CANADIAN CENTRE FOR CYBER SECURITY

CANARIE
Cybersecurity Monthly Webinar
Cyber Centre and Services
January 2021

Canadian networks need to be *secured* from adversaries and personal information of Canadians must be *protected*.

Securing these systems is not simply a matter of operational efficiency; it is a matter of *national security*, *sovereignty* and *privacy protection*.

CSE'S ROLE IN CYBER SECURITY

- CYBER SECURITY LEAD IN CANADA
- ACCESS TO UNIQUE FOREIGN INTELLIGENCE
- AHEAD OF EMERGING THREATS
- MONITOR GC SYSTEMS 24/7 FOR CYBER THREATS
- SAFEGUARDS CANADA'S MOST IMPORTANT INFORMATION

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Information Technology Security (CSE) + Security Operations Centre (Shared Services Canada) + Canadian Cyber Incident Response Centre (Public Safety) = Canadian Centre for Cyber Security

Increased Cyber Security Service Scope

National Defence Act (NDA)

CSE could provide advice, guidance and services to protect information infrastructures of importance to the GC.

CSE Act

August 2019 - CSE is now authorized to provide more robust cyber defense services by deploying its cyber defence tools to critical non-Government networks designated as being of importance to Canada.

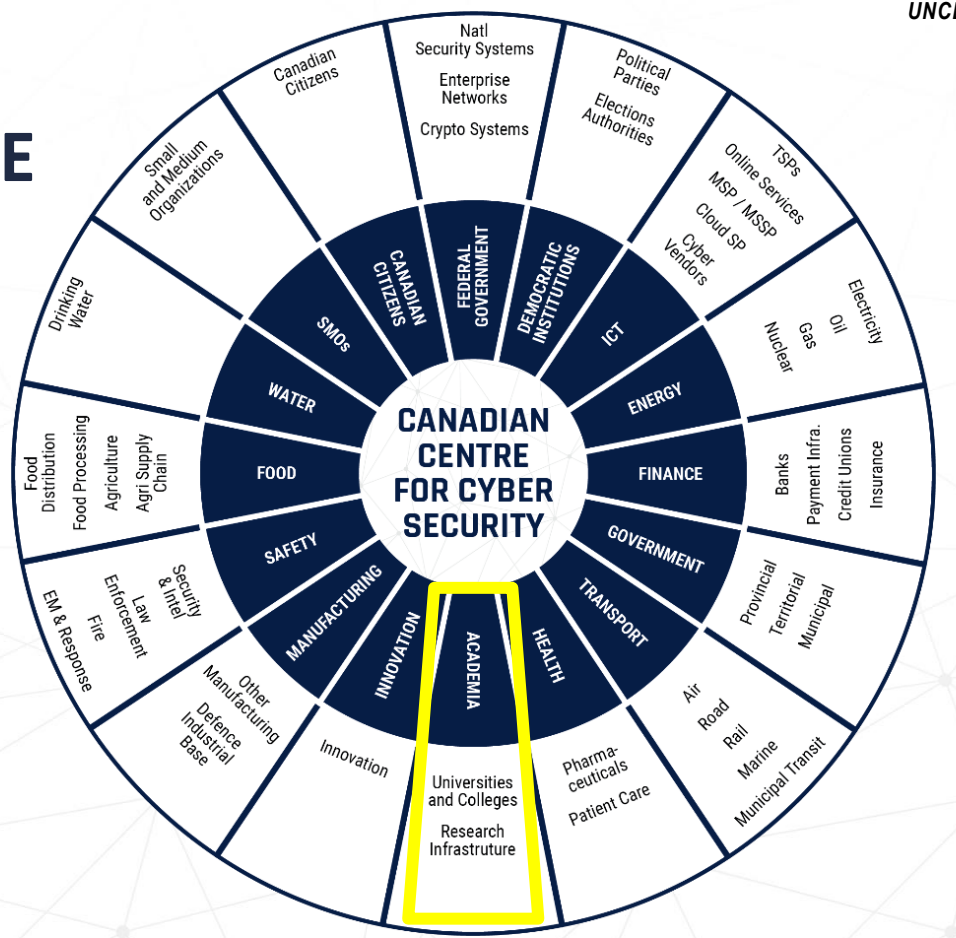
CYBERSECURITY AND INFORMATION ASSURANCE

DEFEND IMPORTANT NON-GOVERNMENT OF CANADA NETWORKS

Upon request, deploy CSE's cybersecurity tools on non-government systems

Remove legal barriers to sharing cyber threat information and mitigation advice

CYBERSECURITY CRITICAL INFRASTRUCTURE SECTORS



WHO WE SERVE

We welcome partnerships that help build a stronger, more resilient cyber space in Canada. We hold unclassified, multi-purpose spaces for the joint use of government, private industry and academia.

GOVERNMENT

We are the centralized voice and resource for senior leadership in government on cyber security operational matters.

EXTERNAL PARTNERS

We are the primary federal government point of contact on cyber security operational matters for external partners, including incident response and coordination.

LAW ENFORCEMENT

We are the single authoritative source of technical cyber security expertise to support lead agencies in their policing, security and intelligence work.

CANADIANS

We inform, communicate, and educate Canadians about cyber security issues by providing clear, practical advice backed up by unique expertise and insight.

