RBC® Be Cyber Aware

Little Book of Big Scams

A Guide to Fraud Prevention for Small to Medium-Sized Businesses

rbc.com/cyber/business

RBC®

Cyber security is a shared responsibility. We all have a role to play. From co-owners and managers to employees and contractors – it takes all of us working together to strengthen our cyber security defence.

1/5

of Canadian businesses reported that cyber security incidents affected their operations in 2017

41%

of large businesses reported cyber security incidents

28%

of medium businesses reported cyber security incidents

19%

of small businesses reported cyber security incidents[1]

Contents

[1] Statistics above sourced from Canadian Survey of Cyber Security and Cybercrime, 2017

Message from
Laurie Pezzente
Senior Vice President of
Global Cyber Security &
Chief Security Officer,
Royal Bank of Canada (RBC)

As a small or medium business owner, it's easy to think your organization is too small to warrant the attention of cyber criminals. However, smaller businesses are attractive to cyber criminals for several reasons: they often have limited technology resources, linkages to larger companies, information of value, and money.

As the digital landscape evolves, cyber criminals are adaptive in the types of scams they use, often taking advantage of new ways of communicating, timely events in the news, and new technology. In most cases, they attempt to create convincing stories to get you or your employees to send them money or valuable information.

To help our business clients, RBC has partnered with the Toronto Police Service to identify the most common cyber security threats impacting small and medium businesses. With The Little Book of Big Scams we hope to increase your awareness of cyber threats and help you avoid the scams currently affecting businesses like yours. Inside you'll find best practices and simple steps you can take to protect yourself, your company, and your employees.

RBC is committed to helping our clients and their businesses stay secure online.

Visit rbc.com/cyber/business for more ways to get cyber security working for you!

Message from
Shawna Coxon
Deputy Chief,
Toronto Police Service

I've personally seen the devastating effects cybercrime has on people and businesses. It's not just about stealing information or other assets – it's about the impact of having your personal life or business taken over by a criminal. Trying to rectify things can be overwhelming, and expensive. For a small business, we know this can be particularly difficult to manage. That's why the Toronto Police Service is partnering with the Royal Bank of Canada to keep you informed. We know that when it comes to cybercrime, knowledge can help prevent you from becoming a target.

Cybercrime is a growing concern for small and medium-sized businesses. In 2017, more than 1/5 of Canadian businesses were affected by cyber-security incidents that impacted their operations. Unfortunately, only 19% of those businesses reported the incident to a police service. We want you to know you're not alone. We want to work with you to help keep you safe.

5 Things to Do Right Now to Ensure Your Business Is Cyber Safe

Improve cyber security in your organization by adopting these five simple best practices.

1. Regularly back up data off-site.

Businesses hold valuable information that cyber criminals are looking for, like employee and customer records or financial information. Consistently back up your data so if your company is ever attacked by ransomware, you can minimize the impact. The best way to back up files is by using a secure off-site system that continuously creates new versions of all of a company's data.

2. Implement formal security policies.

Establishing security practices and policies, and enforcing them, is essential to protecting your systems. Protecting the office network should be on everyone's mind since those who use it can be a potential target for attackers. Explain security practices and policies to employees to help them understand why they are in place, how they apply to them and what the potential risks are, to them and the business, if they are not followed.

3. Keep your software up to date.

Software and hardware manufacturers routinely issue updates and what are called “patches” to improve security. Hackers, along with malicious programs or viruses, find weaknesses in software (called vulnerabilities) that they exploit to access computers, smartphones or tablets. Installing updates fixes these vulnerabilities and helps keep these devices secure. For optimal security, every device at a small business must download and install all updates and patches on a regular basis.

4. Develop an incident response plan.

An incident response plan contains the instructions and procedures your business can use to identify, respond to, and mitigate the effects of a cyber incident. The plan should indicate who is responsible for handling incidents, as well as relevant contact information for communicating with external parties, stakeholders, and regulators. Review the plan quarterly and make updates accordingly.

5. Educate your employees.

Teach your employees about cyber threats and the different ways cyber criminals can infiltrate your systems. Show them how to protect the business’s data by training them on how to recognize the signs of a breach and how to stay safe while using the company’s network. If your employees understand these threats, they can help avoid them.


