IS YOUR TECHNOLOGY BUDGET READY FOR FALL? A PLANNING GUIDE FOR ONTARIO BUSINESSES

As summer winds down, many Ontario businesses begin shifting their focus toward the busy fall season. September often brings new projects, year-end planning, budget discussions, and strategic initiatives. While many organizations review staffing, marketing, and operational expenses, technology is often left until something breaks.

The problem? Emergency IT purchases almost always cost more than planned upgrades.
Taking the time to review your technology now can help you avoid unexpected downtime, improve security, and make smarter financial decisions before the end of the year.

Five Questions Every Ontario Business Should Be Asking

1. Are Any of Your Computers Reaching End of Life?

Older computers don't just run slower, they eventually stop receiving the latest security features and struggle to support modern business applications. As Microsoft continues to evolve Windows 11 and Microsoft 365, older devices may no longer meet hardware requirements or deliver the performance your team needs. Replacing aging equipment proactively allows you to budget appropriately instead of making emergency purchases when a device fails.

2. Are You Paying for Microsoft Licenses You No Longer Need?

Over time, employees leave, departments change, and software requirements evolve. employees still have access to the tools they need.

Many businesses continue paying for unused Microsoft 365 licenses or have users assigned higher-tier licenses than their role requires.

A simple licensing review can often uncover opportunities to reduce monthly costs while ensuring

3. Is Your Cybersecurity Keeping Up? Cybersecurity isn't a one-time purchase, it's an ongoing process.

Review whether your business has:

- Multi-Factor Authentication (MFA)
- Endpoint Detection & Response (EDR)
- Employee security awareness training
- Email filtering and phishing protection
- Reliable backup and recovery solutions

The cost of strengthening security is often far less than the cost of recovering from a cyber incident.

4. Is Your Hardware Holding Your Team Back?

Technology should help your employees work efficiently—not create frustration.

If your team regularly experiences slow computers, unreliable Wi-Fi, or aging equipment, those small delays add up over hundreds of working hours each year.

Investing in productivity often delivers returns far beyond the initial hardware cost.

5. Do You Have a Technology Roadmap?

The most successful businesses don't replace everything at once.

Instead, they create a technology roadmap that spreads investments over several years

Planning ahead makes budgeting easier, reduces unexpected expenses, and ensures critical systems are refreshed before they become a problem.

Small Changes Today Prevent Big Expenses Tomorrow
Technology shouldn't be a surprise expense.

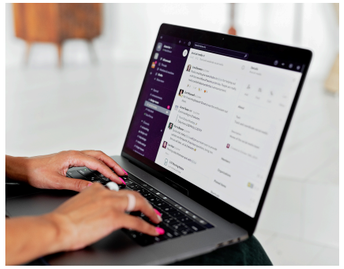
A proactive review of your hardware, Microsoft licensing, cybersecurity, and IT roadmap can help your business reduce risk, improve productivity, and make informed budgeting decisions before year-end.
Whether your organization has 10 employees or 200, now is an excellent time to prepare for a productive and secure fall season.

Need Help Planning?

At Attitude IT, we work with Ontario businesses to review their technology environment, identify opportunities to optimize licensing, improve security, and create practical hardware lifecycle plans that align with their budget—not just today's needs, but tomorrow's growth.
If you'd like a second opinion before finalizing your IT budget, we'd be happy to help.

ATTITUDE CHRONICLE

Insider Tips To Make Your Business Run Faster, Easier And More Profitably



HOW TO STOP SCAMMERS SENDING EMAIL IN YOUR COMPANY'S NAME

Right now, with no hacking at all, someone could send an email that looks like it came from your company. They put your domain in the “from” line and email your clients or suppliers, asking them to pay a fake invoice or move money to a new account.

Because the message carries your name, the people who trust you are far more likely to act on it. It works because email was never built to check that senders are who they claim to be.

The three records that stop it

- **SPF** is a list of the mail servers allowed to send email for your domain.
- **DKIM** adds a tamper-proof signature that proves a message really came from you and wasn't changed on the way.
- **DMARC** ties the two together and tells receiving mail servers what to do with anything that fails the check.

The setting most businesses get wrong

Having the records isn't quite enough. DMARC has three settings, and most businesses stop at the wrong one. On “monitor only,” it watches and reports but never blocks a fake.

Real protection starts when it's set to “quarantine” or “reject.” One thing these records don't stop: a lookalike domain (like yourcompany-invoices.com), or a display name that shows your company over a random address. So staff should still check the full email address before acting on any payment request.

How to switch it on without blocking your own email

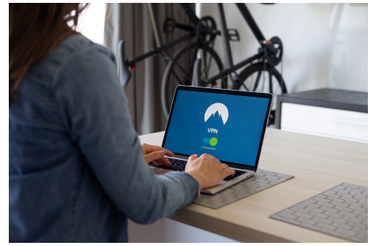
DMARC is best turned up in stages. Start on “monitor only” and read the reports it sends, which show every source sending email as your domain, including the ones that shouldn't.

Once you've confirmed your real email passes, move to “quarantine,” then to “reject.” Done gradually, you close the door on impersonation without sending your own invoices and quotes to the spam folder.

