

Cybersecurity Readiness 2027: A Guide for Small Businesses

Five changes every small business should prepare for, and the simple fix for each.

Attacks on small businesses are now **faster, more automated and far more convincing**, largely because of AI. The good news: most of the protection comes from a handful of basics, run well. This guide covers the five that matter most heading into 2027, plus a tear-out **AI Readiness Toolkit** for you and your team on pages 6–7.

1  AI-powered fraud Fake voices, videos and invoices	2  Faster attacks Unpatched software and old devices	3  Weak sign-ins Stolen and phished passwords	4  Shadow AI Client data in unapproved tools	5  One network One breach reaches everything
--	--	---	--	--

THE PICTURE IN THREE NUMBERS

31% of breaches began with an exploited software flaw, now the #1 way in Verizon DBIR 2026	US\$3.05B lost to business email compromise, reported to the FBI in 2025 FBI IC3 2025	48% of breaches involved a third party such as a supplier, up 60% in a year Verizon DBIR 2026
--	---	---

1

AI makes fraud sound and look real



IMPACT One convincing call, video or invoice can empty an account. Accounting firms in tax season, clinic front desks and retail managers paying suppliers are prime targets.

REAL CASE · HONG KONG · JANUARY 2024

A finance employee at engineering firm Arup doubted an email from the CFO. Then came a video call with the CFO and several colleagues, all faces and voices they knew.

Every other person on the call was an AI deepfake.

Fifteen transfers later, about **US\$25.6 million** was gone.

Source: CNN, May 2024

US\$893M

AI-related losses reported to the FBI in 2025, its first year tracking AI as a category

FBI IC3 2025

+40%

higher success rate for scams by text and phone than by email

Verizon DBIR 2026

UNDERLYING PROBLEM

Payments are approved on trust: a familiar voice, a known email address, a routine invoice. AI now fakes all three, and many of these messages carry no link or attachment for a filter to catch.

EASY FIX · THIS WEEK

- ✓ Verify any payment or bank-detail change by calling a number you already have
- ✓ Require two people to approve new payees and large transfers
- ✓ Agree a code word with key staff and clients for urgent requests

2

Attacks now move in hours, not months



IMPACT A software flaw left unpatched for a few weeks used to be a manageable risk. Today it is the most common way attackers get in, often before a business knows an update exists.

31%

of breaches began by exploiting a software flaw, up 55% in a year and now ahead of stolen passwords

Verizon DBIR 2026

43 days

median time to fully fix a critical vulnerability, almost two weeks slower than the year before

Verizon DBIR 2026 · SMB infographic

UNDERLYING PROBLEM

Updates wait for a quiet week and nobody checks they happened. Older devices quietly stop receiving fixes at all: Windows 10 support ended in October 2025, and extended updates now cost extra each year.

EASY FIX · THIS MONTH

- ✓ Turn on automatic updates for computers, phones and business apps
- ✓ Ask your IT provider to confirm updates monthly, including router and firewall firmware
- ✓ List unsupported devices and budget to replace them in 2027

3

Passwords alone no longer protect you



IMPACT One stolen password can open email, banking and client files, and lets an attacker quietly read invoices before redirecting a payment.

1 Exploited software flaws

31%

2 Stolen passwords

close behind

Stolen passwords are still the second most common way into a business. Two-step sign-in blocks most of these attacks, even when the password is known.

Verizon DBIR 2026

UNDERLYING PROBLEM

Shared Wi-Fi and app passwords, accounts left open after staff leave, and staff trained to approve any sign-in prompt that pops up.

EASY FIX · THIS MONTH

- ✓ Turn on two-step sign-in (MFA) for email, banking and cloud apps
- ✓ Remove leavers' accounts on their last day; retire shared passwords
- ✓ Move owner, finance and admin accounts to passkeys next, the option US cyber agency CISA rates strongest

4

Your team is already using AI tools



IMPACT Patient notes, tax returns or case files pasted into a free AI tool may be stored or used by the provider, which can breach client confidentiality and privacy laws such as PIPEDA, HIPAA and India's DPDP Act.

15% → 45%

rise in employees frequently using AI tools at work in one year; shadow AI is now the #3 cause of accidental data leaks

Verizon DBIR 2026

1 in 5

breached organizations reported a breach involving shadow AI; only 37% had policies to manage it

IBM Cost of a Data Breach 2025

UNDERLYING PROBLEM

No approved tool and no rules. Staff reach for whatever is free, often on personal accounts the business cannot see or shut off.