THE CYBER CENTRE VISION AND MISSION

VISION - *OUR PURPOSE*

A SECURE DIGITAL CANADA

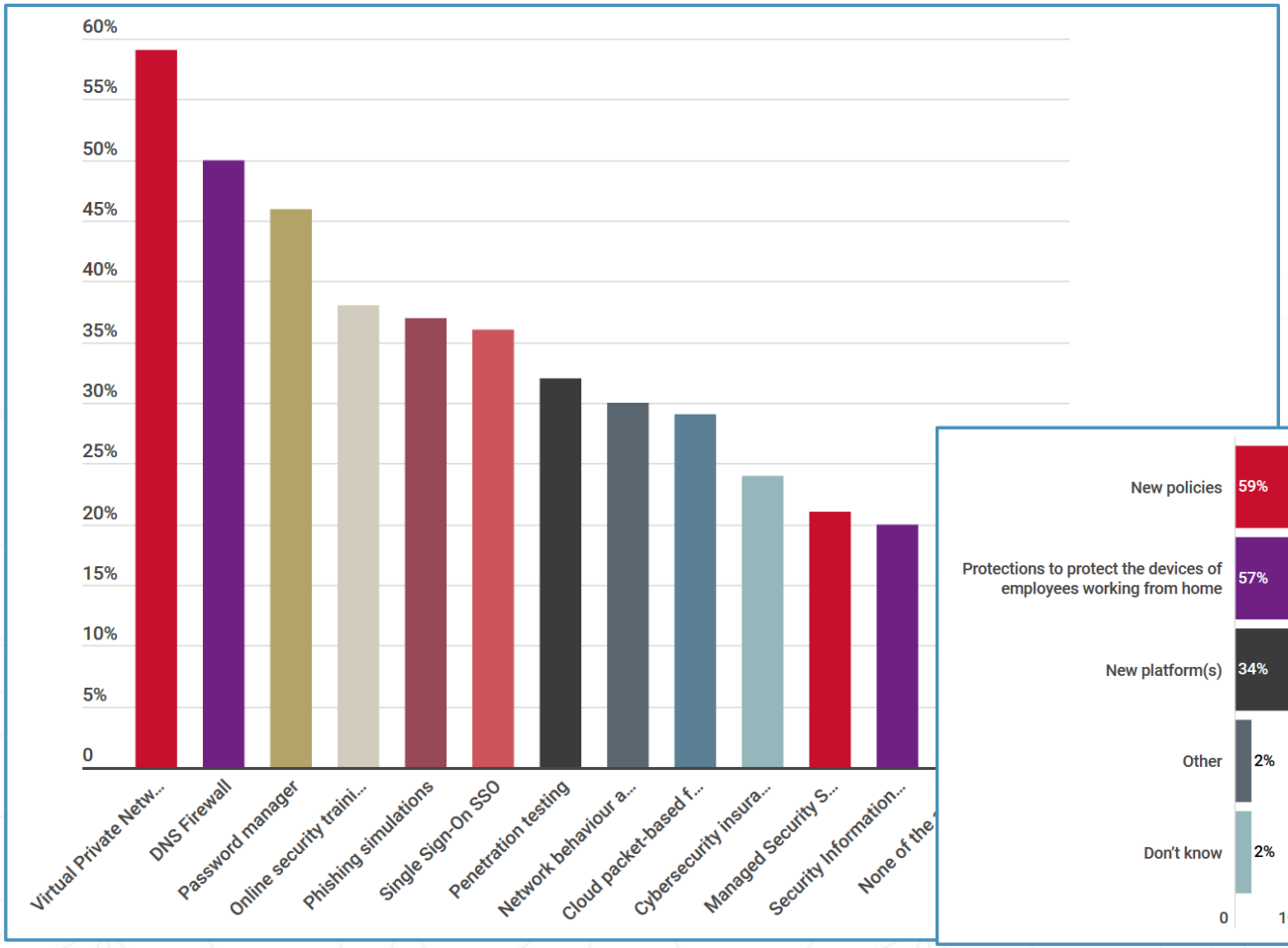
MISSION - *OUR PROMISE*

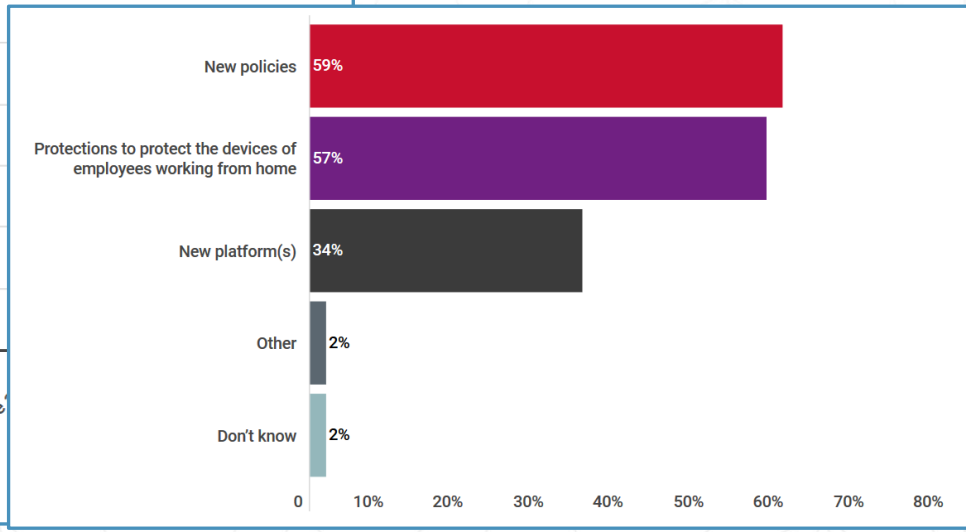
CCCS NATIONAL CYBER THREAT ASSESSMENT 2020

- Number of cyber attacks is increasing and becoming more sophisticated
- Cybercrime and ransomware will continue to target CI sectors
- State-sponsored programs of China, Russia, Iran and North Korea pose the greatest strategic threat to Canada as they conduct espionage against Canadian businesses, **academia** and government to steal Canadian IP

New Protections (2020)

Reference : https://www.cira.ca/cybersecurity-report-2020





Cyber Attacks Per Year (2020)

