CANADIAN CENTRE FOR CYBER SECURITY

Learning Hub

Cyber Security Training for the Government of Canada

Communications Security Establishment   Centre de la sécurité des télécommunications

Canada

Canadian Centre for Cyber Security (Cyber Centre)

- Operates under the Communications Security Establishment (CSE)
- Canada's national cyber security authority
  - Single unified source of expert advice, guidance, services, and support on cyber security
  - National authority on communications security (COMSEC)
  - Integrated incident response within the federal government
  - Collaboration with the RCMP and other partners on cybercrime and cyber security matters
  - Critical infrastructure engagement program addresses complex cyber security challenges
- Serves federal, provincial, territorial, and municipal governments in Canada, critical infrastructure, private sector, and academia

Learning Hub

- The Cyber Centre Learning Hub (LH) offers COMSEC and cyber security instructor-led and online courses and workshops for various audiences, as well as custom solutions
- This training is offered primarily to the Government of Canada (GC) but is also available to other levels of government, publicly funded institutions, and eligible private sector companies
- Services include
  - In-class and virtual instruction
  - Custom and tailored training
  - Elearning

Is Cyber Security Proactive or Reactive?

Three Thoughts about Cyber Security

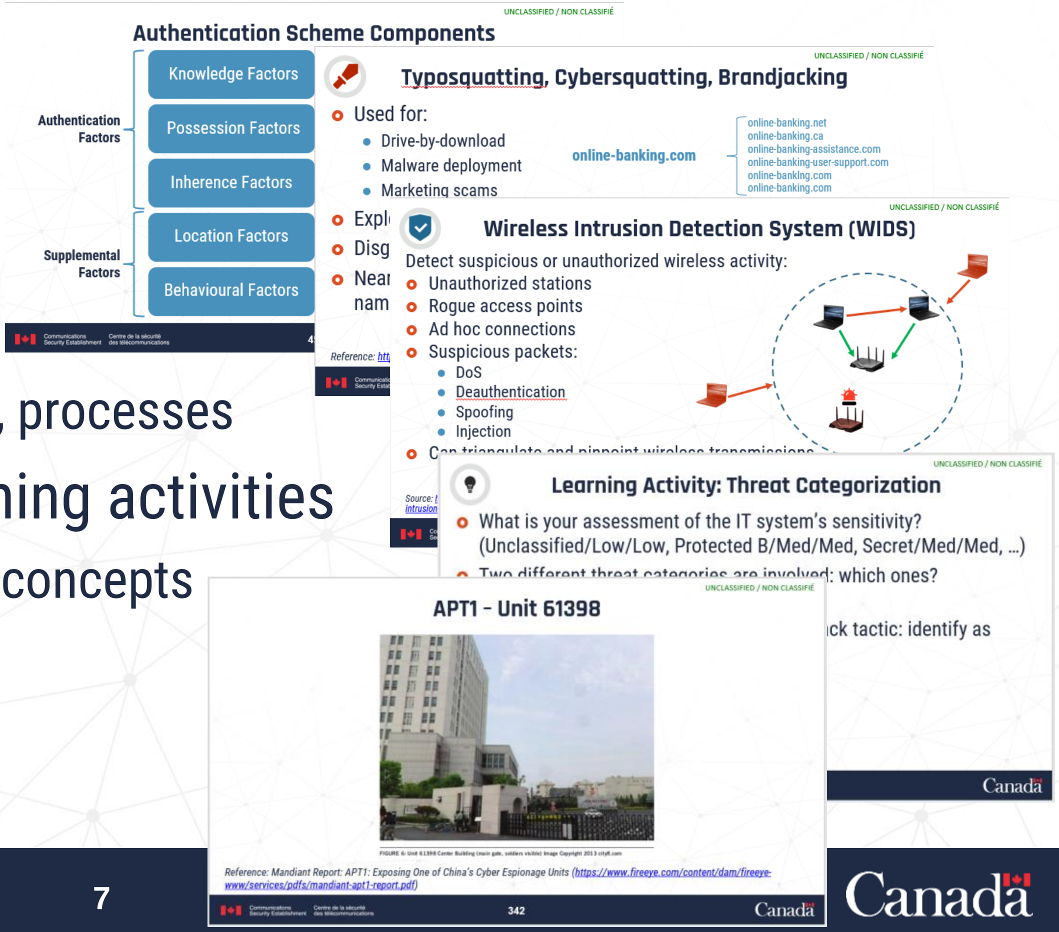
- The Internet was not built with security in mind
- We have built a colossus on top of this foundation
- There is nearly endless room for creativity and for exploitation

What Do We Do About It?

