ROGERS cybersecure catalyst

Secure Use of Artificial Intelligence

March 2026

Lester Chng

CISSP, PMP
lester.chng@torontomu.ca

Senior Cybersecurity Advisor
Rogers Cybersecure Catalyst,
Toronto Metropolitan University

Agenda

- AI Demystified
- Dangers of Using AI
- Scenarios & Discussions
- Q&A

Have you used an AI tool in the last 30 days? (ChatGPT, Google Gemini, Copilot, Claude, Siri, etc.)

What This Session About

This session **IS** about:

- Understanding what AI tools do with your data
- Knowing which uses are safe and which are risky
- Walking away with practical rules you can use immediately

This session is **NOT** about:

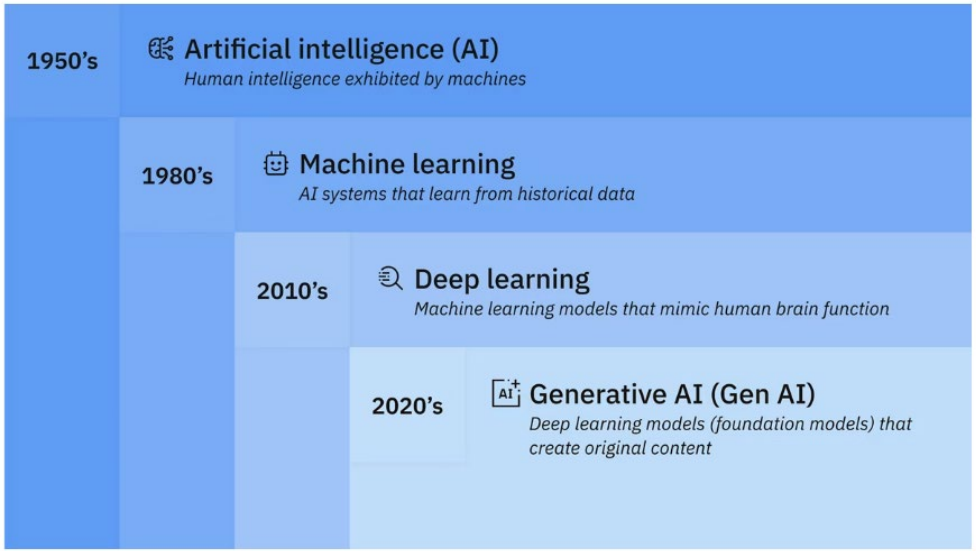
- Whether AI is good or bad
- Whether your organization should adopt AI
- Technical deep-dives

AI Demystified

Understanding AI

Artificial intelligence (AI) is technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy.

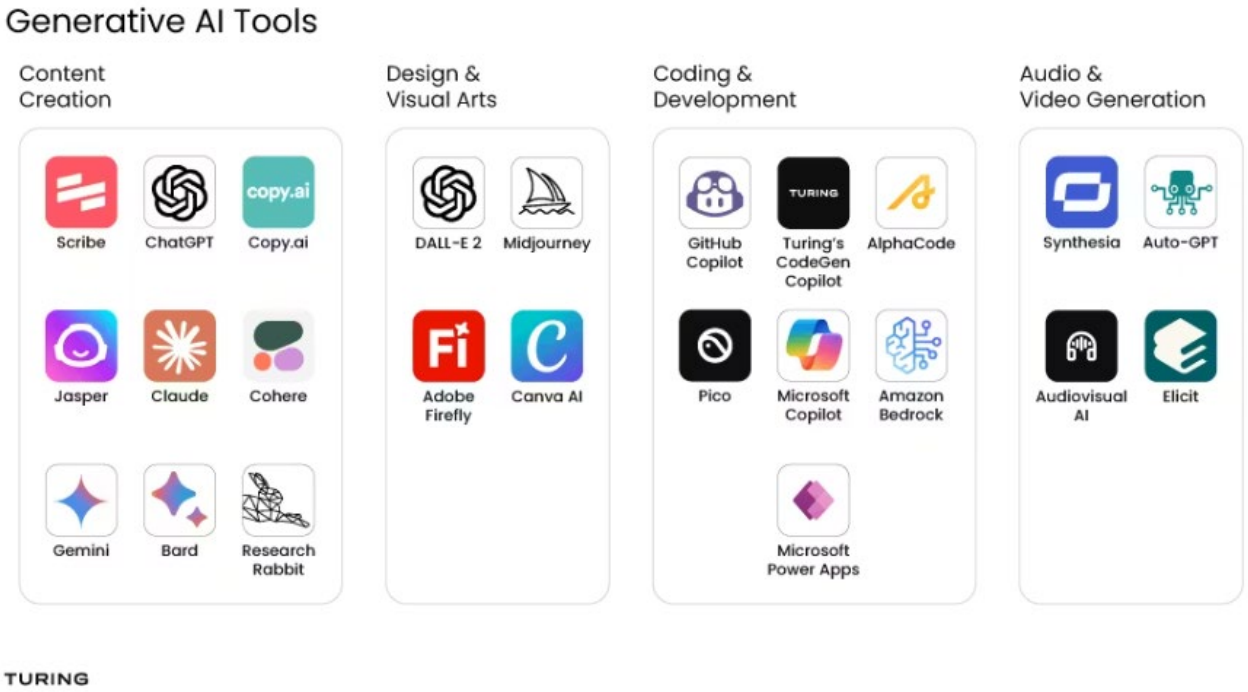
Generative AI, sometimes called "gen AI", refers to deep learning models that can create complex original content such as long-form text, high-quality images, realistic video or audio and more in response to a user's prompt or request.



