ATTITUDE IT
Keeping Your Technology On Course

CANADIANSME NATIONAL BUSINESS AWARDS 2025
TECH BUSINESS OF THE YEAR 2025
ATTITUDE IT
Keeping Your Technology On Course
TECH BUSINESS OF THE YEAR
2025
NOMINEE
CanadianSME National Business Awards
Shipping Partner
Preferred HR and Payroll Partner
ups
ADP
www.smeawards.ca
#SMEAWARDS2025

Join Us in Welcoming Our New Staff Member!

Mark, he joins our tech team as a network technician

STRIKE UP 2026

YOU'RE INVITED!

Live Viewing Party

Thursday February 26th @ 10 am - 3:30 p.m.

Join us at Venture13 for a networking event and watch party of the inspiring StrikeUP Digital Conference for Women Entrepreneurs.

Custom gift bags for the first 30 guests, specially made with a local touch.

739 D'Arcy Street, Cobourg
Venture13 - Lecture Hall

Sponsored by

beneco SòOPAK CUSTOM PACKAGING

ATTITUDE IT Keeping Your Technology On Course

RBC

Hosted by:

V13 VENTURE13

20 YEARS NMA NORTHUMBERLAND MANUFACTURERS ASSOCIATION

ATTITUDE CHRONICLE

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

THE "DEEPFAKE CEO" SCAM
URGENT CEO VOICE CALL
FAKE MONEY TRANSFER
WIRE TRANSFER
FORM
ACCOUNT
SEND
TO A FRAUDULENT ACCOUNT
MULTI-FACTOR VERIFICATION
VERIFY REQUESTS
SCAM AWARENESS TRAINING

How Ontario Businesses Can Protect Themselves from AI Voice Cloning and Synthetic Fraud

The phone rings, and it's your boss.

The voice is unmistakable, the same tone, cadence, and inflection you hear every day. They sound rushed and stressed. They're asking for a favour: an urgent wire transfer to finalize a vendor agreement, or immediate access to sensitive client or employee information.

Everything about the call feels legitimate. You trust the voice. You trust the urgency. Your instinct is to help.

But what if the person on the line isn't your boss at all?

What if every word, pause, and emotional cue has been perfectly replicated by artificial intelligence?

In seconds, a routine phone call can turn into a costly mistake.

For Ontario businesses, AI voice cloning scams represent a rapidly growing threat that targets people, trust, and organizational process.

The Rise of AI Voice Cloning Scams

Cybercriminals have evolved far beyond poorly written phishing emails. Today's attackers leverage artificial intelligence to impersonate real people with alarming accuracy. AI voice cloning requires only a short audio sample — often just a few seconds — to recreate someone's voice. These samples are easy to obtain from publicly available sources such as:

- Webinars and virtual conferences
- Media interviews and podcasts
- Marketing videos and social media content
- Public presentations and recorded meetings

Once collected, attackers use widely available AI tools to generate realistic voice models capable of delivering scripted, emotionally charged messages. The barrier to entry is low, the tools are inexpensive, and the realism improves daily.

How This Changes Business Email Compromise

Traditional Business Email Compromise (BEC) relied on phishing, spoofed domains, or compromised inboxes to trick employees into sending money or sensitive data. While these attacks are still common, improved email filtering and security controls have raised the bar.
Voice-based attacks bypass these defences entirely.
AI-powered vishing (voice phishing) exploits urgency and authority — two factors that email cannot replicate as effectively. When a request comes from a familiar voice, especially from leadership, employees are far less likely to pause and verify. Emotion replaces analysis, and speed replaces caution.

Why AI Voice Cloning Works So Well

These scams succeed because they exploit human behaviour rather than technical weaknesses.

Employees are conditioned to respond quickly to leadership. Questioning a senior executive feels uncomfortable. Add urgency, stress, or confidentiality, and rational decision-making breaks down.

Attackers often time calls before weekends, after hours, or during busy periods when verification feels inconvenient.

Continued on page 2

Continued from page 1

Modern AI can convincingly replicate emotional states such as frustration, fatigue, or urgency ,all designed to pressure the victim into acting quickly.

