



BUILT FOR
SMALL
BUSINESSES

5 – 250
EMPLOYEES



BE SMART. BE SAFE. BE READY.

SMALL BUSINESS CYBER ROAD TRIP

Navigate today's threats.
Prepare for tomorrow's **AI risks**.

A practical guide to help small businesses
build cyber resilience, protect what matters,
and stay ahead.



PROTECT

Your Business



EMPOWER

Your Team



PREPARE

For What's Next



UNDERSTAND
COMMON SCAMS



BUILD STRONG
FOUNDATIONS



PREPARE FOR
AI-POWERED THREATS



PRACTICE WITH
YOUR TEAM



STAY READY.
STAY SECURE.



CYBERSECURITY IS A TEAM EFFORT.
TOGETHER, WE CAN BUILD A SAFER DIGITAL FUTURE.

LET'S HIT THE ROAD.
YOUR JOURNEY STARTS NOW.



1

WELCOME TO THE JOURNEY

WELCOME TO THE JOURNEY

Cybersecurity isn't just an IT problem—it's a business priority. Small businesses are big targets for cybercriminals because they often have valuable data but fewer resources and protections.

This guide will help you build strong foundations, understand today's threats, and prepare for tomorrow's **AI-powered risks**.

A SECURE
BUSINESS IS A
STRONG BUSINESS.



PROTECT
YOUR DATA



PROTECT
YOUR TEAM



PROTECT
YOUR REPUTATION



PROTECT
YOUR FUTURE



THE REALITY: 60% of small businesses close within 6 months of a major cyberattack.

Source: U.S. National Cyber Security Alliance

QUICK SELF-ASSESSMENT

Where is your business on the road to cyber resilience?
Check the box that best describes **your business today**.

AREAS TO CONSIDER



NOT YET

We haven't started.



IN PROGRESS

We're working on it.



YES

We've got this!



We use strong passwords and multi-factor authentication (MFA).

☐
☐
☐


Our team knows how to spot phishing and scams.

☐
☐
☐


We back up our important data regularly and test our backups.

☐
☐
☐


We have a plan for what to do if we experience a cyber incident.

☐
☐
☐


We understand the risks of AI tools and know how to use them safely.

☐
☐
☐


**EVERY JOURNEY STARTS
WITH A CLEAR VIEW.**

Use this assessment as your starting point. You'll revisit it at the end of the guide to see how far you've come!

YOUR ROADMAP TO CYBER RESILIENCE

Great journeys have a plan. Use this roadmap to guide your team through the essential steps to strengthen your business and prepare for what's ahead.

**EACH STOP BUILDS CONFIDENCE.
EACH MILE MAKES YOU STRONGER.
LET'S HIT THE ROAD.**



**A SAFER BUSINESS.
A STRONGER FUTURE.**
Let's build it together.



**STOP
1**

BUILD THE BASICS

Understand common scams targeting small businesses and what you need to protect.

PAGES
3-4



**STOP
2**

SECURE YOUR BUSINESS

Strengthen passwords, devices, and everyday habits that keep you safe.

PAGES
5-6



**STOP
3**

PROTECT COMMUNICATIONS

Spot phishing, invoice scams, and payment fraud before they impact you.

PAGES
7-8



**STOP
4**

UNDERSTAND AI RISKS

Explore AI tools, new threats, and how attackers are using AI today.

PAGES
9-10



**STOP
5**

VERIFY & RESPOND

Learn verification steps, deepfake risks, and how to respond with confidence.

PAGES
11-12



**STOP
6**

PREPARE & RECOVER

Build backups, create a response plan, and know what to do if something happens.

PAGES
13-14



**STOP
7**

BUILD A STRONG CULTURE

Make cybersecurity a team effort and keep improving every day.

PAGES
15-16



**YOU'VE REACHED
YOUR DESTINATION!**

A more resilient business.
A more secure future.

