

NC3

NATIONAL CYBERCRIME
COORDINATION CENTRE

CNC3

CENTRE NATIONAL DE COORDINATION
EN CYBERCRIMINALITÉ

- What is Cybercrime?
- Why is it impactful?
- Types of threats/incidents
- What we are doing about it
- How you can help



First Slido Question: I associate the term Cybercrime with?

1. Online scams
2. Ransomware
3. When networks are hacked and data stolen
4. When I get an email with a suspicious link



Defining Cybercrime (not easy...)



Cybercrime: Just a Property crime?

- Preventing delivery of key services – Healthcare
- Threatening Economic Integrity- businesses shuttered
- Exposing peoples' most intimate data
- Fear of being online (particularly the vulnerable)
- Mental anguish from extortion tactics (e.g., financially based sextortion)
- Physical injury and death caused by cybercrime?
 - Technically possible now, but yet to see wide scale use (how to monetize it?)

WebMD Health News

Recent Cyberattack Disrupted Cancer Care Throughout U.S.

Abortion data from Medibank hack posted on dark web as Clare O'Neil pledges to pursue 'scumbags'

Australian Federal Police warn public it is a criminal offence to seek out the data posted by a Russian ransomware group

Too many 'sextortion' suicides

By: John R. Wiens

Posted: 2:01 AM CDT Wednesday, Jul. 20, 2022



Facing a Highly Motivated, Unscrupulous and Adaptive Human Adversary

Malware scam circulates after Saskatchewan stabbings

Medibank: Hackers release abortion data after stealing Australian medical records

Ransomware attack delays patient care at hospitals across the U.S

[Saskatchewan](#) / [News](#) / [Local News](#) / [Crime](#)

RCMP warning public about cyber scam impersonating officer

N.L. health-care cyberattack is worst in Canadian history, says cybersecurity expert

More than half the ransomware attacks in Canada target critical infrastructure

Fake COVID notification apps and websites aim to steal money and personal data

{ SECURITY }

Cyber-mercenaries for hire represent shifting criminal business model

Emerging threat group offers a broad range of attack services

Jeff Burt

Mon 25 Jul 2022 // 17:00 UTC

B.C. health authority hit with ransomware attack



Cybercrime – Human focussed problem

- Facing highly adaptive human adversary, not machines
- Largely financially motivated humans
- Individuals and groups with almost no moral compass
- Potential victims who are hard-wired to click without thinking
- Complex software and inter-connected systems that are nearly impossible to build (by humans) without vulnerabilities
- Individual reluctance to report – embarrassed, mistrust of government/police, legal-reputational worries

= a significant human-based challenge to solve



Second Slido Question:

I have been a victim of a cybercrime or online fraud (e.g., sent money to scammer, had their data stolen directly or as part of large data breach)?

1. Yes
2. No

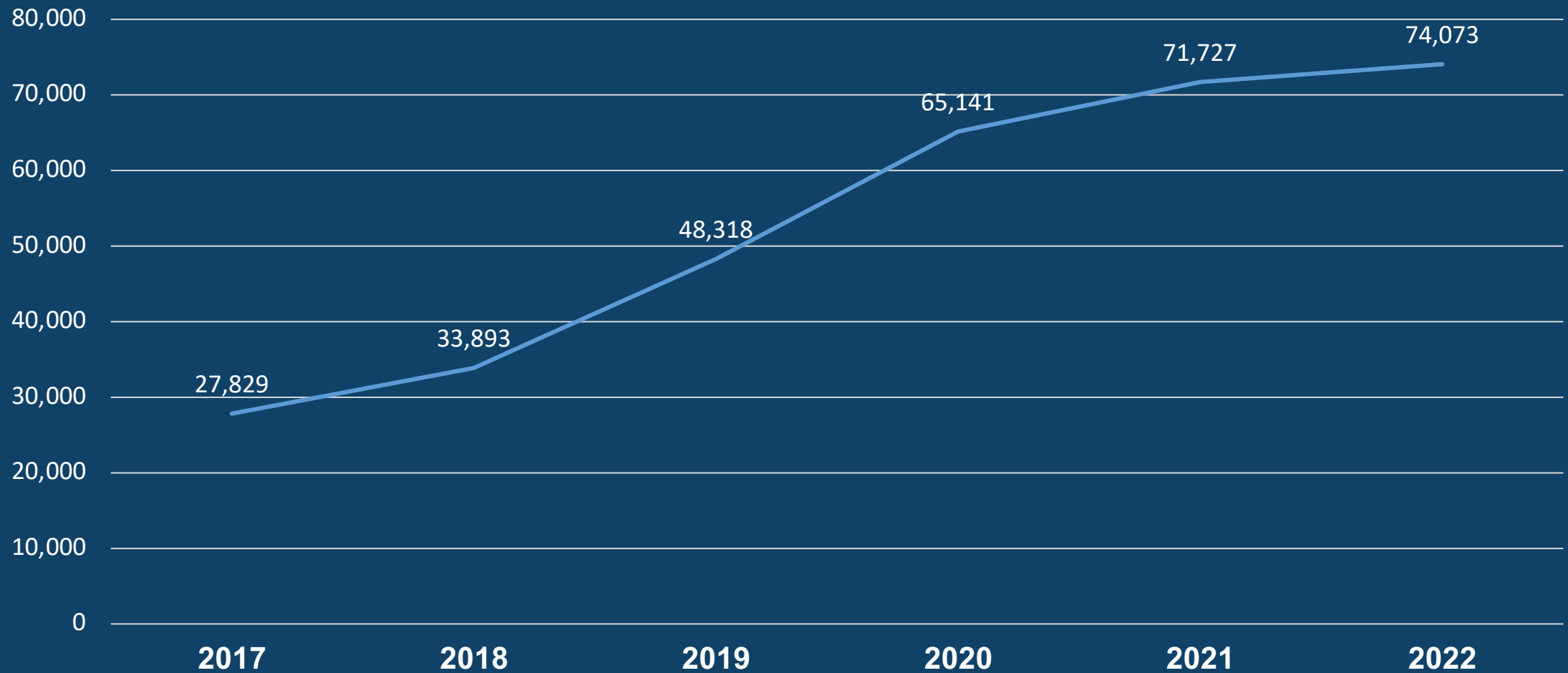
Third Slido Question - If yes, I reported it to law enforcement (e.g., local police or Canadian Anti-Fraud Centre

1. Yes
2. No



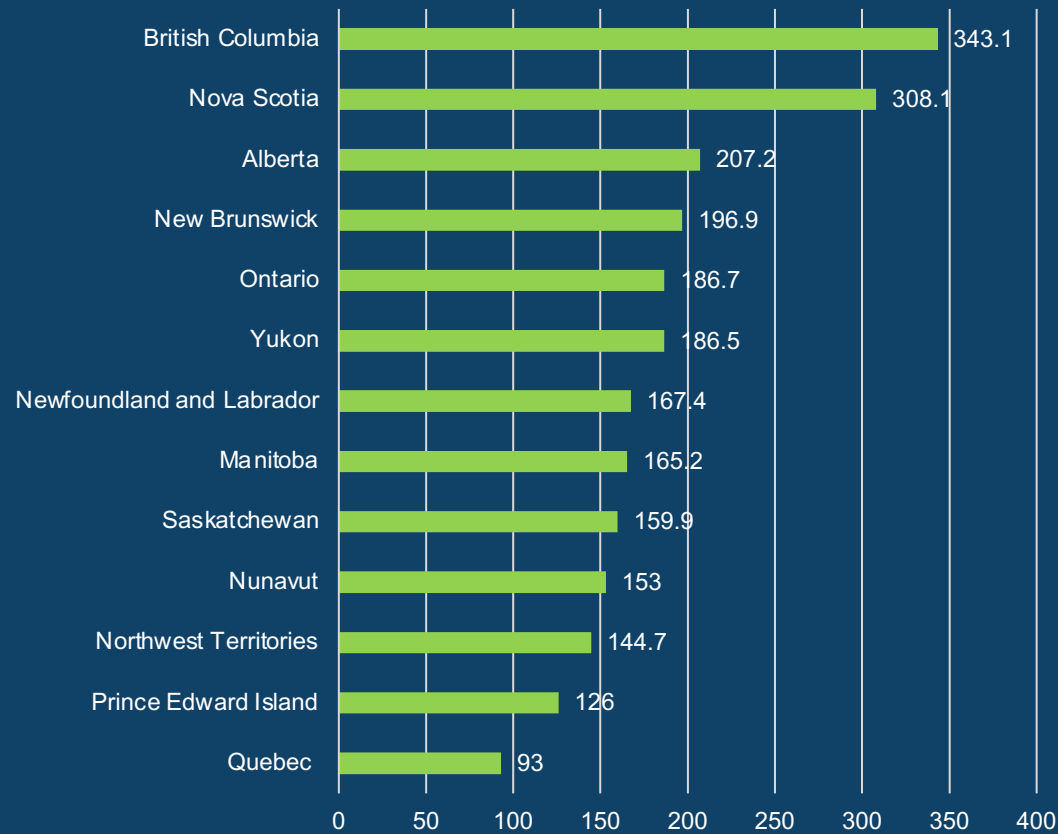
Total Reported Cybercrimes in Canada

NUMBER OF CYBER CRIME INCIDENTS



Police-Reported Cybercrime Rates across Canada (2022)

