

continued from page 3...

Common signs of a phishing email

- Sender address that's close to correct but not quite right
- Urgent or threatening language pushing quick action
- A request to change banking or payment details
- Generic greetings like "Dear Customer"
- Unexpected attachments or links, especially asking for a login
- A link that shows a different address when you hover over it
- Requests that skip your normal approval process

Trust your instincts

If an email feels slightly off — even if you can't say exactly why — that instinct is worth listening to. Attackers are patient, and the best fakes are built to feel completely routine.

If you spot a phishing email

- Don't click links or open attachments
- Don't reply, even to say "wrong person"
- Report it to IT using your normal process
- Warn a colleague if they were copied too

If you already clicked

- Tell IT immediately — speed matters more than anything else
- Disconnect the device from Wi-Fi if you can
- Change the password for that account right away
- Don't worry about looking embarrassed. A quick report is normal and expected; a quiet one is what causes real damage.

Introducing...



JOLLY BUBBLE Backpack Buddies

Jolly Bubble Whitby
1624 Dundas St E Unit 1, Whitby, ON L1N 2K8

We're hosting a community drive to ensure students have the essentials they need with all donations going to IDLF's Make a Difference Depot. Give back and help a student feel fed, confident, and ready to thrive.

ITEMS NEEDED:

- Deodorant
- Backpacks
- Art supplies
- Lunch bags
- Water Bottles
- New Running Shoes
- Non-Perishable Proteins
- Shelf-Stable Milk
- Juice
- Condiments

- School Snacks
- Soup
- Fruit Cups
- Flour
- Canned/Dried Beans & Lentils
- Cooking Oils
- Dried Fruit
- Boxed Meals (Hamburger Helper, Side Kicks, etc.)

BACKUP & DISASTER RECOVERY: THE BASICS EVERY BUSINESS NEEDS

Most businesses assume backup is happening somewhere — a cloud service, an external drive, an old server in the closet. Few have actually tried restoring from it.

Backup and disaster recovery are related but different. Backup is having a copy of your data. Disaster recovery is having a plan to actually get your business running again — systems, logins, and all — after a ransomware attack, a hardware failure, a fire, or simple human error.

A backup you've never tested isn't a backup plan. It's a guess.

Why this matters here: The Canadian Centre for Cyber Security names ransomware one of the top threats facing Canadian organizations, and publishes its own backup guidance (ITSAP.40.002) built around the 3-2-1 rule.

Industry data (ITIC, 2024) puts the average cost of downtime for a small business at roughly \$100,000 per hour — making a tested backup one of the cheapest insurance policies your business can have.

The 3-2-1 rule

The Cyber Centre's guidance boils down to one simple structure:

- 3 copies of your data — the original plus two backups
- 2 different storage types — for example, a local disk and a cloud service
- 1 copy kept off-site or offline, disconnected from your main network

That last copy matters most. Ransomware actively hunts for connected backups and encrypts them too. A second drive plugged into the same computer, or a backup folder synced live to the network, doesn't count as protection — it's just another target.

Know your numbers: RPO and RTO Two questions decide whether a backup plan actually fits your business:

- Recovery Point Objective (RPO): how much data can you afford to lose? An hour's worth? A day's?
- Recovery Time Objective (RTO): how quickly do you need to be back up and running? An hour? A weekend?

Not every system needs the same answer. Customer orders and financial records may need near-zero data loss and fast recovery; an old archive folder can probably wait.

Test it — on purpose Schedule a real restore at least once a quarter, not just a backup-completed notification. That's the only way to know it actually works before you need it to.

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

WHY YOUR EMPLOYEES SHOULDN'T HAVE ADMINISTRATOR ACCESS TO THEIR COMPUTERS

Administrator access often starts with one request. An employee needs to install a printer, update a specialist program, or change a setting on their computer.

Giving them administrator access gets the job done. The problem is that the access usually stays after the request has been completed. From then on, the employee can approve other software installations and make changes that would normally require help from IT.

If they install the wrong program, or someone takes control of their account, those same permissions can be used to change the computer.

Why this matters

In Ontario: Bill 194 is raising cybersecurity expectations across Ontario's public sector and its vendors, cyber insurers now ask about privileged access controls, and PIPEDA breach-reporting rules mean an over-privileged account can turn a small incident into a much bigger one.

