Toronto Metropolitan University

ROGERS cybersecure catalyst

Cybersecurity Risks and Practical Strategies

Ontario First Nations Economic Developers Association
January 27, 2026

Agenda

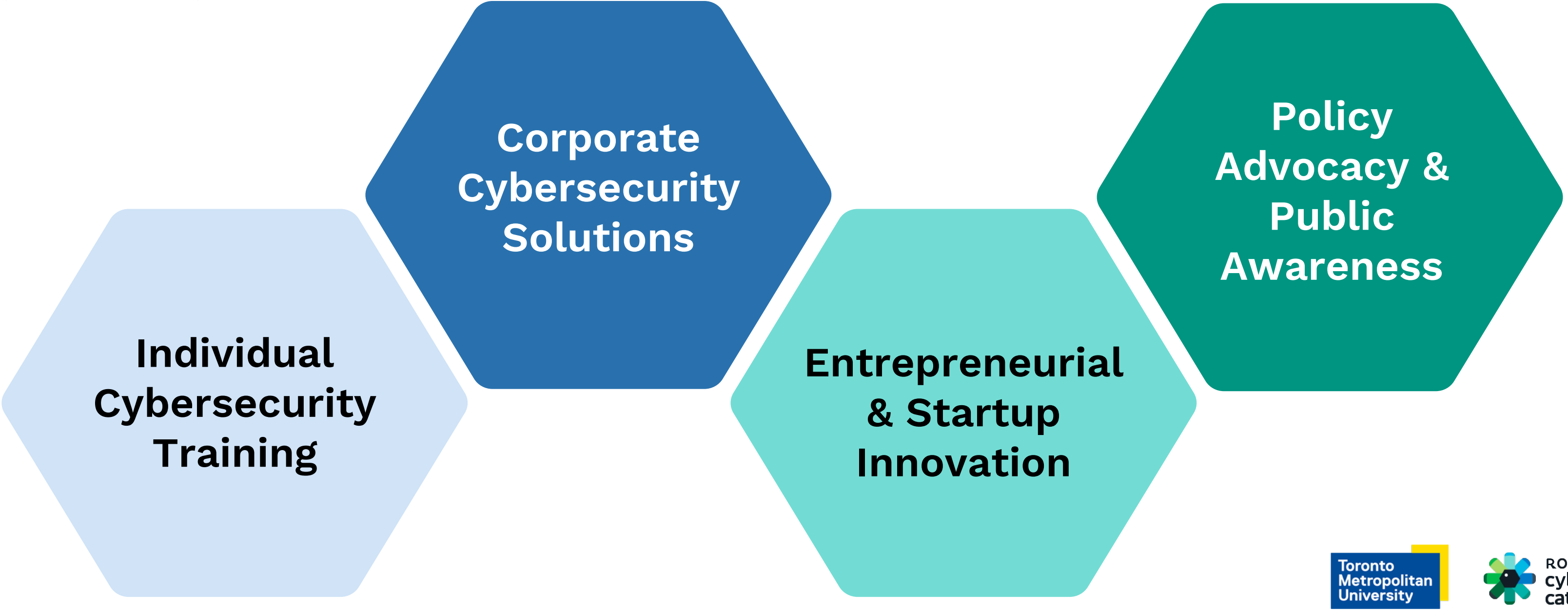
- Introduction
- Why does cybersecurity matter?
- The Canadian cyber threat landscape
- Cybersecurity threats
- Key Cybersecurity Concepts and Baseline controls
- AI - What are the dangers and how to use it securely
- Incident Response – What to do when something goes wrong

Toronto Metropolitan University

ROGERS cybersecure catalyst

Introduction

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:



Individual Cybersecurity Training

Corporate Cybersecurity Solutions

Entrepreneurial & Startup Innovation

Policy Advocacy & Public Awareness

Introduction

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

Nexova

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

Toronto Metropolitan University ROGERS cybersecure catalyst okta mastercard

Introduction

Lester Chng

CISSP, PMP

lester.chng@torontomu.ca

Senior Cybersecurity Advisor
Rogers Cybersecure Catalyst,
Toronto Metropolitan University

Toronto Metropolitan University

ROGERS cybersecure catalyst

Introduction

In the chat, please share:

- Your name
- Your community/organization
- One word: How do you feel about cybersecurity?

Why Does Cybersecurity Matter?

Toronto Metropolitan University

ROGERS cybersecure catalyst

Why Does Cybersecurity Matter?

A failure to protect
our **systems** and **information**,
is a failure to protect those whom we serve.

Why Does Cybersecurity Matter?

- Breach of Confidentiality and Privacy
- Loss of Trust
- Service Disruption
- Financial Costs
- Reputational Damage

Toronto Metropolitan University

ROGERS cybersecure catalyst

Do not edit

How to change the design

Join at slido.com

#5968690

ⓘ The Slido app must be installed on every computer you’re presenting from

slido

Do not edit

How to change the design

Which is your most concerning impact?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

The Canadian Cyber Threat Landscape

Toronto Metropolitan University

ROGERS cybersecure catalyst

The Canadian Cyber Threat Landscape

National Cyber Threat Assessment 2025 - 2026

Cybercrime threats remains a persistent, widespread, and disruptive threat to individuals and organizations.

Factors contributing to this rise:

- Cybercrime-as-a-service
- Increased digitalization of organizations
- AI improves and allows scale of phishing attacks

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Toronto Metropolitan University

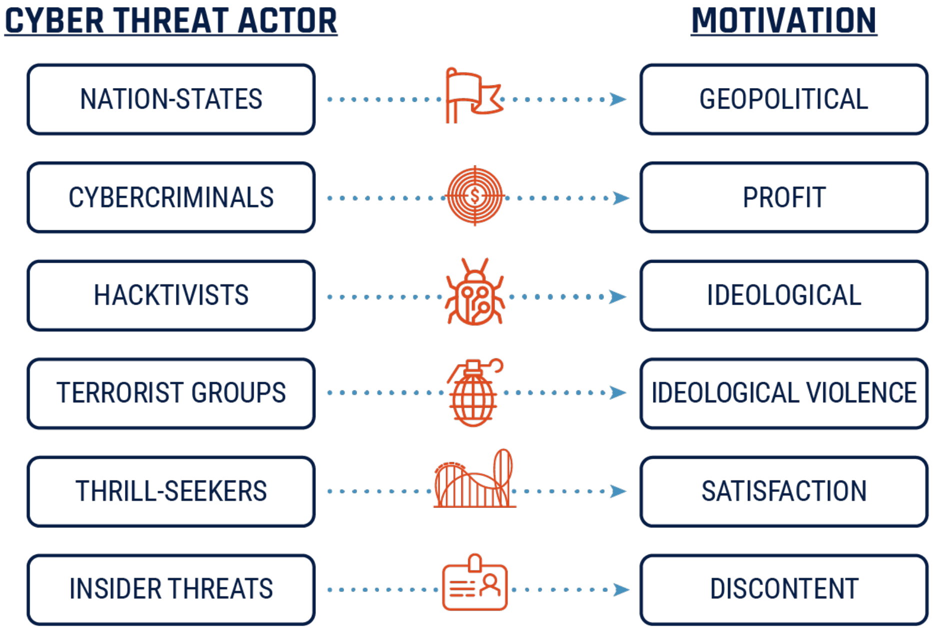
ROGERS cybersecure catalyst

The Canadian Cyber Threat Landscape

Cybercrime Threats - The Factors and Trends

- Cybercrime-as-a-service facilitates the prevalence of cybercrime
- Ransomware incidents on the rise
- Cyber threat surface keeps expanding
- Fraud and scams remain a persistent threat
- Artificial Intelligence amplifies cyber threats

