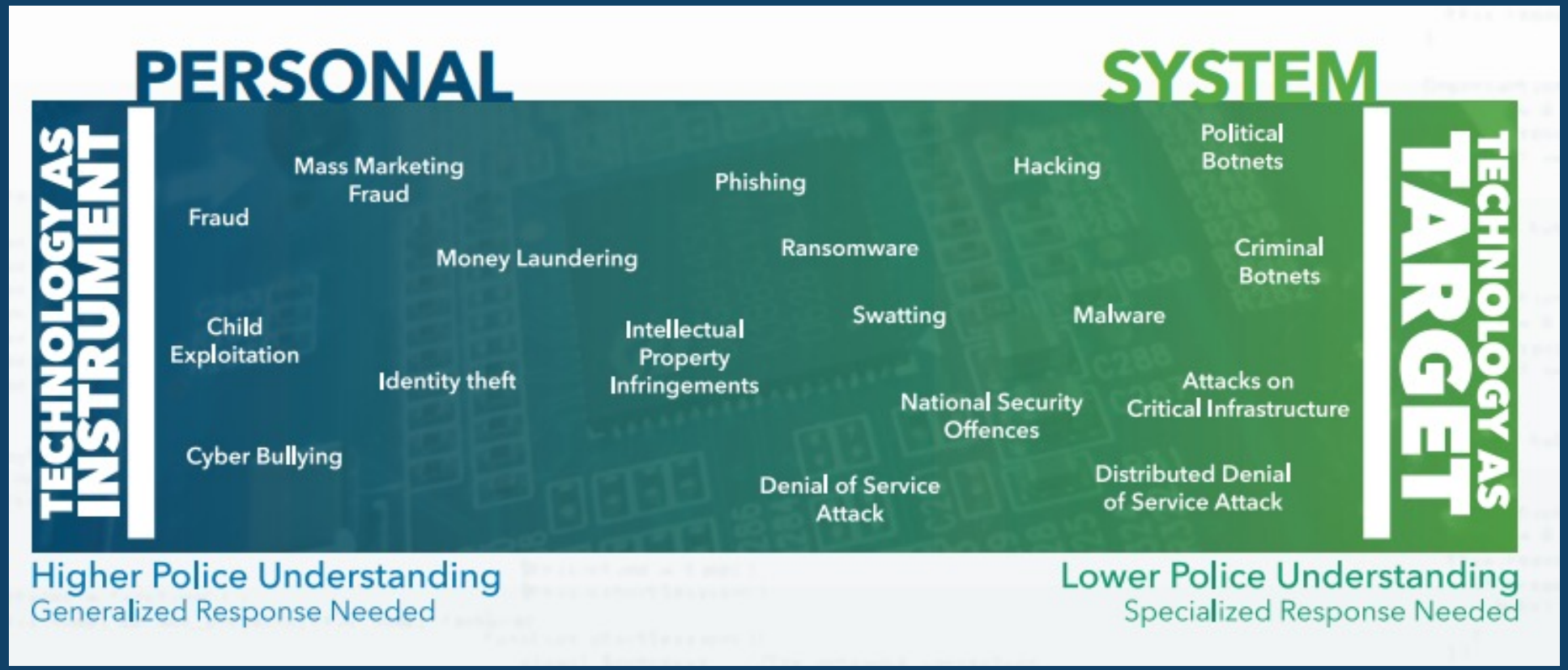

NC3
NATIONAL CYBERCRIME COORDINATION CENTRE
CNC3
CENTRE NATIONAL DE COORDINATION EN CYBERCRIMINALITÉ

- Qu’est-ce que la cybercriminalité?
- Quelles sont les répercussions?
- Types de menaces ou d’incidents
- Mesures que nous prenons à cet égard
- Comment vous pouvez aider

Première question Slido : J'associe le terme cybercriminalité aux...?

1. Escroqueries en ligne
2. Rançongiciels
3. Actes de piratage de serveurs et aux vols de données connexes
4. Courriels contenant des liens suspects que je reçois

Définir la cybercriminalité (pas une tâche facile…)



La cybercriminalité, juste un crime contre les biens?

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

- Empêche la prestation de services importants – soins de santé
- Menace l'intégrité économique – fermeture d'entreprises
- Expose les données les plus personnelles des personnes
- Suscite une crainte d'être en ligne (surtout chez les personnes vulnérables)
- Provoque de l'angoisse mentale liée aux techniques d'extorsion (p. ex. l'extorsion sexuelle fondée sur l'argent)
- Cause des blessures physiques et des décès?
  - Cela est techniquement possible de nos jours, mais il n'y a pas encore d'usage à grande échelle (comment le monnayer?)


