and test it at regular intervals.

2. Establish prevention strategies

Both your business leaders and your employees have a role to play in keeping your organization safe. The following best practices can help keep scams and fraud from making their way into your business.

☐ **Create regular off-site backups**
Backing up your data at a secure, off-site facility – and regularly refreshing that backup with new versions – will help you quickly restore your systems should your data get trapped by ransomware.

☐ **Prioritize patching**
Regularly issue and install updates on every device on your network to eliminate vulnerabilities that may be known to cyber criminals.

☐ **Implement formal security policies**

By establishing formal security policies across your business, employees don't have to guess about security. Mandate the use of strong, unique passwords, utilize multi-factor authentication when available, and limit employee access to only the data that's necessary for their jobs.

☐ **Educate employees**

All it takes is one employee clicking a link or downloading a malicious file to cost your company millions. Train employees about common attacks so they can learn how to spot suspicious emails or unsafe files. In addition, make sure they know who to call in IT if they click a suspicious link or if their computer experiences an attack.

☐ **Prioritize cyber security technology investments**

There are thousands of different cyber security products available that can reduce the risk of cyber attacks. Work with your IT team to identify weak points in your systems so you can strategically invest your time, money, and resources in securing the company and reducing its risk.

3. Have a response plan

For many businesses, the natural inclination is to keep an attack quiet to avoid negative press. In fact, only 9.6 percent of businesses report incidents to the police.* However, this can prevent you from getting the support you need to effectively respond while allowing the criminals to remain free to exploit the next victim.

The next section outlines who to contact in the event of a cyber attack. Be sure to have the information handy so that you can act quickly – and minimize the damage.

Reporting and Response: Who to Contact

Reporting fraud promptly can limit the impact on your business and help prevent similar attacks on others. If your business experiences a scam or cyber incident, here's what to do.

1. Notify your bank

If your business has experienced fraud, your bank can help you protect your accounts and prevent further loss. Contacting them right away means affected accounts or company credit cards can be locked, monitored, and replaced quickly. Your bank also has dedicated fraud specialists who can guide you through next steps and help secure your information.

RBC Clients

If you're an RBC client and have been a victim of fraud, please contact your branch, local office, or call immediately. For general inquiries or comments regarding Privacy and Security, please also call us.

- 1-800-769-2511 (telephone banking)
- 1-800-769-2555 (online/mobile banking)
- 1-800-769-2512 (credit cards)
- 1-800-769-2535 (RBC Express online banking Client Support Centre)
- RBC Bank (Georgia), N.A.: 1-800-769-2553
- TDD/TYY: 1-800-661-1275

If your business is located in the U.S., please also contact your local authorities as well as the FTC (Federal Trade Commission) at 1-877-438-4338.

2. Alert credit reporting agencies

If a fraudster has accessed your company's systems, contact the credit reporting agencies right away. They can place a fraud alert on your file, which makes it harder for someone to open unauthorized accounts in your business's name. It's also a good idea to request a copy of your credit report and review it for suspicious activity.

There are two major credit bureaus: Equifax and TransUnion. It's best to contact both, as they operate independently and may not share information.

Canada:

TransUnion
1-877-525-3823
transunion.ca

Equifax
1-877-323-2598
equifax.ca

United States:

TransUnion
1-800-888-4213
transunion.com

Equifax
1-800-685-1111
equifax.com

Experian
1-888-397-3742
experian.com

International (British Isles):

Experian
+44-844-481-8000
dialing from outside the UK

0844-481-8000
dialing locally within the UK
experian.co.uk

Equifax
equifax.co.uk
(all contact is online, unless someone is a member of the Equifax service)

3. Contact law enforcement and anti-fraud agencies

Reporting a cyber attack to authorities can help ensure you get the support your business needs to respond – and it can help them in their criminal investigations.

Law enforcement
Local or federal law enforcement has trained specialists who can help provide a rapid response and coordinate with other government departments for assistance. They will also be crucial in collecting evidence and conducting a criminal investigation so that the attackers can be brought to justice.

The Canadian Anti-fraud Centre (CAFC)
The Canadian Anti-fraud Centre (CAFC) is a national police service that gathers intelligence on fraud across Canada and assists Police of Jurisdiction with enforcement and prevention efforts. Report online at reportcyberandfraud.canada.ca, or call toll free: 1-888-495-8501

The Canadian Centre for Cyber Security
The Cyber Centre works with law enforcement, businesses, and the public sector to lead the government's response to cyber security events. Email contact@cyber.gc.ca or call toll free: 1-833-CYBER-88 (1-833-292-3788)

If you do business outside of Canada, contact the following organizations:

United States:
• Federal Trade Commission (FTC): reportfraud.ftc.gov
• FBI Internet Crime Complaint Center (IC3): ic3.gov

United Kingdom:
• Action Fraud (UK's national reporting centre): actionfraud.police.uk

Cyber threats are a reality for businesses of all types and sizes. But, with the right processes, tools, and awareness, they don't have to mean an immediate crisis. By putting strong safeguards in place, training your team, and preparing for the unexpected, you can reduce your risk and respond with confidence if an incident occurs.

Cyber security isn't solely an IT issue – it's a business imperative. The more prepared your team is, the harder it is for scammers to cause damage or disruption.

Notes

Checklist

- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐

For more cybersecurity content visit: rbc.com/cyber

Sources: Public Safety Canada, Profile of Canadian Businesses Who Report Cybercrime to Police.

Created: October 2025
Last Updated: December 2025