How artificial intelligence, machine learning, deep learning and generative AI are related.

IBM: https://www.ibm.com/think/topics/artificial-intelligence

Common AI Tools



Turing: https://www.turing.com/resources/generative-ai-tools

Use of AI Tools

- Save hours on writing and administration
- Improve clarity and professionalism
- Generate options and thinking support
- Turn information into usable outputs faster

Draft funding/business proposals

Improve email campaign

Conduct market analysis

Generate economic reports

The quality of output relies heavily on **specific user input**

Dangers of Using AI

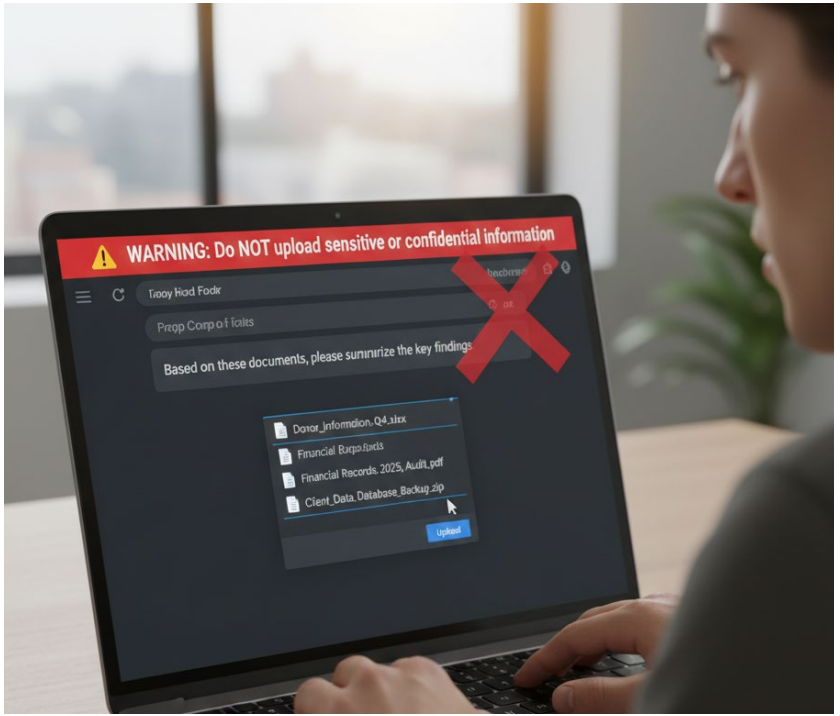
Dangers of Using AI

- Data Leakage
- Hallucinations
- Bias and Cultural Sensitivity
- Fraud and Impersonation

Data Leakage

Do we know what happens to the data when we enter prompts into ChatGPT?

- “We may use content submitted to ChatGPT and our other services for individuals to improve model performance.”
- “We share content with a select group of trusted service providers that help us provide our services.”



OpenAI: https://help.openai.com/en/articles/7039943-data-usage-for-consumer-services-faq

Data Leakage: Example

The scenario: A settlement worker is helping a client prepare for their refugee hearing. She uses ChatGPT to help draft a support letter, and pastes in:

- The client's full name
- Their country of origin
- Details of their persecution claim
- Their current housing situation

The output is a professionally written letter.

But what could go wrong here?