YOUR PROGRESS TRACKER

Check off each stop as you go. Every stop you complete brings you closer to your goal.



**STOP 1
BUILD THE BASICS**

☐


**STOP 2
SECURE YOUR
BUSINESS**

☐


**STOP 3
PROTECT
COMMUNICATIONS**

☐


**STOP 4
UNDERSTAND
AI RISKS**

☐


**STOP 5
VERIFY &
RESPOND**

☐


**STOP 6
PREPARE &
RECOVER**

☐


**STOP 7
BUILD A STRONG
CULTURE**

☐


**FINISH STRONG.
STAY SECURE.**

Revisit this guide anytime
to keep your business
on the right path.



STOP
1

BUSINESS BASICS BOULEVARD



PROTECT WHAT MATTERS MOST

Cybercriminals know small businesses are busy, resource-strained, and often less protected—that's why you're a prime target. Understanding common scams is the **first step** to stopping them.

STRONG FOUNDATIONS
LEAD TO A SAFER
BUSINESS.



COMMON SCAMS TARGETING SMALL BUSINESSES



PHISHING EMAILS

Fake emails that look real, tricking you into clicking links or sharing sensitive information.

Example: "Your account will be locked" unless you verify."



CEO / PAYMENT SCAMS

Attackers impersonate executives or trusted vendors to trick you into making urgent payments.

Example: "Please wire payment today—confidential."



FAKE INVOICES

Fraudulent invoices that look legitimate but change bank details or amounts.

Example: Slight changes to vendor emails or invoice numbers.



TECH SUPPORT SCAMS

Scammers pretend to be from Microsoft, your bank, or an IT provider to gain remote access or payment.

Example: "We detected a virus—call us now."



LOYALTY / PRIZE SCAMS

Too-good-to-be-true offers designed to steal your information or install malware.

Example: "Claim your reward now!"



HAVE YOU SEEN THIS?

Check the scams your team has encountered or noticed. Use this as a starting point for conversations and training.

	✓ WE'VE SEEN IT	? NOT SURE	✗ NOT YET
 SUSPICIOUS EMAILS Emails asking for passwords, account verification, or urgent action.	☐	☐	☐
 UNEXPECTED PAYMENT REQUESTS Requests from executives or vendors to send money or gift cards.	☐	☐	☐
 INVOICE CHANGES Unexpected changes to bank details or payment instructions.	☐	☐	☐
 UNSOLICITED TECH SUPPORT CONTACT Calls or pop-ups claiming to fix issues or remove viruses.	☐	☐	☐
 UNREAL OFFERS OR PRIZES Messages promising prizes, refunds, or special deals.	☐	☐	☐
 UNKNOWN ATTACHMENTS / LINKS Unexpected attachments or links from people you don't know.	☐	☐	☐



DISCUSS WITH YOUR TEAM!

Share examples, discuss what happened, and learn from each other.



WHY IT MATTERS

A single click or payment can lead to:

- Financial loss and fraud
- Data breaches and downtime
- Damage to your reputation
- Loss of customer trust

**AWARENESS TODAY.
PROTECTION TOMORROW.**





KNOW YOUR BUSINESS ASSETS

YOU CAN'T PROTECT WHAT YOU DON'T KNOW.

Every business relies on assets—things that help you operate, serve customers, and grow. If these assets are lost, stolen, or disrupted, your business could face serious consequences. Identify what matters most so you can protect it.



**YOUR ASSETS.
YOUR BUSINESS.**

TYPES OF BUSINESS ASSETS



INFORMATION

Data, customer records, financial information, IP and documents.



PEOPLE

Employees, contractors and partners.



DEVICES

Computers, phones, tablets, servers and peripherals.



SYSTEMS & SOFTWARE

Operating systems, applications, cloud services and tools.



FACILITIES

Office space, equipment and physical locations.



THIRD PARTIES

Vendors, suppliers and service providers.

ASSET INVENTORY WORKSHEET

List the key assets your business relies on. Be as specific as possible. Then rate how critical each asset is to your operations.