- How do we train people in a rapidly-changing, complex and dynamic environment?
- How do we train people to recognize shifting contexts and understand a rapidly-changing, complex and dynamic environment?
- How do we train people how to manage risk that is influenced by a rapidly-changing, complex and dynamic environment?

An Evolving Model

- Context and language
- Threats
  - Motivations, actors and TTPs
- Countermeasures
  - Security controls, technologies, processes
- Case studies linked with learning activities
  - Linking real world examples to concepts



UNCLASSIFIED / NON CLASSIFIÉ

Authentication Scheme Components

UNCLASSIFIED / NON CLASSIFIÉ

Typosquatting, Cybersquatting, Brandjacking

- Used for:
  - Drive-by-download
  - Malware deployment
  - Marketing scams
- Expl
- Disg
- Near nam

Reference: htt

UNCLASSIFIED / NON CLASSIFIÉ

Wireless Intrusion Detection System (WIDS)

Detect suspicious or unauthorized wireless activity:

- Unauthorized stations
- Rogue access points
- Ad hoc connections
- Suspicious packets:
  - DoS
  - Deauthentication
  - Spoofing
  - Injection
- Can triangulate and pinpoint wireless transmissions

Source: intrusion

UNCLASSIFIED / NON CLASSIFIÉ

Learning Activity: Threat Categorization

- What is your assessment of the IT system's sensitivity? (Unclassified/Low/Low, Protected B/Med/Med, Secret/Med/Med, …)
- Two different threat categories are involved: which ones?

ck tactic: identify as

UNCLASSIFIED / NON CLASSIFIÉ

APT1 - Unit 61398

FIGURE 6: Unit 61398 Center Building (main gate, soldiers visible) Image Copyright 2013 city8.com

Reference: Mandiant Report: APT1: Exposing One of China's Cyber Espionage Units (https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf)

Communications Security Establishment
Centre de la sécurité des télécommunications
342
Canada

National Cyber Threat Assessments

- Produced by the Cyber Centre to help build Canada’s resilience to cyber threats
- Based on an analysis of the threat landscape using both classified and unclassified sources

Communications Security Establishment Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

CYBER THREAT BULLETIN: The Ransomware Threat in 2021

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada

CANADIAN CENTRE FOR CYBER SECURITY

National Cyber Threat Assessment

ISSN 2816-9182

2023 2024

Communications Security Establishment Centre de la sécurité des télécommunications

Canada

CANADIAN CENTRE FOR CYBER SECURITY

NATIONAL CYBER THREAT ASSESSMENT 2020

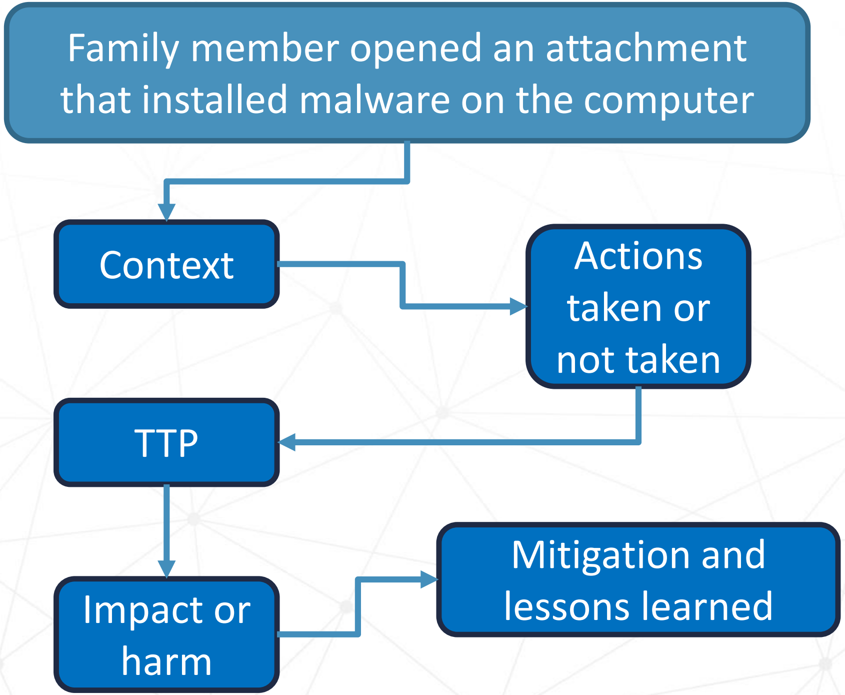
Communications Security Establishment Centre de la sécurité des télécommunications