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**

Lutte contre un adversaire humain très motivé, sans scrupules et capable de s'adapter

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

Malware scam circulates after Saskatchewan stabbings

Une attaque par rançongiciel retarde les soins de patients dans des hôpitaux américains

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

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

B.C. health authority hit with ransomware attack

Medibank: Hackers release abortion data after stealing Australian medical records

Saskatchewan / News / Local News / Crime

RCMP warning public about cyber scam impersonating officer

More than half the ransomware attacks in Canada target critical infrastructure

{* 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

La cybercriminalité : un problème humain

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

- Lutte contre un adversaire humain amplement capable de s'adapter, et non contre des machines
- Personnes fortement motivées par l'argent
- Personnes et groupes qui n'ont aucun sens moral
- Victimes possibles qui sont « programmés » pour cliquer sans réfléchir
- Logiciels complexes et systèmes interconnectés qui sont pratiquement impossibles à concevoir (par des humains) sans failles
- Réticence des victimes à signaler le crime (gêne, méfiance à l'égard du gouvernement ou de la police, préoccupations liées à la réputation et aux processus judiciaires)

= **un important défi humain à relever**

Deuxième question Slido

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

J’ai déjà été victime d’un cybercrime ou d’une fraude en ligne (p. ex. j’ai envoyé de l’argent à un fraudeur, ou mes données ont été volées soit directement, soit à la suite d’une importante atteinte à la protection des données)?

1. Oui
2. Non

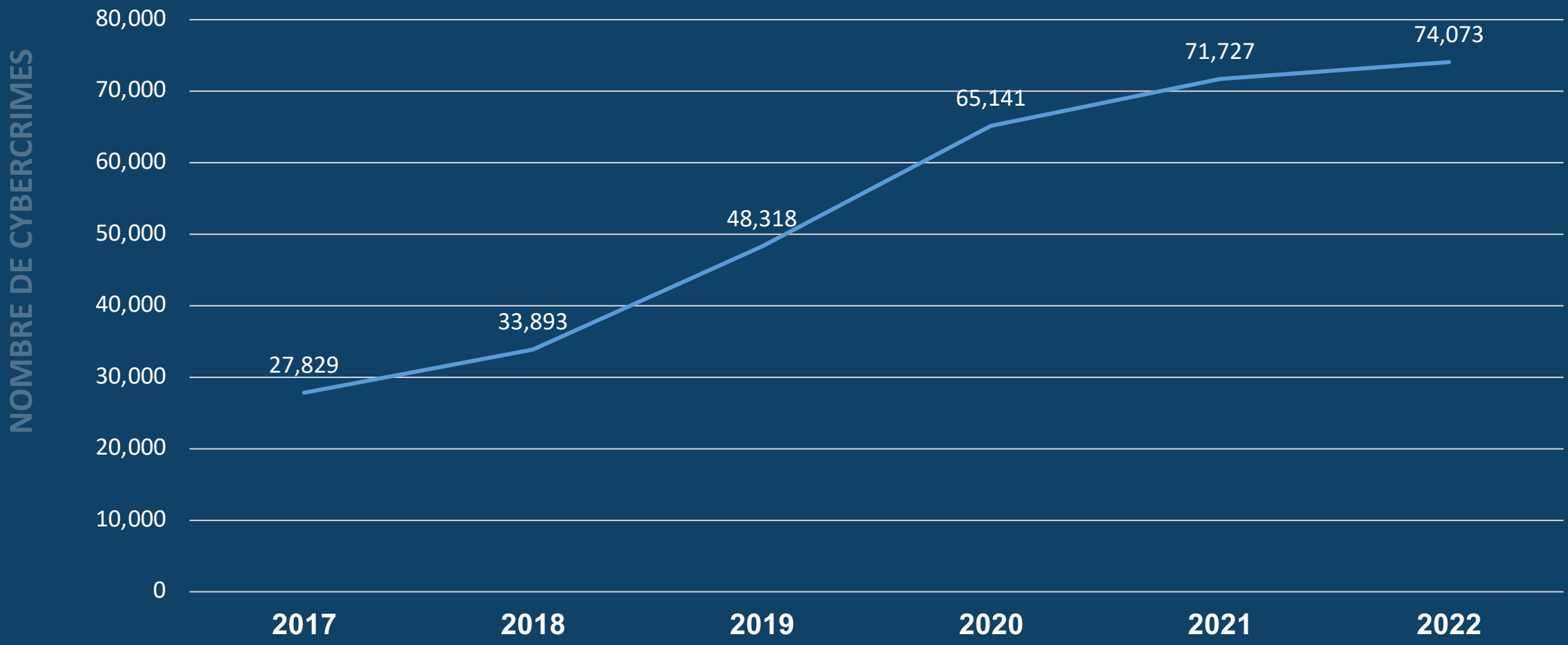
Troisième question Slido

J’ai signalé le crime à un organisme d’application de la loi (p. ex. les services de police locaux ou le Centre antifraude du Canada)?