ASSET CATEGORY (Choose from above)	DESCRIPTION OF ASSET (Be specific)	EXAMPLES (e.g. QuickBooks server, employee laptop, customer list)	OWNER / RESPONSIBLE PERSON	CRITICALITY (Circle one)
				1 2 3 LOW MEDIUM HIGH
				1 2 3 LOW MEDIUM HIGH
				1 2 3 LOW MEDIUM HIGH
				1 2 3 LOW MEDIUM HIGH
				1 2 3 LOW MEDIUM HIGH
				1 2 3 LOW MEDIUM HIGH

CRITICALITY GUIDE

How critical is this asset to your business?

- 1 LOW**
Loss or disruption would cause minor inconvenience.
- 2 MEDIUM**
Loss or disruption would impact operations and productivity.
- 3 HIGH**
Loss or disruption would stop critical business functions or cause significant financial or reputational damage.



WHAT'S NEXT?

Once you know your critical assets, you can focus on the biggest risks and strongest protections.

Which 3 assets are most critical to your business?

1

2

3



TIP

Review this list regularly. As your business grows, your assets and risks change.





PASSWORD PARKWAY

STRONG PASSWORDS. STRONGER PROTECTION.

Weak passwords are one of the easiest ways for attackers to break in. Strong passwords, multi-factor authentication (MFA), and password managers create powerful layers of defense.

Make it strong. Make it unique. Make it yours.



3 ESSENTIAL HABITS FOR A STRONGER BUSINESS



STRONG PASSWORDS

Use long, unique passwords with a mix of upper/lowercase letters, numbers, and symbols.

WHY IT MATTERS:

Makes it much harder for attackers to guess or crack your passwords.



MULTI-FACTOR AUTHENTICATION (MFA)

Add an extra step to verify your identity—such as a code from your phone, an app, or a fingerprint.

WHY IT MATTERS:

Even if your password is stolen, attackers can't get in without the second factor.



PASSWORD MANAGERS

Store and generate strong, unique passwords for all your accounts in one secure place.

WHY IT MATTERS:

Helps you keep track of passwords safely and saves time.

PASSWORD SCORE ACTIVITY

Rate the passwords below using the scoring guide. Then write one action you can take to make them stronger.

PASSWORD EXAMPLE	YOUR SCORE (1-5)	WHY THIS SCORE?	HOW I CAN IMPROVE IT
1 Welcome123	1 2 3 4 5		
2 P@sswOrd!	1 2 3 4 5		
3 Summer2024\$\$	1 2 3 4 5		
4 Blz7#qLk9\$TmPz	1 2 3 4 5		
5 r3ady\$3tCyb3r26!	1 2 3 4 5		

SCORING GUIDE

- 5 EXCELLENT**
Long, unique, complex. Great job!
- 4 GOOD**
Strong, but could be stronger or longer.
- 3 FAIR**
Could be cracked with time or tools.
- 2 POOR**
Weak and easy to guess or crack.
- 1 DANGEROUS**
Very weak. Change it immediately!



TIP

Aim for at least 14 characters. Avoid personal info, common words, and reused passwords. Turn on MFA wherever possible—and use a password manager to make it easy.



NEED HELP CHOOSING A PASSWORD MANAGER?
Scan to see our top picks.



STOP 2.5 TEAM PIT STOP

STRONG TEAMS. STRONGER DEFENSE.

Cyber threats move fast—so should your team. Good teamwork, clear communication, and shared habits help stop problems before they stop you.

Check in. Speak up. Back each other up.
That's how we keep business moving.



TEAM HABITS THAT KEEP US AHEAD.

- ✓ COMMUNICATE OPENLY
- ✓ VERIFY BEFORE YOU ACT
- ✓ REPORT EARLY



TEAM HABITS IN ACTION

These everyday habits help your team prevent, detect, and respond to security risks—together.