The Canadian Cyber Threat Landscape



CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

Source: Canadian Centre for Cyber Security (2018), *An Introduction to the Cyber Threat Environment* https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Toronto Metropolitan University

ROGERS cybersecure catalyst

Cybersecurity Threats

Cybersecurity Threats

- Phishing Campaigns
- Malware/Ransomware
- Data Breach
- Deepfake Impersonation
- Business Email Compromise
- Case Studies

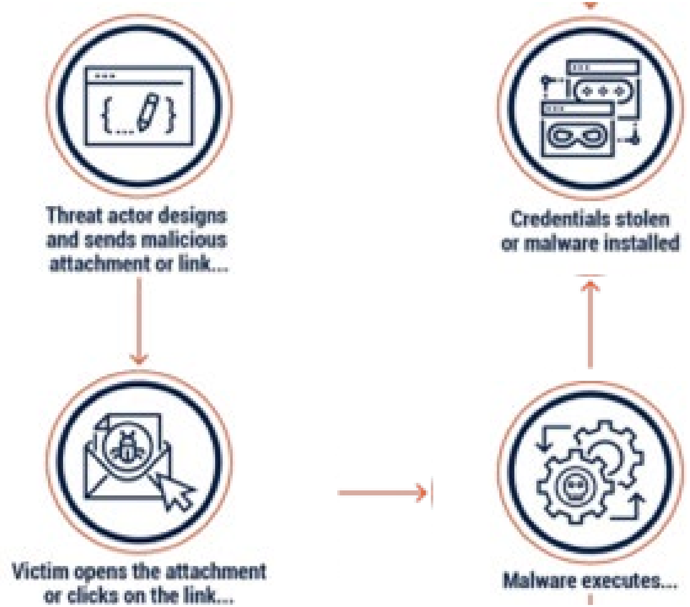
Deep Dive into Phishing Campaigns

Objectives of campaigns include:

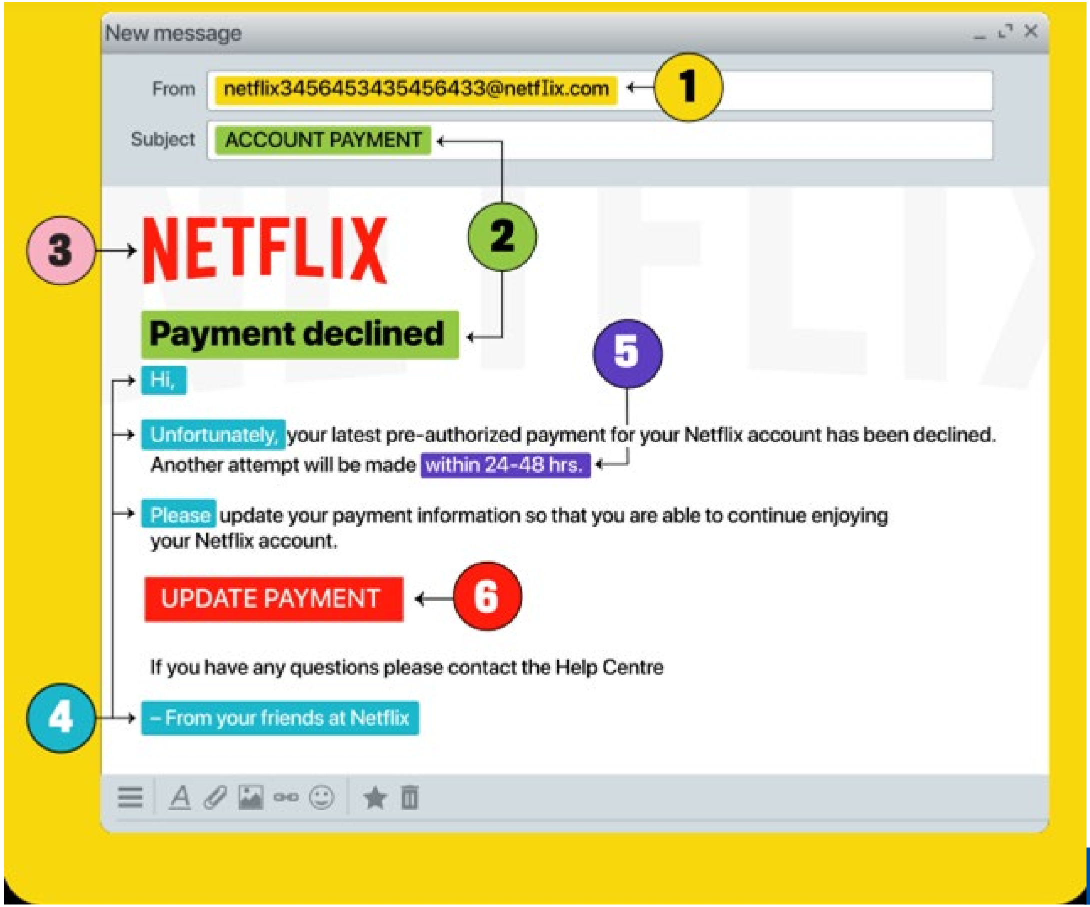
- Steal valuable data
- Distribute malware via links/exe
- Compel user to take action

Tactics

- Impersonate trusted brands
- Redirect to a spoofed website
- Include links or files
- Permissions request


Threat actor designs and sends malicious attachment or link...
Victim opens the attachment or clicks on the link...
Malware executes...
Credentials stolen or malware installed

Source: Canadian Centre for Cyber Security (2018), *An Introduction to the Cyber Threat Environment*



New message

From netflix3456453435456433@netflix.com

Subject ACCOUNT PAYMENT

NETFLIX

Payment declined

Hi,

Unfortunately, your latest pre-authorized payment for your Netflix account has been declined. Another attempt will be made within 24-48 hrs.