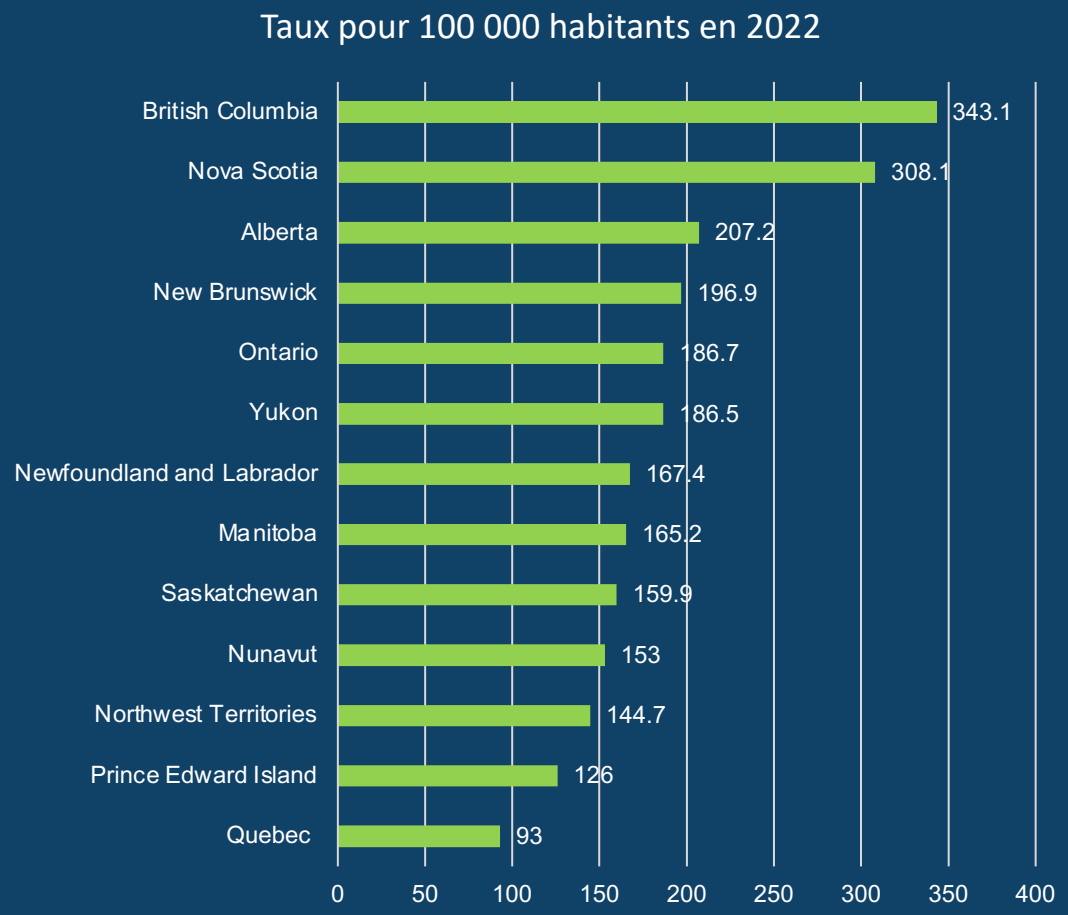
1. Oui
2. Non

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

Total des cybercrimes signalés au Canada



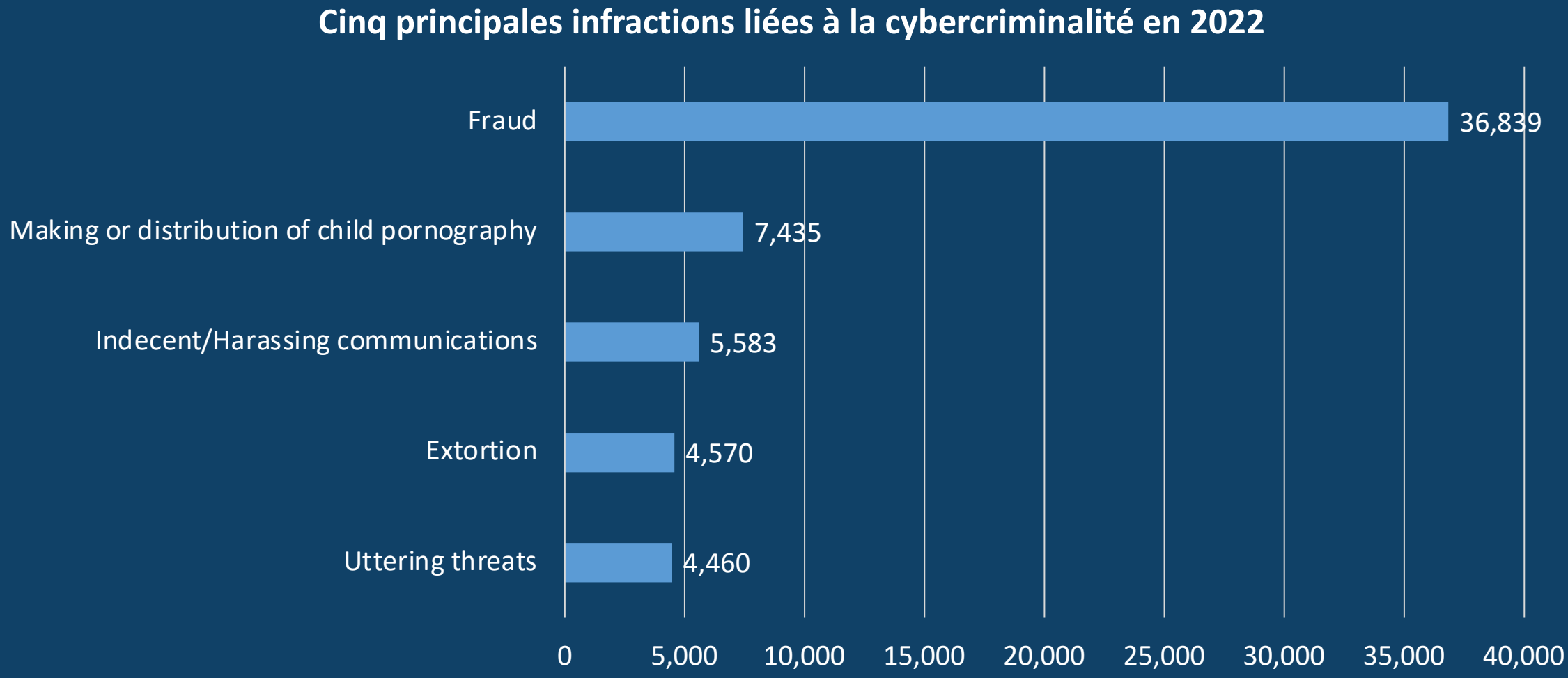
Taux de cybercrimes déclarés par la police au Canada (2022)