80%

Percentage of organizations that faced a cyber-attack in the last year

21%

Percentage of organizations that faced more than 10 attacks in the last year

Reference : https://www.cira.ca/cybersecurity-report-2020

Patching Policy (2020)

Reference : https://www.cira.ca/cybersecurity-report-2020

Our Services

1. Join our Sector Community Calls
2. Complete the Canadian Cyber Security Tool
3. Participate in Training and Awareness
4. Cyber Threat Notifications
5. Leverage Tailored Cyber Defense Tools

1. ACADEMIC SECTOR COMMUNITY CALL

Purpose Is To Share Sector Relevant Cyber Expertise

- Build Community of Trust
- Provide Situational Awareness
- Offer at Regular Cadence (bi-weekly beginning Feb 2021)

To join: email **marie-claude.belanger@cyber.gc.ca**

2. Canadian Cyber Security Tool (CCST)

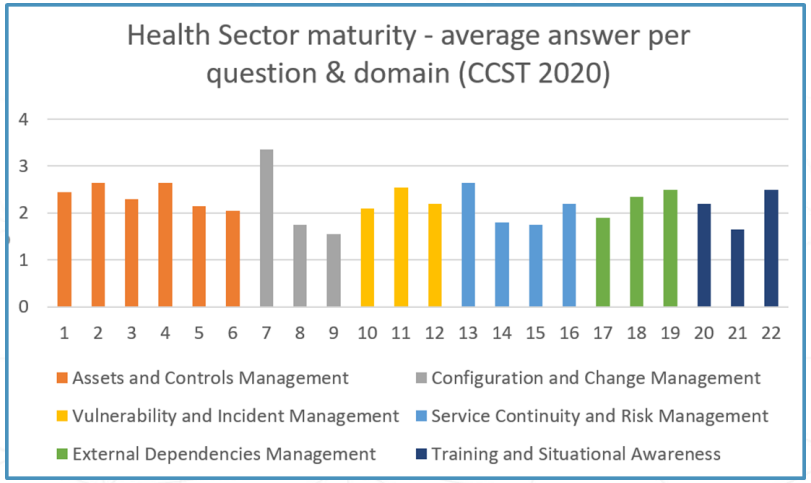
- What is it:
  - On-line, self assessment tool designed to be completed in under 60 mins
  - Relevant for entities with a wide range of cyber postures
- The Goal:
  - Understand the RISK you are facing in order to better serve institution with appropriate guidance, services and support
- Tool reports
  - Tailored advice and guidance and entity specific scores and peer based comparisons

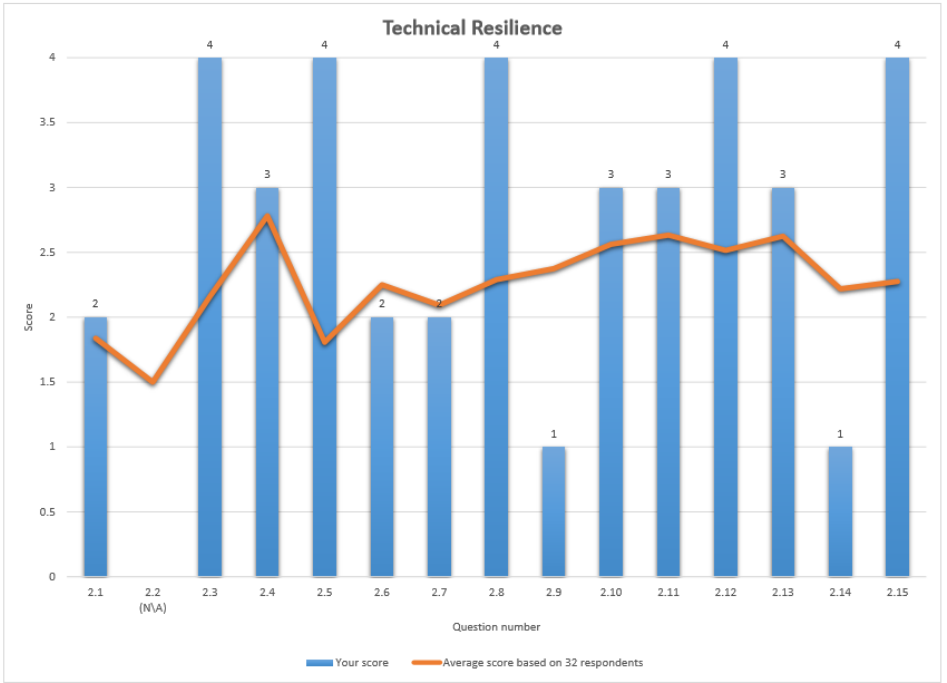
To join: email marie-claude.belanger@cyber.gc.ca