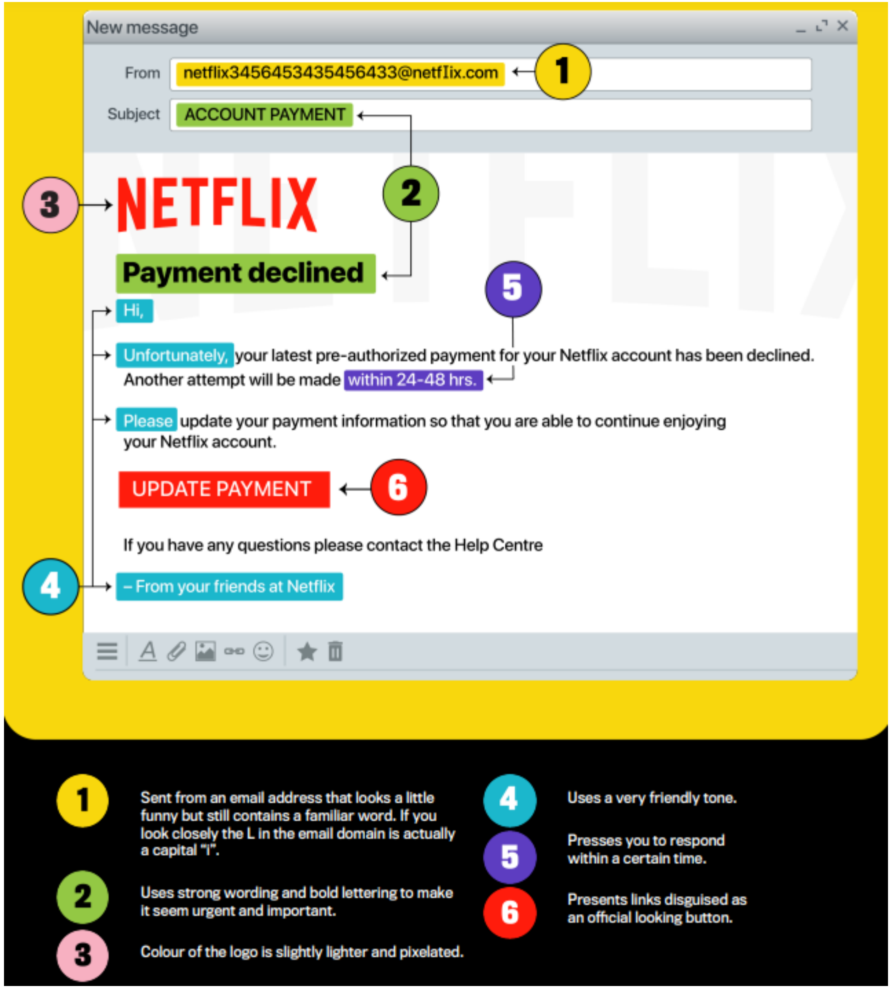
Please update your payment information so that you are able to continue enjoying your Netflix account.

UPDATE PAYMENT

If you have any questions please contact the Help Centre

– From your friends at Netflix

Source: Get Cyber Safe. *Government of Canada. https://www.getcybersafe.gc.ca/en*



New message

From netflix3456453435456433@netfIix.com

Subject ACCOUNT PAYMENT

NETFLIX

Payment declined

Hi,

Unfortunately, your latest pre-authorized payment for your Netflix account has been declined. Another attempt will be made within 24-48 hrs.

Please update your payment information so that you are able to continue enjoying your Netflix account.

UPDATE PAYMENT

If you have any questions please contact the Help Centre

– From your friends at Netflix

1. Sent from an email address that looks a little funny but still contains a familiar word. If you look closely the L in the email domain is actually a capital "i".
2. Uses strong wording and bold lettering to make it seem urgent and important.
3. Colour of the logo is slightly lighter and pixelated.
4. Uses a very friendly tone.
5. Presses you to respond within a certain time.
6. Presents links disguised as an official looking button.

Source: Get Cyber Safe. *Government of Canada. https://www.getcybersafe.gc.ca/en*

Toronto Metropolitan University

ROGERS cybersecure catalyst

Deep Dive into Phishing Campaigns

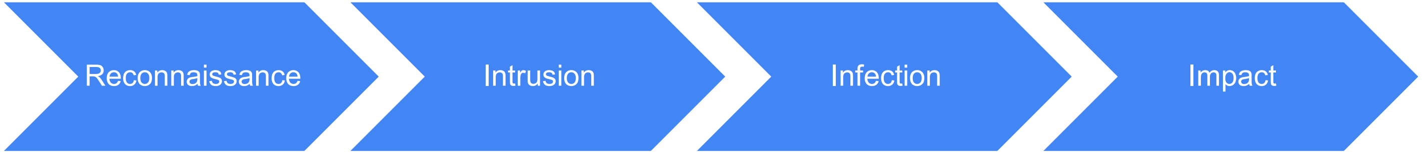
Mitigation Measures

- Employee training and awareness
  - Security awareness programs
  - Phishing simulations
  - Phishing email inbox
  - Reporting mechanisms

- Technical measures
  - Email authentication protocols
  - Email filtering

Cybersecurity Threats

Malware/Ransomware


Reconnaissance

Intrusion

Infection

Impact

Gather information on targets

- OSINT (Open-source Intelligence)
- Dark web search
- Wide scanning

Gain unauthorized access

- Stolen credentials
- Phishing campaigns
- Exploit vulnerabilities

Spread infection

- Install malware
- Gain access
- Move across network

Execute on objective

- Exfiltrate
- Encrypt
- Demand ransom

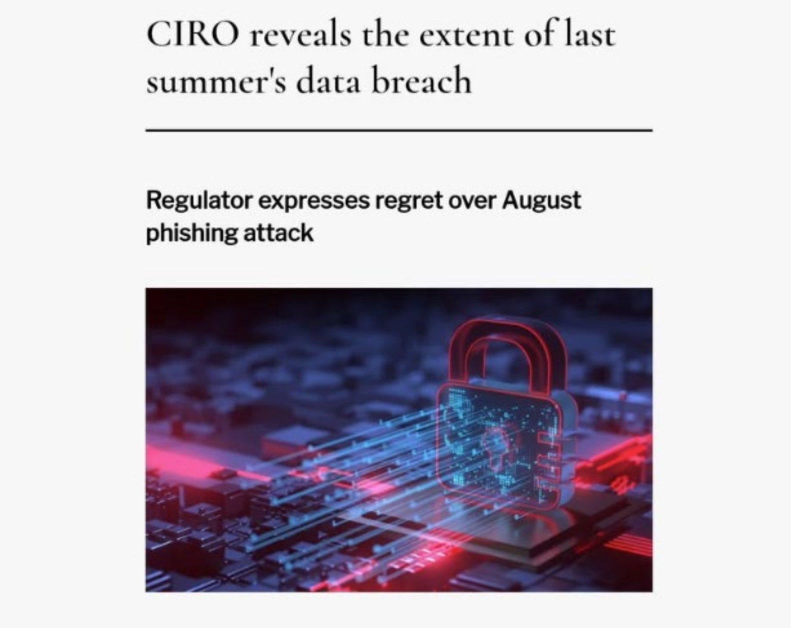
Cybersecurity Threats

Data Breach

Organizations that hold sensitive data such as health, social service, financial information are high-value targets.

As part of ransomware campaigns, the cyber criminals usually steal data from their victims and threaten to release their data to the public.

This is part of the threat as they demand a ransom.



CIRO reveals the extent of last summer's data breach

Regulator expresses regret over August phishing attack

Cybersecurity Threats

Deepfake Impersonation

- A finance worker in at MNC was tricked into transferring USD $25.6 million to fraudsters
- The worker received a suspicious message from the “CFO” regarding a secret transaction
- A video call was set up where the criminal created deepfake videos and impersonated the CFO and other colleagues
- 15 financial transactions were made following the call

Cybersecurity Threats

Business Email Compromise and Invoice Fraud

Business Email Compromise (BEC) is when a scammer **pretends to be a trusted person** (a vendor, EDO, finance staff, or project partner) by using a look-alike email address or a hacked inbox.