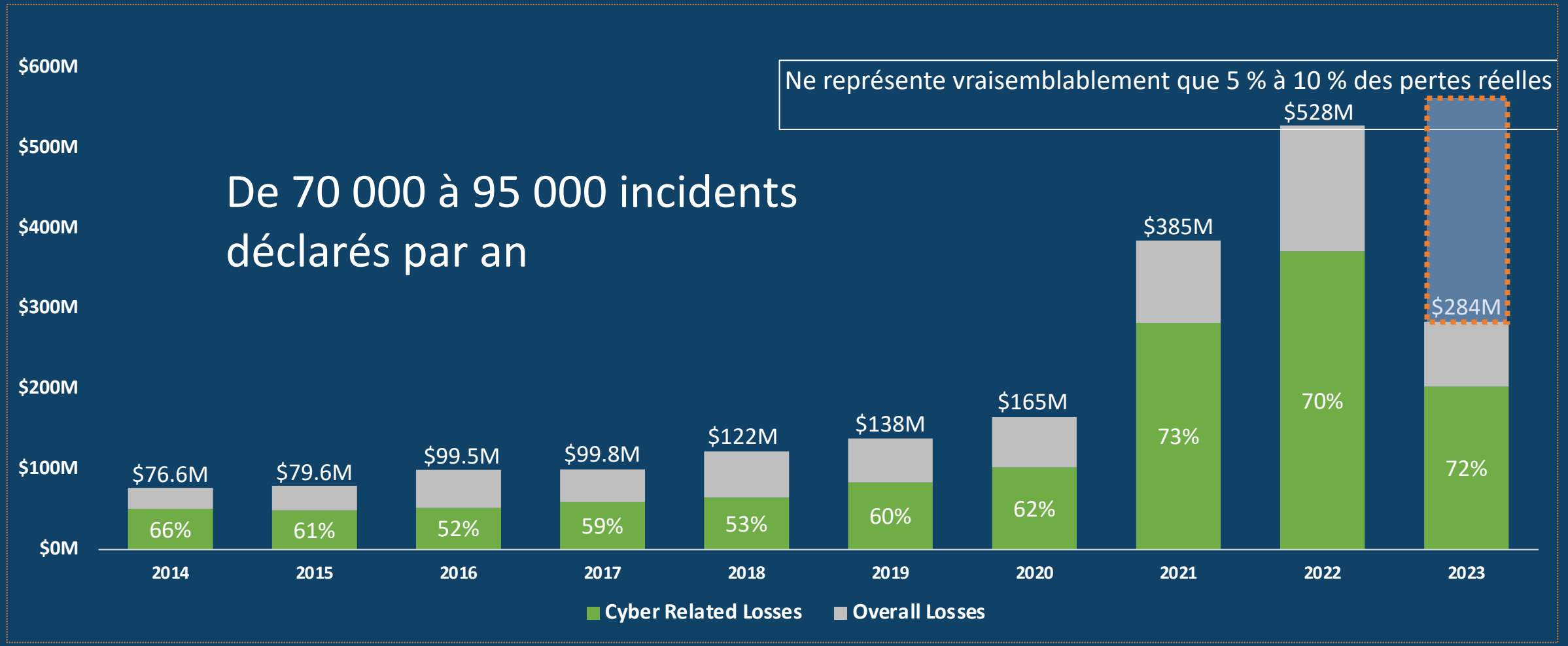
Carte de densité – Taux de cybercrimes déclarés par la police pour 100 000 habitants en 2022 par province (augmentation de 300 % depuis 2014)