Rate Per 100,000 in 2022

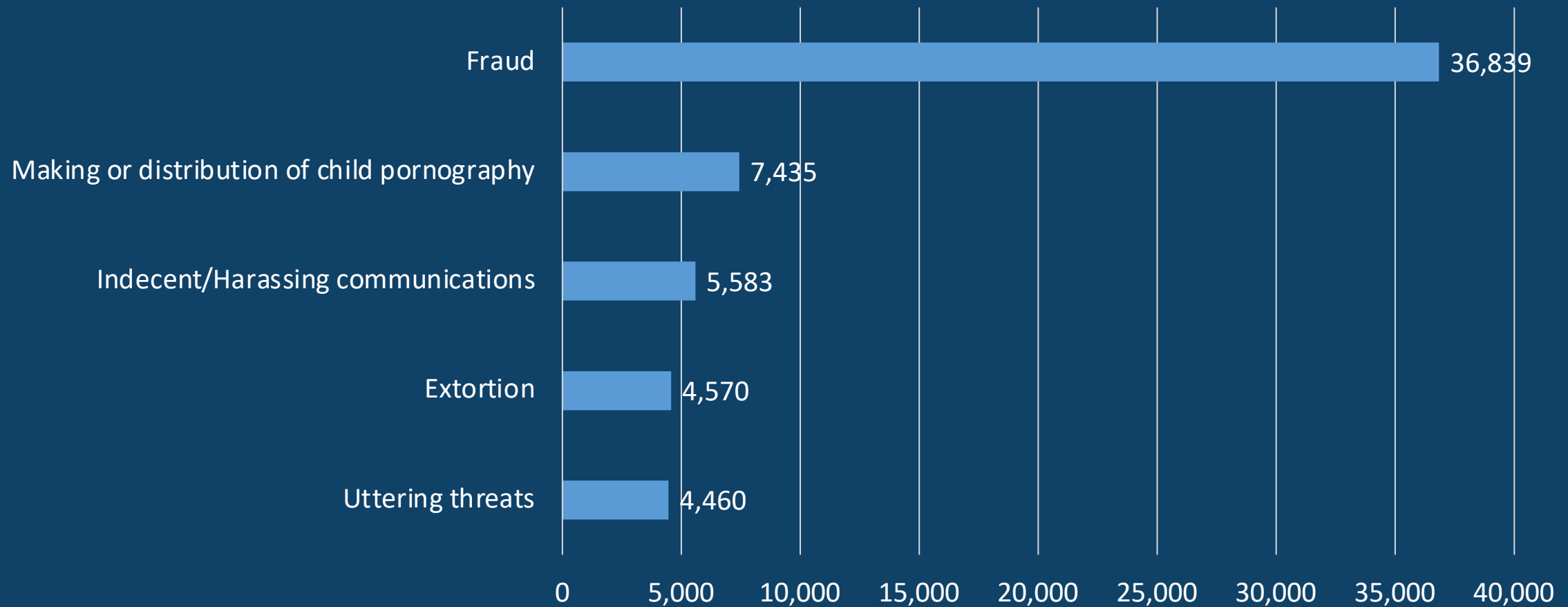


Heat Map - Police reported Cybercrime Rate per 100,000 population in 2022 by Province (300% increase since 2014)