Data Leakage: Mitigation

3 ways to protect your clients' data:

1. **Anonymize before you type** Strip all identifying details before using any AI tool. Replace names, countries, dates, and case specifics with generic descriptors.

2. **Know your tools' privacy settings** Free tools ≠ safe tools. If your organization uses Microsoft 365 or Google Workspace on a paid business/enterprise plan, those tools offer contractual data protections.

3. **Build a simple "AI checkpoint" into your workflow** Before using any AI tool for work tasks, staff should ask three questions:
    - Does this involve a real client?
    - Have I removed all identifying information?
    - Would I be comfortable telling my supervisor I did this?

Hallucinations

The scenario: A program coordinator asks an AI chatbot: *"What documents does a refugee claimant need to apply for a work permit in Canada?“*

The AI gives a detailed, confident, well-formatted answer.

The coordinator forwards it to three clients without double checking the answer.

Two of the answers are out of date.
One document on the list doesn't exist.

Hallucinations

Potential Impacts of Hallucinations

- Fictitious information produced during research
- Made up case studies and references
- Limited by available research

Loss of trust with clients

Damage to reputation

Hallucinations: Mitigation

3 ways to keep AI from misleading your clients:

1. **Never let AI be the final source — always verify** Treat every AI output like a first draft from a well-meaning but unreliable intern. Useful starting point. Never the final word. For anything client-facing, always verify through official sources: IRCC.gc.ca, Settlement.Org, or a qualified colleague.

2. **Build a "Verified Sources" shortcut list for your team** Give workers the right tools before they reach for AI in a pinch. Bookmark trusted, regularly updated sources for the most common client questions. When the right answer is one click away, AI becomes less tempting as a shortcut.

3. **Add a disclosure habit for AI-assisted content** Any document, letter, or information sheet that involved AI assistance should be reviewed and initialed by a staff member before it goes to a client.

Bias and Cultural Sensitivity

An agency uses an AI tool to help prioritize intake to determine which clients get an appointment soonest based on urgency.

The AI was trained on historical data.

That historical data reflected past human decisions which were themselves shaped by **systemic bias**.

The AI now replicates and amplifies that bias, invisibly, at scale.

Bias and Cultural Sensitivity: Mitigation

3 ways to protect against AI bias in your work:

1. **Keep humans in every decision that affects individuals** AI can help you organize, draft, and research. It must never screen, rank, score, or prioritize individual clients. Any decision with consequences for a real person — intake order, service eligibility, referral — requires a human being who can be accountable for it.

2. **Apply your organization values to AI outputs, not just human behaviour** Your organization already values and principles. Apply them to AI. When reviewing AI-generated content, ask: does this make assumptions about culture, language, or background? Does it reflect the full dignity of the person it describes? If it does not, change the ouput.

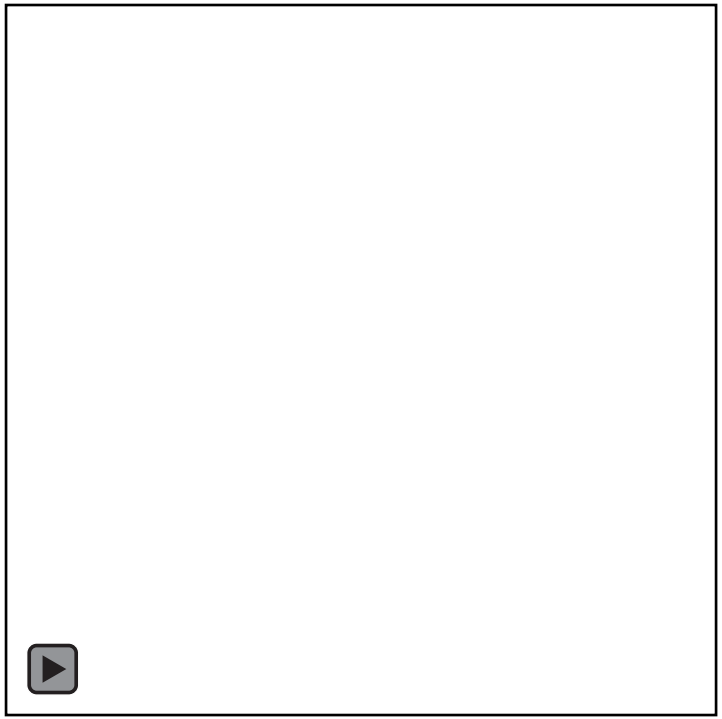
3. **Name it in your team discussions** Bias in AI is invisible unless you're looking for it. Build the habit of asking "what assumptions is this making?" when reviewing AI outputs, especially for communications involving specific communities. The critical eye your team already applies to systemic inequity is the right tool here.