The Limits of Detection

Unlike phishing emails, fake voices are extremely difficult to detect. Early AI-generated voices often sounded robotic, but modern tools have eliminated many obvious flaws.

Human hearing is unreliable, and the brain naturally fills in gaps to make voices sound familiar. Relying on employees to "trust their instincts" is not a sustainable defence.

For Ontario businesses ,particularly those subject to PIPEDA, professional standards, or client confidentiality obligations — defensible process must replace instinct.

What This Means for Ontario Business Owners

For business owners, partners, and directors, AI voice cloning is not just a cybersecurity issue — it is a business risk.
A successful impersonation attack can result in:

- Direct financial loss that may not be recoverable
- Exposure of confidential client or employee information
- Reputational damage and loss of trust
- Regulatory scrutiny under PIPEDA and contractual obligations
- Increased personal accountability for leadership

Increasingly, insurers and auditors ask not how sophisticated the attack was, but whether reasonable safeguards were in place and enforced.

Why Cyber Insurance Alone Is No Longer Enough

Many Ontario businesses assume cyber insurance will cover fraud-related losses. In reality, insurers are tightening requirements.
Today, insurers commonly expect:

- Documented verification procedures
- Dual approval for financial transactions
- Security awareness training that includes vishing scenarios
- Evidence that policies are enforced, not just written

If required controls are missing or bypassed, coverage may be reduced or denied — even when the fraud involves AI.

Verification protocols and training are no longer optional. They are financial safeguards.

Establishing Clear Verification Protocols

The most effective defence against AI voice cloning is a formal verification process.

Ontario businesses should adopt a zero-trust approach for any voice-based request involving money, credentials, or sensitive data.
Best practices include:

- Hanging up and calling back using a known internal number
- Confirming requests through secure platforms such as Microsoft Teams
- Requiring secondary approval for wire transfers or account changes
- Using internal challenge-response phrases or "safe words"

If verification cannot be completed, the request is declined — without exception.

Training Your Team to Respond with Confidence

Security awareness training must evolve to reflect AI-driven threats.

Employees should be trained to:

- Treat urgency as a warning sign
- Follow verification steps without fear of reprimand
- Escalate suspicious requests immediately
-

Effective programs include simulated vishing scenarios, role-specific training for finance, HR, IT, and executive assistants, and regular refreshers.
Verification should be positioned as a requirement — not a lack of trust.

Governance, Not Mistrust

One of the biggest barriers to implementing verification protocols is concern about trust.
Strong controls are not about mistrusting employees or leadership.
They are about governance.

Good governance:

- Protects employees from pressure
- Removes judgment calls in high-stress situations
- Shields leadership from preventable financial and legal exposure

When verification is standardized, the process — not the individual — makes the decision.