EASY FIX · THIS QUARTER

- ✓ Pick one or two approved AI tools on business terms, signed in with work accounts
- ✓ Share a one-page rule: never paste client, patient, tax or ID data into other tools
- ✓ Ask your IT provider which AI apps and extensions are in use

5

One network, one breach, everything exposed



IMPACT When staff laptops, guest phones, cameras and card terminals share one network, one infected device can reach your files and your backups. That is how ransomware stops a business.

48%

of all breaches now involve ransomware

Verizon DBIR 2026

>7%

of annual revenue lost in the worst small-business breaches (top 2.5% of cases)

Verizon Breach Impact Study 2026 · SMB infographic

UNDERLYING PROBLEM

A home-grade router, one shared Wi-Fi password, no filtering of harmful websites, and backups connected to the same network. Suppliers with open-ended access widen the gap: they now feature in 48% of breaches.

EASY FIX · NEXT 60 DAYS

✓ Separate staff, guest and device Wi-Fi networks

✓ Turn on protective DNS filtering to block known malicious sites

✓ Keep backups separate from the network, and test a real restore

WHERE CYBIRD FITS

PEOPLE

Payment rules, training, AI policy

ACCOUNTS

MFA and passkeys

DEVICES

Updates and endpoint protection

NETWORK

Business Wi-Fi · guest separation · firewall · protective DNS · device visibility

Cybird

DATA

Tested backups, encryption

Cybird is a small-business security gateway that managed service providers use to deliver the network layer. The other areas are covered by your IT provider with other tools and simple business rules.

2027 DATES TO KNOW

NOW

In force today

Breach-reporting rules already apply in Canada, India and to US accounting firms.

INDIA

13 May 2027

Main DPDP Act obligations apply: security safeguards, breach notification, consent.

US HEALTH

July 2027

Target date for the updated HIPAA Security Rule: MFA, encryption, asset inventories.

ALL

October 2027

Microsoft's extended Windows 10 updates reach their next cut-off; plan PC replacements.

YOUR FIVE FIXES AT A GLANCE

1

Verify every payment change

Call back on a known number; two-person approval

2

Update automatically

And replace devices that no longer get fixes

3

MFA everywhere

Then passkeys for owner, finance and admin

4

Approve your AI tools

And one rule on what never to paste in

5

Separate and filter

Split Wi-Fi, block bad sites, test backups

Quick check: how ready are you?

- ☐ Payment and bank-detail changes are always verified by phone
- ☐ Updates install automatically, and someone confirms they did
- ☐ No computers or network devices are out of support
- ☐ Every account uses two-step sign-in (MFA)
- ☐ Leavers lose access on their last day
- ☐ Staff know which AI tools are approved, and what never to paste in
- ☐ Guests, staff and devices are on separate networks
- ☐ Backups are separate from the network and a restore has been tested

Fewer than 6 ticks? Start with the 90-day plan. A gap on 1, 4 or 8 deserves attention now, whatever your score.

Your 90-day plan**DAYS 1-30**

Payment-verification rule · MFA everywhere
· remove leavers · automatic updates on

DAYS 31-60

Separate Wi-Fi networks · protective DNS filtering · test a backup restore · AI use policy

DAYS 61-90

Passkeys for key accounts · supplier access review · one-page incident plan · replace-or-retire list for old devices

EVERY QUARTER

Review progress with your IT provider

Book a 30-minute readiness review

Bring this guide and your quick-check answers to your IT provider. Agree your top three fixes, who owns each one, and a date for the first. **MSPs:** send this guide ahead of your next client review.

**Cybird****cybird.net**

Partners: partners@cybird.net

Sources. Verizon, 2026 Data Breach Investigations Report (May 2026), 2026 SMB infographic and 2026 Breach Impact Study (June 2026) · FBI IC3, 2025 Internet Crime Report (April 2026) · IBM, Cost of a Data Breach Report 2025 · CNN, Arup deepfake scam (May 2024) · CISA, Implementing Phishing-Resistant MFA · TechRepublic, Windows 10 ESU (Aug 2026) · AMLEGALS, DPDP compliance deadline (July 2026) · Linklaters, CERT-In directions (2022) · Office of the Privacy Commissioner of Canada · Akin Gump, FTC Safeguards Rule (2024) · Davis Wright Tremaine, HIPAA rulemaking timeframes (July 2026). Figures describe the datasets named, not the odds for any one business. Dates about 2027 reflect announced plans and may change. General information, not legal advice. © 2026 Cybird Technologies.