COMMUNICATE OPENLY

- Share concerns and ask questions.
- No issue is too small to speak up about.



VERIFY BEFORE YOU ACT

- Double-check requests, links, and information.
- If in doubt, verify through a trusted channel.



REPORT EARLY

- Report suspicious activity right away.
- Early reports stop attacks from spreading.



LOOK OUT FOR EACH OTHER

- We're stronger when we watch out for each other.
- Call it in, not out.



LEARN & IMPROVE TOGETHER

- Review what happened and what we can do better.
- Small improvements build big resilience.



TEAM CHECK-IN

Use this quick check-in to reflect on how your team works together to stay secure.

DISCUSSION QUESTION	OUR TEAM NOTES
 What's one security habit our team does really well?	
 Where do we have room to improve?	
 What's one action we can take this week to strengthen our team's security?	

SCORING GUIDE

- 5 EXCELLENT**
We work together seamlessly to stay secure.
- 4 GOOD**
We communicate and support each other.
- 3 FAIR**
We're improving, but not consistent yet.
- 2 POOR**
We rarely talk about security as a team.
- 1 DANGEROUS**
We don't look out for each other.



TIP

Great teams don't just react to problems—they prevent them. Keep the conversation going and make security everyone's game.



TOOLS TO HELP YOUR TEAM SUCCEED

Scan to access communication templates, reporting guides, and team resources.



EMAIL EXPRESSWAY SPOT THE PHISH

Phishing emails can look real, but they're designed to trick you. Learn the key red flags before you click, share information, or make a payment.

BEFORE YOU CLICK, CHECK:



SENDER

Do I recognize the address?



URGENCY

Are they rushing me?



REQUEST

Are they asking for money, information, or a login?



LINK

Do I know where it actually goes?



A CLOSER LOCK

Suspicious email address (not your company)

Mon 9:14 AM

From: HR Department <hr-update@payroll-secure.com>

To: you@yourbusiness.ca

Subject: Action Required: Update Your Payroll Information

Creates a sense of urgency

Hello,

Your payroll information needs to be updated immediately to avoid a delay in your next payment.

Rushing you to take action

Please click the link below to verify your details:

Update My Information

Link may go to a fake website

Thank you,
HR Department



**WHEN IN DOUBT,
VERIFY ANOTHER WAY.**

Contact the person or organization directly using a trusted phone number or website — not the details in the email.

PAYMENT DETOUR BEFORE YOU PAY

Scammers often target payments with fake invoices, changed banking details, or urgent requests from trusted contacts.

COMMON PAYMENT SCAMS



FAKE INVOICES

Look real but ask you to send money to scammers.



CHANGED BANKING INFO

You receive new account details out of the blue.



CEO OR VENDOR REQUESTS

Urgent payment requests, often outside normal processes.



LOOKS REAL

Uses real logos, branding and familiar language to trick you.

VERIFY
BEFORE **YOU PAY.**

SAME REQUEST?
A QUICK CHECK CAN
STOP FRAUD.



A CLOSER LOOK

Can you spot the red flags in this invoice request?

From: Accounts <ap@acme-corp.com> **Suspicious email address (not the usual domain)**

To: you@yourbusiness.ca

Subject: Invoice #45872 – Urgent Payment Required **Creates a sense of urgency**

Hi,

Please process the attached invoice for \$4,850 today. **Asks for immediate payment**

We've updated our banking information.
Please use the details below for all future payments. **New banking details (out of the blue)**

New Bank Details:
Bank: Global Trust Bank
Account Name: Acme Corp
Account Number: 1234 5678 9012
Transit Number: 98765

Invoice_45872.pdf
248 KB **Unexpected attachment**

Regards,
Accounts Team

Tue 9:14 AM



**WHEN IN DOUBT,
VERIFY ANOTHER WAY.**

Contact the vendor or person directly using a known phone number to confirm any payment request or banking changes.

