



# 4 POPULAR SCAMS TO WATCH OUT FOR

Keeping up with cybercriminals is like trying to nail jelly to the wall. Just as you think you're up to speed, a new scam hits the headlines. Using new tech innovations like AI, scammers are getting much better at impersonating banks, health care providers and...us. This year has been no exception, with a slew of fresh scams hitting cell phones and bank accounts everywhere. Here are four scams to watch out for this year.

**How to avoid it:** If you receive an urgent call like that, call your loved one directly to verify that they are safe. If they don't answer, call other family members to see if they can verify the situation. Remember, the criminals will try to convince you to keep it a secret – don't.

## 1. Phony Cell Provider E-mails

Increasingly, cybercriminals are taking advantage of cell service outages to scam customers. It's happening all over the US with AT&T customers, who, after an outage, receive bogus e-mails offering refunds or credits.

**How to avoid it:** Never click on links or payment instructions in an e-mail. Always verify that any communication from a provider is coming from an official domain, like @att.com, or call AT&T directly using their official number or website.

## 3. Check "Cooking"

Banks reported nearly 700,000 instances of check fraud in 2022, according to reporting by Associated Press. We've talked about criminals stealing checks from mailboxes, but recently they've started taking pictures of checks instead. Then they use off-the-shelf digital tools to make counterfeit checks, deposit the digital one using a mobile banking app or sell the checks online.

**How to avoid it:** Use your credit card as much as possible. When a paper check is unavoidable, skip your mailbox and take it directly to the post office.

## 4. Home Improvement Scams

In 2023, a study by JW Surety Bonds reported that one in 10 Americans had been a victim of a contractor scam, losing an average of \$2,500. These scammers often demand up-front payments or deposits and then fail to complete the work, deliver substandard results or disappear altogether, leaving homeowners out of pocket and with unfinished projects.

**How to avoid it:** Ensure the contractor is licensed and insured, get everything in writing, don't skim the contract and never pay the full fee up front.

**DISASTER RECOVERY & STAYING PROTECTED**  
ENERGY/POWER FACILITY NETWORK  
Disruption to our power supply, our ability to communicate and our facilities can cost us money and production time!

**Expert Panel Discussion**  
When disaster strikes - facility flood or fire, power outages & cyber/network attacks what is your plan, who are the stakeholders, and how do you prevent it from happening again?  
Join us for a panel discussion and hear from experts in the field of restoration, IT networking and power.

- Disaster Recovery Plans
- Pro-Active Solutions
- Learn from Case Studies
- First 5 steps when disaster strikes

Thursday, June, 5 2025  
9:00am-10:00am  
Venture13 Innovation Centre  
739 D'Arcy Street, Cobourg

Please share this invite with your maintenance, IT, Finance & Leadership Teams

### YOUR PHOTOS ARE MORE REVEALING THAN YOU THINK!

Did you know that when you send someone a photo from your smartphone, you might be sharing information such as when, where and how the photo was taken? If that makes you feel uncomfortable, you can turn this feature off.

On an iPhone, open the photo, tap the share icon, then "Options." Switch off "Location," then tap "Done." You can also stop location tracking altogether in Settings > Privacy & Security > Location Services. Scroll to "Camera" and toggle to "Never." On an Android, click the photo you want to send, tap "Details" (look for a three-dot menu) and select "Remove location data."



# ATTITUDE CHRONICLE

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

## WHAT'S NEW

May was a month of meaningful community initiatives for Attitude IT. We joined Campkins' 52nd Annual Open House with Big Brothers & Big Sisters North Durham, supported Easter Seals Red Shirt Day for National Accessibility Week, and took on Restoring Kindness Canada's 30 Acts in 30 Days challenge. We also welcomed Muhammad and Vivian as Onsite and Help Desk Engineers in training through our Co-Op program, launched in May. Looking ahead, we're excited for upcoming events. The Herizon House Golf Charity Tournament on June 4 supports survivors of domestic violence, and on June 5, we're hosting a Disaster Planning Panel at Venture 13 with Surge Arrest, Watton Restoration, and the Northumberland Manufacturers Association. As summer storms threaten power and equipment, it's crucial to prepare. Let us help you minimize downtime with an emergency response and disaster recovery plan. Call today to schedule your summer Network Audit. .