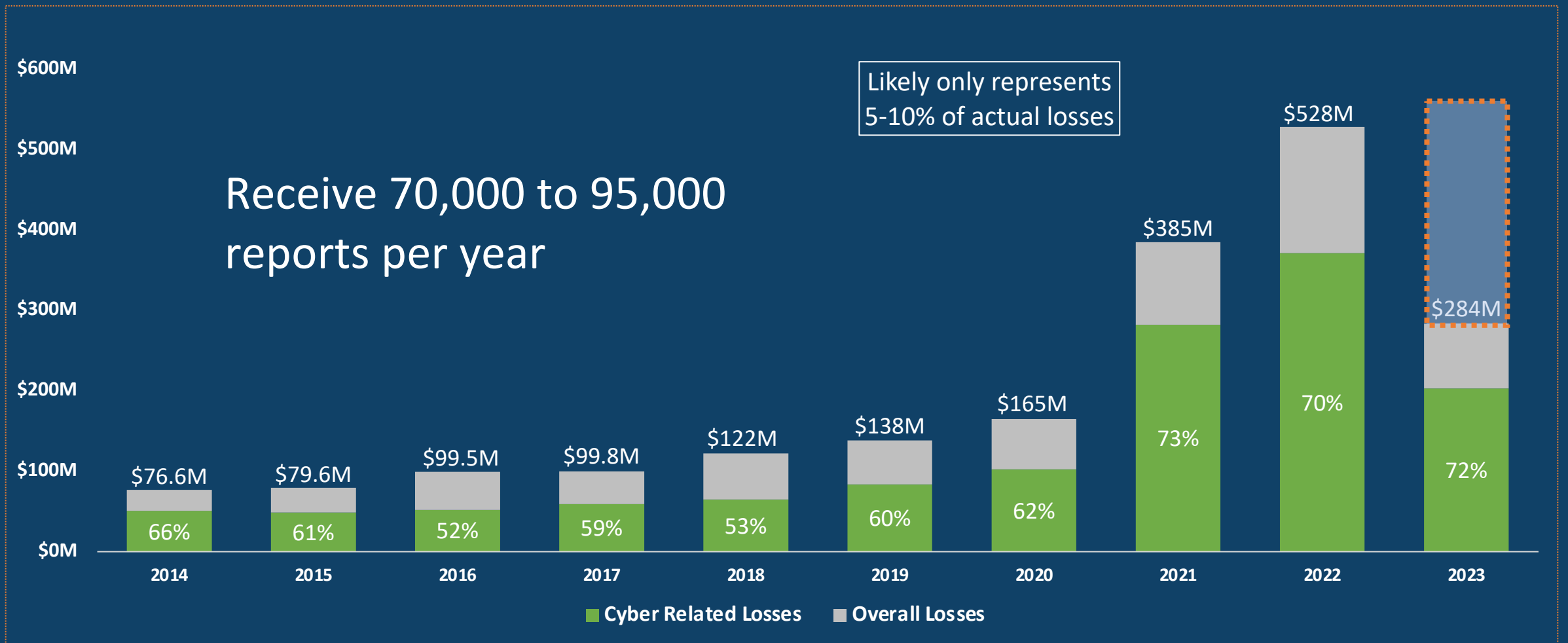


Police-Reported Cybercrimes by Violation

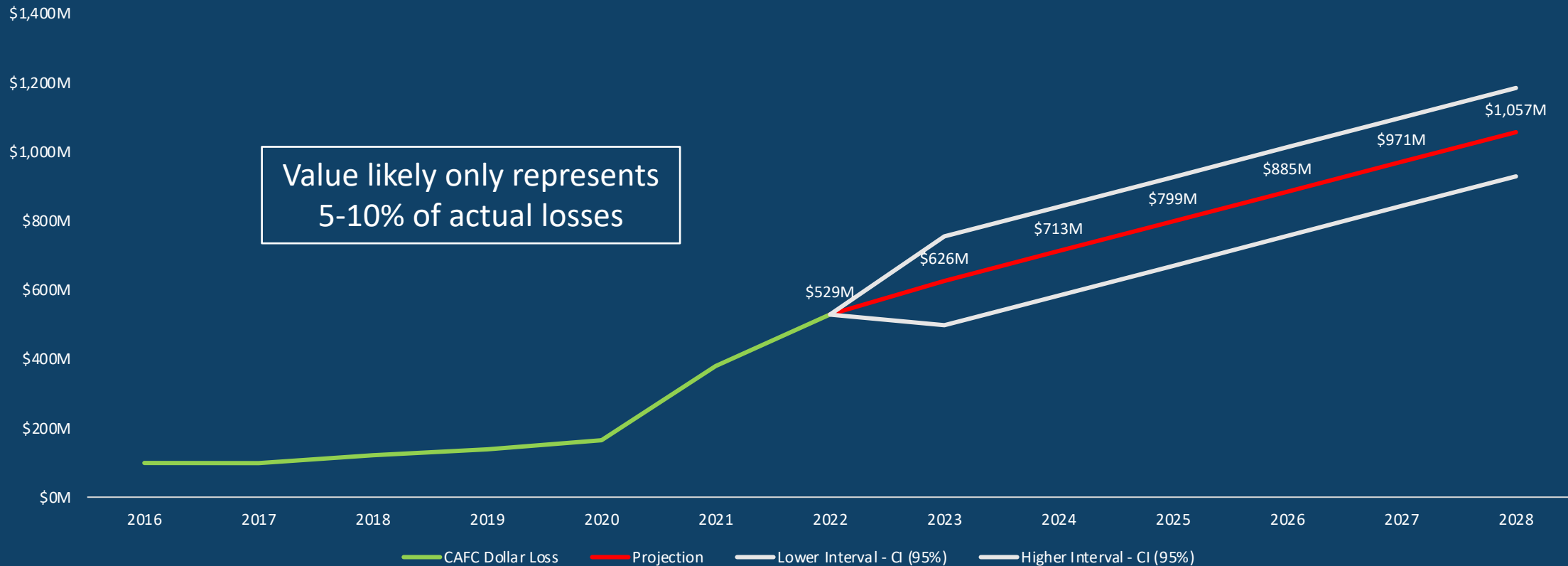
Top 5 Cyber-Related Violations in 2022



Cyber Fraud / Fraud Reported Losses Trend



Cyber Fraud Projection



	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
Projected % Cyber-Enabled Fraud	65%	60%	52%	60%	53%	60%	62%	73%	70%	70%	71%	71%	71%	71%	71%

What we're seeing...



Significant Impact - Ransomware

- Ransomware is the most disruptive threat to Canadian businesses
- Growing sophistication from ransomware actors to maximize profits
 - Profitability of ransomware further fuels other parts of the cybercriminal economy
- Use multi-extortion techniques to compel victims to pay ransom

Kaseya says up to 1,500 businesses compromised in massive ransomware attack



By [Alex Marquardt](#), CNN Business

Updated 10:14 AM EDT, Tue July 6, 2021

Nfld. & Labrador

N.L. health-care cyberattack is worst in Canadian history, says cybersecurity expert

'It has real impacts on human life and safety'

CBC News · Posted: Nov 04, 2021 6:00 AM NT | Last Updated: November 4, 2021

Who are the cybercriminals?

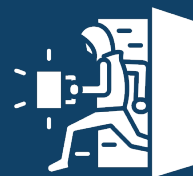
- This can be tough to articulate... and can depend on the activity.
- Think of it as a spectrum... Everyone from bored individuals to highly skilled and funded state backed groups who steal money to circumvent international sanctions which bring financial hardships.
- Ransomware groups for example could have:



IAB



Affiliate



Data Exfil & support



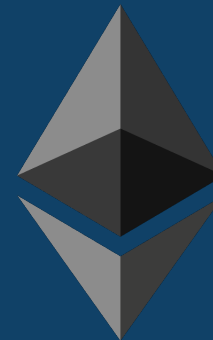
Negotiator / Customer
Victim Support



Money Manager /
Lauderer

Cryptocurrency

- The use of cryptocurrency exchanges and mixers continues to be a preferred method by cybercriminals to obfuscate the movement of illicit funds, making their traceability challenging
- Decentralized financial (DeFi) platforms are increasingly used by cybercriminals to evade detection and as a target to steal crypto
- Chainalysis identified more than \$1.2 billion USD in crypto ransomware payments in 2021 and 2022
- illicit addresses represented just 0.24% of all transaction volume in 2022. Despite being a small percentage of all transactions, illicit addresses still received \$20.6 billion USD, up from \$18 billion USD in 2021



AI Threats to Canada

- Recent AI advances in large language models (LLMs) (ChatGPT, Bard, Claude, WormGPT).
 - Cybercrime specific LLMs being actively developed.
- Cybercriminals are likely to use AI tools to force multiply operations.
- Deep fake technology as an emerging risk – increased effectiveness of cyber-enabled fraud and social engineering.



How we tackle Cybercrime...



PREVENTION Through timely sharing of information, generating awareness products, educating citizens and industry, cyber offender diversion

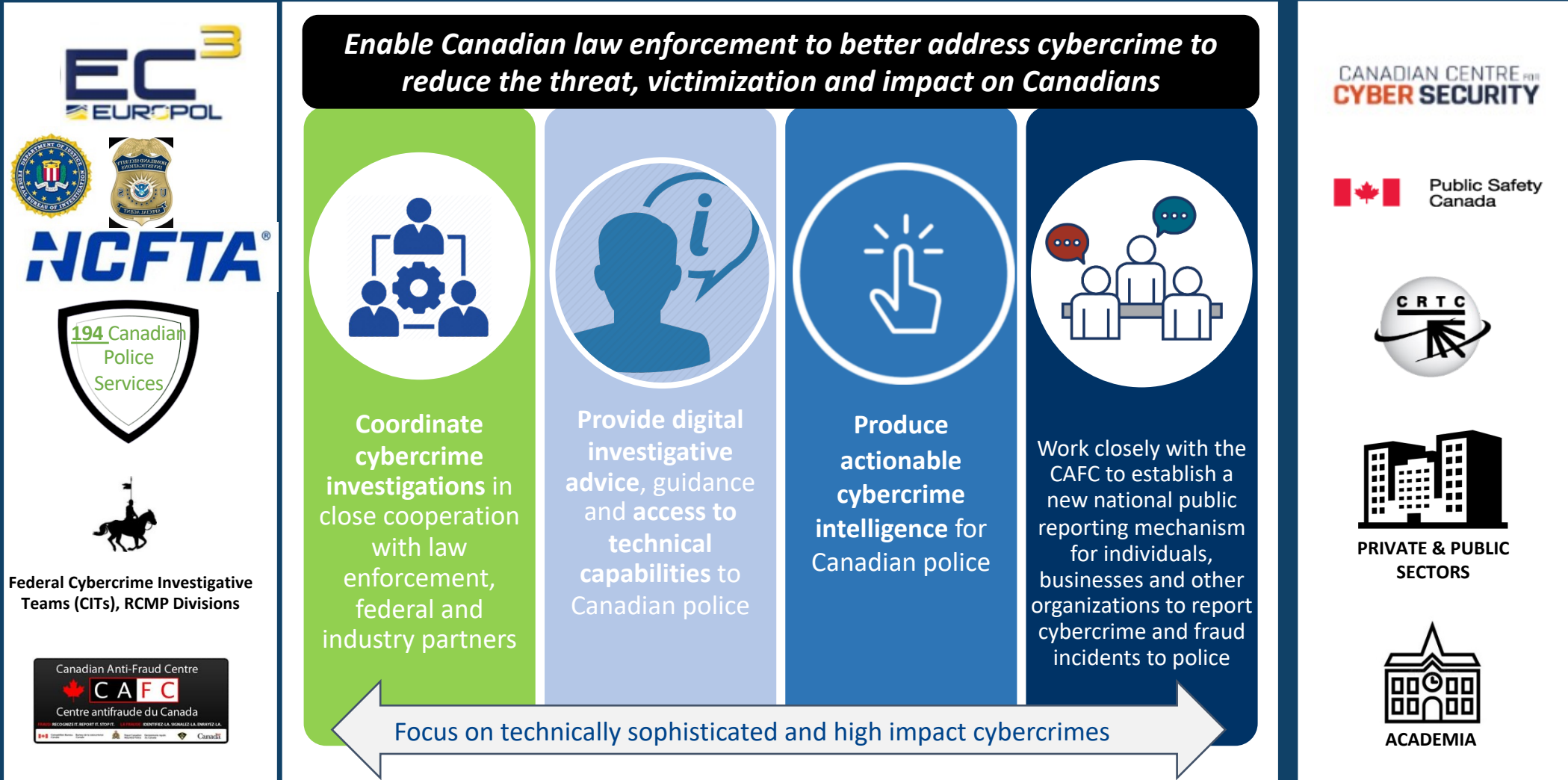
HARM REDUCTION Timely action to warn victim and stop further damage – allow them to “pull the plug”

DISRUPTION Seizing criminal infrastructure, markets, and payment systems which enable cybercrime

APPREHENSION By apprehending those who enable, support or commit the offences in Canada and abroad.