Example

Step 1: Hacker takes over a trusted vendor’s email inbox

Step 2: They observe invoice schedule and workflows

Step 3: They send a request to change account details and ask to send the payment to the new account

Step 4: Your finance team makes that change and sends the payment. Funds are difficult to recover and the relationship with the vendor may be strained.

Case Studies

First Nations Health Authority (BC) FNHA Cyber Incident (2024)

Unauthorized access and exfiltration of files

Method

- IT Team detected unusual activity and mitigated the incident
- Personal information was accessed by an unauthorized 3rd party
- Client and employee information was impacted

Response and Recovery

- Set up an FNHA Cyber Incident Support Centre
- Provided Credit Monitoring and Identity Theft Restoration Services

Lessons Learned

- Strong recovery support post-incident

Case Studies

‘Na̲mg̲is First Nation (BC) – Fraudulent Email Incident (2025)

Redirect transfer to a fake bank account

Method

- Cyber criminals took over a trusted contractor’s email account
- Payment was due for the construction of a 16-bed Wellness and Treatment Centre
- Criminals convinced the office to change the wire transfer destination
- Transferred $406,000 to new account

Response and Recovery

- Alert Bay, BC RCMP was able to investigate and initiated a freeze on the transfer
- Linked to an organized crime group from Eastern Canada

Do not edit
How to change the design

What are your top cybersecurity concerns?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Break

Recap

- **Why does cybersecurity matter?**
- **The Canadian cyber threat landscape**
- **Cybersecurity threats**
- Key Cybersecurity Concepts and Baseline controls
- AI - What are the dangers and how to use it securely
- Incident Response – What to do when something goes wrong

Key Cybersecurity Concepts

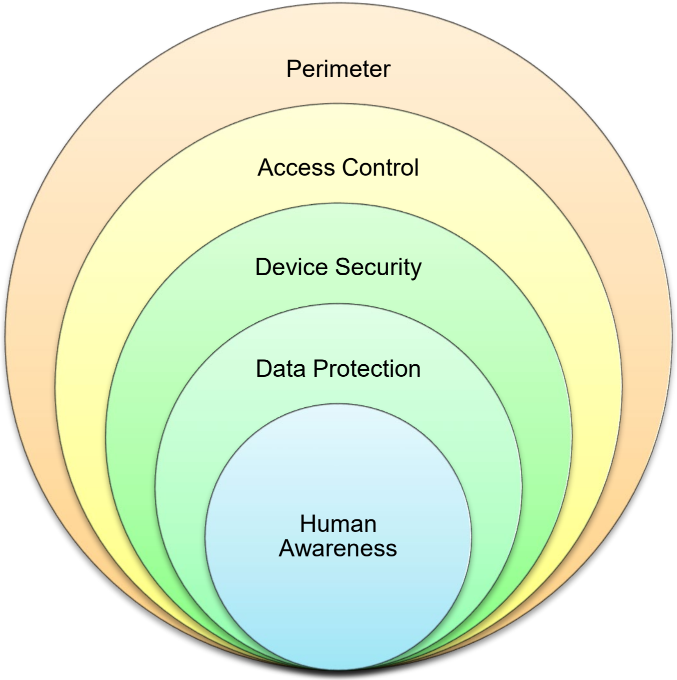
Key Cybersecurity Concepts

- Defence in Depth
- Principle of Least Privilege
- Attack Surface Reduction
- Operational Resilience > Cybersecurity

Defence in Depth

Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.

- Administrative Controls
- Physical Controls
- Technical Controls



Principle of Least Privilege

The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

- System access
- Account access
- Financial system access
- Sensitive information access

Attack Surface Reduction

Attack surface reduction is having a clear inventory of all your assets and making it harder for a cybercriminal to find a way in

- Laptops
- Features
- Accounts
- Software
- Devices

Methods:

- Removal
- Updates
- Limit access
- Block

Toronto Metropolitan University

ROGERS cybersecure catalyst

Operational Resilience > Cybersecurity

Operational Resilience:
The ability of systems to resist, absorb, and recover from, or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of the ability to perform mission-related functions.

If you experience a significant cybersecurity incident

- Can you continue operations (sub-optimal)?
- Are you able to recover quickly?

This is enabled by:

- Incident response planning
- System design – data backup, alternatives
- Business continuity
- Disaster recovery

Toronto Metropolitan University

ROGERS cybersecure catalyst

Do not edit
How to change the design

Which of these concepts are already in practice at your organization?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Baseline Controls

Baseline Controls

1. **Develop an Incident Response Plan**
2. **Automatically Patch Operating Systems and Applications**
3. Enable Security Software
4. Securely Configure Devices
5. **Use Strong User Authentication**
6. Provide Employee Awareness Training
7. **Backup and Encrypt Data**
8. Secure Mobility
9. Establish Basic Perimeter Defences
10. Secure Cloud and Outsourced IT Services
11. Secure Websites
12. Implement Access Control and Authorization
13. Secure Portable Media

Develop an Incident Response Plan
Automatically Patch Operating Systems and Applications
Enable Security Software
Securely Configure Devices
Use Strong User Authentication
Provide Employee with Awareness Training
Back up and Encrypt Data
Secure Mobility
Establish Basic Perimeter Defences
Secure Cloud and Outsourced IT Services
Secure Websites
Implement Access Control and Authorization
Secure Portable Media

CCCS Baseline Cyber Security Controls -
https://www.cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Starting Point

Four Controls to Start with:

- Develop an incident response plan
- Patch operating systems and applications
- Enforce strong user authentication
- Backup and encrypt data

Developing an Incident Response Plan

Having an incident response plan (IRP) allows your organization to:

- Manage incidents
- Mitigate threats and risks
- Recover quickly from the incident

Simplified Incident Response Plan includes:

- Key stakeholder contact list
- Critical asset list
- Alternative processes
- Back-up options

Developing an Incident Response Plan

Incident Response Plan Development:

- Conduct a risk assessment
- Establish your response team
- Develop your policies
- Create your communications plan
- Educate your employees

Phases of Incident Response

1. Preparation
2. Detection and analysis
3. Containment
4. Eradication
5. Recovery
6. Post-incident activities and lessons learned

Patch Operations Systems and Applications

Cybercriminals exploit vulnerabilities in outdate systems and applications.

Risk of not patching:

- system lags or crashes during use
- unresponsive applications
- vulnerabilities that are exploited to infect devices with malware
- hackers gaining access to, stealing or encrypting your sensitive information, or preventing your device from working
- inaccessible features on applications

Activate **automatic** patches and updates for all software and hardware.

Important to have a good inventory of all your assets.

Are you aware of how your vendor/third-party manage their updates?

Enforce Strong User Authentication

Password Policies and Management

Passwords are used for devices, accounts, website log-ins. Most passwords are re-used and this creates additional risks.

- Use complex passwords
- Avoid common password mistakes
- Use password managers

Best practices for passphrases and passwords (ITSAP.30.032)
https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032

Multi-Factor Authentication (MFA)

Implementing MFA provides an additional layer of authentication and does not rely on passwords alone.