Canada

National Cyber Threat Assessments - Canadian Centre for Cyber Security

Techniques

- Case studies and tech demos
- Activities and mapping exercises
- Open dialog
- Training material life cycle
- Engaging SMEs and experts
- Linking security to threats
- Addressing biases and misunderstandings



Family member opened an attachment that installed malware on the computer

Context

Actions taken or not taken

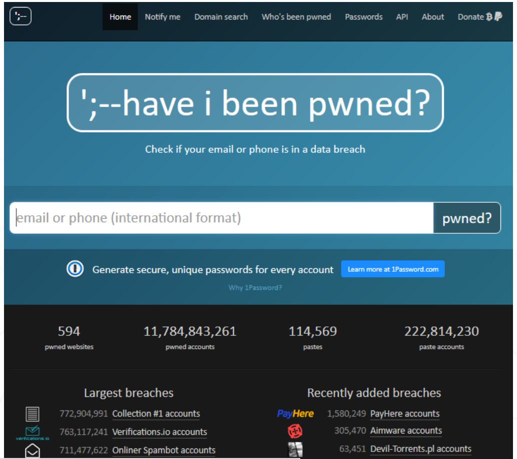
TTP

Impact or harm

Mitigation and lessons learned

Keep it Interesting

- Threats, responses and new technologies are fascinating
- Real world examples resonate with learners
  - Case studies, reports and mapping exercises



';--have i been pwned?

Check if your email or phone is in a data breach

email or phone (international format) pwned?

Generate secure, unique passwords for every account Learn more at 1Password.com

Why 1Password?

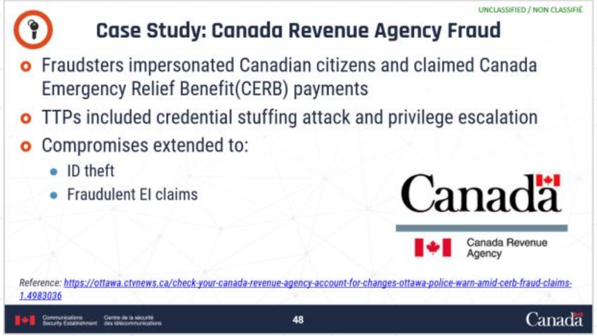
594	11,784,843,261	114,569	222,814,230
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts

Recently added breaches

1,580,249	PayHere accounts
305,470	Aimware accounts
63,451	Devil-Torrents.pl accounts
4,101,101	Avvo accounts
471,376	Travelio accounts
420,873	Royal Enfield accounts
746,682	ZAP-Hosting accounts
19,218,203	CDEK accounts
5,003,937	Robinhood accounts



UNCLASSIFIED / NON CLASSIFIÉ

Case Study: Canada Revenue Agency Fraud

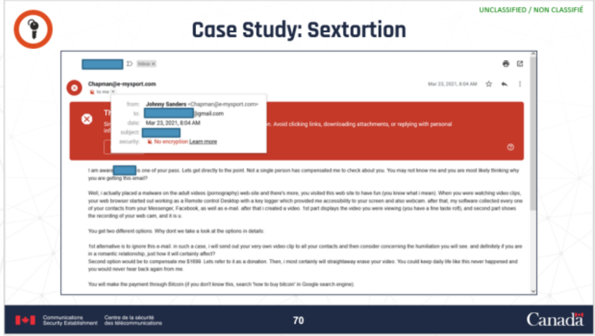
- Fraudsters impersonated Canadian citizens and claimed Canada Emergency Relief Benefit(CERB) payments
- TTPs included credential stuffing attack and privilege escalation
- Compromises extended to:
  - ID theft
  - Fraudulent EI claims

Canada

Canada Revenue Agency

Reference: https://ottawa.ctvnews.ca/check-your-canada-revenue-agency-account-for-changes-ottawa-police-warn-amid-cerb-fraud-claims-1.4983036

Communications Security Establishment Centre de la sécurité des télécommunications 48 Canada



UNCLASSIFIED / NON CLASSIFIÉ

Case Study: Sextortion

[redacted] Inbox ×

Chapman@e-mysport.com

to me

Mar 23, 2021, 8:04 AM

from: Johnny Sanders <Chapman@e-mysport.com>
to: [redacted]@gmail.com
date: Mar 23, 2021, 8:04 AM
subject: [redacted]
security: No encryption Learn more

n. Avoid clicking links, downloading attachments, or replying with personal

I am aware [redacted] is one of your pass. Lets get directly to the point. Not a single person has compensated me to check about you. You may not know me and you are most likely thinking why you are getting this email?