NC3 Mandate: A Coordination and Enabling Hub



GoldDust

Five affiliates to Sodinokibi/REvil unplugged

- Sodinokibi (REvil) ransomware
- 7000 worldwide infections, 600 in Canada
- Canadian investigation led by Calgary Police Service, assisted by NC3, RCMP Federal Policing, Canadian police partners
 - Ongoing from January 2020 to November 2021
- Five international threat actors arrested in **November 2021**

Calgary Police Service and RCMP contribute to ransomware arrests and seizures overseas in Operation GoldDust

“Though these arrests happened thousands of kilometers away, the crimes these suspects committed had a very real impact on citizens in Calgary, and across Canada...”

Insp. Phil Hoetger, Calgary Police Service Technical Investigations Section



Coda

- Parallel investigations by US FBI, and Ontario Provincial Police, supported by NC3, Europol
 - Multi-year investigation
- Suspect tied to ransomware campaigns, cybercrime forums, banking frauds, cyber compromise of Alaskan government departments, medical facilities
- **Canadian suspect arrested in December 2021**

Canadian Ransomware Arrest Is a Meaningful Flex, Experts Say

Ottawa man charged after OPP, RCMP and FBI investigate years of cyber attacks

“The FBI alongside our international partners, OPP and RCMP, will continue to investigate these malicious cyber actors who continue to target US and Canadian infrastructure....”

Brian Abellera, FBI Assistant Legal Attaché, Ottawa



Nectar

- Hive targeted 1,500 victims globally, received over \$100M in ransom payments
 - At least 71 Canadian organizations were victimized
- Canadian lead, Peel Regional Police, coordination by NC3, collaboration with Canadian / international police partners
 - Multi-year investigation
- NC3 facilitated Canadian victim access to decryption keys, avoided 6-7 figure ransomware payouts in some cases
- **International takedown of Hive infrastructure in January 2023**

Cybercriminals stung as HIVE infrastructure shut down



“In working together with our national and international policing partners, we leverage the very best intelligence data to hold accountable those threat actors that victimize our communities....”

Peel Deputy Chief Nick Milinovich



Cookie Monster

- Genesis market, traded in stolen credentials, account access
- Offering 1.5M “bots” (credentials/access) for sale
- Multi-national investigation/disruption effort
 - 4+ year investigation
- International takedown of Genesis market in April 2023
 - 18 countries, 28 Canadian police of jurisdiction, CRTC
 - 79 distinct police actions in Canada
 - Arrests, search warrants, cease/desist

How police in Canada helped the FBI in crackdown on the stolen data market



“The Genesis Market takedown proves the impact that law enforcement and partners can have when working together...”

RCMP Deputy Commissioner Bryan Larkin, Specialized Policing Services

Cyber Offender Prevention Efforts - Google Ads DDOS Campaign

Government of Canada / Gouvernement du Canada | Canada.ca | Services | Departments | Français

Canadian Anti-Fraud Centre

[Browse scams](#) | [Protect yourself](#) | [Report fraud](#) | [What to do if you're a victim](#)

Distributed Denial of Service attacks

- [What is a Distributed Denial of Service attack](#)
- [Make the right choice](#)
- [Consequences of committing a Distributed Denial of Service attack](#)
- [What the law says](#)
- [Reporting cybercrime](#)
- [Related links](#)

What is a Distributed Denial of Service attack

A **Distributed Denial-of-Service Attack** is a crime in which the perpetrator floods an online server with internet traffic to prevent users from accessing connected services and sites.

Distributed Denial of Service attacks:

- are illegal
- have real consequences for victims and attackers
- are not as anonymous as you think

It is **not** illegal to enter the term "DDoS" or other related terms into a web browser or search engine.

The RCMP and Canadian police services work with national and international partners to find and apprehend offenders, and to protect Canadians from cybercrime.

9:23 | 26 | 5G

Google

how do you do a ddos...

Videos | Images | Someone on Discord

Ad · <https://www.antifraudcentre-centreantifraude.ca/>

Thinking of DDoSing? - It is a criminal offence

There are better - and legal - ways to use your skills. Click to find out more.

Ad · <https://www.cloudflare.com/>

Under DDos Attack? - Stop The DDoS Attack Now

Don't let an attack cripple your business operations. Get advanced DDoS defense today. Under attack? Click for Cloudflare's attack...

Ad · <https://www.zscaler.com/>

What Is a Denial-of-Service (DoS) Attack? | Zscaler - zscaler.com

CRIME CENTRE

How you can help...



1. Be Cyber aware...



Fourth Slido Question: I would rate my cyber hygiene practices as?

1. Very Good (I am very cyber savvy)
2. Average (I am cautious and use protection techniques)
3. Below Average (I could do better)
4. Very bad (the Inter-what?)

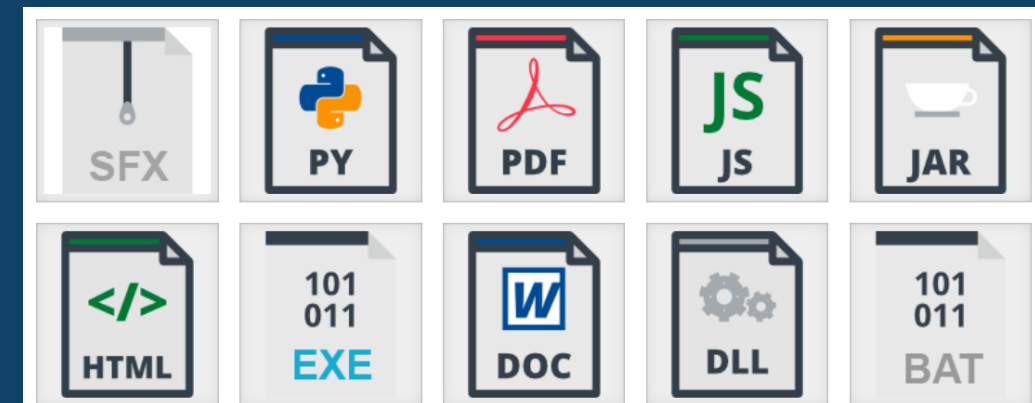
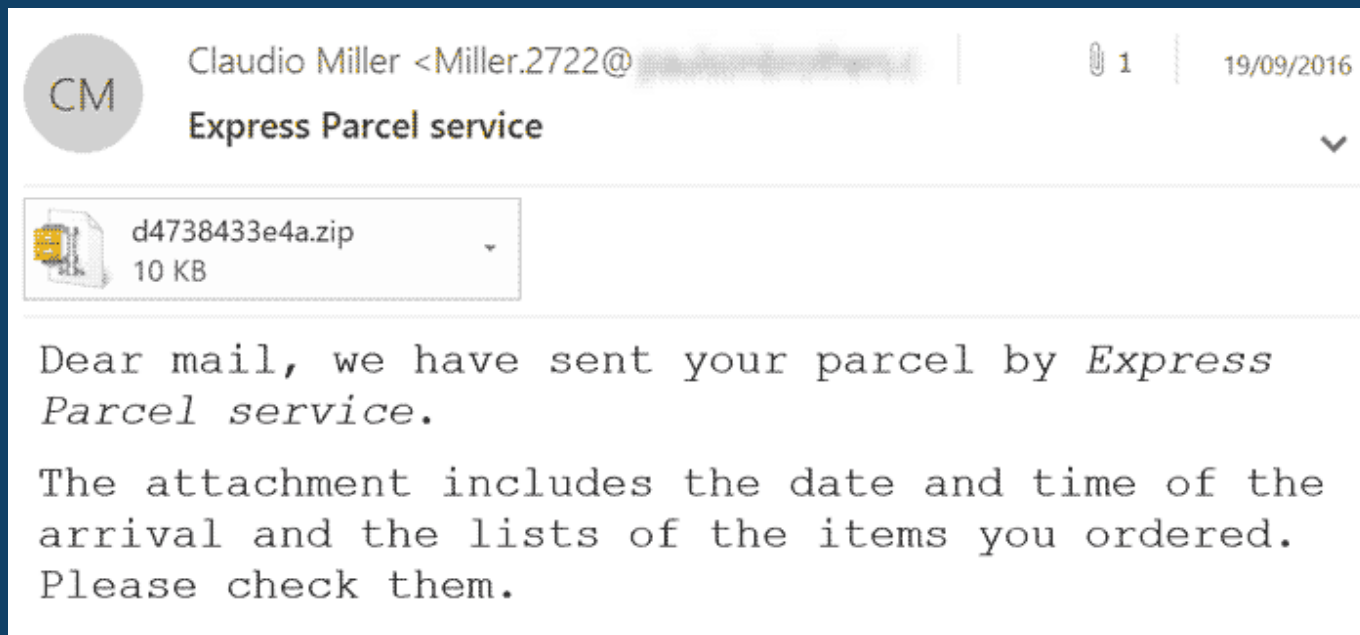


- Cybercriminals profit from your data
- Getting compromised puts you and your contacts at risk
- Impacts to your financial security



Watch out for that Attachment!