AI CHANGES THE SCAM

Scammers now use AI to create realistic voices, videos, emails, and even fake identities. It's getting harder to tell what's real.

HOW SCAMMERS USE AI



VOICE CLONES

Sound like a trusted colleague, executive, or family member.



DEEPFAKES

Fake or altered videos that look and sound real.



AI-WRITTEN PHISHING

More convincing and personalized emails with fewer mistakes.



FAKE IDENTITIES

Realistic profiles used to build trust and trick you.

SAME VOICE.
SAME FACE.
STILL A SCAM.

AI MAKES IT EASIER
TO PRETEND.
STAY ALERT.



REAL OR FAKE?

This message looks real. What red flags can you spot?



Daniel Park
VP, Operations

Today 10:24 AM

Hi, can you do me a quick favour?

I'm in a meeting right now and can't take calls.
I need you to purchase 5 x \$100 gift cards for a client and send me the codes ASAP.

I'll reimburse you this afternoon.
Please keep this confidential.



Type a message...



POSSIBLE RED FLAGS



URGENCY

"I need this ASAP."



UNUSUAL REQUEST

Asking for gift cards or non-standard payments.



AVOIDING CALLS

"Can't take calls right now."



COULD BE A DEEPFAKE

Voice or video may look real, but it could be AI-generated.



VERIFY IMPORTANT REQUESTS THROUGH A SECOND CHANNEL.

If you receive a sensitive request — like a payment, gift cards, or account changes — contact the person directly using a known phone number or verified channel.

USE IT SAFELY

AI tools can boost productivity, but they also come with risks. What you share can be stored, used to train models, or seen by others.

WHY IT MATTERS



DATA MAY BE STORED

Your inputs could be saved and used to train future models.



NOT ALWAYS PRIVATE

AI tools may not be designed to keep sensitive information confidential.



IT CAN LEAVE YOUR ORGANIZATION

Information you share could be accessed by others or used in unexpected ways.

BE SMART
WITH AI.

WHAT YOU SHARE
CAN GO FURTHER
THAN YOU THINK.



WHAT SHOULD YOU SHARE?

Always think about what's safe before you type, upload, or paste.



OK TO SHARE



General questions

Ask for explanations or learning resources.



Public information

Content already available publicly.



Brainstorming support

Ideas, outlines, or creative suggestions.



Generic examples

Non-sensitive, made-up scenarios.



DO NOT SHARE



Sensitive or confidential information

Client data, internal documents, financial information, or unpublished plans.



Personal information

Employee, customer, or personal details (e.g., names, emails, phone numbers).



Proprietary code or intellectual property

Source code, product designs, or trade secrets.



Non-public business information

Strategy, financial results, mergers, or anything marked confidential.



**WHEN IN DOUBT,
DON'T SHARE.**

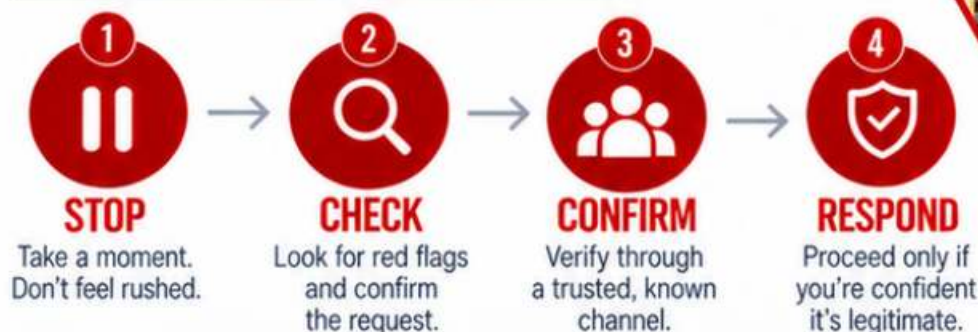
Treat AI tools like any other external platform. Follow your organization's policies and only share information that is safe and appropriate.