Worth having even if you barely send email

Beyond protecting your name, these records help your messages arrive. Since early 2024, Google and Yahoo have required bulk senders to use SPF, DKIM, and DMARC, and Microsoft began applying similar rules to Outlook.com in 2025.

Even below those volumes, a properly set-up domain is more likely to land in the inbox than the spam folder. You can check what yours has in place with a free DMARC checker, or ask your IT provider to confirm it and walk the policy up to full protection safely.



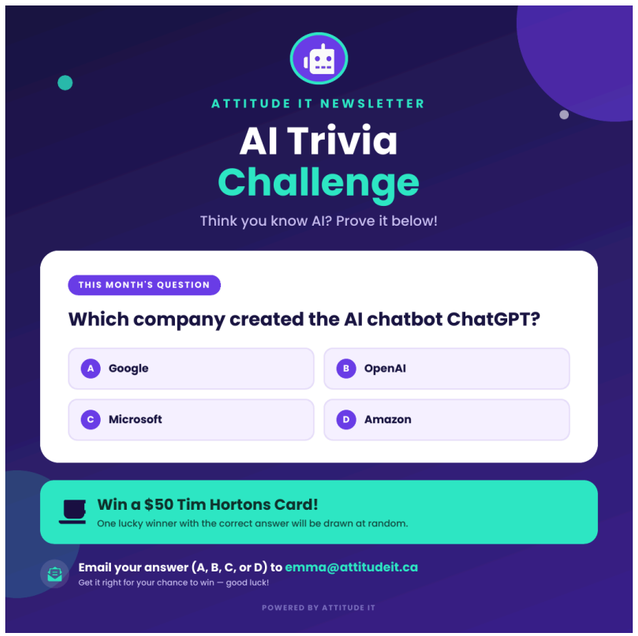
your business is hit by a cyberattack, the first hour decides how bad it gets.

The instinct is to start fixing things, and that's usually what makes it worse. Work through these five steps instead.

- Disconnect the affected devices from the network. Unplug the network cable and turn off Wi-Fi so the problem can't spread to other computers or your backups. Try not to power the machine off, because that can wipe evidence of what happened.
- Call your IT provider, by phone. Don't email, in case the attacker is watching your inbox. If you have cyber insurance, call them next, since many policies want their incident team involved early.
- Leave the evidence alone. Don't wipe, reinstall, or tidy up the affected machines yet. Screenshots are fine, but keep the originals.
- If money was sent, call your bank immediately. Ask them to recall the transfer. With wire fraud, the first few hours make the biggest difference.
- Reset passwords from a clean device, and turn on MFA. Start with email and admin accounts, using a device you know isn't affected.

Then have your team document the incident and show the remediation taken.

Do you have an incident response plan that your team can follow? Start one today.



Cartoon of the Month

WHO CAN SEE WHAT YOUR AI NOTE-TAKER RECORDS?

WAI note-takers join your meetings, record every word, and store it on the vendor's servers. They're worth using, but before you let one into a client or staff meeting, run these quick checks.paces or areas with foot traffic

- Pick one approved tool, and ask staff not to connect others to company meetings.
- Turn off auto-join, so it only records when someone chooses to.
- Announce the recording and get everyone's consent before it starts.
- Check whether the tool uses your conversations to train its AI.
- Prefer a tool that keeps recordings inside your own Microsoft or Google account.
- Check who the summary gets emailed to by default.
- Keep bots out of legal, HR, and confidential client meetings.

The 4-Step Legacy IT Debt Audit Your Business Needs

Windows 10 stopped getting security updates in October 2025. The computers still work, which is why it's easy to leave them, but every new flaw found now stays unpatched. That makes those machines easier to attack and can cause problems with compliance and your cyber insurance. Here's how to move off it:

- List every computer still running Windows 10.
- Check which ones can upgrade to Windows 11 (free if the hardware qualifies) using Microsoft's free PC Health Check app.
- Upgrade the ones that qualify. The upgrade keeps your files and programs in place.
- For the rest, choose between paid Extended Security Updates as a short-term bridge or replacing the PC.
- Your IT provider can run this inventory quickly and tell you the best option for each machine.

Your IT provider can run this inventory quickly and tell you the best option for each machine.

Passkeys: The Login That Can't Be Phished

Passwords are the weak point in most businesses. People reuse them, write them down, and type them into fake login pages. Passkeys replace them: you sign in with the same fingerprint, face, or PIN you use to unlock your phone, and there's no password for anyone to steal, guess, or phish.

- Why they're safer: nothing to phish, nothing for a hacker to steal in a breach, and nothing to reuse or forget.
- Where they work: Microsoft, Google, and Apple accounts, plus a growing list of banks and business tools.
- Included with Microsoft 365 at no extra cost.
- They're faster: Microsoft says a passkey sign-in takes about 3 seconds, against 69 for a password plus a code.
- Two types: a synced passkey is backed up to your account and works across your devices, while a device-bound passkey stays on one device or a physical security key.
- Start with your most sensitive accounts: administrators, finance, and anyone who can move money.
- Let everyone else add a passkey alongside their password at first.
- Give each person a backup, like a second device or a security key, so a lost phone doesn't lock anyone out.
- Keep passwords for the few systems that don't support passkeys yet.

Passwords won't disappear overnight, but passkeys are the strongest login upgrade most businesses can make.