## HOW TO PUT GENERATIVE AI TO WORK FOR YOUR BUSINESS



The rapid evolution of AI over the past year has been nothing short of revolutionary, particularly generative AI – technologies that generate text, images, video, 3-D models and even code – which saw a breakout year in 2023. In ChatGPT's first month, it amassed 57 million users, making it the fastest-growing consumer application in history, according to research from investment bank UBS. Despite its popularity, there's an undercurrent of uncertainty among some business leaders. SMB leaders are asking big questions: What's the real deal with AI (beyond all the buzz)? How do I actually get it to work for my business? How do we use this responsibly and keep our customers' data safe? The key to navigating these questions is all about experimenting with AI, focusing on the big wins it can bring to the table and learning best practices for using the technology responsibly.

### What AI Can Do For Your Business

Of businesses using the generative AI platform ChatGPT today, one in four have already saved more than \$75,000. That's according to a 2023 survey by ResumeBuilder, which also found that 49% of companies are already using ChatGPT and that an additional 30% plan to use it in the future. Generative AI tools like ChatGPT, Claude and DALL-E are popular because they're affordable (subscriptions run around \$20 per user/month) and effective. Generative AI's versatility allows it to take on many valuable roles, like whipping up content. Businesses save a lot of money creating engaging content for their audience without paying more for ads or agencies. AI can also quickly examine market trends and crank out reports, cutting down on research and paperwork

This Monthly Publication Provided by Brandon Jones CEO Attitude IT



### OUR MISSION:

To build a community of secure Ontario businesses that do not have to worry about data breaches or downtime.

continued on page 2..

...continued from cover

costs so leaders can spend more time on higher-value activities.

More ways AI can go to work for you:

- **Content Assistant:** Tools like ChatGPT and Claude can create marketing materials, blog posts and social media content, ensuring a consistent brand voice and tone across all channels. They can also analyze thousands of online resources to craft the perfect job description and write SOPs, proposals, contracts and leases.
- **Get To The Point:** Generative AI can distill lengthy documents, articles and e-mails into concise summaries, making it easier to grasp key points quickly.
- **Personalize Your Marketing:** Generate tailored e-mail marketing campaigns or personalized product recommendations to enhance customer engagement and increase sales.
- **Product Discovery And Innovation:** Leverage AI to analyze customer feedback and market trends for new product ideas or improvements, speeding up innovation.

- **Data Analyst:** Employ AI for deep data analysis, uncovering insights into customer behavior, operational efficiencies and market opportunities.
- **Automate Routine Tasks:** From scheduling to invoicing, AI can automate repetitive, time-consuming tasks, such as drafting meeting summaries or generating reports, allowing teams to focus on strategic work.

**AI Best Practices**

While AI can dramatically enhance efficiency and creativity, there are best practices to ensure its use is both effective and ethical:

- **Never Share Sensitive Information:** To protect privacy, avoid using personally identifiable information (PII) or protected health information (PHI) with AI tools. Assume anything that you input into ChatGPT is public information.
- **Verify and Review:** AI is a powerful tool, but it's not infallible. It can sometimes inherit biases from training data or generate fabricated or wrong answers. Always review its outputs as you would a human co-worker's work.

- **Experiment:** The best way to understand AI's potential is to experiment. Start small, like using ChatGPT prompts to write a social media post. As you gain confidence, integrate generative AI in places where it can add the most value, like automating routine tasks, enhancing creative processes or improving decision-making with data analysis.

**The Consequences Of Ignoring AI**

AI isn't coming – it's arrived. Driven by billions in investment and some of the brightest minds on the planet, it's reshaping the business landscape in ways we're only beginning to understand. Choosing not to integrate AI into business operations would be like refusing to use e-mail in the 1990s. Without it, you might soon find yourself in a world you don't know how to work in. Instead of viewing AI as a looming threat, see it as an opportunity to tackle old problems with novel solutions. Yes, AI is changing the business playbook, but it's also empowering us to deliver extraordinary value to our customers in new ways, dream bigger and achieve more.

**Do You Safeguard Your Company's Data And Your Customers' Private Information BETTER THAN Equifax, Yahoo And Target Did?**

Our 100% FREE and 100% confidential, exclusive CEO Dark Web Scan is your first line of defense. To receive your report in just 24 hours, visit the link below and provide us with your name and company e-mail address. Hopefully, it will be ALL CLEAR and you can breathe easy. But if your company, your profits and your customers are AT RISK, we'll simply dig a little deeper to make sure you're protected.

Don't let cybertheft happen to you, your employees and your customers.

**Reserve your exclusive CEO Dark Web Scan now!** If the answer is "NO" – and let's be honest, the answer is no – you are leaving yourself and your company open to massive liability, millions in fines and lost business, lawsuits, theft and so much more.