What administrator access allows someone to do

An administrator has more control over a computer than a standard user. On Windows, members of the local Administrators group have full control over that computer's resources.

Microsoft's guidance on local accounts recommends limiting the number of users in that group. Depending on the computer and how it is managed, an administrator may be able to:

- Install and remove software
- Add drivers for printers and other equipment
- Create, change, or remove user accounts
- Change system settings
- Change permissions on files and folders
- Install services that continue running in the background
- Make changes to some security settings

Mac computers also have standard and administrator accounts. Apple says administrators can install and remove software, manage other users, and change settings.

Apple recommends limiting the number of administrative users and using a standard account when administrator rights aren't required.

Standard accounts are suitable for everyday work

A standard account can still be used for normal business tasks, including:

- Reading and sending email
- Using a web browser
- Working in Microsoft 365 or Google Workspace
- Accessing approved business applications
- Joining online meetings
- Printing with an installed printer
- Opening and saving files
- Changing personal settings that do not affect other users

Some applications can be installed for one user without administrator access. Others need administrator approval because they add drivers, services, or files in protected parts of the computer.

Continued on page 2....

4 • Get More Free Tips, Tools And Services At Our Website: www.attitudeit.ca 905-432-7751

Get More Free Tips, Tools And Services At Our Website: www.attitudeit.ca 905-432-7751 • 1

continued from page 1

An employee should not receive permanent administrator access because one program needs an update. IT can approve the installation, deploy the update remotely, or use a separate administrator account for that task.

How to handle software installations

Employees can still get software installed without keeping administrator access. Your IT team can install it remotely, approve a request when it is needed, or deploy updates to several computers at once. If a program expects the user to be an administrator, your IT provider may be able to change its setup or find a supported alternative.

Keep a separate administrator account for approved technical work. Do not use it for email, web browsing, or everyday tasks, and protect it with multifactor authentication where the system supports it.

Check who has access now

Ask your IT provider to review the administrator accounts on every company computer and account. Before removing access, confirm that IT still has a tested way to perform administrator tasks on every device.



COOL GADGETS: HALLIDAY G2 AI GLASSES

A pair of AI-powered glasses built for live meetings. A heads-up display shows real-time translations, notes, and prompts right in your line of sight, following conversations across 45+ languages and sending a summary once the meeting ends. A built-in voice assistant handles hands-free questions, and a 4-mic array manages calls and music. No camera, encrypted data, privacy-first by design.

SHOULD EMPLOYEES USE PERSONAL DEVICES FOR WORK?

Allowing employees to use personal phones or computers can be convenient. They already know the device, and they can check email or join a meeting without carrying another piece of equipment.

But the business still needs to decide what work is allowed, which applications employees may use, and what happens to company information if a device is lost or an employee leaves.

Personal devices can be suitable for limited work when they meet your security requirements. Company-owned devices are the better choice for sensitive work, administration, or jobs that require large amounts of business data stored on the device.

Ontario note: if you have 25+ employees, the ESA's electronic monitoring policy rule (from the Working for Workers Act) means you need a written policy disclosing whether and how you monitor devices used for work — personal or company-owned.

What counts as a personal device used for work?

Bring your own device, often shortened to BYOD, includes reading company email on a personal phone, opening documents in mobile apps, or using a home computer to connect to a business system.

Files may remain in the Downloads folder, and accounts can stay signed in after the work is finished.

Decide what employees may do Set the rules according to the work and the information involved. You might allow employees to read email through an approved mobile app but require a company computer for customer database exports, payroll, system administration, or access to sensitive client records.

Staff should know which devices and applications are permitted, whether they may download files, and what they must do before selling or replacing the device.

Set minimum security requirements

A personal device should run an operating system that still receives security updates. It should have a screen lock, device encryption where available, current updates, and multifactor authentication on company accounts.

Keep business information inside approved applications or a managed work profile where possible. Device and app management tools can apply security settings and, on supported platforms, remove company data from managed apps without touching personal photos or messages.