VERIFICATION CHECKPOINT

STOP. CHECK. CONFIRM.

Before you give money, information, credentials, or access — take a moment to verify. A few simple steps can stop a scam or mistake.

THE VERIFICATION PROCESS



COMMON SCENARIOS

When in doubt, verify. Here's how to apply the process:



SUSPICIOUS EMAIL

"Can you send me this file ASAP?"

VERIFY BY:

Checking with the sender directly using a known email or chat, not by replying to the message.



PAYMENT REQUEST

"Please process this payment today."

VERIFY BY:

Confirming with Finance and the requester through a separate, trusted channel (e.g., phone).



ACCESS REQUEST

"I need access to this system urgently."

VERIFY BY:

Validating with your manager or IT through a known contact before granting access.



UNUSUAL MESSAGE

"I'm in a meeting and can't talk — just do this."

VERIFY BY:

Reaching out directly to the person using a known phone number or in-person.



**WHEN IN DOUBT,
VERIFY IT.**

Scammers create pressure. You create protection. A quick check can prevent financial loss, data breaches, and serious impacts to your organization.



SOMETHING HAPPENED. NOW WHAT?

If you think you've clicked a suspicious link, shared information, or something doesn't feel right — act quickly. Fast action can limit the damage.

IMMEDIATE RESPONSE STEPS



COMMON INCIDENTS & WHAT TO DO

Here's how to respond to common situations:



YOU CLICKED A SUSPICIOUS LINK

- 1 Stop and don't enter any information.
- 2 Disconnect from the internet if instructed.
- 3 Report to IT/security.
- 4 Change your passwords if required.



YOU THINK YOUR ACCOUNT IS COMPROMISED

- 1 Change your password immediately.
- 2 Enable multi-factor authentication (MFA).
- 3 Report to IT/security.
- 4 Review recent activity for anything suspicious.



YOU SENT A PAYMENT TO THE WRONG PERSON

- 1 Contact your manager and finance team immediately.
- 2 Report to IT/security.
- 3 Do not send additional payments.
- 4 Preserve all communication details.



YOU SHARED SENSITIVE INFORMATION

- 1 Report to IT/security right away.
- 2 Provide details on what was shared and to whom.
- 3 Change your passwords if needed.
- 4 Follow your organization's incident response process.



**WHEN IN DOUBT,
REPORT IT.**

It's always better to report something that turns out to be nothing, than to stay silent and risk a larger security incident. Your security team is here to help.



BACKUP ROUTE

PREPARE BEFORE SOMETHING
GOES WRONG.

A little preparation goes a long way. Having the right systems, backups, and recovery plans in place can help you get back on track faster if something goes wrong.

KEY AREAS TO PREPARE



BACKUPS

Keep important files and data backed up safely.



UPDATES

Keep devices, software, and security tools up to date.



RECOVERY ACCESS

Maintain access options (e.g., secondary emails, recovery codes, backup accounts).



KEY CONTACTS

Know who to contact internally and externally if something goes wrong.



PRACTICAL TIPS

Simple steps you can take today to be better prepared:



BACK IT UP

- ✓ Use secure, automatic backups.
- ✓ Keep copies in a separate location (e.g., cloud + external drive).
- ✓ Regularly test your backups to make sure they work.



STAY UPDATED

- ✓ Turn on automatic updates.
- ✓ Update your operating system, apps, and security tools regularly.
- ✓ Don't ignore update notifications.



KEEP A WAY BACK IN

- ✓ Set up and test recovery options (e.g., secondary email, phone number).
- ✓ Store recovery codes in a safe place.
- ✓ Use a password manager to securely store important credentials.



KNOW WHO TO CONTACT

- ✓ Save your IT/security contact details.
- ✓ Know your organization's incident reporting process.
- ✓ Keep important vendor and support contacts accessible.



**BE PREPARED
SO YOU CAN
RECOVER FASTER.**

Good preparation can reduce downtime, limit damage, and help you get back to business as usual faster. Plan now — it's easier than you think.