Why? Because you are a hacker's #1 target. They know you have access to financials, employee records, company data and all that juicy customer information – Social Security numbers, credit card numbers, birthdates, home addresses, e-mails, etc.

Don't kid yourself. Cybercriminals and hackers will stop at NOTHING to steal your credentials. And once they have your password(s), it's only a matter of time until they destroy your business, scare away your customers and ruin your professional and personal life.

Claim your Free Dark Web Scan Today! Call 416-900-6047



**IT DISASTER PREPAREDNESS FOR ONTARIO BUSINESSES: ENSURING CONTINUITY IN THE FACE OF EMERGENCIES**

In today's digital-first business landscape, IT infrastructure is the backbone of operations. For Ontario businesses, disasters such as power outages, cyberattacks, and hardware failures can disrupt productivity, compromise data, and lead to financial setbacks. Proactive disaster planning and preparedness ensure continuity, safeguarding valuable assets. Here's how businesses can protect their IT systems against emergencies.

**1. Implement a Comprehensive Emergency Response Plan**

An IT emergency response plan outlines protocols for immediate action when systems fail due to a disaster. Essential components include:

- **Incident Identification & Reporting:** Establish guidelines for detecting, assessing, and reporting IT disruptions. Roles & Responsibilities: Assign employees to specific response tasks to streamline recovery.
- **Communication Strategy:** Ensure clear communication channels for staff, customers, and vendors during emergencies. Alternative Workflows: Prepare contingency plans, such as remote access solutions, to maintain operations if onsite systems are compromised.

**2. Prioritize Hardware & Software Redundancy**

- Technology failures—whether from equipment damage or software corruption—can halt business operations. Preventive measures include:
- **Regular Hardware Maintenance:** Conduct routine checks to ensure servers, workstations, and network devices are functioning optimally.
  - **Redundant Systems:** Invest in backup servers, secondary storage solutions, and duplicate hardware to reduce downtime.
  - **Virtualized Infrastructure:** Consider cloud computing or virtualization to minimize reliance on physical equipment.
  - **Strengthen Data Backup & Recovery Strategies**
  - **Losing critical business data can be devastating.** To safeguard information: Automated Backups: Schedule daily, weekly, or real-time data backups to cloud-based or offsite storage.

- **Multi-Layered Backup Solutions:** Use a combination of cloud storage, external drives, and network backups for redundancy.
- **Data Encryption & Security:** Protect backups with strong encryption and access controls to prevent unauthorized breaches.
- **Recovery Testing:** Regularly test data restoration processes to ensure backups are functional when needed.

**4. Prepare for Cybersecurity Threats**

- Cyberattacks, such as ransomware and phishing scams, can cripple business operations. Preventative steps include:
- **Firewall & Antivirus Protection:** Maintain up-to-date security software to defend against attacks.
  - **Multi-Factor Authentication (MFA):** Require additional verification layers beyond passwords.
  - **Incident Response Plan:** Set protocols to contain, investigate, and recover from cyber breaches.
  - **Employee Training:** Educate staff on recognizing cybersecurity threats and following best practices.

**5. Conduct Regular Risk Assessments & Drills**

To stay prepared, businesses should continuously evaluate vulnerabilities and refine their disaster response.

- **Tabletop Exercises:** Simulate emergency scenarios to assess response strategies.
- **Penetration Testing:** Evaluate cybersecurity defenses through ethical hacking.
- **Compliance Checks:** Ensure alignment with Ontario's data protection and IT security regulations

Ontario businesses must prioritize IT disaster preparedness to prevent disruptions, minimize downtime, and protect valuable data. By developing a structured emergency response plan, maintaining hardware and software redundancies, fortifying data backup strategies, and implementing cybersecurity protocols, businesses can confidently navigate potential emergencies while safeguarding their operations.

**WELCOME TO THE ATTITUDE IT TEAM: MUHAMMAD AND VIVIAN!**



**JUNE 18<sup>TH</sup> AT 1PM**

**ATTITUDE IT**  
Empowering Your Technology Success

**CYBER PROTECTION IN ONTARIO: INSURANCE VS. WARRANTY WITH ATTITUDE IT**

TO RESERVE A SPOT EMAIL: [EMMA@ATTITUDEIT.CA](mailto:EMMA@ATTITUDEIT.CA) OR CALL 416-900-6047

**CARTOON OF THE MONTH**