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

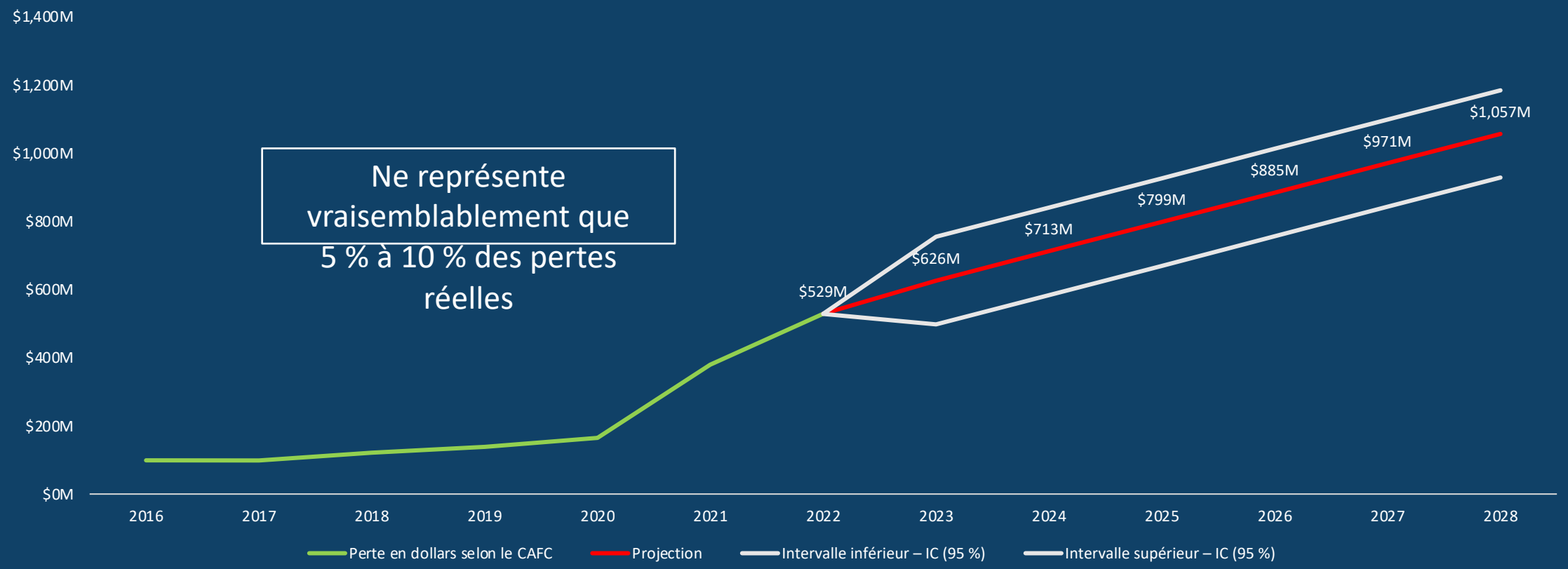
Cybercrimes déclarés par la police par infraction



Tendance des pertes déclarées attribuables aux fraudes/à la cyberfraude



Prévisions en matière de cyberfraude



	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
Prévisions en matière de cyberfraude en %	**65 %**	**60 %**	**52 %**	**60 %**	**53 %**	**60 %**	**62 %**	**73 %**	**70 %**	**70 %**	**71 %**	**71 %**	**71 %**	**71 %**	**71 %**

Ce que nous constatons…

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

Répercussions importantes – Le rançongiciel

- Les rançongiciels constituent la menace la plus perturbatrice pour les entreprises canadiennes.
- Les auteurs de rançongiciels sont de plus en plus ingénieux afin de maximiser leurs profits.
  - L'argent tiré des rançongiciels finance d'autres secteurs de l'économie cybercriminelle.
- Des techniques d'extorsion multiple sont utilisées pour contraindre les victimes à payer la rançon.

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

Qui sont les cybercriminels?

- Cela est difficile à dire… et peut dépendre de l'activité.

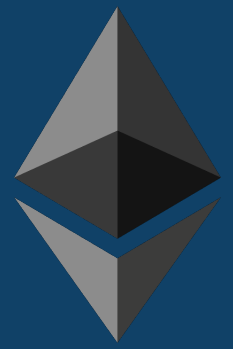
- Il faut considérer cela comme un ensemble… Il peut aussi bien s'agir de personnes qui s'ennuient que de groupes hautement qualifiés et financés par l'État qui volent de l'argent pour contourner les sanctions internationales provoquant des difficultés financières.