INVOICE
$
$
$

Fake Invoice Scams

Cyber criminals often target small and medium businesses, non-profits, municipalities, and other small organizations with fake invoices hoping to trick them into redirecting payments to an alternate, fraudulent account.

An employee may receive an email from a company they do business with about an invoice that's overdue, telling them to pay immediately or they will be charged a high-interest fee. Or the email may indicate that they have recently switched banks and prompt them to redirect payments to the "new" account number.

At first glance, many of these “invoices” appear to be legitimate bills, and may include threatening language or confusing legal jargon that creates a false sense of urgency to pressure recipients to make quick payments.

To protect your business, ensure all employees handling payments for your business always:

- **Validate** new payment instructions received via email – even if the email is internal.
- **Pick up the phone,** whenever possible, and speak directly with the individual requesting the transfer.
- **Contact** the vendor or client directly to confirm any requests for payment method changes, validating the changes are legitimate before processing.
- **Carefully review** all payments before they are sent and ensure all correspondence is validated and documented in a unified way across your business.

Incorporating these simple security safeguards in your payment process can go a long way to help prevent becoming a victim.

Protect Your Business

BE AWARE
Employees responsible for processing payments should remain vigilant and watch for changes to payment instructions. If you are suspicious about whether a supplier has truly changed their bank details, call them directly to confirm the bank details over the phone.

BE CAUTIOUS
Review all invoices closely. Never pay an invoice unless you know the bill is for items that were actually ordered and delivered. Tell your staff to do the same.

BE SUSPICIOUS
Remember that email addresses and websites that look legitimate are easy for scammers to fake. Stop and think about whether it could be a scam before you click.

BE PROACTIVE
Before doing business with a new company, search the company's name online with the term "scam" or "complaint." Read what others are saying about that company.

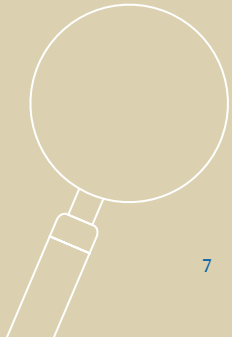
Spot the Signs!

Creates a sense of urgency. Beware of unsolicited emails from individuals or financial institutions presenting an urgent situation requiring immediate attention.

Imitates someone or a supplier you trust. They make themselves seem believable by pretending to be connected with a company you work with.

Contains malicious links and attachments. Be wary of clicking on any links or attachments; they can contain viruses and spyware.

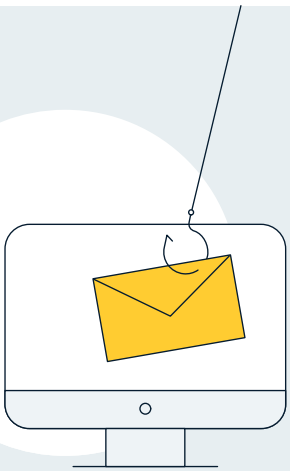
If you suspect a scam always report it!
Go to pages 16 and 17 for more information.



Executive Email Scams

Email scams have been around since the start of the Internet. What's different now is that cyber criminals target their scams to specific individuals by impersonating a senior executive, like a CEO or a CFO within an organization, thereby increasing the chances of someone taking the bait.

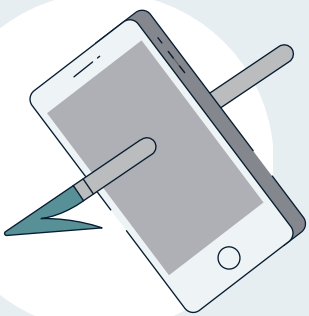
While there are many scams out there that target senior executives, two in particular are more common among small and medium-sized businesses: business email compromise (BEC) and spear-phishing.



Business Email Compromise (BEC)

According to the Canadian Anti-Fraud Centre (CAFC), BEC fraud has cost businesses worldwide, including Canadian businesses, more than $5 billion.

BEC fraud is an exploit in which the criminal impersonates a senior executive at a company, either by gaining access to their corporate email account or by creating a fake one. Through the use of social engineering tactics and research, often through social media, the criminal will craft credible emails and send them to someone within the company who likely has the authority to move money in hopes of tricking them into transferring money to a fraudulent account.



Spear-phishing

Spear-phishing is an email spoofing scam where criminals target a specific organization or employee with tailored messages to gain unauthorized access to sensitive information, funds, or computer systems.