- Phishing emails can have email attachments that are viruses
- If you don't trust who it came from, don't download it



These files types can have computer viruses baked in!

Phishing and SMiShing

- Get a strange SMS with a link about your Canada Post package?
- Or an email with lots of typos from an “friend” who won the lottery?

CanadaPost: We tried delivering your parcel, but you weren't in or there was no safe place to leave it. A reschedule is required:
<http://canadapost-serve.ca>

Friday, September 2

Notice: Your annual income tax has been reviewed by (CRA). In addition, a return of \$381.70 was received. Please visit <http://162.213.253.140> to finalize your (GST/HST) entitlement.

Data rates may apply

7:51 p.m.

From: Netflix <rahma-cakupuyje-vakangenlaaywa@bihvgh.com>
Date: September 14, 2020 at 6:05:32 AM GMT+2
To: [REDACTED]
Subject: Re: Update Payment Subscription - We can't authorize payment September 13, 2020.
Order Number : 38443246

NETFLIX

Update current billing information

Hi,

Unfortunately, we cannot authorize your payment for the next billing cycle of your subscription, Netflix was unable to receive a payment because the financial institution rejected the monthly charge.

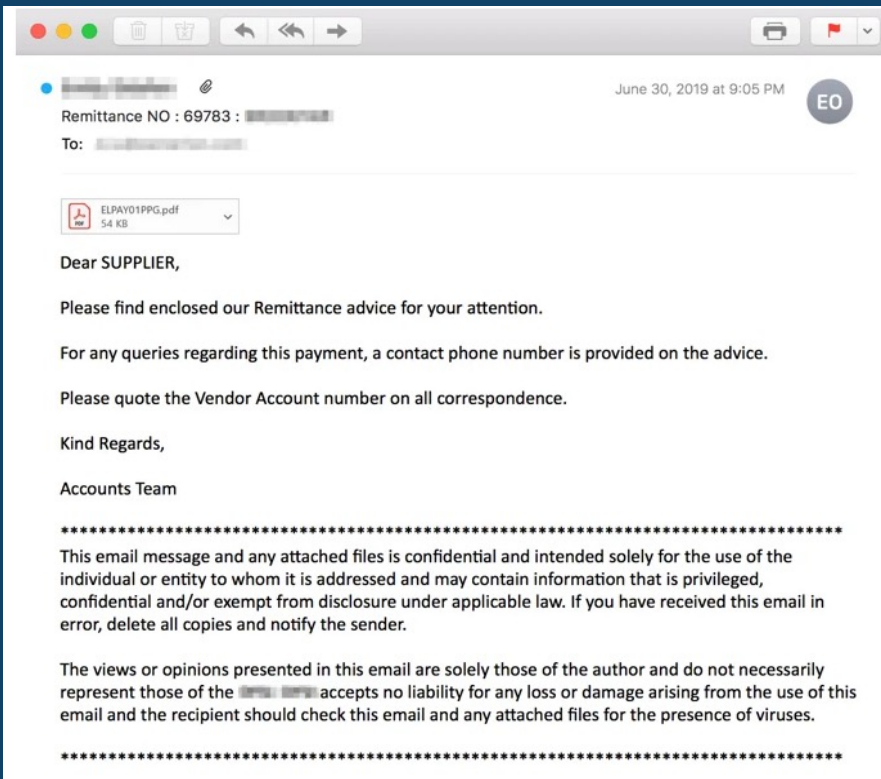
TRY AGAIN PAYMENT

Obviously we'd love to have you back. If you change your mind, simply restart your membership and update your payment to enjoy all the best TV shows & movies without interruption.

- Netflix Team

Financial Professionals are Juicy Targets

- Business Email Compromise
- Supplier invoice scam
- Authorized push payments fraud



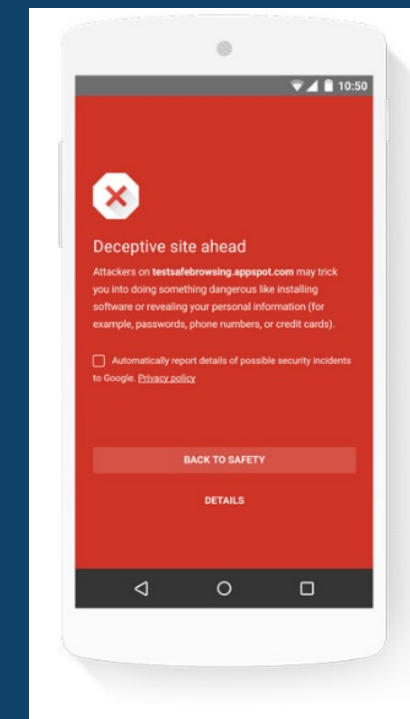
Cyberattacks on the rise for accountancy firms | Naq

Top Cyber Hygiene Tips



CIRA Canadian
Shield
*Free public DNS
for Canadians*

- MFA
- Strong and unique passwords
- CIRA's Canadian Shield
- Safe browsing mode
- Anti-Virus software and dark web monitoring
- Backups
- Update devices
- Careful with "free wifi" – use VPN
- Be suspicious of every link/attachment



<https://www.cyber.gc.ca/en/guidance/cyber-hygiene>



Be careful of your social media presence

The Anatomy of a LinkedIn Social Engineering Scam (that Targeted Me)

