ATTITUDE IT

Keeping Your Technology On Course

SUPERNOTE NOMAD

Boost your productivity with the Supernote Nomad.

This ultra-portable digital notebook features a 7.8-inch glass E Ink screen and weighs just 266 grams. The device runs on a specialized Android 11-based OS, supports a wide range of document formats and offers a natural writing feel.

Whether you're brainstorming in a café or outlining your next big project, Supernote Nomad is your essential companion with being on the go

From Physical Locks to Digital Shields: The Future of SME Data Security

NANCY MORGENROTH
POP-A-LOCK

MONIFA BROOKS
GARABYTE

ALEXANDRA CLARKE
JONES DESLAURIERS

EMMA ELKIND
ATTITUDE IT

Join Us for Data Privacy Day: A Live Panel Event for Ontario Businesses

Explore how physical security, cybersecurity, cyber insurance, and privacy best practices all work together to protect your organization's most important assets.

January 28th
Wednesday, 4:00PM

The Loft Event Studio
190 Station Street Unit 14, Ajax, ON, L1S 1R9

905-432-7751 www.attitudeit.ca

HOW TO PREVENT LEAKING PRIVATE DATA THROUGH PUBLIC AI TOOLS

Most public AI tools use the data you provide to train and improve their models. This means every prompt entered into ChatGPT or Gemini could be part of their training data. A single mistake by an employee could expose client information, proprietary code and processes. As a business owner, it's essential to prevent data leakage before it turns into a serious liability.

Establish a Clear AI Security Policy

Your first line of defense is a formal policy that clearly outline show public AI tools should be used. This policy must define what counts as confidential information and specify which data should never be entered into a public AI model, such as social security numbers, financial records, or product roadmaps.

Implement Data Loss Prevention Solutions with
AI Prompt Protection

You can prevent leakage of personal information by implementing data loss prevention (DLP) solutions that stop data leakage at the source. Cloudflare DLP and Microsoft Purview offer advanced browser-level context analysis, scanning prompts and file uploads in real time before ever reaching the AI platform.

Conduct Continuous Employee Training

Conduct interactive workshops where employees practice crafting safe and effective prompts using real-world scenarios from their daily tasks. This hands-on training enables them to de-identify sensitive data, turning staff into active participants in data security while still leveraging AI for efficiency.

Make AI Safety a Core Business Practice

Integrating AI into your business workflows is no longer optional, it's essential for staying competitive and boosting efficiency. That makes doing it safely and responsibly your top priority. The four strategies we've outlined provide a strong foundation to harness AI's potential while protecting your most valuable data.

ATTITUDE CHRONICLE

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

Why Construction Companies Need the Right IT Partner for Digital Transformation

Why Construction Software Struggles Without the Right IT Foundation

Construction companies across Ontario are investing heavily in digital tools like Bluebeam, Jonas, SmartBuild, Procore, and cloud-based project management platforms. These systems promise better collaboration, faster estimating, improved jobsite communication, and more accurate project tracking. But even with the right software in place, many construction firms still struggle to get consistent performance or reliable results. In most cases, the problem isn't the software, it's the underlying IT environment that supports it.

When Software Isn't the Problem — Infrastructure Is

Modern construction tools require stable networks, up-to-date devices, correct browser configurations, secure remote access, jobsite connectivity, and proper user permissions.

When these pieces aren't aligned, tools like Bluebeam lag, Jonas throws sync errors, and SmartBuild struggles to update. Software vendors can't troubleshoot these issues because they fall outside their scope; their support teams are not responsible for diagnosing network performance, device problems, outdated operating systems, Wi-Fi issues, or slow workstations. This often leaves construction teams stuck between vendor support and internal staff who don't have the time—or expertise—to chase down what's really causing the problem.

When staff call their vendor for support they often get **"This looks like an IT issue not a software issue"** Often the underlying network of a business can make or break how well their software tools can perform. Issues like patches not being updated, older equipment or slow internet can really bog down software from performing.

How an MSP Prevents Issues Before They Reach Vendors

This is where a strategic Managed Services Partner (MSP) becomes essential. The right MSP understands the realities of construction work: tight budgets, tight timelines, remote crews, inconsistent jobsite connectivity, and the pressure to keep projects moving. They can triage issues before they ever hit a software vendor, quickly identifying whether the problem is browser-related, hardware-related, or network-related. The MSP resolves the root cause and gets teams back to work faster.

Tight Budgets Don't Mean Weak Technology

A strategic MSP also helps construction companies make better technology decisions without overspending. With margins under pressure, no contractor wants to buy unnecessary hardware or pay for software they don't fully utilize. An experienced MSP helps teams choose the right equipment, prepare for software upgrades, secure remote workflows, and strengthen cybersecurity—all while keeping costs predictable. When the infrastructure is aligned properly, construction software runs smoother, field teams experience fewer delays, and operations remain stable.

A Proactive Partner for Digital Transformation

Ultimately, digital transformation in construction is not just about buying great software—it's about building a strong foundation of secure, reliable IT around it. With the right managed services partner, construction teams gain the confidence that their systems will work the way they need them to, every day, on every jobsite.

DATA PRIVACY DAY: ESSENTIAL BEST PRACTICES EVERY ONTARIO BUSINESS SHOULD IMPLEMENT IN 2026

Data Privacy Day is more than a reminder about compliance, it's an opportunity for Ontario businesses to step back, review their current security posture, and set stronger privacy practices for the year ahead. With cyber threats rising, remote work expanding, and digital tools becoming core to everyday operations, businesses can no longer rely on ad-hoc or outdated approaches to data protection.