Canadian Cyber Security Tool

BUILDING A SAFE AND RESILIENT CANADA

Program and Technical Resilience Results...to the entity





3. TRAINING AND AWARENESS: Learning Hub

- Pre-recorded (3 hrs)
  - 107 – Cyber Security for non-IT Employees
  - 110 – Cyber Security and Online Exposure
  - 111 – Cyber Security for Home and Telework

https://cyber.gc.ca/en/learning-hub

- E-learning (30-60 min)
  - 602 – Discovering Cyber Security

- Live Mini-Sessions (90 min)
  - IoT: industry standards, regulations, security concerns, and unintended consequences
  - Authentication: best practices for passwords, hardware tokens, biometrics, and 2FA/MFA
  - Teleworking: Security measures for a work-from-home setting
  - Privacy: protection of personal data, a standards and regulations perspective
  - Cybercrime: security measures against account and device takeover

4. Subscribe to Cyber Threat Notifications

ALERTS
Pro-active Notifications on New Cyber Threats

ALERTS | **Microsoft Security Advisory**

Number: AV20-308
Date: 21 August 2020

On 19 August 2020 Microsoft released an out-of-band security update to address vulnerabilities in the following versions of Windows:

- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 R2

https://support.microsoft.com/en-ca/help/4578013/security-update-for-windows-8-1-rt-8-1-and-server-2012-r2

An actor with execution rights on affected systems could exploit a memory handling flaw in Windows Remote Access to escalate privileges.

The Cyber Centre encourages users and administrators to review the provided web link and apply the necessary updates as soon as possible.

Email Alerts

Cyber Centre Website
https://www.cyber.gc.ca/en/alerts-advisories

CYBER FLASH
Urgent Notifications on Active Security Issues

Actionable information** sent to describe an **immediate security issue.

```
TITLE
-----
Active exploitation leading to PoisonPlug / ShadowPad malware

SUMMARY
-------
The Cyber Centre has become aware of…

DETAILS
-------

SUGGESTED ACTIONS
-----------------

INDICATORS OF COMPROMISE
------------------------
```

Email Alerts

WEEKLY TECHNICAL REPORTS
Reports on activities and incidents

Weekly summaries of cyber activities, incidents and indicators of compromise (IOCs) related to the GoC and Critical Infrastructure.

Emails

5. Tailored Cyber Defence Tools

NCTNS NOTIFICATIONS
Cyber Threats Seen on Your IP Space

*Sent to you when a **sign of compromise** or a vulnerable service is seen on **your IP space** to notice cyber threats faster and **better protect your organization**.*