Fraud and Impersonation

AI tools are getting better at:

- Video and image generation
- Voice generation
- Persuasive writing

Leads to an increase in fraud cases, business email compromise, and scams.



Credits: Stu Panensky - LinkedIn

Fraud and Impersonation

A client receives an email that looks exactly like it came from their settlement worker. It uses their worker's name, their agency's logo, and even references their last appointment.

It asks the client to send copies of their passport, SIN card, and work permit "for file updating purposes.“

The client complies. The email was not from their worker.

Fraud and Impersonation: Mitigation

3 ways to protect your clients and your organization:

1. **Establish a "call-back protocol" for all sensitive requests** Any for client data, financial information, or document transfers should never be acted on immediately. Always hang up and call back on a number you already have on file. Urgency is a manipulation tactic.

2. **Educate clients about what you will never ask for** Tell clients explicitly, early, and repeatedly: *"We will never ask you to send identity documents by email. We will never ask for payment to access services. If you receive a message that claims to be from us and asks for these things, call us directly before doing anything."* Make this part of your intake process.

3. **Build internal verification habits for unusual requests** Create a standing rule: any unusual request from a funder, government body, or colleague must require a second confirmation through a different channel.

Secure Use of AI – 4Ps

1. PROTECT (Privacy & Confidentiality)
- Never input confidential or sensitive information (community member data, financial details, strategic plans)
- Anonymize and generalize before using AI (remove identifiable information)
- Use enterprise versions when possible

2. POLICY (Governance & Guidelines)
- Develop organizational AI policy (clear rules about what can/cannot be shared)
- Train staff on safe AI use

3. PROOF (Verification & Accuracy)
- Always fact-check AI outputs (verify statistics, funding programs, requirements)
- Treat AI as a draft assistant, not a decision-maker (AI suggests, you decide)

4. PERSPECTIVE (Cultural Judgment)
- Apply cultural filter to all AI suggestions
- Maintain human oversight

Scenarios & Discussions

Scenarios & Discussions

We're going to look at three real-world scenarios from settlement organizations.
For each one:

1. Read the scenario

2. Vote: **Green / Yellow / Red**
Green (safe to proceed), Yellow (proceed with caution / need safeguards), or Red (don't do this)

3. Discuss

There are no trick questions. There are no perfect answers. The goal is to build judgment.

A program coordinator needs to shar information about an upcoming employment workshop with Tigrinya-speaking clients. She doesn't have access to a Tigrinya interpreter this week.

She pastes the English flyer text into ChatGPT and asks it to translate to Tigrinya. The translation looks good to her. She prints 50 copies and distributes them at a drop-in.

together a summary of program out s from the last quarter. She copies and pastes her last board report into ChatGP and asks it to summarize the key achievements in two pages.

The board report includes:

Program statistics (clients served, demographics, languages)
Two brief anonymized case vignettes

A settlement worker is meeting wit
client who has received a confusing r
about their work permit renewal. The
worker isn't sure of the exact process.
While the client waits, the worker opens
ChatGPT on their phone and types:

"What is the process for renewing an
open work permit for a refugee claimant in
Canada whose current permit expires in 6
weeks?"
They get a clear, step-by-step answer and
walk the client through it

Recap

- AI Demystified
- Dangers of Using AI
- Scenarios & Discussions
- Q&A

Secure Use of AI – 4Ps

1. PROTECT (Privacy & Confidentiality)
- Never input confidential or sensitive information (community member data, financial details, strategic plans)
- Anonymize and generalize before using AI (remove identifiable information)
- Use enterprise versions when possible

2. POLICY (Governance & Guidelines)
- Develop organizational AI policy (clear rules about what can/cannot be shared)
- Train staff on safe AI use

3. PROOF (Verification & Accuracy)
- Always fact-check AI outputs (verify statistics, funding programs, requirements)
- Treat AI as a draft assistant, not a decision-maker (AI suggests, you decide)

4. PERSPECTIVE (Cultural Judgment)
- Apply cultural filter to all AI suggestions
- Maintain human oversight

Next Steps

🟢 **Immediate (this week):**
Share today's 4 Ps with your team
Find out whether staff are using AI tools at work

🟡 **Short-term (1–3 months):**
Develop a simple 1-page AI use policy for your organization
Audit which software tools you use that have built-in AI features