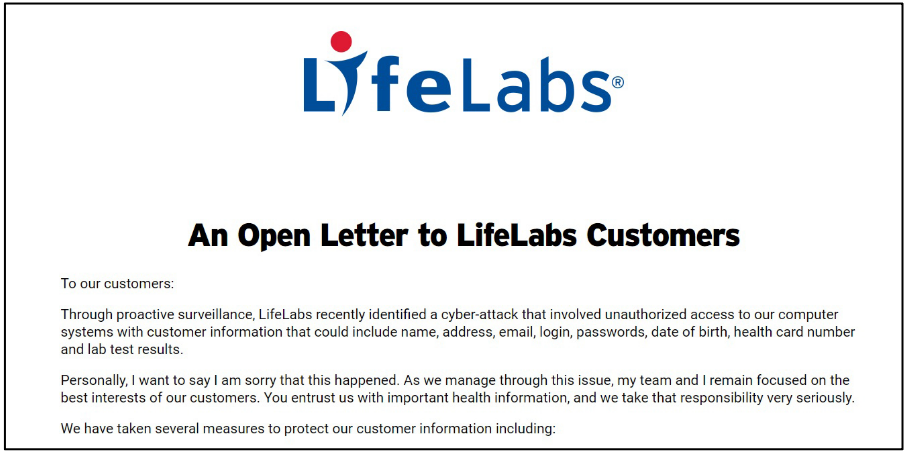
- Enable in all available devices/accounts
- Prioritize where to implement

Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)
https://www.cyber.gc.ca/en/guidance/secure-your-accounts-and-devices-multi-factor-authentication-itsap30030

Backup and Encrypt Data

These controls address 2 key risks:

- Disruption to operations
- Disclosure of sensitive information



An Open Letter to LifeLabs Customers

To our customers:

Through proactive surveillance, LifeLabs recently identified a cyber-attack that involved unauthorized access to our computer systems with customer information that could include name, address, email, login, passwords, date of birth, health card number and lab test results.

Personally, I want to say I am sorry that this happened. As we manage through this issue, my team and I remain focused on the best interests of our customers. You entrust us with important health information, and we take that responsibility very seriously.

We have taken several measures to protect our customer information including:

Toronto Metropolitan University

ROGERS cybersecure catalyst

Backup and Encrypt Data

Having tested and validated backups gives you options for responding to a cybersecurity incident.

When are backups used:

- Failure or outage
- Ransomware
- Denial of service attack
- Natural disasters
- Lost or stolen devices

Backup and Encrypt Data

Where to store are backups:

- Onsite [Removable storage media, Network-attached Storage]
- Offsite [Vendor storage]
- Cloud-based storage

3-2-1 rule for data storage

- 3 copies of your information (1 original and 2 backups),
- 2 different media types,
- 1 copy kept off site

Remember to test your backups!

Tips for backing up your information (ITSAP.40.002)
https://www.cyber.gc.ca/en/guidance/tips-backing-your-information-itsap40002#when

Break

Recap

- Why does cybersecurity matter?
- The Canadian cyber threat landscape
- Cybersecurity threats
- **Key Cybersecurity Concepts and Baseline controls**
- AI - What are the dangers and how to use it securely
- Incident Response – What to do when something goes wrong

Toronto Metropolitan University

ROGERS cybersecure catalyst

AI
What are the dangers and how to use it securely

Do not edit
How to change the design

Have you used AI tools like ChatGPT or Copilot for work?

ⓘ The Slido app must be installed on every computer you’re presenting from

Do not edit
How to change the design

What's your biggest concern about AI?

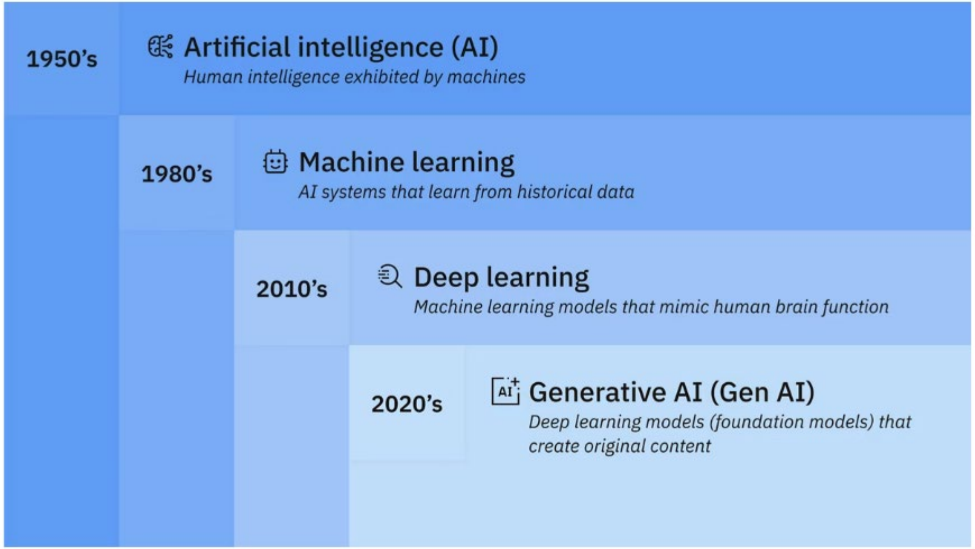
ⓘ The Slido app must be installed on every computer you're presenting from

slido

Understanding AI

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

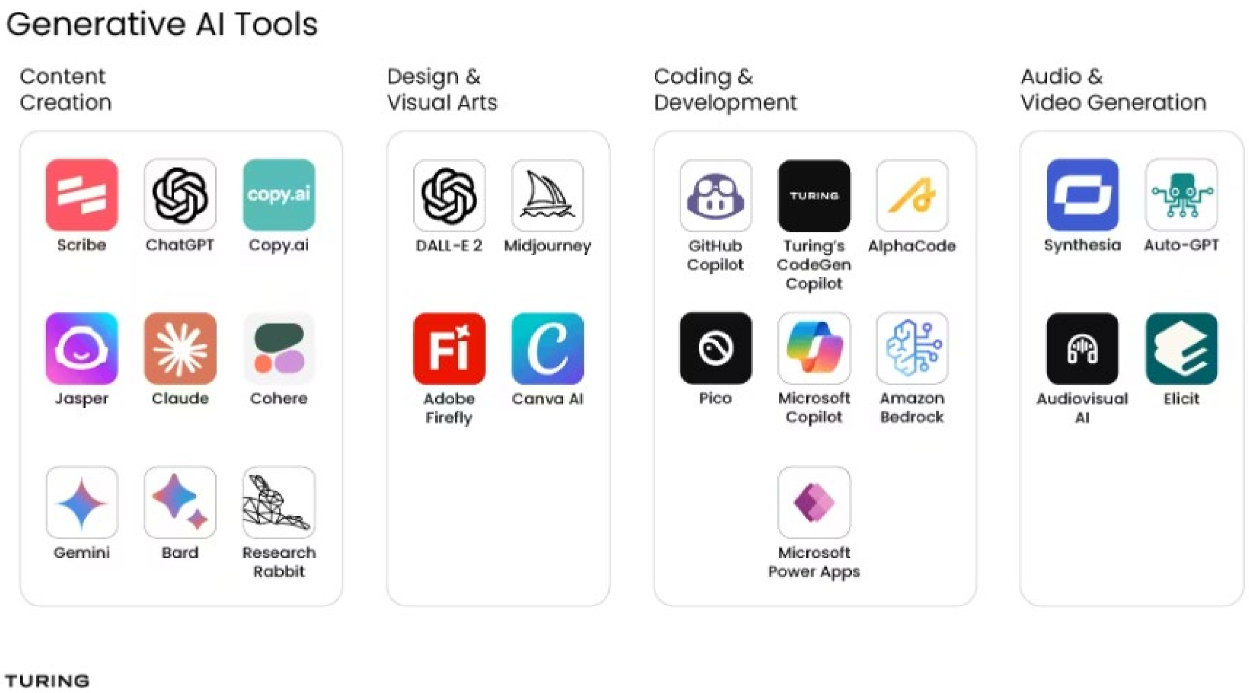
Generative AI, sometimes called "gen AI", refers to deep learning models that can create complex original content such as long-form text, high-quality images, realistic video or audio and more in response to a user's prompt or request.