- Vetted data to ensure quality and a low percentage of false positive

Email Notifications

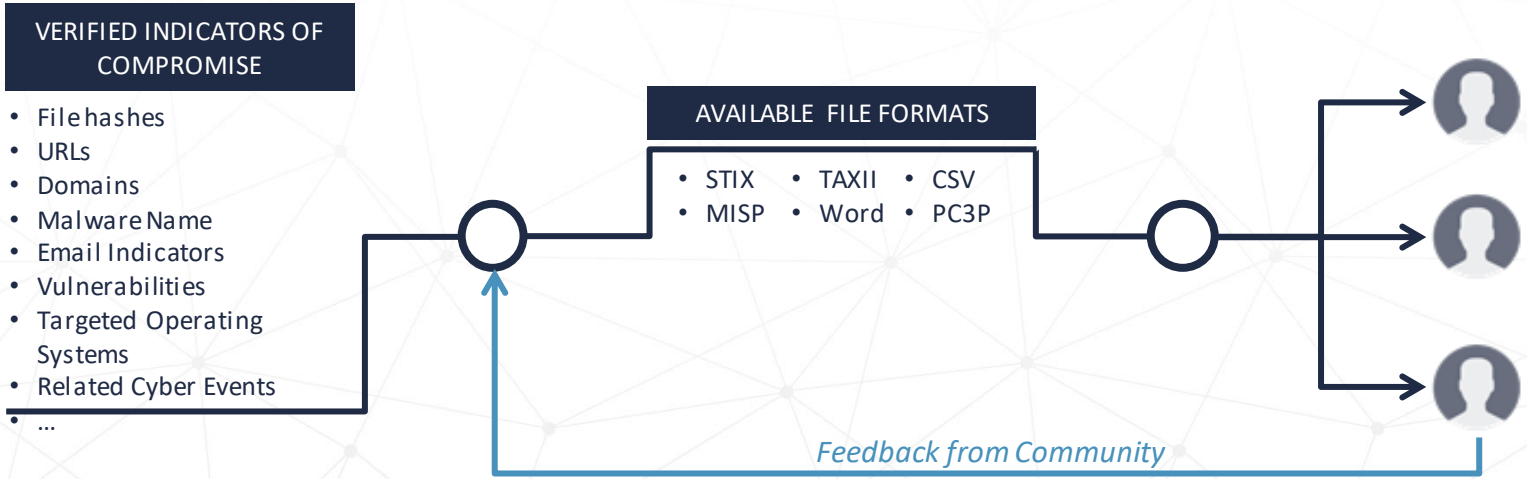
API
(In development)

Requirements

- Accept the Terms of Use
- Provide contact information for the person who will be receiving and using the notifications
- Share the IP range specific to your organization

AVENTAIL
Real-time IOC sharing

*Sharing relevant and **verified information** on Indicators of Compromises (IoCs) at **machine speed***



Requirements

- Sign a Non-Disclosure Agreement
- Provide us with the IP address of your MISP server

Other Services and Products

MALWARE INTAKE

To Email Suspicious Files to the Cyber Center for Analysis

*Cyber Centre **malware analysts** and **automated systems** assess whether files are malicious or not*

Results of analysis sent by email

RECEPTION OF DISCOVERY OF SOMETHING SUSPICIOUS

SUSPICIOUS FILE → **malware@ccirc.ca**

NOT A FILE (Indicators of Compromise, phishing, etc.) → cyberincident@cyber.gc.ca

Rules of Engagement

- Files will be detonated on the Internet
- Unless otherwise specified, resulting IoCs will be shared with the community without attribution
- Files have to be UNCLASSIFIED (NO PB or CLASSIFIED data)