INCIDENT ROADMAP

YOUR RESPONSE PLAN

When something goes wrong, having a clear plan helps you respond faster, reduce the impact, and get back to normal. Use this worksheet to define who to contact and what happens first.

1 KEY CONTACTS

Who do you call? Fill in the key people and their contact details.



IT / SECURITY TEAM

Name: _____

Phone: _____

Email: _____



MANAGER / SUPERVISOR

Name: _____

Phone: _____

Email: _____



ADDITIONAL CONTACTS

(e.g., HR, Legal, Facilities)

Name: _____

Phone: _____

Email: _____



EXTERNAL SUPPORT

(e.g., Vendor, Law Enforcement)

Name: _____

Phone: _____

Email: _____

2 WHAT HAPPENS FIRST?

List the first steps to take based on the type of incident.



SUSPICIOUS CLICK

- 1 _____
- 2 _____
- 3 _____
- 4 _____



COMPROMISED ACCOUNT

- 1 _____
- 2 _____
- 3 _____
- 4 _____



WRONG PAYMENT

- 1 _____
- 2 _____
- 3 _____
- 4 _____



SENSITIVE INFORMATION

- 1 _____
- 2 _____
- 3 _____
- 4 _____

3 OTHER THINGS TO REMEMBER

Check off the items below to make sure you're prepared.

- | | | |
|--|---|--|
| ☐ Keep important files backed up. | ☐ Store key contact details in an accessible location. | ☐ Review and update this plan periodically. |
| ☐ Keep devices and software updated. | ☐ Understand your organization's incident reporting process. | ☐ Keep a copy of this plan somewhere you can access it even if your main systems are unavailable. |
| ☐ Know where to find recovery codes and access options. | ☐ Test your backups regularly. | |



**A PLAN TODAY
MAKES A BIG DIFFERENCE
TOMORROW.**

The more prepared you are, the easier it is to respond, limit the damage, and get back on track.



SECURITY IS EVERYONE'S JOB

PEOPLE. AWARENESS. ACTION.

Technology and plans are important, but people make the biggest difference. A strong security culture helps catch issues early, reduce risks, and keep your organization resilient.

KEY PILLARS OF A STRONG CULTURE



OPEN CONVERSATIONS

Talk about security regularly.



NO-BLAME REPORTING

Encourage people to speak up.



EVERYONE PLAYS A PART

Security is a shared responsibility.



LEADERSHIP SUPPORT

Set the tone and lead by example.

PRACTICAL WAYS TO BUILD IT



MAKE IT EASY
TO REPORT



KEEP THE
CONVERSATION GOING



EMPOWER
YOUR TEAM



LEAD
BY EXAMPLE



**A STRONG SECURITY CULTURE
KEEPS PEOPLE AND ORGANIZATIONS STRONG.**

When security is part of everyday decisions, everyone is safer, smarter, and more prepared.

16

FINAL CHECKPOINT >>>

YOU'RE READY!

BE SMART. BE SAFE. BE READY.

You've completed the road map. Now it's time to put it into action and keep the momentum going. A more resilient organization is within reach — and it starts with you.

YOUR NEXT STEPS



1 REVIEW YOUR PLAN

Make sure it's up to date and tested regularly.



2 KEEP THE CONVERSATION GOING

Talk about security in everyday work.



3 PRACTICE AND IMPROVE

Run exercises, learn from lessons, and refine your approach.



4 LEAD BY EXAMPLE

Show that security is a priority at all levels.



A STRONGER, SAFER TOMORROW STARTS TODAY.

By working together, staying prepared, and making security part of everyday decisions, we can reduce risk, recover faster, and build a more resilient Canada.



PEOPLE

Are aware, empowered, and connected.



PROCESSES

Are clear, practiced, and continuously improved.



ORGANIZATIONS

Are stronger, safer, and ready for what's next.