1950's
Artificial intelligence (AI)
Human intelligence exhibited by machines
1980's
Machine learning
AI systems that learn from historical data
2010's
Deep learning
Machine learning models that mimic human brain function
2020's
Generative AI (Gen AI)
Deep learning models (foundation models) that create original content

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

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

Common AI Tools



Generative AI Tools

Content Creation
- Scribe
- ChatGPT
- Copy.ai
- Jasper
- Claude
- Cohere
- Gemini
- Bard
- Research Rabbit

Design & Visual Arts
- DALL-E 2
- Midjourney
- Adobe Firefly
- Canva AI

Coding & Development
- GitHub Copilot
- Turing's CodeGen Copilot
- AlphaCode
- Pico
- Microsoft Copilot
- Amazon Bedrock
- Microsoft Power Apps

Audio & Video Generation
- Synthesia
- Auto-GPT
- Audiovisual AI
- Elicit

TURING

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

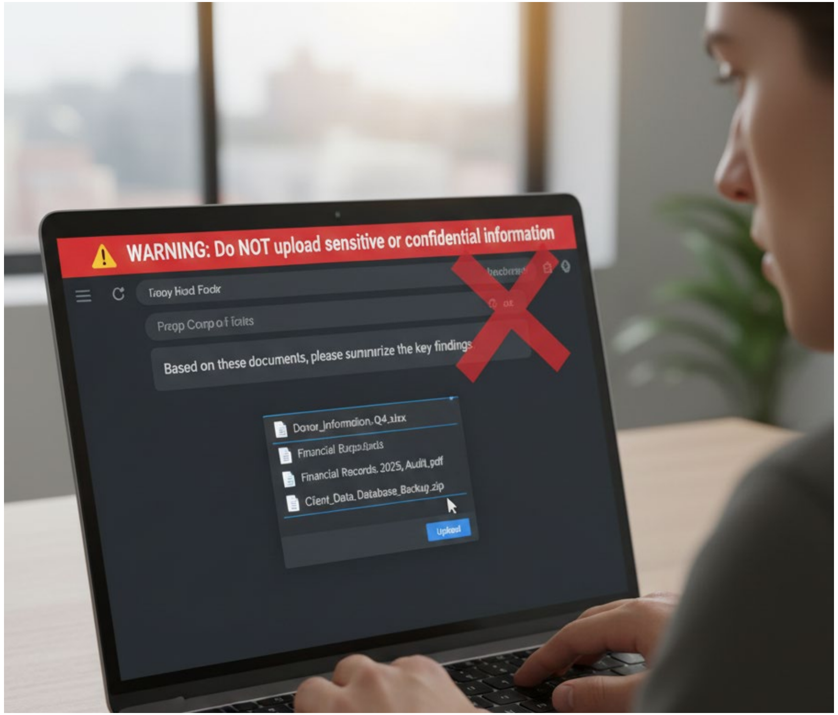
- Data Leakage
- Hallucinations
- Fraud and impersonation
- Bias and Cultural Sensitivity

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.”


WARNING: Do NOT upload sensitive or confidential information
Based on these documents, please sumnrize the key findings
Donor_Informdion_Q4.xlsx
Financial Records 2025 Audit.pdf
Client_Data_Database_Backup.zip
Upload

Toronto Metropolitan University

ROGERS cybersecure catalyst

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

Do not edit
How to change the design

What types of data should you avoid using when prompting an AI tool?

ⓘ The Slido app must be installed on every computer you’re presenting from

slido

Do not edit
How to change the design

Which of the following should you avoid entering into AI tools?

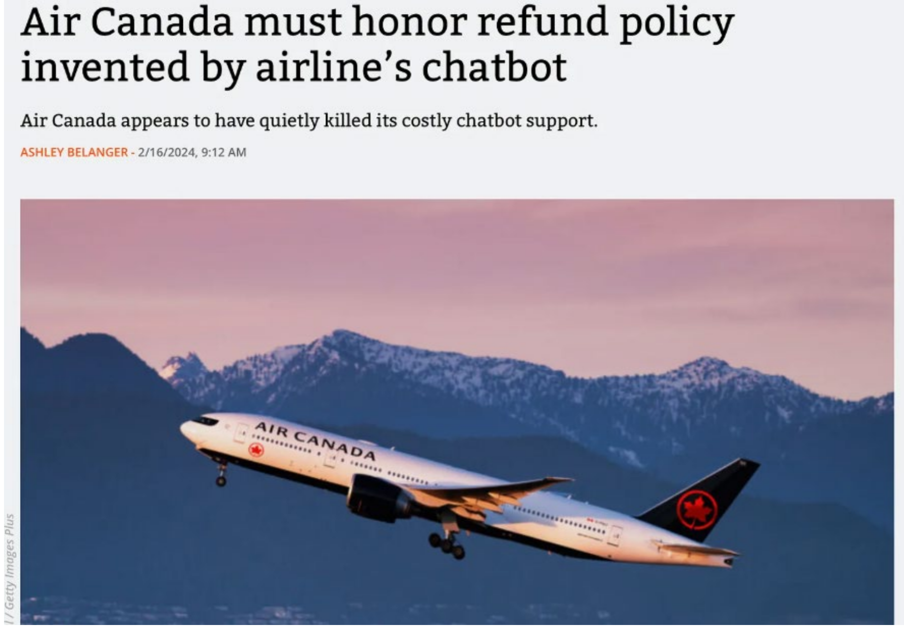
ⓘ The Slido app must be installed on every computer you're presenting from

slido

Hallucinations

Hallucinations often occur when the model fills in gaps based on similar contexts in its training data, or when it is trained on biased or incomplete data.

- Air Canada Chatbot incident
- A Canadian lawyer used “fictitious” cases generated by ChatGPT in court



Air Canada must honor refund policy invented by airline’s chatbot

Air Canada appears to have quietly killed its costly chatbot support.

