



CYBERSECURITY AWARENESS MONTH

Shadow AI

The Cybersecurity Risk Hiding in Plain Sight

A Practical Guide for Canadian Businesses

AI is changing the way we work. The challenge isn't whether employees will use it. **It's making sure they use it responsibly.**

CALL
807-345-2900

EMAIL
sales@teleco.ca

WEB
teleco.ca



THE BASICS

What is Shadow AI?

Artificial intelligence has quickly become part of everyday work.

Employees are using AI to draft emails, summarize documents, analyze information, create presentations, troubleshoot problems and save time on repetitive tasks.

That can be a good thing.

The concern starts when employees use AI tools that haven't been approved, reviewed or managed by their organization.

This is known as Shadow AI.

It can be as simple as an employee copying information into a public AI chatbot because it helps them get something done faster.

There may be no bad intent. In many cases, the employee is simply trying to be productive.

But once company information leaves an approved environment, the organization may have limited visibility into where that information goes, how it is stored, how it may be used, or who ultimately has access to it.

Shadow AI can include:

- Using personal AI accounts for work
- Uploading company documents to public AI platforms
- Asking AI to summarize confidential emails or meeting notes
- Installing unapproved AI browser extensions
- Using AI transcription or meeting tools without IT approval
- Entering customer information into an AI chatbot
- Connecting third-party AI applications to company systems

The issue isn't AI itself. The issue is using AI without the appropriate oversight.

WHY IT HAPPENS

Why Employees Turn to Unapproved AI

Most Shadow AI doesn't begin with someone intentionally ignoring cybersecurity.

It usually begins with a simple thought:

Employees may discover an AI application online, hear about one from a colleague, or already use an AI platform in their personal life.

Within seconds, they can create an account and start using it at work.

That convenience is exactly what makes Shadow AI difficult for organizations to manage.

“

This tool can help me get this done faster.”

CONSIDER THIS SCENARIO

- 1 An employee needs to summarize a lengthy customer document.
- 2 Rather than spending an hour reviewing it, they upload the document to an AI platform and ask for a summary.
- 3 Thirty seconds later, the job is done.

But what information was contained in that document?

Customer names?

Pricing?

Financial information?

Contracts?

Internal strategy?

Personally identifiable information?

And does the organization know where that information has now gone?

Convenience can create blind spots.

When technology adoption happens outside established IT and security processes, businesses lose visibility.

You can't properly protect technology you don't know is being used.

WHY IT MATTERS

The Business Risks Behind Shadow AI

AI can deliver significant productivity benefits, but organizations need to understand the risks that can come with unmanaged use.

 Data Exposure	Employees may unintentionally enter confidential, proprietary or customer information into third-party AI platforms. Once information leaves your controlled environment, managing how that information is handled becomes more difficult.
 Privacy & Compliance	Organizations have responsibilities surrounding the information they collect, store and process. Depending on your industry and the information involved, using an external AI service could introduce privacy, contractual, regulatory or compliance considerations.
 Intellectual Property	Employees may use AI to work with internal documents, product information, processes, source material or other intellectual property. Organizations should understand how the AI platforms they authorize handle submitted information.
 Inaccurate Information	AI-generated answers can sound confident while still being incomplete or incorrect. Employees need to understand that AI output should be reviewed rather than automatically trusted.
 Unauthorized Applications	AI tools, browser extensions and integrations can request access to email, documents, calendars and other business systems. Without proper review, organizations may not know what permissions have been granted or what information is accessible.
 Lack of Visibility	Perhaps the biggest issue is simply not knowing. If employees are independently adopting AI applications, IT and security teams may have difficulty identifying where company information is being shared.

BEFORE YOU PUT COMPANY INFORMATION INTO AI

Stop. Think. Check.

AI should be treated like any other technology your organization uses to handle business information. Before entering company information into an AI platform, employees should ask a few simple questions.

The 7-Question AI Check

1 Is this AI tool approved by my organization?

If you're not sure, check before using it for company work.

2 What information am I about to share?

Consider whether it contains customer, employee, financial, confidential or proprietary information.

3 Would I be comfortable sending this information to an unknown third party?

If the answer is no, don't paste it into an unapproved AI platform.

4 Do I understand how the provider handles my data?

Business and consumer versions of AI services may have very different privacy and data-handling terms.

5 Does the application need access to other systems?

Be cautious when AI applications request access to email, cloud storage, calendars or other business platforms.

6 Have I verified the answer?

AI can make mistakes. Important information should always be reviewed by a qualified person.

7 When in doubt, have I asked IT?

A quick conversation can prevent a much larger problem.

A USEFUL RULE

If information shouldn't be shared publicly, don't enter it into an unapproved public AI tool.

WHAT BUSINESS LEADERS CAN DO

Don't Just Block AI. Manage It.

Simply telling employees not to use AI may not address the underlying issue.

People are adopting these tools because they see value in them.

A better approach is to give employees clear boundaries, approved options and practical guidance.

START WITH THESE FIVE STEPS

1**Create an AI Acceptable Use Policy**

Clearly explain what employees can and cannot do with AI. Keep the policy understandable and practical.

2**Identify Approved AI Platforms**

Give employees safe alternatives. If approved tools meet their needs, they're less likely to look elsewhere.

3**Define What Data Can Be Used**

Employees should understand which types of information can be entered into AI systems and which information must remain protected.

4**Educate Your Team**

AI awareness should become part of cybersecurity awareness. Show employees real examples rather than relying entirely on technical language.

5**Review AI as Part of Your Security Strategy**

AI applications should go through appropriate technology, privacy and cybersecurity reviews before being adopted across the organization.

A SIMPLE AI POLICY STARTING POINT

What Should an AI Policy Cover?

Every organization will have different requirements, but a practical AI policy can start by addressing a few fundamental questions. Your policy should make clear:

☒ Which AI tools are approved?	Employees should know where to find the current list.
☒ What information is prohibited?	Define restrictions around confidential information, personal information, customer data, passwords, financial records and other sensitive material.
☒ Who can approve new AI applications?	Give employees a straightforward process for requesting new tools.
☒ How should AI-generated content be reviewed?	Employees should remain responsible for checking accuracy, appropriateness and quality.
☒ Can AI connect to business systems?	Define who can authorize integrations with email, file storage, CRM platforms and other systems.
☒ Who should employees contact when they're unsure?	Make asking for help easy.

THE GOAL IS RESPONSIBLE ADOPTION

A good AI policy shouldn't exist simply to say "no."

It should help employees understand how to say "yes, safely."

THE BOTTOM LINE

AI Isn't Going Away. Neither Is the Need for Cybersecurity.

AI has tremendous potential to help businesses work smarter, solve problems and improve productivity.

But new technology also creates new responsibilities.

Organizations need visibility into the tools employees are using, the information being shared and the risks being introduced into their environment.

The answer isn't to fear AI. It's to understand it, manage it and use it responsibly.

That starts with good policies, employee education, appropriate security controls and a technology strategy that keeps pace with the way people actually work.

LET'S TALK

Make Technology Work for Your Business

For more than 40 years, Teleco has helped organizations navigate changing technology.

Today, that means looking beyond individual products and helping businesses bring together the technology, security and support they need to operate confidently.

If Shadow AI has you asking questions about your organization's cybersecurity, technology policies or overall IT environment, we'd be happy to start a conversation.

Start the conversation



TELECO
Integrating Technologies

CALL
807-345-2900

EMAIL
sales@teleco.ca

WEB
teleco.ca