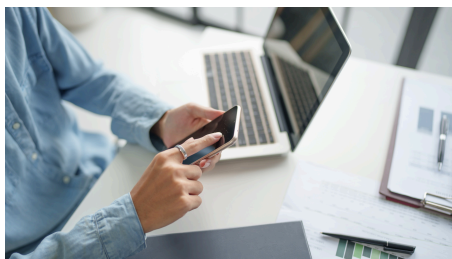
Plan for a lost device or departing employee

If a personal device is lost, IT may need to revoke active sessions, reset affected passwords, and remove company information from managed apps.

When an employee leaves, disable their account at the agreed time and confirm that business information has been returned or deleted.

When to provide a company device Use a company-owned device when an employee handles sensitive information, needs administrator access, stores a large amount of data locally, or requires specialist software.

BYOD can work, but only when the rules are clear and the device can meet them.



SMALL BUSINESS IT BUDGET: WHAT TO INCLUDE

An IT budget should reflect the systems your business uses and the changes expected during the year. Start with an inventory of computers, network equipment, software, cloud services, phone systems, websites, domains, backups, and support contracts.

Separate normal running costs (in CAD) from one-time purchases and projects, and don't forget to budget for HST on new hardware and services.

Review the budget every quarter against actual invoices, and check for unused licenses, price changes, and projects running over expected cost.

HOW LONG BUSINESS COMPUTERS LAST AND WHEN TO REPLACE THEM

Three to five years is a practical replacement range for many business computers, but age alone shouldn't decide it.

Start reviewing each device at three years, then check its security support, reliability, performance, warranty, and repair history.

Security comes first. Replace a computer if it can no longer run an operating system that receives security updates or the software your business requires. Before an old computer is sold, donated, or returned, transfer the required data and have its storage properly erased.

In Ontario, the Recycle My Electronics program offers free, certified drop-off recycling for old business computers and other e-waste — a straightforward way to dispose of hardware securely once data has been wiped.

Ask your IT provider to review your computers at least once a year and help plan replacements before something fails.

WHY GUEST WI-FI SHOULD BE SEPARATE FROM YOUR BUSINESS NETWORK

Guest Wi-Fi should give visitors internet access without allowing their devices to connect to your business computers, cameras, file storage, or network equipment.

A different Wi-Fi name and password do not prove that networks are separated. The router, wireless access points, and firewall must be configured so guest devices cannot reach the internal network.

Ask your IT provider to test the guest Wi-Fi and confirm it can reach the internet but not internal systems. Keeping this separation in place also supports your safeguarding obligations under PIPEDA for any customer or employee data on your network.



WHAT HAPPENS TO YOUR DATA WHEN YOU CANCEL A CLOUD SERVICE?

Every cloud provider handles cancellations differently. One may leave your information available for a limited time, while another restricts access as soon as the subscription ends. An account may become read-only, remain available only to an administrator, or be scheduled for deletion.

Check the provider's current documentation and your contract before cancelling. Confirm when employees lose access, how long data stays available, and what the export contains.

Before you cancel: list what's stored, export what the business needs, test any migration first, check connected systems (payment tools, forms, workflows), and update any sign-ins tied to that account. Ontario businesses often need to retain financial, employee, or contract records for a set period — check requirements with your accountant or legal adviser before deleting anything.

PHISHING & EMAIL SECURITY: WHAT EVERY EMPLOYEE SHOULD KNOW

Phishing is still the easiest way into a business. Instead of breaking through a firewall, an attacker sends an email that looks like it's from a supplier, a courier, your bank, or even your own CEO — and asks someone to click a link, open a file, or send money.

These emails work because they create urgency: an invoice that's overdue, a delivery that needs attention, a password that's about to expire.

The goal is to get someone to act before they stop to think.

The costliest version is business email compromise, where an attacker impersonates an executive or supplier to redirect a real payment or payroll deposit. No malware involved — just a convincing email and a distracted moment.

Why this matters here:

Statistics Canada found 16% of Canadian businesses experienced a cyber incident in 2023, and the Canadian Centre for Cyber Security has tracked attackers running phishing campaigns that specifically target Canadian Microsoft 365 accounts to redirect payroll deposits.

Suspected fraud should be reported to the Canadian Anti-Fraud Centre, and breaches involving personal information must be reported under PIPEDA.

continued on page 4...