ASHLEY BELANGER - 2/16/2024, 9:12 AM

/ Getty Images Plus

Hallucinations

Potential Impacts of Hallucinations

- Fictitious information produced during research
- Made up case studies and references
- Legal and regulatory requirements

Loss of trust in reporting

Damage to reputation

Liability and fines

Do not edit
How to change the design

What are some ways you mitigate against hallucinations?

ⓘ The Slido app must be installed on every computer you're presenting from

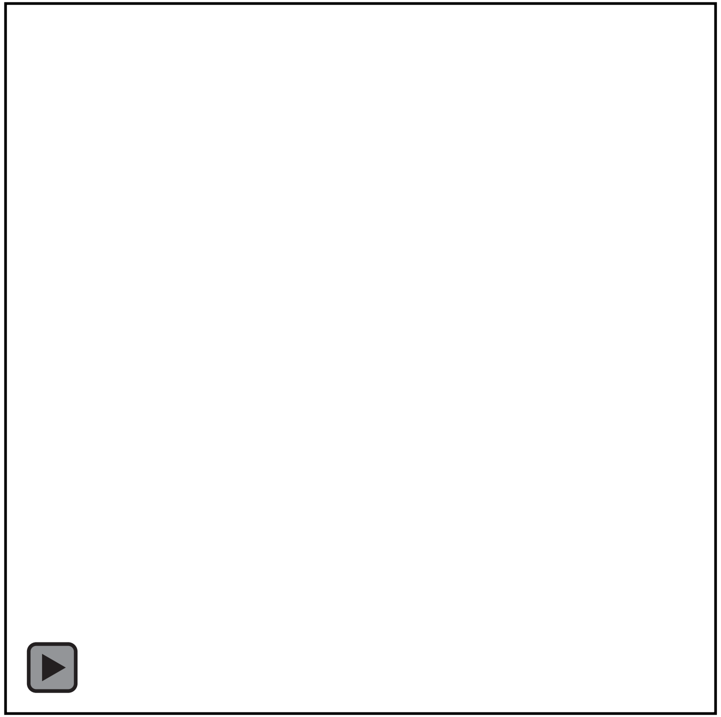
slido

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

Bias and Cultural Sensitivity

AI can **repeat stereotypes** or erase nuance (because it learns from the internet)

It may produce **harmful or insensitive phrasing** about communities, culture, or history

Bias in facial recognition, job recruitment, and loan eligibility

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

Incident Response

Developing an Incident Response Plan

Having an incident response plan (IRP) allows your organization to:

- Manage incidents
- Mitigate threats and risks
- Recover quickly from the incident

Simplified Incident Response Plan includes:

- Key stakeholder contact list
- Critical asset list
- Alternative processes
- Back-up options

Developing an Incident Response Plan

Phases of Incident Response

1. Preparation
2. Detection and analysis
3. Containment
4. Eradication
5. Recovery
6. Post-incident activities and lessons learned

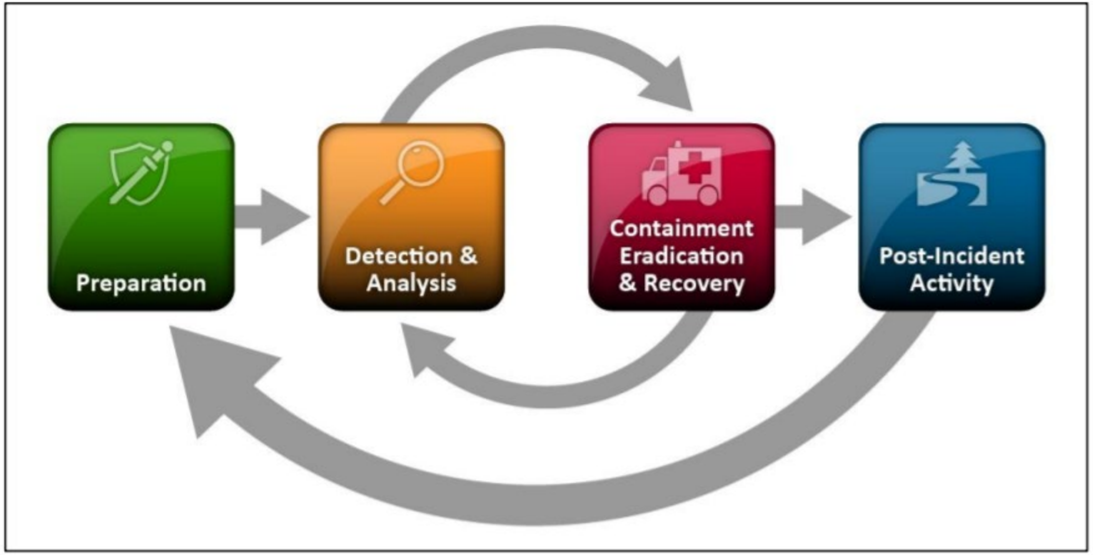


Figure 3-1. Incident Response Life Cycle

Source: NIST 800-61 Rev 2. Computer Security Incident Handling Guide

Types of Incidents

- Email compromise
- Ransomware (files locked/encrypted)
- Lost or stolen device with work data
- Successful phishing attack (someone clicked and entered credentials)
- Data breach (information exposed or leaked)
- Malware infection (virus or suspicious software)
- **Business email compromise**

Southern Lakes Regional Council

Fictional Organization

Southern Lakes Regional Council serves residents and visitors of the Southern Lakes Region. The council has embarked on an ambitious construction project (Project Regen) that looks to refresh the region.

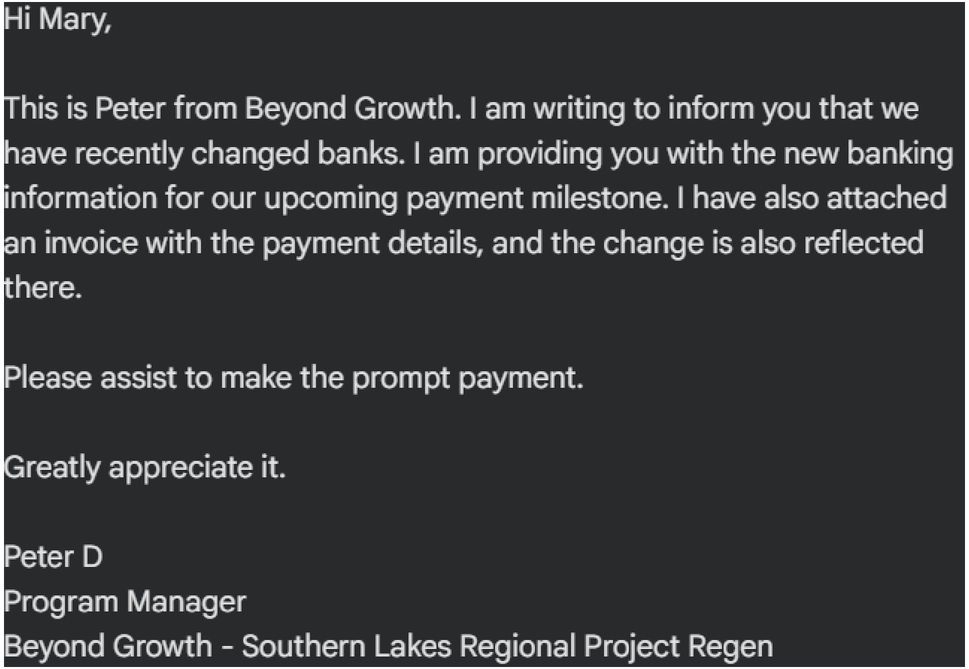
They have contracted a long-time consulting firm, **Beyond Growth**, to oversee Project Regen. Beyond Growth has been an approved vendor for more than 20 years and provides a suite of services to the council. This project is underway and the council is very excited with the current progress.