- Les groupes menant des attaques par rançongiciel peuvent notamment faire appel à :

La cryptomonnaie

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

- Le recours aux services d'échange et aux mélangeurs de cryptomonnaie demeure une méthode privilégiée par les cybercriminels pour brouiller le mouvement des fonds illicites, ce qui rend leur traçabilité difficile.
- Les cybercriminels utilisent de plus en plus les plateformes financières décentralisées (DeFi) pour échapper à la détection et ils les ciblent pour voler de la cryptomonnaie.
- Selon Chainalysis, les paiements de rançons en cryptomonnaie s'élevaient à plus de 1,2 milliard de dollars américains en 2021 et en 2022.
- Les transactions comprenant des adresses illicites représentaient seulement 0,24 % de tout le volume de transactions en 2022. Même s'il s'agit d'un faible pourcentage de toutes les transactions, les adresses illicites ont tout de même reçu 20,6 milliards de dollars américains, soit une augmentation par rapport aux 18 milliards de dollars américains en 2021.



NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

Menaces liées à l'IA au Canada

- Récemment, il y a eu des avancées de l'IA dans les grands modèles de langage (GML), comme ChatGPT, Bard, Claude, WormGPT.
  - Des GML propres à la cybercriminalité sont en cours d'élaboration.
- Il est probable que les cybercriminels utilisent l'IA pour multiplier leurs activités.
- La technologie de l'hypertrucage constitue un risque nouveau – elle permet d'augmenter l'efficacité des cyberfraudes et des attaques par manipulation psychosociale.

Ce que nous faisons pour lutter contre la cybercriminalité…

Comment les organismes d'application de la loi luttent contre la cybercriminalité

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

PRÉVENTION	Communication de renseignements en temps opportun, création de produits de sensibilisation, éducation des citoyens et de l'industrie, détournement des cybercriminels
RÉDUCTION DES RISQUES	Intervention rapide pour avertir la victime et éviter des conséquences plus graves – lui permettre de limiter les dégâts
PERTURBATION	Saisie des infrastructures, des marchés et des systèmes de paiements illégaux qui facilitent la cybercriminalité
APPRÉHENSION	Appréhension des personnes responsables des infractions commises au Canada et à l'étranger, qui les facilitent ou qui y contribuent

Mandat du CNC3 : Un centre de coordination et de soutien

Aider les organismes d'application de la loi canadiens à mieux lutter contre la cybercriminalité afin de réduire la menace, le nombre de victimes et les répercussions de la cybercriminalité au Canada.

EC3 EUROPOL

NCFTA®

194 services de police canadiens

Équipes fédérales d'enquête sur la cybercriminalité (EEC), Divisions de la GRC

Canadian Anti-Fraud Centre
CAFC
Centre antifraude du Canada

Coordonner les enquêtes sur la cybercriminalité en étroite collaboration avec des organismes d'application de la loi ainsi que des partenaires fédéraux et de l'industrie.

Offrir aux services de police **des avis**, des conseils et **des capacités techniques dans le domaine des enquêtes numériques.**

Produire du renseignement utilisable sur la cybercriminalité pour les services de police canadiens.

Travailler en étroite collaboration avec le CAFC pour mettre en place un nouveau mécanisme national de signalement public pour permettre à la population, aux entreprises et à d'autres organisations de signaler des cybercrimes et des fraudes aux services de police.

Mettre l'accent sur les cybercrimes sophistiqués sur le plan technique et ayant de grandes répercussions

CANADIAN CENTRE FOR CYBER SECURITY

Public Safety Canada

CRTC

SECTEURS PUBLIC ET PRIVÉ

MILIEU UNIVERSITAIRE

GoldDust

Five affiliates to Sodinokibi/REvil unplugged

- Rançongiciel Sodinokibi (REvil)
- Au total, 7 000 infections dans le monde, et 600 au Canada
- Enquête canadienne menée par le Service de police de Calgary, avec l'aide du CNC3, de la Police fédérale de la GRC et de services de police partenaires canadiens
  - Menée de janvier 2020 à novembre 2021
- Cinq auteurs de cybermenaces internationaux arrêtés en **novembre 2021**

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

« Même si ces arrestations ont été réalisées à des milliers de kilomètres, les crimes qu'on reproche à ces suspects ont eu de véritables répercussions sur des citoyens de Calgary et du Canada… »

Inspecteur Phil Hoetger, Section des enquêtes techniques du Service de police de Calgary

Coda

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

- Enquêtes menées en parallèle par le FBI et la Police provinciale de l'Ontario (OPP), avec le soutien du CNC3 et d'Europol
  - Enquête de plusieurs années
- Suspect lié à des campagnes de rançongiciels, à des forums sur la cybercriminalité, à des fraudes bancaires et à la compromission informatique de services gouvernementaux et d'établissements médicaux en Alaska
- Suspect canadien arrêté en **décembre 2021**

« Le FBI ainsi que ses partenaires internationaux, l'OPP et la GRC poursuivront leurs enquêtes sur ces auteurs de cybermenaces malveillants qui continuent de cibler les infrastructures des États-Unis et du Canada… »