🔵 **Longer-term:**
Include AI use in your staff onboarding and annual training

Q & A

Resources

Toronto Metropolitan University

ROGERS cybersecure catalyst

Thank you

Get connected with the Catalyst today

Settlement AtWork.Org

Upcoming Webinars
March 11, 2026: Secure Use of Artificial Intelligence

Info@settlmentatwork.org

Continue the Conversation on SettleNet

https://oca.si/cyber

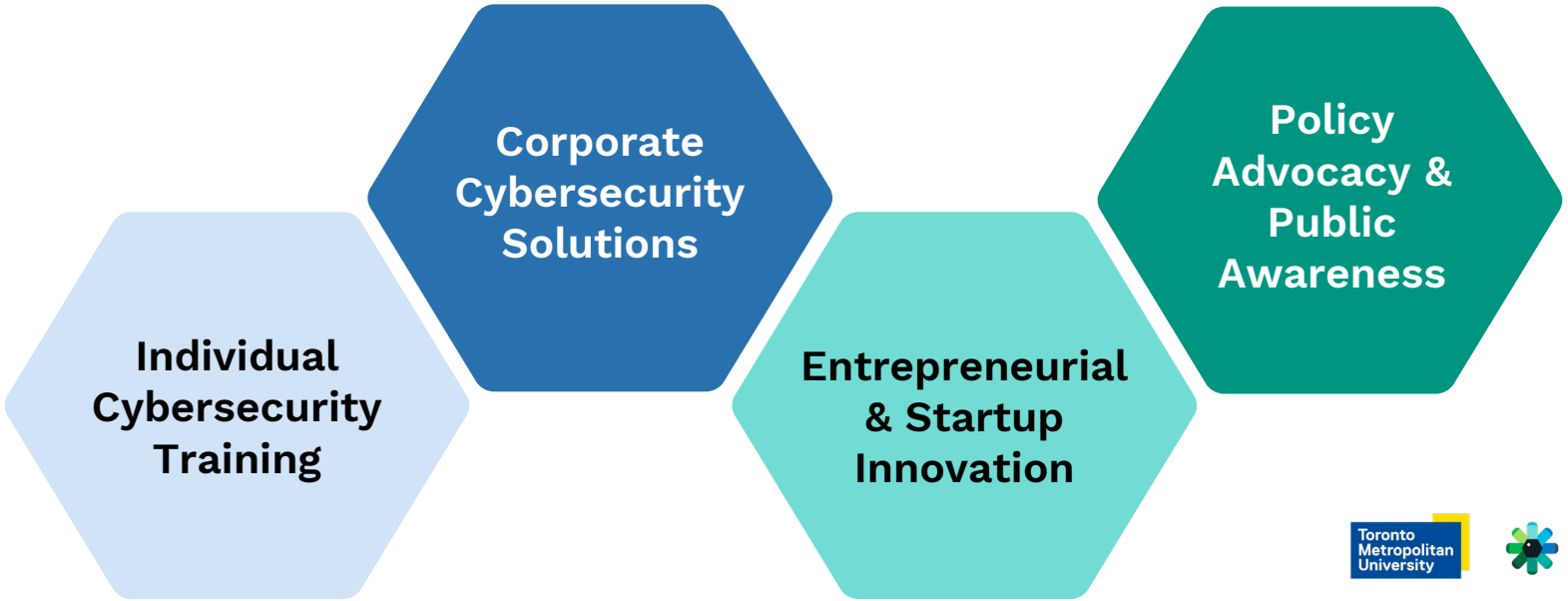
About Rogers Cybersecure Catalyst

Toronto Metropolitan University

ROGERS cybersecure catalyst

Rogers Cybersecure Catalyst

The Catalyst is Canada's cybersecurity hub. Our programs and services across the country, empower individuals and organizations to seize the opportunities and tackle the challenges of cybersecurity. We offer:



Toronto Metropolitan University

ROGERS cybersecure catalyst

Mission

Headquartered in Brampton, Ontario, and offering programs and services across Canada, **the Catalyst empowers individuals and organizations to seize the opportunities and tackle the challenges of cybersecurity**.