Criminals gather information – typically via social networking sites – about their targets, like email addresses, job titles, interests, etc., and use it to send convincing, but fraudulent, emails.

Protect Your Business

BE AWARE
Educate your employees about these types of scams and advise them to be skeptical of urgent or suspicious requests made in an email.

BE CAUTIOUS
Be mindful of what you share on social networking sites. Criminals can use these sites, and your website, to gather information about you that they can repurpose to target your company.

BE SUSPICIOUS
Always check order details, confirm the validity of the customer, and verify the information on invoices before transferring any funds.

BE PROACTIVE
Don't rely on email to coordinate fund transfers. Have an additional communication process in place that requires face-to-face communication or a phone call to verify the request is legitimate.

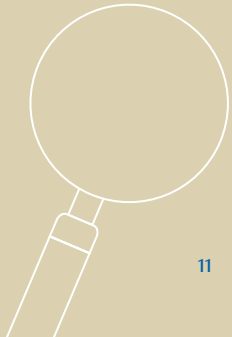
Spot the Signs!

The email looks like it comes from a senior executive, like a CEO or a CFO.

The request sounds urgent and highly confidential. Targeted recipients are typically asked to open a malicious attachment or click on a link that takes them to a spoofed website where they are asked to provide passwords, account numbers, and access codes.

Authentic-looking email addresses. Criminals register domain names that look similar to the target domain such as @yourcompany1.com instead of your real company domain of @yourcompany.com. With these fake domains, scammers can look up company executives and use their real names to make the emails even more convincing.

If you suspect a scam always report it!
Go to pages 16 and 17 for more information.



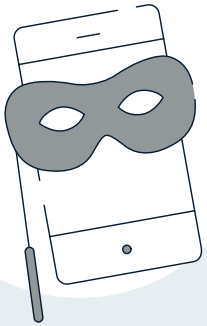
Online Extortion Scams

According to Statistics Canada, roughly 40% of cyber-attacks involving businesses in 2017 involved an attempt to steal money or demand a ransom.[1]

Online extortion is the act of intimidating an individual or company to pay a "ransom" in exchange for gaining back access to stolen digital assets. These assets could include anything related to the victim's personal information, business operations or financial interests, such as documents and database files.

Online extortion can come in different forms: ransomware, online blackmail, and even phishing. Anyone can fall victim to an online extortion scam.

[1] Statistic above sourced from Canadian Survey of Cyber Security and Cybercrime, 2017



Online Blackmail

In most cases, these scams involve a victim receiving an email threatening to reveal explicit photos or videos of the victim that could potentially tarnish their reputation, unless they send money or comply with the criminals' specific demands.

The email may claim that the sender has control of your monitor and webcam, and recorded both you and the explicit material. The criminals seek to embarrass you with the idea of a video or photo, and hope to scare you into paying without thinking.

Ransomware

In 2016-2017, Canadian small to medium-sized businesses lost $5.7 million due to ransomware attacks.[1]

Ransomware is a form of malicious software (malware) that enables cyber criminals to remotely lock down files on your computer or mobile device. The criminals will use the ransomware to extort money from you before they restore your access to the files.

There are a number of ways a computer can be infected by ransomware, but it most commonly involves the victim clicking on a malicious link or attachment received through a phishing email. Once infected, victims will see a ransom note, which is designed to scare or extort them into making a payment.

[1] Datto's Canadian State of the Channel Ransomware Report

Protect Your Business

BE AWARE
Invest in security systems to keep your office networks, computers, and mobile devices secure. Update your security software, change passwords, and back up data regularly. Store the back-ups off-site and offline.

BE CAUTIOUS
Do not open emails, attachments or click on links in emails that are unsolicited or from unknown senders.

BE SUSPICIOUS
If you do receive one of these emails, do not panic, do not respond, and do not send money. Mark the email as phishing and alert your local authorities.

BE PROACTIVE
Ensure all your online accounts are protected with strong, unique passwords, and enable two-factor authentication where possible. If you think your account has been compromised or your password revealed, change it immediately.

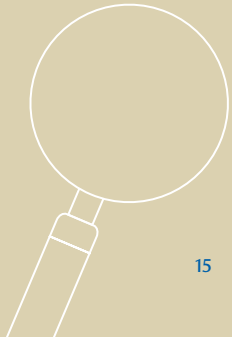
Spot the Signs!