Brian Abellera, attaché juridique du FBI à Ottawa

Canadian Ransomware Arrest Is a Meaningful Flex, Experts Say

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

Nectar

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

- Le groupe HIVE a fait 1 500 victimes partout dans le monde et a reçu plus de 100 M$ en paiements de rançons.
  - Au moins 71 organisations canadiennes comptaient parmi les victimes
- Enquête canadienne menée par le Service de police régional de Peel en collaboration avec des services de police partenaires canadiens et internationaux, et coordonnée par le CNC3
  - Enquête de plusieurs années
- Le CNC3 a permis aux victimes canadiennes d'avoir accès aux clés de déchiffrement, ce qui leur a évité de payer des rançons à six ou sept chiffres dans certains cas
- Démantèlement international de l'infrastructure du groupe HIVE en **janvier 2023**

Cybercriminals stung as HIVE infrastructure shut down

« En collaborant avec nos partenaires des services de police au pays et à l'étranger, nous avons utilisé les meilleurs renseignements afin de tenir responsables ces auteurs de cybermenaces qui font des victimes dans nos collectivités… »

Nick Milinovich, chef adjoint du Service de police régional de Peel

Cookie Monster

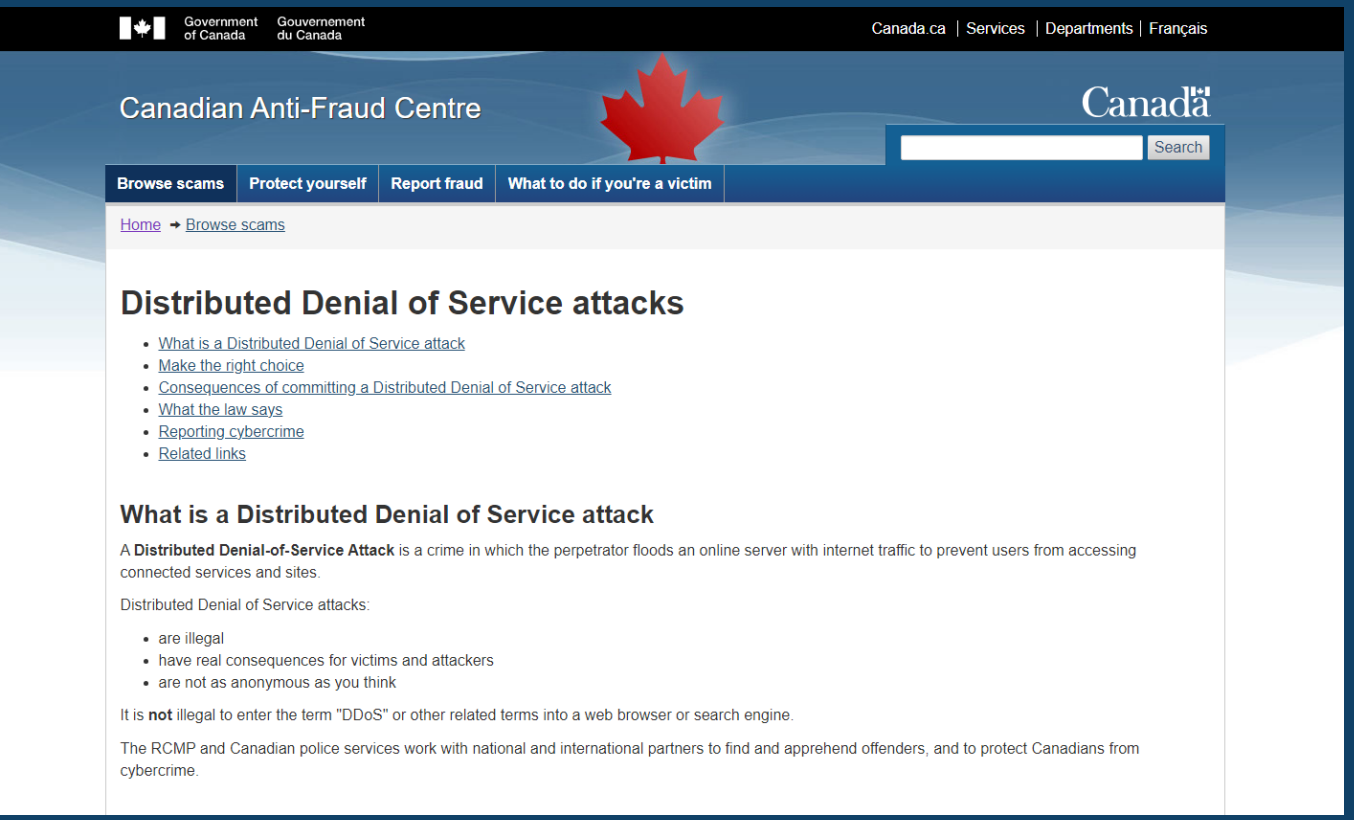
- Genesis Market, un marché qui faisait la vente de justificatifs d'identité volés (accès à des comptes)
- Faisait la vente de 1,5 million de « robots » (justificatifs d'identité/accès)
- Activités d'enquête/de perturbation multinationales
  - Enquête de plus de quatre ans
- Démantèlement international de Genesis Market en **avril 2023**
  - 18 pays, 28 services de police canadiens compétents, CRTC
  - 79 mesures policières distinctes au Canada
  - Arrestations, mandats de perquisition, ordonnances de cessation et d'abstention