Stop AI scams: the team card

For every staff member
Print it. Pin it. Practise it.

1 The callback script

For any urgent request for money, passwords, data or new bank details, even when the voice or face looks exactly right.

SAY THIS

"No problem. I'll call you straight back on the number we have on file."

- 1 Hang up. Call the number **on file**, never one given in the message.
- 2 Ask for the team code word.
- 3 For payments, get a second person to approve.

Red flag: anyone who resists a callback, asks for secrecy or says "there's no time". And don't trust "turn your head" tests: live deepfakes pass them.

2 Set a code word in 5 minutes

- 1 Pick an unusual word or phrase that isn't online anywhere.
- 2 Share it **in person or by phone** only, never by email or chat.
- 3 Give it to the owner, finance staff and anyone who can move money; agree one with key clients too.
- 4 Change it when someone leaves, and every six months.

Why it works: AI can copy a voice from a short clip. It can't know a word that was never written down.

3 Redact before you paste into any AI tool

SECTOR	NEVER PASTE	REPLACE WITH
Clinic	Patient name, date of birth, health card number	"Patient A, 40s"
Accounting	Client name, SIN / SSN / PAN, account numbers	"Client B, sole proprietor"
Law firm	Party names, case and file numbers	"Party 1 v. Party 2"
Retail	Customer emails, phone numbers, card details	"Customer C"

And never paste passwords, bank details or anything marked confidential, in any tool, approved or not.

4 10-minute team drill: "Would you pay this?"

Read each scenario aloud at a staff meeting. Let the team decide, then reveal the rule.

"It's the owner. I'm stuck in a meeting. Send \$18,000 to this new vendor before 5 pm and keep it quiet."

THE RULE

Hang up, call back on the number on file, ask for the code word, and get a second approval.

A regular supplier emails: "We've changed banks. Please use these details for today's invoice."

THE RULE

Call the supplier on the number from past invoices or the contract, never the email.

A text from "IT support": "Security update. Approve the sign-in request on your phone now."

THE RULE

Never approve a sign-in you didn't start. Tell your IT provider right away.

AI READINESS TOOLKIT · PAGE 2 OF 2

Use AI safely: the owner's checklist

For the owner or manager
About 30 minutes in total

5

5 questions before approving any AI tool

- ☐ **Training:** does it use our data to train its models, and can we switch that off?
- ☐ **Business plan:** is there a business version with admin controls?
- ☐ **Work login:** can staff sign in with work accounts, so access ends when they leave?
- ☐ **Retention:** how long is our data kept, and can we delete it?
- ☐ **Location and law:** where is data stored? Healthcare in the US: get a signed HIPAA business associate agreement before any patient data. Check PIPEDA (Canada) and the DPDP Act (India) for client data.

6

15-minute AI exposure check

- ☐ **Connected apps:** which AI apps can access your Microsoft 365 or Google Workspace email and files? Your admin console lists them.
- ☐ **Browser extensions:** which AI extensions are on company browsers? Some can read everything on screen.
- ☐ **Personal accounts:** is anyone using a personal AI account for work?
- ☐ **Your public voice:** how much of your and your finance lead's voice and video is online? Webinars and podcasts are raw material for voice cloning.

7

Rules for AI assistants that can take actions

AI assistants that can read email, open files or send messages can be tricked by hidden instructions planted in an email or document, known as **prompt injection**. Three rules keep them safe:

AI drafts, a human sends

Nothing leaves the business without a person pressing send.

No AI near the money

No assistant gets access to payments, banking or payroll.

Minimum access

Connect each assistant only to the mailbox or folder it needs.

8

Put AI to work for your security

Three safe prompts for your approved AI tool. Remove names and links first.

"Here is an email I received [names and links removed]. List the warning signs that it may be a scam." · Check a suspicious message

"Draft a one-page payment-verification policy for a 20-person [clinic / accounting firm / store]." · Write your policy

"Write a friendly 5-minute team briefing on spotting fake calls, texts and sign-in requests." · Brief your team

CALL YOUR INSURER

"Are we covered for social engineering fraud, including deepfake calls, and what is the limit?"

Many cyber policies treat this separately, often with a lower limit than the main cover. Confirm rather than assume.

