CANADIAN CENTRE FOR CYBER SECURITY

CYBER 101

Joanne Smith
Indigenous Partnerships

COPYRIGHT

THE CYBER CENTRE VISION AND MISSION

VISION - *OUR PURPOSE*

A SECURE DIGITAL CANADA

MISSION - *OUR PROMISE*

PROTECT
Safeguard Canada with advanced cyber security capabilities.

INFORM
Provide trusted and authoritative cyber security advice and guidance for Canada.

EMPOWER
Strengthen Canada's cyber security capacity through collaboration, innovation, and partnerships.

CANADA'S PLACE IN A DIGITAL WORLD

- Digital technologies are now an integral part of our daily lives, with new developments emerging every day. Technologies connect Canadians from coast to coast to coast while linking us into a dynamic global network.
- Virtually everything Canadians do is touched by technology in some way – As of the third quarter of 2023, Canadians spent an average of one hour and 17 minutes per day using social media and **more than six hours per day** using the internet in general.

DEFINING CYBER THREATS

A Cyber Threat

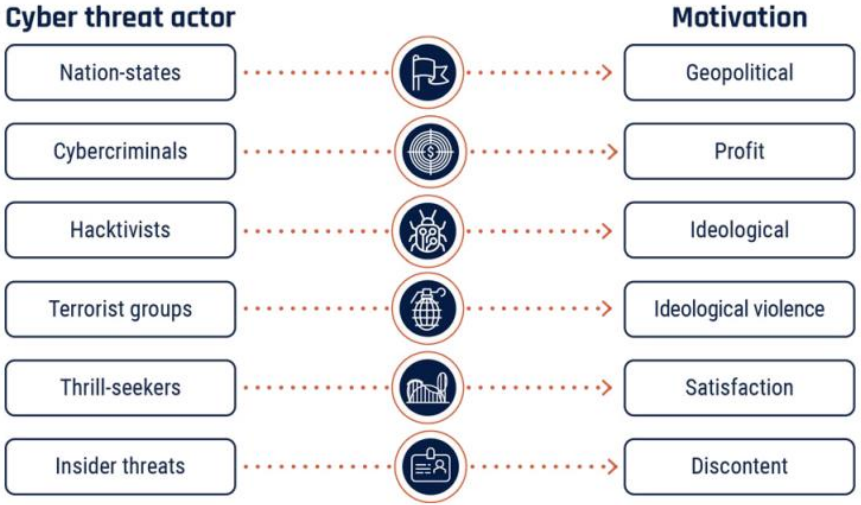
Activity intended to **compromise** the **security of an information system** by altering the availability, integrity, or confidentiality of a system or the information it contains, or to disrupt digital life in general

Cyber Threat Environment

Online space where cyber threat actors conduct **malicious cyber threat activity**. It includes the networks, devices, and processes that are connected to the Internet and can be targeted by cyber threat actors, as well as the methods threat actors use to target those systems

WHO OR WHAT IS A CYBER THREAT ACTOR?

- Groups or individuals who, with malicious intent, aim to exploit weaknesses in an information system or exploit its operators to gain unauthorized access to or otherwise affect victims' data, devices, systems, and networks.
- Categorized by their motivations and degrees of sophistication.



WHAT ARE CYBER THREAT TARGETS?

- Cyber threat actors value access to anything connected to or residing on the Internet, including:
  - Devices (e.g., personal cell phones, computers, servers)
  - Information (e.g., intellectual property, banking details or logins)
  - Financial resources (e.g., fiat currency and digital assets including cryptocurrency)
  - Opinions and reputations (e.g., influencing specific events including elections)
- The globalized nature of the Internet allows threat actors to be physically located anywhere in the world and still affect the security of information systems in Canada.

NO ONE IS IMMUNE TO CYBER THREATS

Cyber criminals are targeting organization of all sizes

Cybercriminals target small to medium organizations because they:

- Lack adequate cyber security resources to protect their information which makes them easier to hack;
- May not be backing up their data which makes them vulnerable to ransom threats;
- Store valuable data, such as personal and financial information;
- Serve as a gateway to larger organizations that procure services and supplies from these smaller organizations.