Well, i actually placed a malware on the adult videos (pornography) web-site and there's more, you visited this web site to have fun (you know what i mean). When you were watching video clips, your web browser started out working as a Remote control Desktop with a key logger which provided me accessibility to your screen and also webcam. after that, my software collected every one of your contacts from your Messenger, Facebook, as well as e-mail. after that i created a video. 1st part displays the video you were viewing (you have a fine taste rofl), and second part shows the recording of your web cam, and it is u.

You get two different options. Why dont we take a look at the options in details:

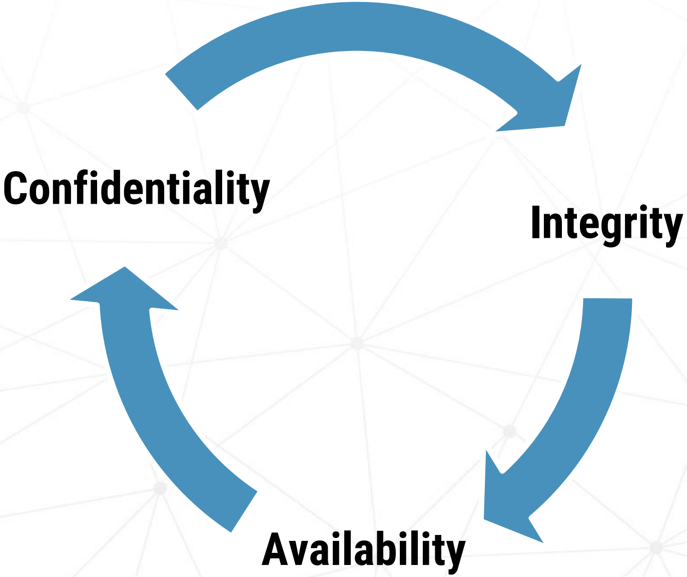
1st alternative is to ignore this e-mail. in such a case, i will send out your very own video clip to all your contacts and then consider concerning the humiliation you will see. and definitely if you are in a romantic relationship, just how it will certainly affect?
Second option would be to compensate me $1699. Lets refer to it as a donation. Then, i most certainly will straightaway erase your video. You could keep daily life like this never happened and you would never hear back again from me.

You will make the payment through Bitcoin (if you don't know this, search 'how to buy bitcoin' in Google search engine).

Communications Security Establishment Centre de la sécurité des télécommunications 70 Canada

Cyber Security Goals

- To protect and maintain information and infrastructure in support of business requirements:
  - Confidentiality
  - Integrity
  - Availability
- Additional goals:
  - Assurance
  - Authenticity
  - Non-repudiation



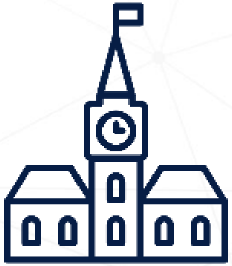
Confidentiality

Integrity

Availability

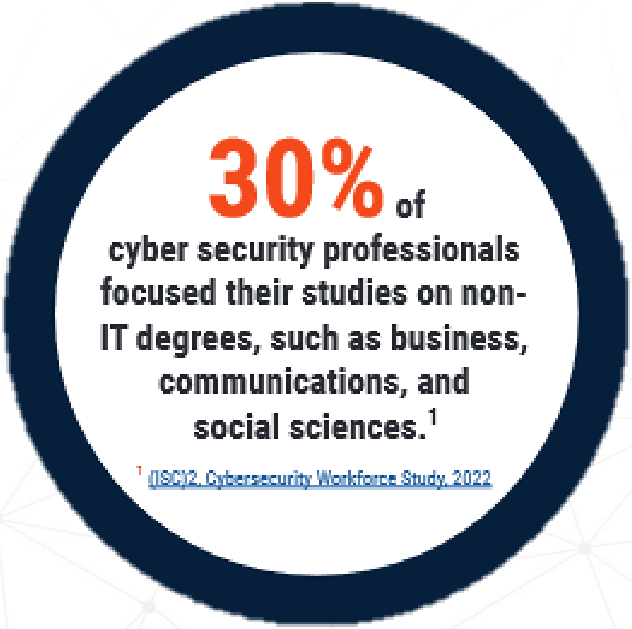
Audiences

- Federal, provincial, territorial and municipal governments in Canada, critical infrastructure and academia
- Strengthening skills and providing context for experts
- Helping new experts emerge and grow
- Building cyber resilience for everyone



Cyber Security is a Team Sport!

