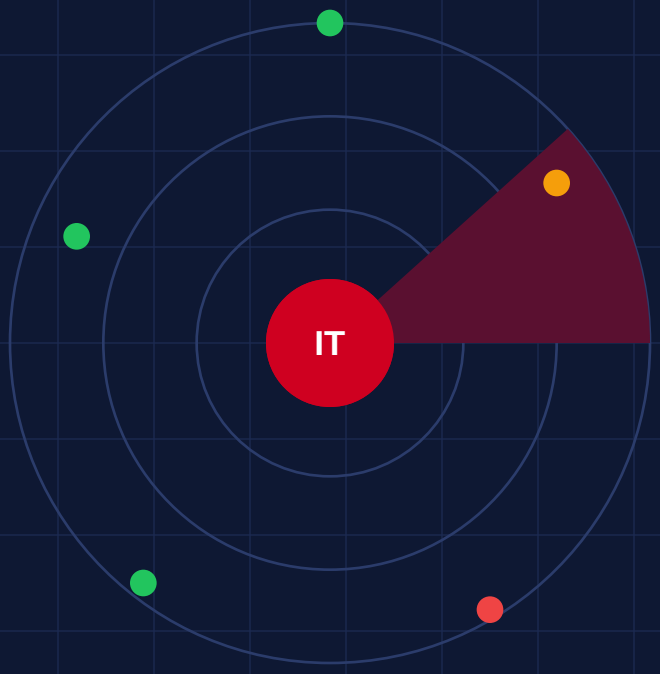
PING SYSTEMS · FREE GUIDE

The Small Office Cyber Security Playbook

10 practical steps to protect your business, your IT and your clients' data in the age of AI.



Ping Systems Inc.

November 2026 edition · For small offices in Ottawa, Gatineau and beyond

pingsystems.ca · 613-510-1264 · info@pingsystems.ca

Why this matters now

Artificial intelligence has changed the speed of cyber attacks. The same tools that help software makers find and fix flaws also help criminals find weak spots, write convincing scams and copy voices.

The basics of good defence have not changed. What has changed is how little time you have to put them in place.

1 in 6

Canadian businesses were affected by a cyber security incident in 2025.

Statistics Canada, October 2026

0 days

Median time from a flaw becoming public to attacks in the wild in 2026, down from 771 days in 2018.

ESET, citing the Zero Day Clock, September 2026

10,000+

High- or critical-severity vulnerabilities found in one month by partners using a single AI model.

Anthropic, Project Glasswing, May 2026

How to use this playbook

Work through the ten steps in order. Each step has a short checklist. Tick what is already in place, on screen or on paper, then close the gaps, starting with steps 1 to 3. If you are not sure whether something is done, treat it as not done. The scorecard on page 9 gives you a quick overall picture.

STEP 01

1 Patch quickly and automatically

WHY IT MATTERS

Most attacks still use known flaws. When a fix is released, attackers study it, often within hours. Every day an update waits is a day the door stays open.

CHECKLIST

- [ ] Turn on automatic updates for Windows, macOS, web browsers and office apps.
- [ ] Update firewalls, routers, Wi-Fi access points and printers too. They are often forgotten.
- [ ] Apply critical security updates within days, not weeks.
- [ ] Check every month that each device actually installed its updates.

STEP 02

2 Turn on multi-factor authentication everywhere

WHY IT MATTERS

Stolen passwords are one of the most common ways in. A second check stops most of these attacks, even when the password is known.

CHECKLIST

- [ ] Enable MFA on email, Microsoft 365 or Google Workspace, banking, accounting software and remote access.
- [ ] Prefer an authenticator app, passkeys or security keys over text messages.
- [ ] Use phishing-resistant MFA, such as passkeys or security keys, for administrator accounts.
- [ ] Never approve a sign-in prompt you did not start yourself.

STEP 03

3 Back up, and prove you can restore

WHY IT MATTERS

Good backups turn ransomware from a disaster into an inconvenience. Backups that have never been tested often fail on the day you need them.

CHECKLIST

- [ ] Keep three copies of important data, on two types of storage, with one copy offline or unchangeable.
- [ ] Back up cloud data too, including Microsoft 365 or Google Workspace mail and files.
- [ ] Test a restore at least every three months and note how long it took.
- [ ] Protect backup systems with their own strong password and MFA.