The good news: improving data privacy doesn't require massive investment. It requires awareness, structure, training, and a trusted IT partner who understands how to apply practical protections that reduce risk.

Below are some of the most important step's organizations can take to strengthen privacy, protect sensitive information, and build a culture of security across their teams.

1. Start the Year with a Company-Wide Password Reset Day

A strong password strategy is one of the simplest and most effective ways to reduce risk. Yet many breaches originate from weak or reused passwords that attackers can guess or buy on the dark web.

Introduce an annual Password Reset Day:

- Reduce exposure from old or compromised credentials
- Encourage secure passphrases instead of short passwords
- Reinforce healthy habits every employee can adopt
- Provide a checkpoint for reviewing account access
- Go over best practices and company password policies

Your IT provider should help automate this process and ensure that MFA is active and enforced across all critical systems.

2. Train Your Employees to Recognize and Avoid Threats

Most cyber incidents are caused by human error rather than technical failure. This makes employee awareness one of the most powerful tools in your privacy strategy.

Effective training covers:

- How to spot phishing emails
- Safe handling of sensitive data
- Using AI tools responsibly
- Recognizing social engineering tactics
- Safe browsing and file-sharing habits
- Protecting company data when working remotely

Schedule a Lunch & Learn Cyber Training sessions designed to give teams practical, real-world strategies to stay safe.

3. Run Tabletop Exercises to Improve Incident Readiness

No matter how strong your protections are, every organization should expect that incidents may still happen. Tabletop exercises simulate cyber events so leaders and staff can practice how they would respond.

These exercises help teams:

- Understand roles and responsibilities
- Improve communication between departments
- Identify gaps in policies and procedures
- Reduce downtime during a real incident
- Build organizational confidence and resilience

An IT partner should walk your leadership team through these scenarios regularly and update processes based on what you learn.

4. Review Who Has Access to Sensitive Information

Data privacy depends heavily on controlling access. Over time, permissions drift , former employees keep access, departments accumulate unnecessary privileges, and external collaborators retain shared files long after a project ends. Also a good time to review email admin access, check that your administrator has created a separate admin account to monitor the email admin account.

A privacy-focused business should regularly:

- Audit user accounts
- Remove or restrict old access
- Apply the principle of least privilege
- Use secure file-sharing methods
- Review how sensitive information is labeled and stored
-

Your IT provider should support these reviews and automate as much as possible.

5. Keep Systems Updated and Protected with a Security-First Approach

Outdated systems and unpatched software create easy openings for attackers. Businesses should work with their IT partner to ensure:

- Operating systems are supported and patched
- Browsers and applications are up to date
- Endpoint protection is active and monitored
- Backups are tested and recoverable
- Remote workers follow secure access practices

A proactive IT partner reduces risk through ongoing monitoring, strategic guidance, and routine Technical Business Reviews (TBRs).

6. Establish Clear Guidelines for AI Use in the Workplace

With AI tools becoming part of everyday workflows, businesses must define how employees can safely use them and identify business approved applications. Have your appointed IT create business accounts for any approved apps to integrate with email and Microsoft programs.

Key considerations include:

- What types of data can and cannot be entered into AI tools
- Whether third-party AI platforms are permitted
- How to protect client information
- How AI output is reviewed and validated
- How employees should handle privacy concerns

Attitude IT helps businesses create acceptable use policies and provides training, so teams understand how to use AI safely and effectively.

17. Make Data Privacy a Year-Round Commitment

Data Privacy Day is a great starting point , but strong privacy practices must continue throughout the year. That means:

- Regular TBRs with your IT provider
- Quarterly or semi-annual training
- Reviewing software and access controls
- Updating policies as technology evolves
- Ensuring backups and recovery plans remain current
-

A strong IT provider should lead these initiatives and ensure your business stays aligned with modern privacy expectations.

Join Us for Data Privacy Day: A Live Panel Event for Ontario Businesses

To help organizations strengthen their privacy and security posture, Attitude IT is hosting a Data Privacy Day Panel Event in collaboration with:

🔒 Pop-A-Lock – Physical security and access control

💻Garabyte – Digital privacy and secure document handling

💼Attitude IT – Cybersecurity, governance, and IT strategy

Together, we'll explore how physical security, digital systems, and cybersecurity all work together to protect your organization's most important assets.

This session is designed for:

- Business owners
- Executive teams
- Office managers
- HR & operations leads
- Anyone responsible for data handling or technology

Save the Date: January 28th Time 4pm at The Loft Event Studio in Ajax. To save your spot email emma@attitudeit.ca for registration link.

S. Support Your Team With a Cybersecurity Lunch & Learn

If you'd like to take this opportunity to kick off the year with stronger practices, Attitude IT also offers Lunch & Learn employee cyber training sessions for businesses of all sizes.

We cover:

- Data privacy essentials
- Phishing awareness
- Password hygiene
- Safe AI use
- Practical, real-world examples
- Best practices for remote and hybrid teams

Your team will come away with clear, simple steps they can apply immediately. Ready to Strengthen Your Data Privacy in 2026?

Data Privacy Day is a great reminder that protecting your business isn't just about technology . It's about people, processes, and proactive habits.

Attitude IT is here to help you build a stronger foundation.

👉 Join our panel event: https://www.eventbrite.com/e/cyber-resilience-and-privacy-by-design-tickets-1978895113555?aff=oddtdtcreator

👉Book your Lunch & Learn by calling 905-432-7751 or email info@attitudeit.ca

👉Schedule a privacy review with our team

Let's make 2026 your strongest year for data protection and cybersecurity.