Vision

Together with our partners and collaborators, we work to realize a vision of **healthy democracies and thriving societies, powered by secure digital technologies.**

Toronto Metropolitan University

ROGERS cybersecure catalyst

Founding Partners

Canada

ROGERS

BRAMPTON innovation DISTRICT

RBC

Strategic Partners

SANS

BlackBerry

Funding provided in part by the Government of Ontario

Ontario

CCTX

Upskill Canada POWERED BY palette skills

Canada

RHEA GROUP

okta

Achieving Impact: Catalyst Milestones

- More than **7,000 people** have directly benefited from the Catalyst's groundbreaking programs
- Over **500 businesses** have been fueled by the Catalyst
- Over **800 jobs** have been created or filled in the cybersecurity sector through Catalyst programming
- More than **1,000 women, girls and non-binary individuals** have been empowered by the Catalyst
- Over **10,000** cybersecurity experts, mentors, thought leaders, entrepreneurs, program participants, alumni and partners make up the Catalyst community

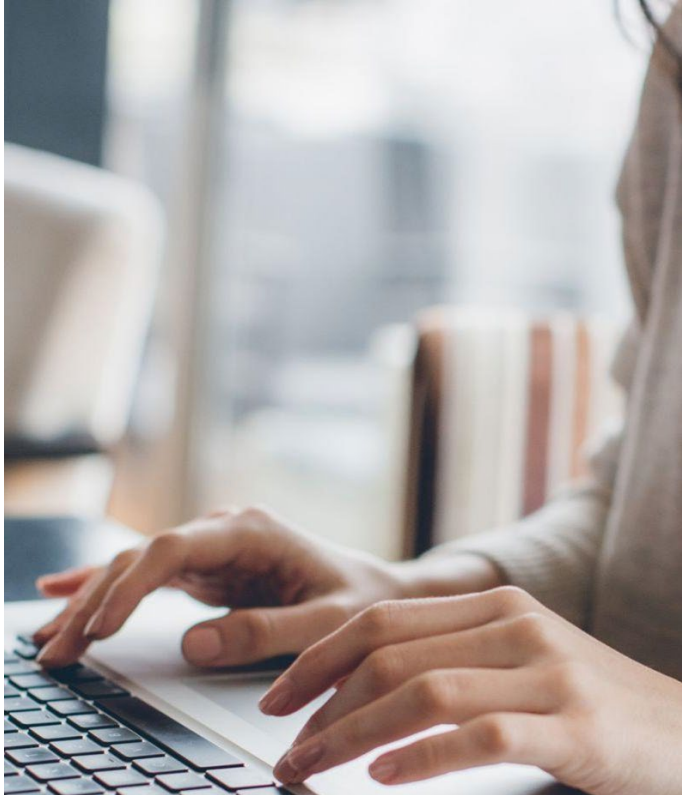
In November 2023, we brought nearly **300 cyber stakeholders** to the Rose Theater to celebrate the 5-year anniversary of Catalyst's founding

Toronto Metropolitan University

ROGERS cybersecure catalyst

Catalyst Cyber Clinic

One of the first of its kind in Canada, the Catalyst Cyber Clinic provides free cybersecurity support to under-resourced and vulnerable non-profit and social impact organizations in Canada. The Clinic is staffed by learners and graduates from Catalyst cyber training programs who, as Cyber Consultants, gain practical, real-world work experience while empowering vulnerable organizations to secure themselves.



We are a proud member of The Consortium of Cybersecurity Clinics

ROGERS cybersecure catalyst | Corporate Training

Toronto Metropolitan University

ROGERS cybersecure catalyst

okta

mastercard

Disclaimer

This disclaimer governs the use of this document. By using this document, you accept this disclaimer in full. You must not rely on the information in this presentation as an alternative to legal, financial, privacy or professional advice outside the area of cybersecurity. Notwithstanding the previous sentence, the Rogers Cybersecure Catalyst (the Catalyst) does not represent, warrant or guarantee that the use of guidance in this document will lead to a particular outcome. The Catalyst is not liable to the client in respect to any business losses, including and without limitation, loss of or damage to profits, income, revenue, use, productions, anticipated savings, business, contracts, commercial opportunities or goodwill.

This document is provided for educational and non-commercial purposes only to the intended recipient(s). Reproduction, distribution, or use of this material, in whole or in part, for any commercial purpose, including but not limited to offering services to third parties, charging fees, or incorporating into commercial products, is strictly prohibited without the express written consent of the Rogers Cybersecure Catalyst.

Connect with us

Subscribe to our **Catalyst Connect** newsletter:
cybersecurecatalyst.ca/subscribe

Follow the Catalyst on social media or email us:

@cybersecure.catalyst

linkedin.com/school/cybersecure-catalyst

cybersecurecatalyst@torontomu.ca

Toronto Metropolitan University

ROGERS cybersecure catalyst