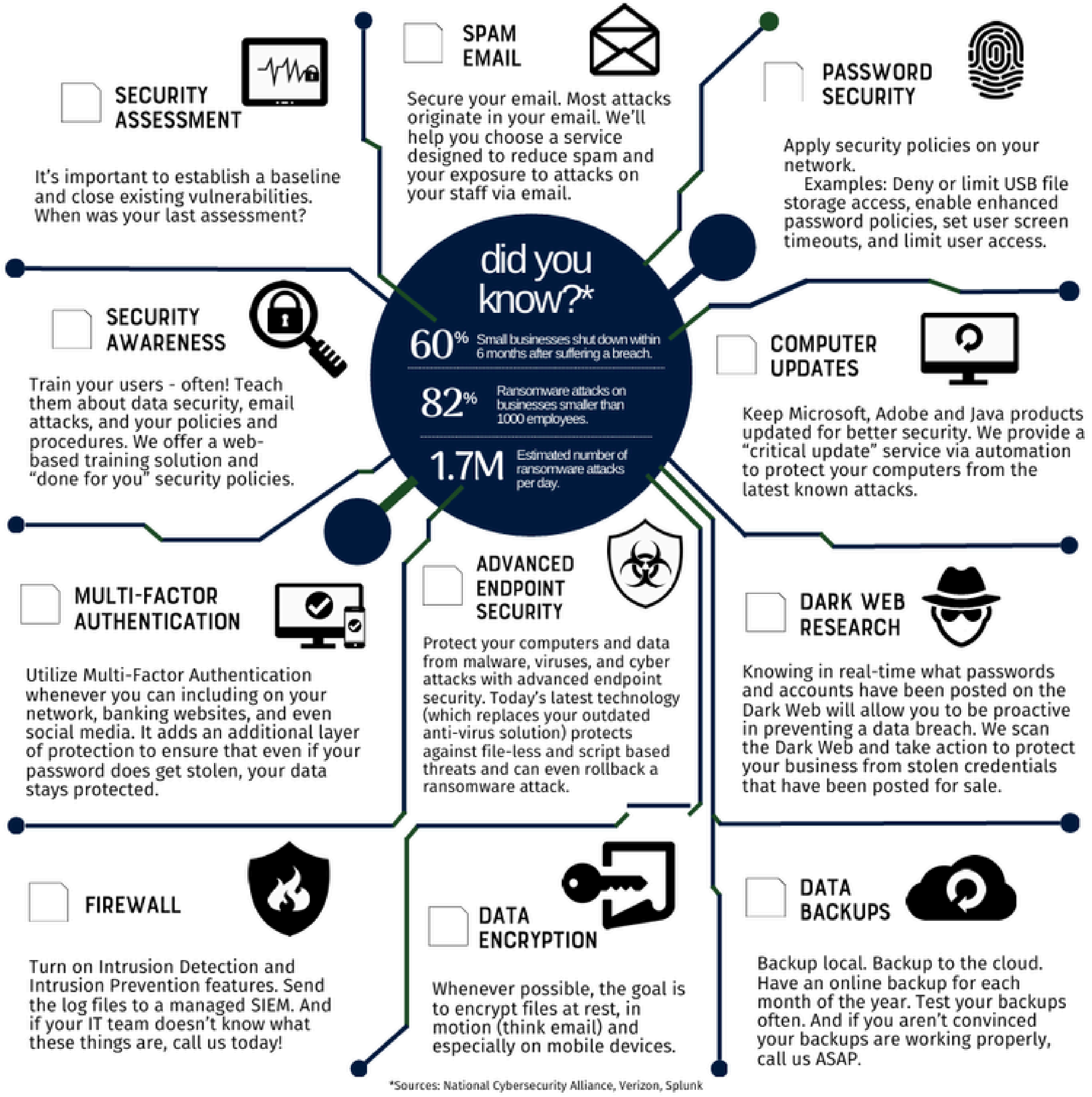
Preparing for the Next Wave of Synthetic Threats

Voice cloning is only the beginning. AI-generated video and real-time impersonation are advancing quickly. Ontario organizations should prepare by:

- Expanding incident response plans to include deepfake scenarios
- Defining how executive communications will be validated
- Establishing clear escalation and response procedures

Waiting until an incident occurs means responding under pressure — exactly what attackers rely on.

12 Ways To Protect Against RANSOMWARE ATTACKS



□ **SECURITY ASSESSMENT**

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

□ **SPAM EMAIL**

Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email.

□ **PASSWORD SECURITY**

Apply security policies on your network.
Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.

□ **SECURITY AWARENESS**

Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.

did you know?*

60% Small businesses shut down within 6 months after suffering a breach.

82% Ransomware attacks on businesses smaller than 1000 employees.

1.7M Estimated number of ransomware attacks per day.

□ **COMPUTER UPDATES**

Keep Microsoft, Adobe and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.

□ **MULTI-FACTOR AUTHENTICATION**

Utilize Multi-Factor Authentication whenever you can including on your network, banking websites, and even social media. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.

□ **ADVANCED ENDPOINT SECURITY**

Protect your computers and data from malware, viruses, and cyber attacks with advanced endpoint security. Today's latest technology (which replaces your outdated anti-virus solution) protects against file-less and script based threats and can even rollback a ransomware attack.

□ **DARK WEB RESEARCH**

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

□ **FIREWALL**

Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM. And if your IT team doesn't know what these things are, call us today!

□ **DATA ENCRYPTION**

Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.

□ **DATA BACKUPS**

Backup local. Backup to the cloud. Have an online backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP.

*Sources: National Cybersecurity Alliance, Verizon, Splunk

Cyber Insurance If all else fails, protect your income and business with cyber damage and recovery insurance policies.