By George Kamide

September 28, 2022

The 3 Most Common LinkedIn Scams and How to Spot Them



Jaime Stathis

Updated: Aug. 15, 2023

LinkedIn

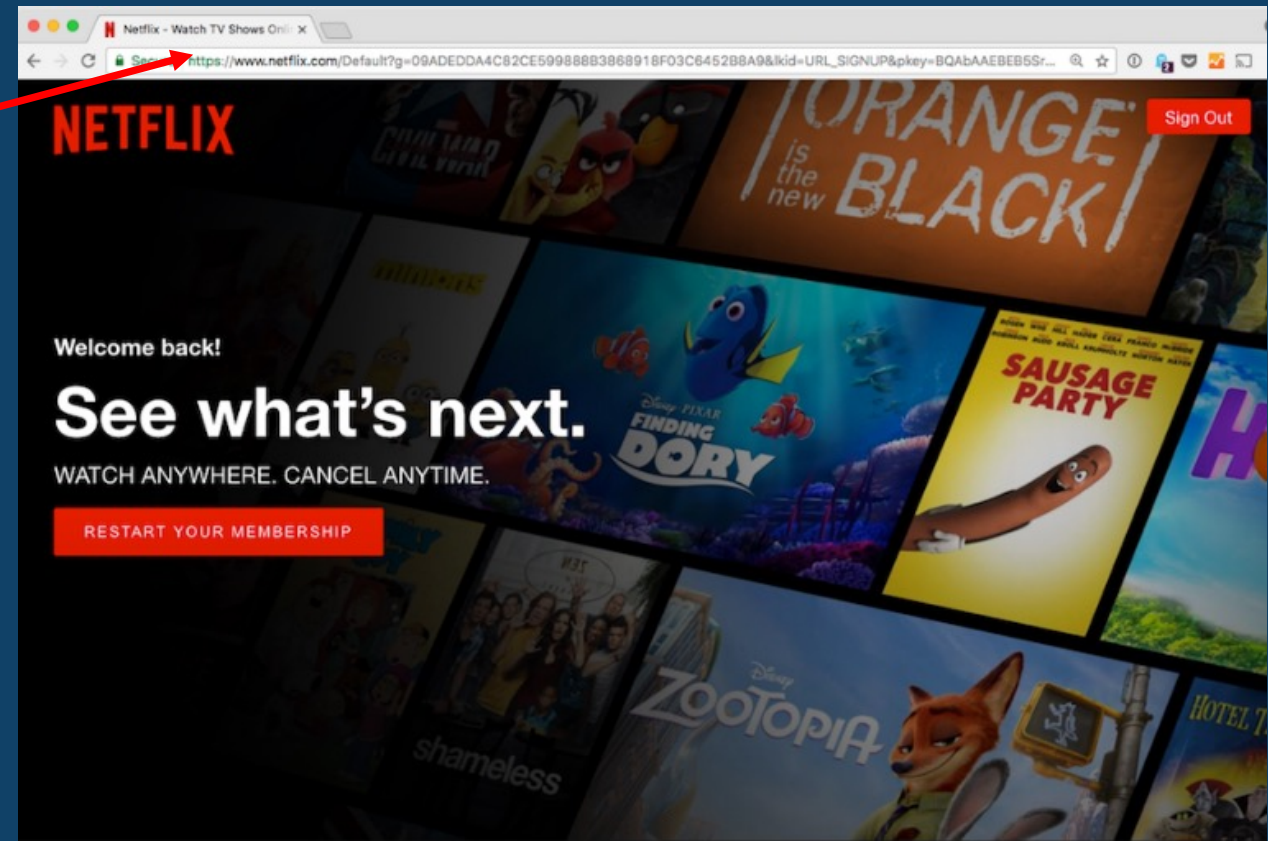


Fifth Slido Question – “Catch the Phish”

- Which is the scamming url:
- 1 or 2?

1. www.Netflix.com/login

2. www.Netflix.com/login

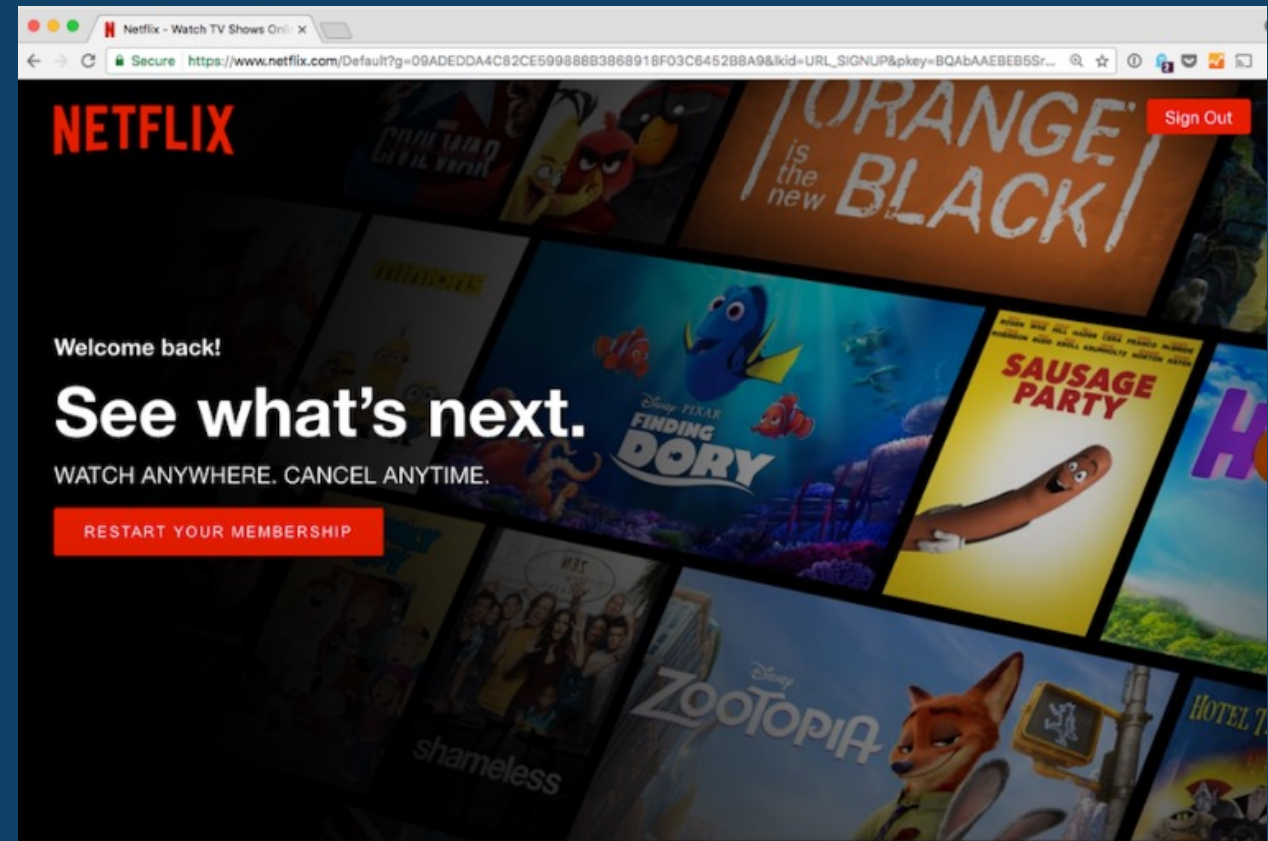
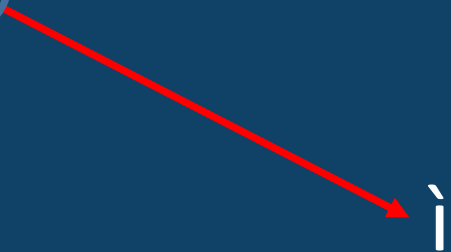


Fifth Slido Question – “Catch the Phish”

- Which is the scamming url:
- Correct Answer: 2

1. www.Netflix.com/login

2. www.Netflix.com/login

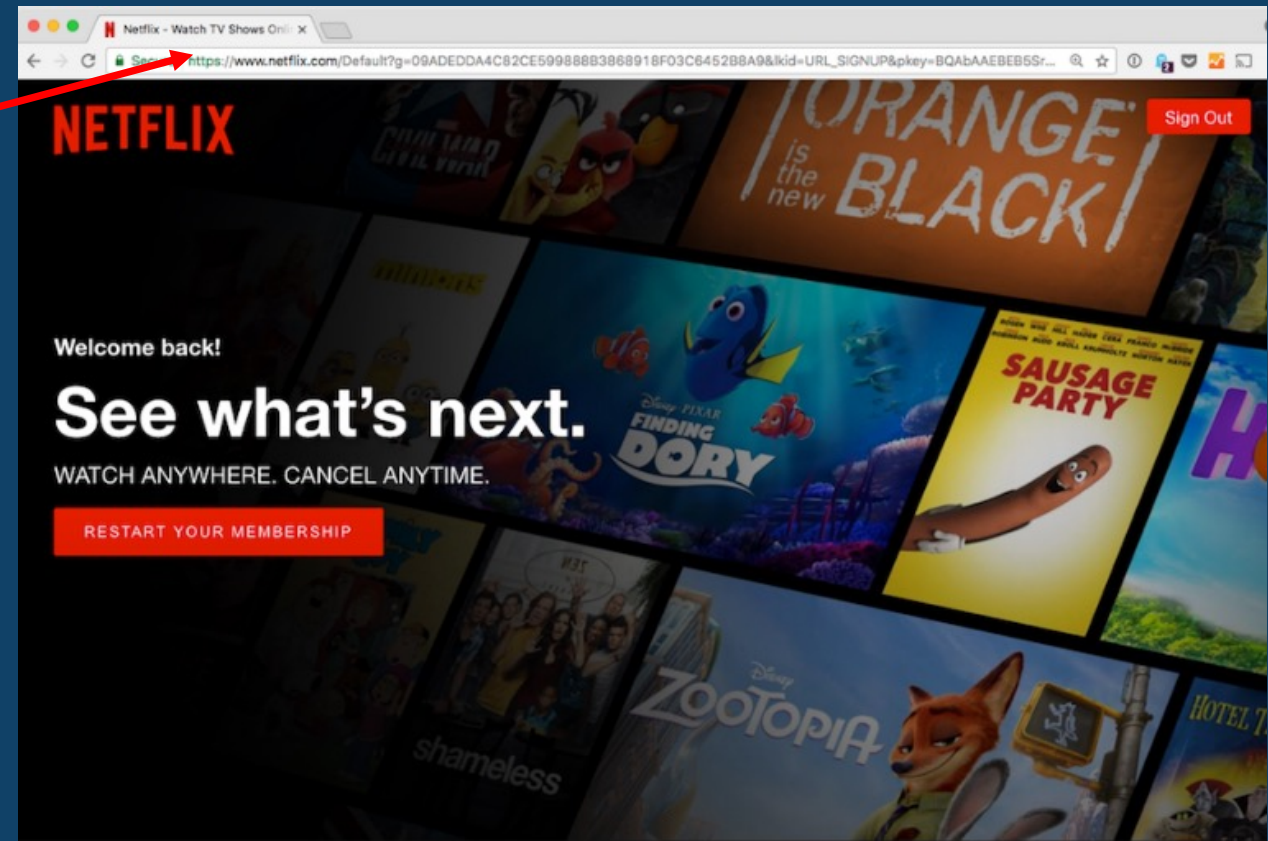


Sixth Slido Question – “Catch the Phish”

- Which is the scamming url (harder this time):
- 1 or 2?