The message sounds intimidating and evokes a sense of fear and panic. For instance, you may receive an email that reveals your password, indicating that a cyber criminal hacked into your computer.

The target is given a short period of time, typically 24 to 72 hours, to pay before the "private key" is destroyed and the files are lost forever.

Payment demands are usually in the hundreds and can be requested by Bitcoin, UKash, Green Dog or other digital payment systems.

If you suspect a scam always report it!
Go to pages 16 and 17 for more information.



Report Cyber Fraud to RBC

RBC will never proactively ask you to verify personal or financial information in an email, over text,or on the phone.

Contact RBC immediately if you believe your identity or personal information has been stolen, or if you think your accounts have been compromised. Our dedicated team of experts can guide you through the appropriate measures that may need to be taken.

RBC Express® online banking Client Support Centre
1.800.769.2535

24/7 Business Helpline
1.888.830.9751

Telephone banking
1.800.769.2511

Online/mobile banking
1.800.769.2555

Credit cards
1.800.769.2512

RBC Bank (Georgia), N.A.
1.800.769.2553

TDD/TYY
1.800.661.1275

Email & Website Fraud

If you believe your confidential information has been stolen or obtained by a fraudulent party either online, by telephone or through any other means, call us immediately.

For phishing emails, please notify us by forwarding the suspicious email to **phishing@rbc.com** for analysis. Please note that phishing@rbc.com is an automated mailbox for reporting phishing and website fraud only – we are unable to provide responses from this mailbox.

If you require a response, please call one of the phone numbers listed above and speak with a representative.

To report fake websites posing as RBC company websites, send an email to **phishing@rbc.com** with the subject "Fake RBC website." Remember to copy and paste the full URL (website address) in the body of the email. For tips to help you spot phishing emails and fake websites, visit **rbc.com/cyber**.

Stay informed on the latest cyber scams affecting RBC clients.
Visit rbc.com/cyber/alerts for more information.

Reporting Advice from the Toronto Police Service

Most Canadian businesses do not report cyber security incidents to law enforcement agencies. Toronto Police Service recommends contacting your local law enforcement to file a report about the fraud or scam. Please remember that every report counts and is a valuable tool for investigators. Make sure you get a report number for reference.

Contact the following organizations as appropriate:

To report cyber incidents or fraud, contact the Canadian Anti-Fraud Centre (CAFC) at 1.888.495.8501 or visit www.antifraudcentre.ca.

Alternatively, you can also "Report an Incident" online through the new, easy to use Fraud Reporting System (FRS).

Critical infrastructure, businesses and provincial/territorial/municipal governments should immediately report the incident to the Canadian Cyber Incident Response Centre (CCIRC) or via email to ps.cyberincident.sp@canada.ca.

CCIRC will assist in mitigation and prevention.

For identity theft issues (PIPEDA), contact the Privacy Commissioner of Canada at 1.800.282.1376, or www.priv.gc.ca for advice and assistance.

Reporting breaches to the Office of the Privacy Commissioner of security safeguards involving personal information is mandatory under the "Personal Information Protection and Electronic Documents Act."

Note: Quebec, British Columbia and Alberta have separate privacy laws, similar to PIPEDA. In these provinces, please contact your Provincial Commissioner.

If your federally issued ID (e.g. SIN or passport) was compromised, call Service Canada at 1.800.O.Canada.

If you believe your driver's licence or health card was compromised, contact your provincial/territorial ministry of transportation/health.

Cyber Security Industry Associations

Cyber security industry associations are a good source for more in-depth information and advice on cyber security for small and medium businesses. They can also provide recommendations on service providers in your area if outside help is needed.

Canadian Cyber Threat Exchange
https://cctx.ca/membership/

Information Systems Audit and Control Association (ISACA)
www.isaca.org/membership/Pages/default.aspx

Information Systems Security Certification Consortium, Inc. (ISC2)
www.isc2.org/chapters/Default.aspx

Information Systems Security Association (ISSA)
www.issa.org/?page=ChaptersContact

RBC® Be Cyber Aware

⚠ Remember!

Having an incident prevention, response, or recovery plan in place can help you be prepared for a cyber incident. To help you, please visit RBC's website for the Cyber Security Crisis Management Template.

To learn more, visit
rbc.com/cyber/business

VPS106325

124144 (12/2019)