Email Communications

Inject 1

Your finance staff has received the following email from Beyond Growth regarding an upcoming $200,000 milestone payment.

The email is professionally written and is from Peter, who is the main point of contact for Project Regen.



Hi Mary,

This is Peter from Beyond Growth. I am writing to inform you that we have recently changed banks. I am providing you with the new banking information for our upcoming payment milestone. I have also attached an invoice with the payment details, and the change is also reflected there.

Please assist to make the prompt payment.

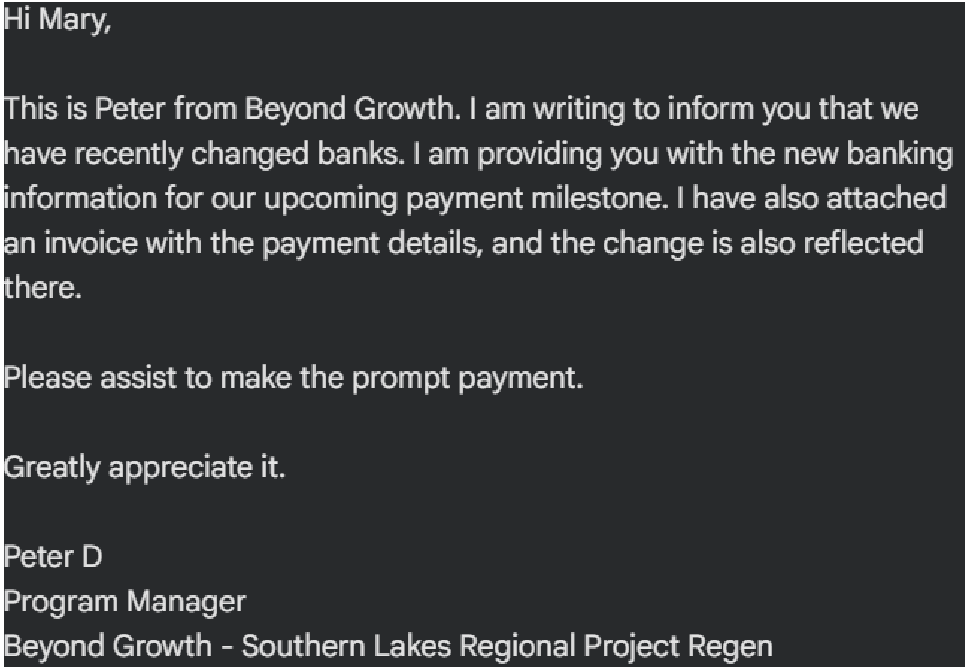
Greatly appreciate it.

Peter D
Program Manager
Beyond Growth - Southern Lakes Regional Project Regen

Email Communications

Question

What concerns or questions do you have if you are on the finance team and receive such an email?



Hi Mary,

This is Peter from Beyond Growth. I am writing to inform you that we have recently changed banks. I am providing you with the new banking information for our upcoming payment milestone. I have also attached an invoice with the payment details, and the change is also reflected there.

Please assist to make the prompt payment.

Greatly appreciate it.

Peter D
Program Manager
Beyond Growth - Southern Lakes Regional Project Regen

Do not edit
How to change the design

What concerns do you have with this email?

What would you do if you receive such an email?

Project Progress and Payment

Scenario

The finance analyst who received the email followed Peter's instructions and updated the banking details. Shje had his suspicions, but she had been working with Peter for the last 5 years, and Peter had been communicative since the start of Project Regen.

The project has also been on track with the progress and the council approved the milestone payment of $200,000. This amount was transferred to the new banking account.

Missed Payment

Inject 2

A couple of days passed since the milestone payment was made. Peter called the Director of Finance to ask whether her staff had processed the $200,000 payment. The Director confirmed that the payment has been made, but Peter has verified that they have not received the payment.

Initial checks have revealed that the $200,000 payment was made but to the wrong banking account.

What would be your top priority at this point?

Investigation Underway

Scenario

The leadership team has been made aware of this incident. Local authorities (Canadian Anti-Fraud Centre and Local Police) have been informed and they advised to contact the banking institution to check if the payment can be reversed.

The full investigation has begun, and Beyond Growth is continuing to pursue payments.

The project has been halted until further notice.

Local News Report

Inject 3

A local news agency wrote an online article about this incident.

The article made overblown claims and alleged gross negligence in the council's handling of the project and the funds entrusted to it.

Fraud and Negligence Cost
Southern Lakes Regional Council
SOUTHERN LAKES
REGIONAL COUNCIL
FRAUD
100
100
FRAUD INVESTIGATION
Council Hit by Major Financial Losses Amid Scandal

Do not edit
How to change the design

How would you respond to the news article?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Payments Reversal

Scenario

The team has been in constant contact with local authorities and the issuing and receiving banks. Police say frontline officers moved quickly, freezing a significant portion of the funds in an account allegedly linked to an organized crime group based in eastern Canada.

The process to recover the funds is ongoing and may take weeks to fully recover.
The communications with Beyond Growth have resumed and Project Regen has recommenced.

The investigation has concluded and new processes are now in place to prevent such a case.

Do not edit
How to change the design

What new processes would you include?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Incident Response Recap

Business Email Compromise is a very common fraud technique.

Train staff to identify Red Flags

- Banking change + urgency
- New PDF “bank letter” as proof
- Slightly different tone, spelling, sign-off
- Request to bypass normal process

Incident Response Recap

Response Checklist

- Stop payment / freeze banking change
- Verify by phone using known contact details
- Save evidence (email, headers, attachments, timestamps)
- Notify finance lead immediately
- If money sent: call the bank to recall/reverse ASAP
- Report to CAFC, local police/RCMP

Recap

- Why does cybersecurity matter?
- The Canadian cyber threat landscape
- Cybersecurity threats
- Key Cybersecurity Concepts and Baseline controls
- AI - What are the dangers and how to use it securely
- Incident Response – What to do when something goes wrong

Toronto Metropolitan University

ROGERS cybersecure catalyst

Why Does Cybersecurity Matter?

A failure to protect
our **systems** and **information**,
is a failure to protect those whom we serve.

Q & A

Toronto Metropolitan University

ROGERS cybersecure catalyst

Connect with us

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

Follow the Catalyst on social media:

@cybersecure.catalyst

linkedin.com/school/
cybersecure-catalyst

Visit cybersecurecatalyst.ca for the latest program info, news & events

Toronto Metropolitan University

ROGERS cybersecure catalyst

Toronto Metropolitan University

ROGERS cybersecure catalyst

Thank you

Get connected with the Catalyst today

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.