STEP 04

4 Shrink what is exposed to the internet

WHY IT MATTERS

Criminals scan the whole internet around the clock, looking for open doors such as remote desktop, old VPNs and admin pages.

CHECKLIST

- [ ] Never expose Remote Desktop (RDP) directly to the internet. Use a secure VPN or remote access service with MFA.
- [ ] Close ports and services you do not use, and change every default admin password.
- [ ] Keep firewall and VPN firmware up to date. These devices are frequent targets.
- [ ] List every service your office exposes online and review the list twice a year.

5

STEP 05

Know what you have, and retire what is unsupported

WHY IT MATTERS

You cannot protect a device or account you do not know about. Systems that no longer receive security updates stay vulnerable for good.

CHECKLIST

- [ ] Keep a simple list of computers, phones, servers, network devices, software and cloud services.
- [ ] Replace or isolate anything that no longer gets security updates, such as Windows 10 computers without extended updates.
- [ ] Remove software and accounts you no longer use.
- [ ] Know who in the office is responsible for each important system.

6

STEP 06

Give people only the access they need

WHY IT MATTERS

When an account is taken over, the damage depends on what that account can reach.

CHECKLIST

- [ ] Do not use administrator accounts for day-to-day work.
- [ ] Remove access on the same day someone leaves.
- [ ] Review who can open shared folders, finance systems and client files every quarter.
- [ ] Use separate, protected accounts for IT administration.

STEP 07

7 Protect devices and email

WHY IT MATTERS

Most attacks arrive by email or through a single compromised computer.

CHECKLIST

- [ ] Use modern endpoint protection with detection and response (EDR), and make sure someone monitors it.
- [ ] Filter incoming email for phishing, malicious links and dangerous attachments.
- [ ] Set up SPF, DKIM and DMARC so criminals cannot easily send email pretending to be you.
- [ ] Encrypt laptops and phones, and make sure you can wipe them remotely if they are lost.

STEP 08

8 Prepare your people for AI-powered scams

WHY IT MATTERS

AI makes scam emails, texts, phone calls and even video look real. Payment-redirection fraud costs Canadian businesses tens of millions of dollars a year.

CHECKLIST

- [ ] Confirm any request to change bank details or send money by calling a number you already know, never the one in the message.
- [ ] Agree on a check for urgent requests from managers or IT, such as a call-back or a code word.
- [ ] Run short awareness training at least twice a year, including fake help-desk and voice scams.
- [ ] Set clear rules for AI tools: no client or personal information in tools the business has not approved.

STEP 09

9 Watch for trouble, and make sure someone responds

WHY IT MATTERS

Attacks spotted early are cheaper and easier to contain. Logs that nobody reads do not protect anyone.

CHECKLIST

- ☐ Collect sign-in and security logs from email, devices and firewalls in one place.
- ☐ Turn on alerts for unusual sign-ins, new mail forwarding rules and mass file changes.
- ☐ Make someone responsible for reviewing alerts, including after hours for critical systems.
- ☐ Separate key systems so a problem in one area cannot spread easily.

STEP 10

10 Keep a one-page incident plan

WHY IT MATTERS

In the first hour of an incident, a plan written in advance saves time, money and costly mistakes.

CHECKLIST

- ☐ Write down who to call: your IT provider, your bank, your insurer and, if needed, a lawyer.
- ☐ Note how to isolate an infected device and where your backups are kept.
- ☐ Know your reporting duties for personal information (see page 8).
- ☐ Rehearse the plan once a year with a short tabletop exercise.

If you think you have been hit

Act quickly, but calmly. These steps limit the damage and protect your options.

1. **Do not pay or reply to the attacker**
   Get advice before any contact or payment.
2. **Isolate affected devices**
   Unplug the network cable or turn off Wi-Fi. Leave the device on: switching it off can destroy useful evidence.
3. **Call your IT provider**
   Ping Systems clients: 613-510-1264.
4. **Call your bank right away if money moved**
   Fast reports improve the chances of stopping or recovering a payment.
5. **Change passwords from a clean device**
   Start with email and administrator accounts.
6. **Report it**
   Contact your local police and report to Report Cybercrime and Fraud: reportcyberandfraud.canada.ca or 1-888-495-8501. You can also report to the Canadian Centre for Cyber Security at cyber.gc.ca.