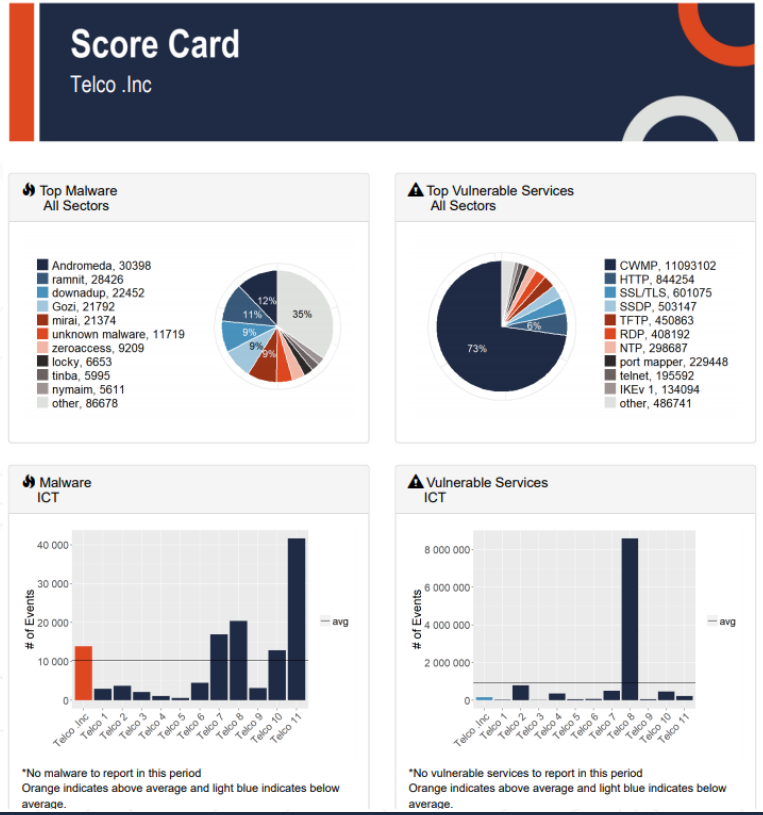
SCORECARDS
Actionable Cyber-Event Information

Report on potential infections, vulnerable services notifications, ***situational awareness data****, and a* ***peer-based comparison*** *to other organizations within your sector.*

PDF reports emailed monthly
(raw CSV data available on request)

Requirements

- Accept the Terms of Use
- Provide contact information for the person who will be receiving and using the Score Cards
- Share the IP range specific to your organization



Publications

- Cyber Threats
  - National Cyber Threat Assessment
  - Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity
- Implementing Cyber Security
  - Baseline security Controls for Small Medium Organizations
  - Rethink your Password Habits to Protect your Accounts from Hackers
  - Secure Your Accounts and Devices with Multi-Factor Authentication
  - Cyber Security Best Practices: Contracting With Managed Service Providers
  - Ransomware: How to Prevent and Recover
  - Protect Your Organization from Malware
  - Don't take the bait: Recognize and avoid phishing attacks
- COVID-19 Related
  - Focused Cyber Security Advice and Guidance During COVID-19
  - Cyber Hygiene for COVID-19
  - Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity
  - Security Tips for Organizations With Remote Workers

VISIT: cyber.gc.ca
for more publications

WHO TO CONTACT AND WHEN

CANADIAN CENTRE FOR CYBER SECURITY → Reporting cyber incidents

cybertip.ca → Child exploitation, trafficking of child porn, child sextortion, etc.

Royal Canadian Mounted Police / Gendarmerie royale du Canada → Cybercrime: Ransomware, Money Laundering, Identity Theft, Cyberbullying, etc.

CANADIAN ANTI-FRAUD CENTRE / CENTRE ANTIFRAUDE DU CANADA (CAFC) → If you receive personal phishing email, telemarketing, tax scam

CONNECT WITH US


contact@cyber.gc.ca


www.cyber.gc.ca


@cybercentre_ca

Cyber Centre Publications :
https://cyber.gc.ca/en/publications

Cyber Center Alert & Advisories:
https://cyber.gc.ca/en/alerts-advisories

To report fraud:
Canadian Anti-Fraud Centre
1-888-495-8501
www.antifraudcentre-centreantifraude.ca

To report a cybercrime:
Local police or
Royal Canadian Mounted Police
www.rcmp-grc.gc.ca

To report a cyber incident
Canadian Center for Cyber Security


cyberincident@cyber.gc.ca