WHAT IS CYBER SECURITY AND CYBER RESILIENCE?

- Cyber Security: The practice of defending and securing computer systems, networks, software, data, and devices against malicious digital attacks.

- Cyber Resilience: An organization's ability to prevent, withstand and recover from cybersecurity incidents.

CYBER THREAT SURFACE

All information systems and services a cyber threat actor may exploit to compromise an individual, organization, or network

It includes all Internet-exposed endpoints, including networks, personal computers, mobile devices, Internet of Things (IoT) devices, servers, processes that communicate with or rely on information systems connected to the Internet

DETERMINE YOUR CYBER SECURITY POSTURE

1. Do you have a list of all assets (e.g., systems, devices) that are connected to your network?
2. What are the different levels of protection that are needed for your assets?
3. Who has access to those assets?
4. Where are they stored?
5. What security controls are currently in place to protect them?
6. What are the likeliest incidents that will threaten those assets?
7. Do you have an Incident Response Plan (IRP) in place (i.e., do you know who to call and what to do when an incident occurs - communications, security, legal, executive)?

Mobile Devices

Check your surroundings. Be aware of anyone who might be listening to your phone call or looking over your shoulder as you enter your password.

Use multi-factor authentication. You can add an additional layer of security to your devices by changing your settings to require two different factors to unlock it. For example, use a password or PIN and a biometric.

Keep your devices in sight. Don't leave them unattended when you're working in a public location and report a lost or stolen device immediately to your IT help desk.

Run updates and patches on your devices. Updates and patches address and fix security vulnerabilities, ensuring that your device is protected against threat actors.

Enable firewalls and anti-virus software. Firewalls block malicious traffic and anti-virus software scans files for malware.

KEEP YOUR BITS TO YOURSELF AND STAY SAFE ONLINE

Impact

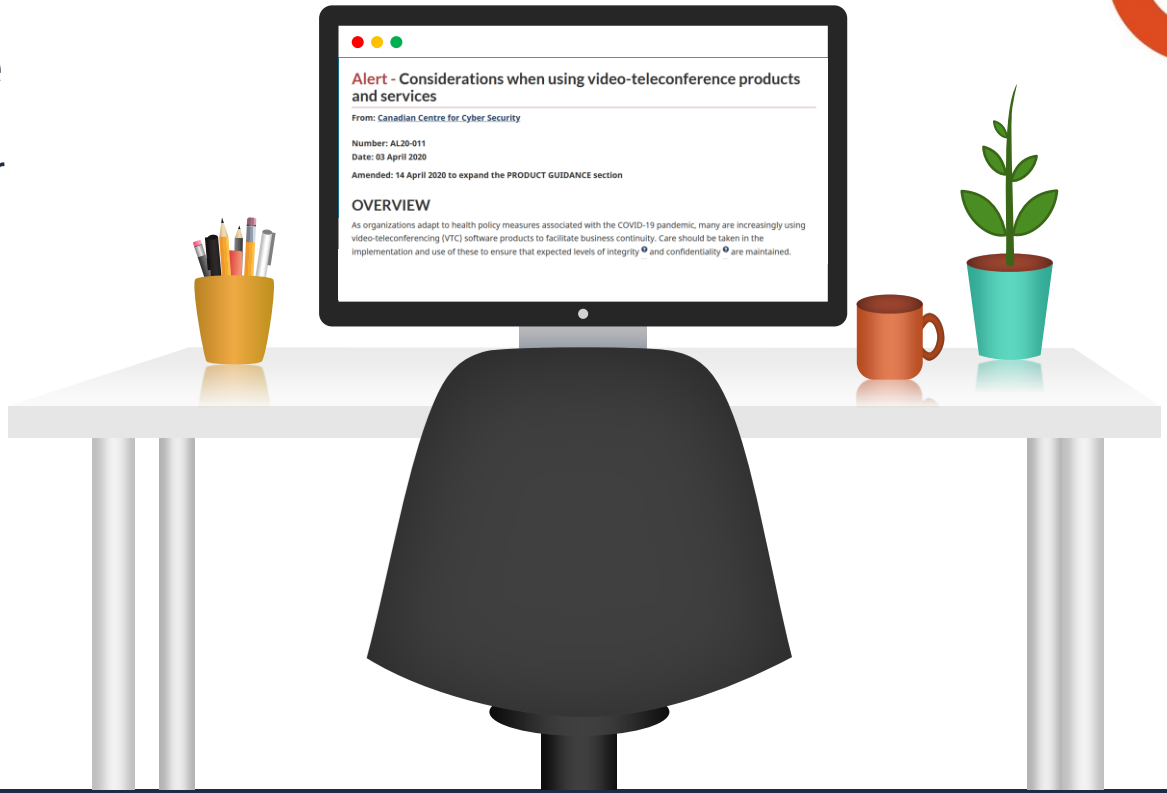
Social media gives you the power to connect with others effortlessly and share information instantly. Since these services and platforms have become so integrated and integral to daily online activities, many employers allow employees to use personal social media accounts at work.