1. www.Netflix.com

2. www.Netflix.com



Sixth Slido Question – “Catch the Phish”

- Which is the scamming url (harder this time):
- Correct answer is 1

1. www.Netflix.com

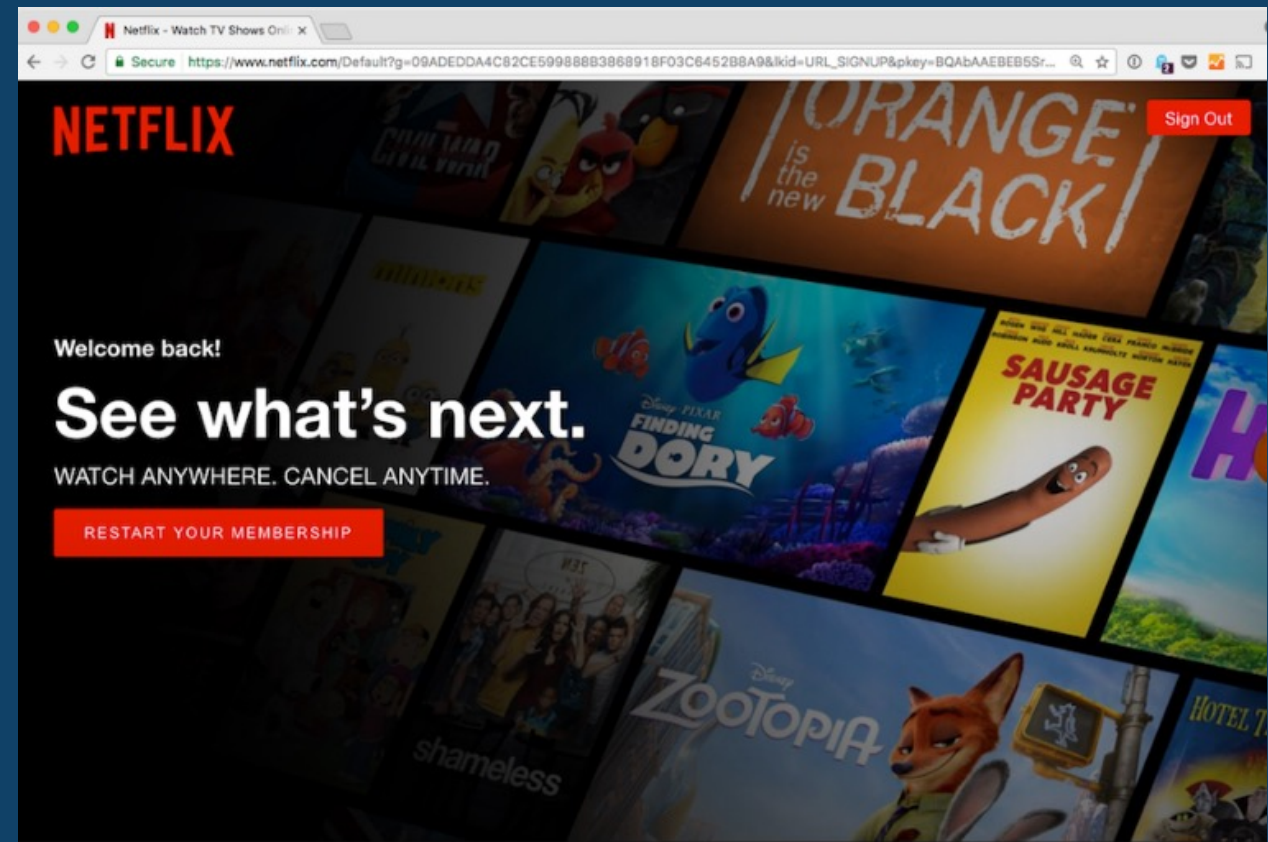


→ I = capital of i

2. www.Netflix.com



→ I = lower case of L



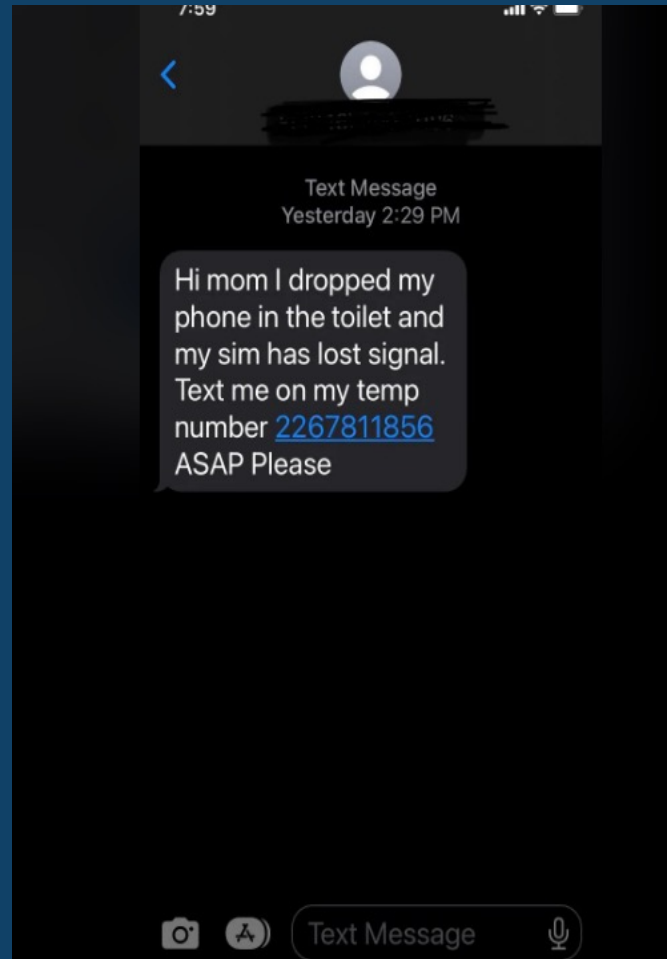
Cybercriminals Social Engineering Tools:

- Spoofing
- Urgency
- Emotional Manipulation
- Threats
- Impersonation
- COUNTERED BY: Take 5!
 - Time is on your side
 - Trust your gut!