Your privacy duties after a breach

Across Canada (PIPEDA)
If a breach involving personal information creates a real risk of significant harm, report it to the Office of the Privacy Commissioner of Canada and notify the people affected as soon as feasible. Keep a record of every breach for 24 months, even small ones.

In Quebec, including Gatineau (Law 25)
Keep a register of all confidentiality incidents. If an incident presents a risk of serious injury, promptly notify the Commission d’accès à l’information and the people concerned.

Health information in Ontario
Clinics and other custodians may also have notification duties under Ontario’s Personal Health Information Protection Act (PHIPA).

This is general information, not legal advice. A lawyer can confirm which rules apply to your organization.

Quick scorecard

Mark each step honestly. A step counts as in place only if every item on its checklist is done.

#		In place	Partly	Not yet
1	Patch quickly and automatically	☐	☐	☐
2	Turn on multi-factor authentication everywhere	☐	☐	☐
3	Back up, and prove you can restore	☐	☐	☐
4	Shrink what is exposed to the internet	☐	☐	☐
5	Know what you have, and retire what is unsupported	☐	☐	☐
6	Give people only the access they need	☐	☐	☐
7	Protect devices and email	☐	☐	☐
8	Prepare your people for AI-powered scams	☐	☐	☐
9	Watch for trouble, and make sure someone responds	☐	☐	☐
10	Keep a one-page incident plan	☐	☐	☐

8 to 10 in place
A strong position. Keep testing backups and reviewing access.

5 to 7 in place
Real gaps remain. Fix steps 1 to 3 first, then work down the list.

0 to 4 in place
High risk. Get help now, starting with updates, MFA and backups.

How Ping Systems helps

As your managed IT and security provider, we put these steps in place and keep them running, so your team can focus on clients.

- [ ] Patching and monitoring of computers, servers and network devices
- [ ] Multi-factor authentication rolled out across your accounts
- [ ] Monitored backups with regular restore tests
- [ ] Firewall management and secure remote access
- [ ] Endpoint protection and email security, including SPF, DKIM and DMARC
- [ ] Staff awareness training in plain language
- [ ] A local team in Ottawa and Gatineau, on site when needed

20+ years of combined experience · English or French · Plain-language advice

Start with a free IT health audit

We review your devices, network, accounts, email, backups and security, then give you a clear written plan. No cost, no obligation.

pingsystems.ca/free-it-health-audit
613-510-1264 · info@pingsystems.ca

Sources

1. Statistics Canada, The Daily: About one in six Canadian businesses were impacted by cyber security incidents in 2025 (October 21, 2026).
2. Canadian Centre for Cyber Security: Statement on frontier artificial intelligence models and their impact on cyber security (June 24, 2026).
3. Canadian Centre for Cyber Security: Ransomware Threat Outlook 2025 to 2027 (January 2026).
4. Canadian Centre for Cyber Security: Baseline cyber security controls for small and medium organizations.
5. Canadian Centre for Cyber Security: Alert AL26-028, help desk voice phishing campaign targeting Canadian organizations (October 28, 2026).
6. Anthropic: Project Glasswing, an initial update (May 22, 2026).
7. SecurityBrief: AI shrinks exploit window to zero days, ESET warns (September 16, 2026).
8. Canadian Anti-Fraud Centre: news release on spear phishing fraud losses in 2025 (January 29, 2026).
9. Office of the Privacy Commissioner of Canada: What you need to know about mandatory reporting of breaches of security safeguards.
10. Quebec: Act respecting the protection of personal information in the private sector, sections 3.5 to 3.8.

This playbook is general information to help small organizations reduce cyber risk. It is not legal, insurance or professional advice, and no set of measures removes all risk. Figures come from the sources listed, as published on the dates shown. This PDF contains no scripts, links or embedded files. Its tick boxes are the only interactive part; they send nothing anywhere. © 2026 Ping Systems Inc. You may share this playbook unchanged and free of charge.