Threat Vectors

When you use personal social media at work, you can be providing threat actors easy and obvious entry points to your organization's networks and systems. You can even be placing your online identity and that of your co-workers at risk.

STAY SAFE WHILE TELEWORKING

Cyber threat actors are adapting to the new reality of telework and will find ways to achieve their goals – whatever they may be. Including basic cyber security hygiene in your work from-home routine should become second nature, both to protect your personal network and information, as well as that of your organization.



DISRUPTIVE TECHNOLIGIES

- Artificial Intelligence and Machine Learning
  - Challenges and opportunities
- Quantum computing
  - Threat to our current cryptographic security
  - Transitioning to quantum-safe algorithms
- Internet of Things (IoT)
  - Increased attack surface
- Cloud technologies
  - Increased reliance on services and data stored in the cloud

SECURITY PROTECTIONS WHEN USING GENERATIVE AI TOOLS

02 Select training datasets carefully.

03 Choose tools from security-focused vendors.

01 Establish generative AI usage policies.

04 Be careful regarding the information you provide.

GENERAL PREVENTION FOR DIGITAL RESILIENCE

These are not a one-size-fits-all approach to cyber security but can assist in creating your organization's cyber security framework.

System Protection

Use strong passphrases and passwords

Enforce MFA including on Administrative accounts

Prevent exposure to known vulnerabilities by implementing automatic updates and patches on all Internet connected devices and systems

Implement user privilege policies and regularly review user privileges.

Network and Endpoint Protection

Prevent security breaches on networks and devices.
Implement:

- Firewalls
- Anti-virus software
- Virtual Private Networks
- Ad blockers
- Anti-Phishing and Anti-Spam software
- Implement protective DNS

Keep business and personal environments separate.

Backup and encrypt data

Data backups are a critical piece of the effort to ensure quick recovery not only from cyber security incidents such as ransomware or malware but also from natural disasters, equipment failures, or theft.

Keep an asset inventory - what assets, information and systems are of value to your organization and where are they located

User Education

Everyone has a role to play in keeping information and assets safe.

Ensure employees are aware and practicing cyber safety best practices.

Develop an incident response plan

It is not IF an incident will occur but WHEN.

Incidents happen no matter the amount of technology and training we implement. Create an incident response plan and test it regularly to ensure you can restore operations and recover quickly in the event of a cyber compromise.

HOW CAN THE CYBER CENTRE ASSIST YOU?

SUMMARY

- You are not alone when it comes to facing cyber threats. We offer organizations of all sizes cyber security solutions that can help enhance and strengthen their cyber security posture and improve their resiliency to cyber threats.
- Our overall objective is to help **YOU** create and maintain a **strong cyber security posture** by establishing a robust cyber security solution.

Thank you

Questions?

CONNECT WITH US


@cse_cst


contact@cyber.gc.ca


www.cyber.gc.ca


@cybercentre_ca