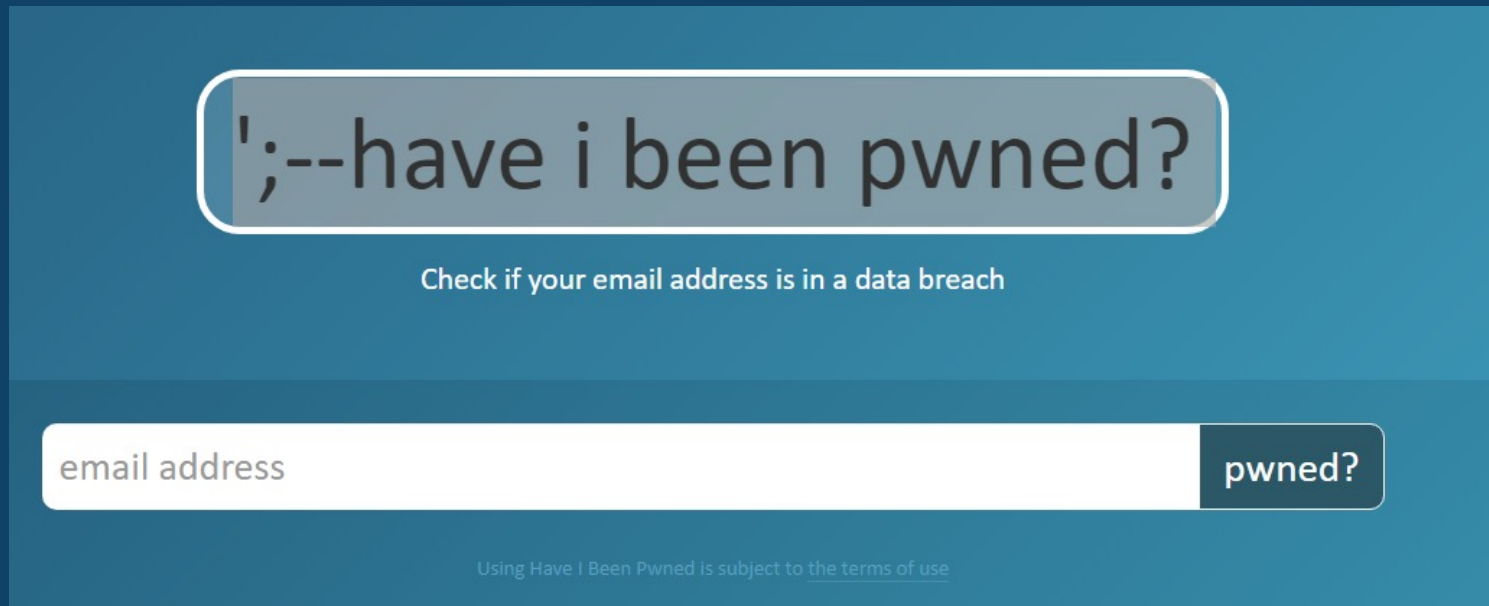


Seventh Slido Question: Be honest who would have fallen for this?

1. I would have likely texted back
2. Not a chance



Check if you are vulnerable



';--have i been pwned?

Check if your email address is in a data breach

email address pwned?

Using Have I Been Pwned is subject to [the terms of use](#)

<https://haveibeenpwned.com/>



2. Help by Reporting...





Impact of Fraud



Why victims don't report?

- Embarrassment / Shame
- Feel law enforcement won't do anything
- Don't want to bother law enforcement
- Feel the courts won't punish
- Report to bank or credit agency instead
- Don't know they've been victimized
- Feel they may have committed a crime themselves

Report Cybercrime and Fraud

Report a scam, fraud or cybercrime online, whether you are the victim or intended target.

Report Online

Update a report

Canadian Anti-Fraud Centre



Browse scams | Pr

[Home](#)

Report fraud and cybercrime

On this page

- [Reporting to the Canadian Anti-Fraud Centre](#)
 - [Report online](#)
 - [Report by phone](#)
- [Why you should report fraud and cybercrime](#)
- [Coming soon: new cybercrime and fraud reporting system](#)

* I'm reporting for:



Myself

I was the target of a scam or cybercrime



Someone I know

Someone I know was the target of a scam or cybercrime



A business or organization

My business or organization, or the business or organization I work for, was the target of a scam or cybercrime

* What best describes your report? (Select all that apply)

- an unwanted call, text message, or email
- a loss of information, merchandise, or money
- malware or ransomware
- a compromised account or computer
- something else

Take Part In Our Research

Help us design a service to report fraud and cybercrime that works for you

As a volunteer, we would like you to test the website and give us your feedback during a video call. The conversation should take about one hour and we can schedule it at a time that's convenient for you.

⚠ Note: By submitting your name and email address to become a volunteer you are not reporting an incident of fraud or cybercrime. If you are currently experiencing a scam, fraud or cybercrime please report it to the [Canadian Anti-Fraud Centre](#) and, if you were a victim, report to your local police. If you are in immediate danger, call 911.

<https://report.con.rcmp-grc.gc.ca/recruitment>

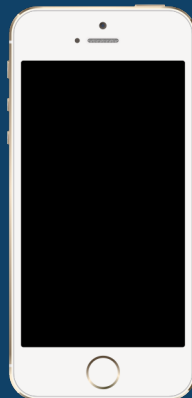


Where to report SMiShing?

Fight Spam by forwarding your text message to **7726!**

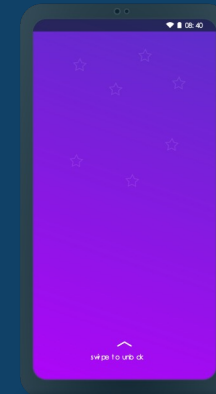
iPhone

1. Touch and hold the message
2. Select “More”
3. Select the message to forward, select arrow in bottom right corner
4. Enter **7726**
5. Select “Send”



Android

1. Touch and hold the message (be careful not to activate a link)
2. Choose Forward (from the menu)
3. Forward to **7726**
4. Select “Send”



3. Get the word out...



Grandparents' Scam

More than \$100,000 stolen in family emergency scams in Saskatoon: police

Three Quebec men are facing 10 counts of fraud over \$5,000.

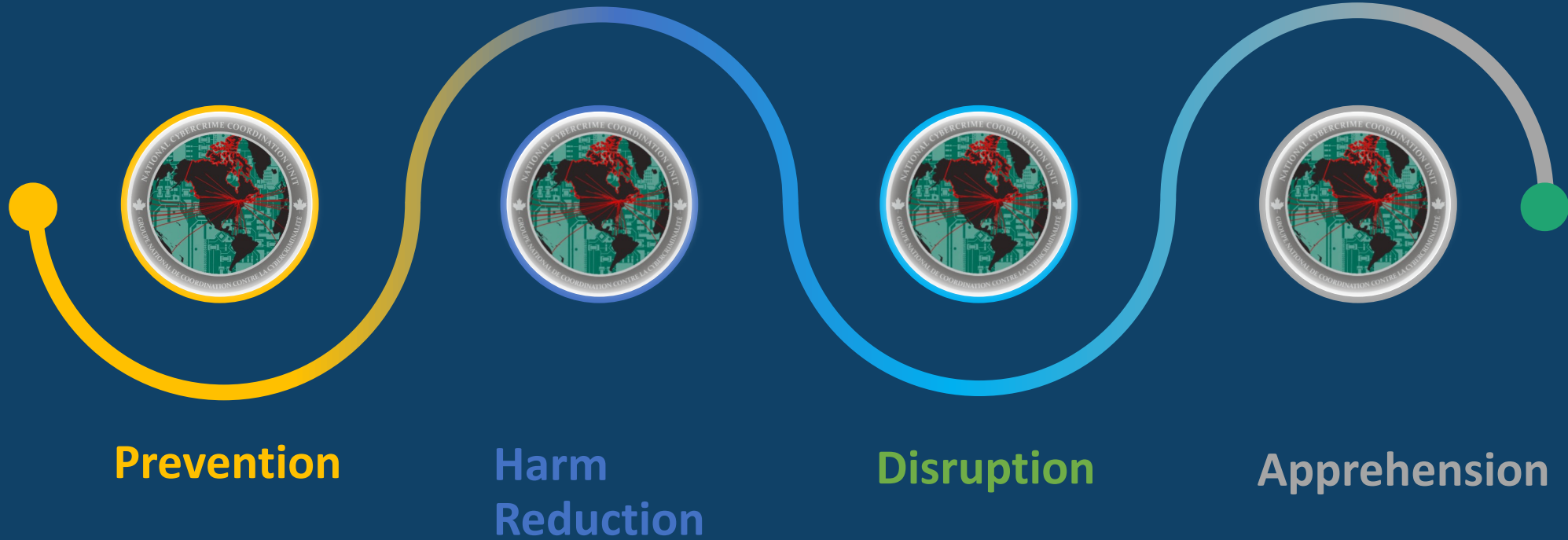
January 12, 2023 Local News



Tell your Loved Ones:

- Never offer information to the caller, including the name of the person they're claiming to be, before they identify themselves;
- Ask the caller personal questions that only that person would know;
- Hang up the phone and attempt to contact another family member to confirm the whereabouts of your loved one; and
- Never send money for payments via gift cards.
- **CALL POLICE RIGHT AWAY!**

NC3 - Team sport – Help us fight Cybercrime



More Information:



Get Cyber Safe is a national public awareness campaign created to inform Canadians about cyber security and the simple steps they can take to protect themselves online.

Reporting to the CAFC:

<https://www.antifraudcentre-centreantifraude.ca/report-signalez-eng.htm>

Learning more:

Visit: <https://www.rcmp-grc.gc.ca/en/nc3#wb-info>

CAFC website: <https://www.antifraudcentre-centreantifraude.ca/index-eng.htm>

Thank you!