- Cyber security needs players with different strengths to be successful. Both technical and non-technical players are needed!
- Cyber security professionals are essential to protecting our citizens, economy, and democracy.
- The field of cyber security is always evolving, and most days bring something new.



30% of cyber security professionals focused their studies on non-IT degrees, such as business, communications, and social sciences.[1]

[1] (ISC)2, Cybersecurity Workforce Study, 2022

Desire to learn

Problem-solving skills

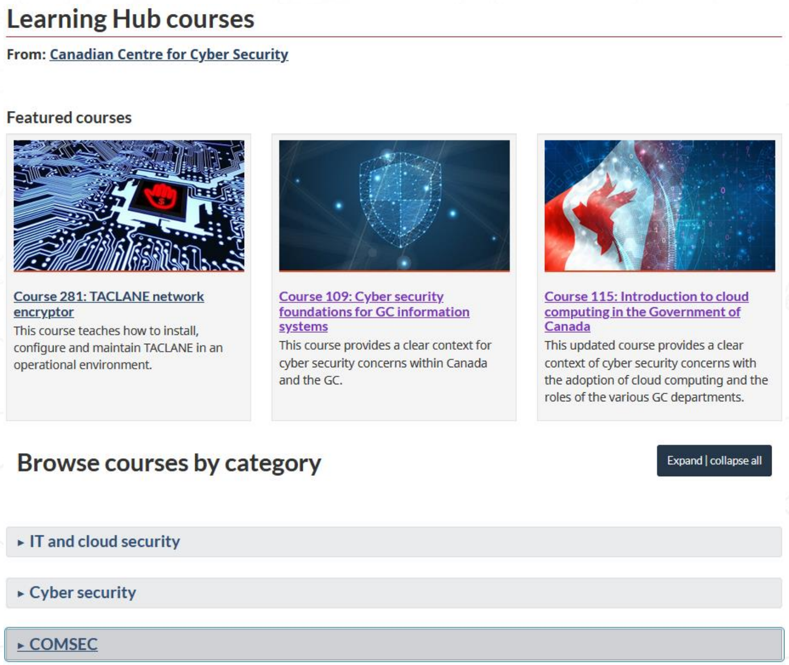
Teamwork

Leadership

Streams

- COMSEC, IT and Cloud Security and Cyber Security
- E-learning and instructor led courses
- Virtual, in-person and hybrid learning
- Group training, custom training and curriculum courses

CYBER CENTRE LEARNING HUB
FOSTERING EXCELLENCE IN CYBER SECURITY



Learning Hub courses

From: Canadian Centre for Cyber Security

Featured courses

Course 281: TACLANE network encryptor
This course teaches how to install, configure and maintain TACLANE in an operational environment.

Course 109: Cyber security foundations for GC information systems
This course provides a clear context for cyber security concerns within Canada and the GC.

Course 115: Introduction to cloud computing in the Government of Canada
This updated course provides a clear context of cyber security concerns with the adoption of cloud computing and the roles of the various GC departments.

Browse courses by category

- ▸ IT and cloud security
- ▸ Cyber security
- ▸ COMSEC

Types of Courses

- Fundamentals
  - Building context and concepts, establishing best practices
  - Collaboration with the Canada School of Public Service
- Activity or technology based
  - IT risk management, cloud security, authentication, telework, IoT, wireless technology, operational technology, software development, cryptography
- Issue based
  - Cybercrime, social engineering, insider threats, event management, TTX, incident response…

Takeaways

- Foster curiosity and exploration
- Communicate ideas, help learners link them to lived experience and real-world examples
- Connect threats with countermeasures
- Prepare learners for future developments
- Leverage our material and explore our courses

Questions

CONNECT WITH US

☎ 833-645-3276

✉ education@cyber.gc.ca

🌐 https://cyber.gc.ca/en/learning-hub