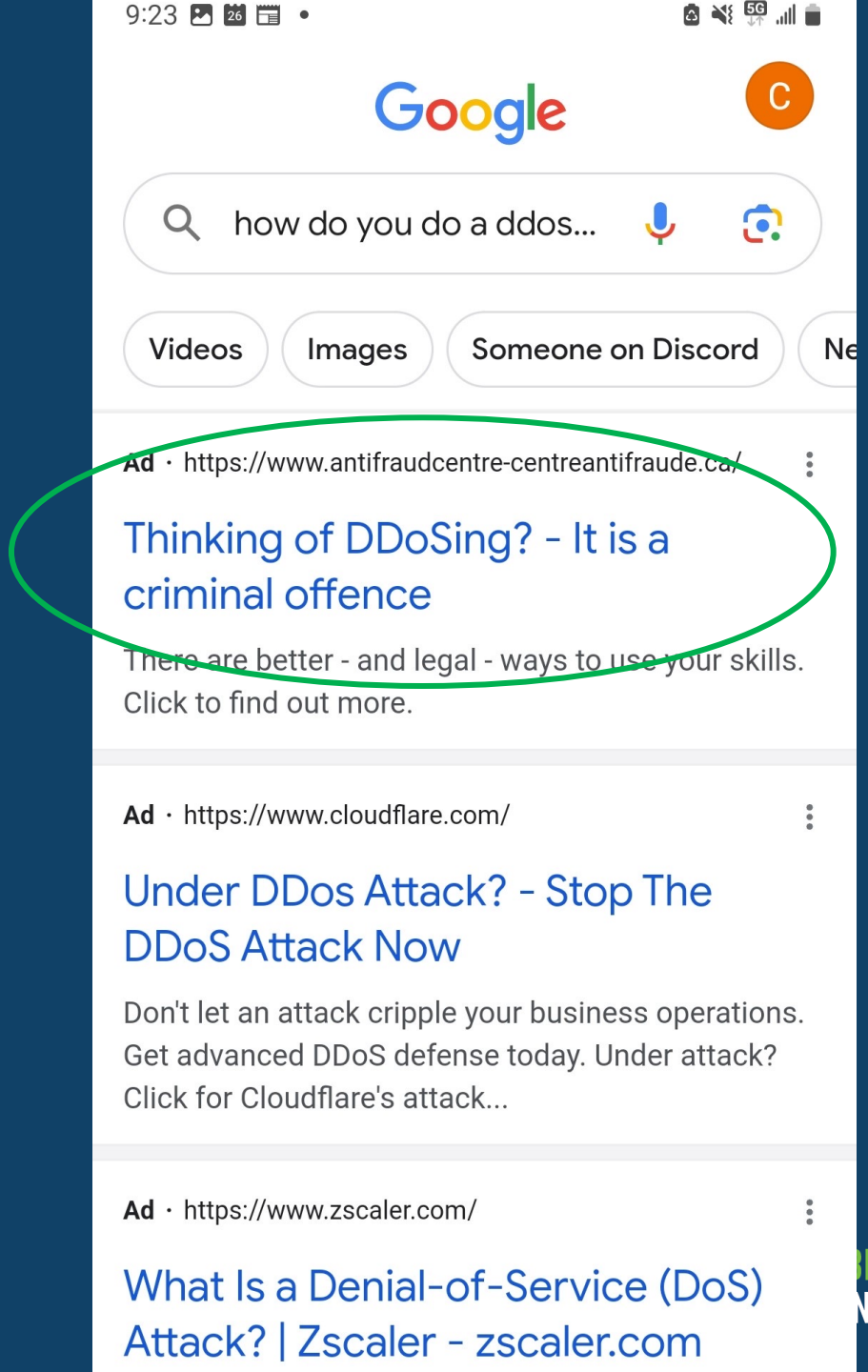
How police in Canada helped the FBI in crackdown on the stolen data market

« Le démantèlement de Genesis Market est une preuve de l'incidence que peuvent avoir les organismes d'application de la loi et leurs partenaires lorsqu'ils travaillent ensemble… »

Bryan Larkin, sous-commissaire de la GRC, Services de police spécialisés

Activités de prévention de la cybercriminalité – Campagne Google Ads sur les attaques par déni de service distribué





Comment vous pouvez aider

1. Soyez cybervigilant...

Quatrième question Slido : Je dirais que mes pratiques en matière de cybersécurité sont…

1. très bonnes (je suis cyberavisé ou cyberavisée)
2. moyennes (je fais preuve de prudence et j'utilise des techniques de protection)
3. inférieures à la moyenne (je pourrais faire mieux)
4. très mauvaises (l'Inter-quoi?)

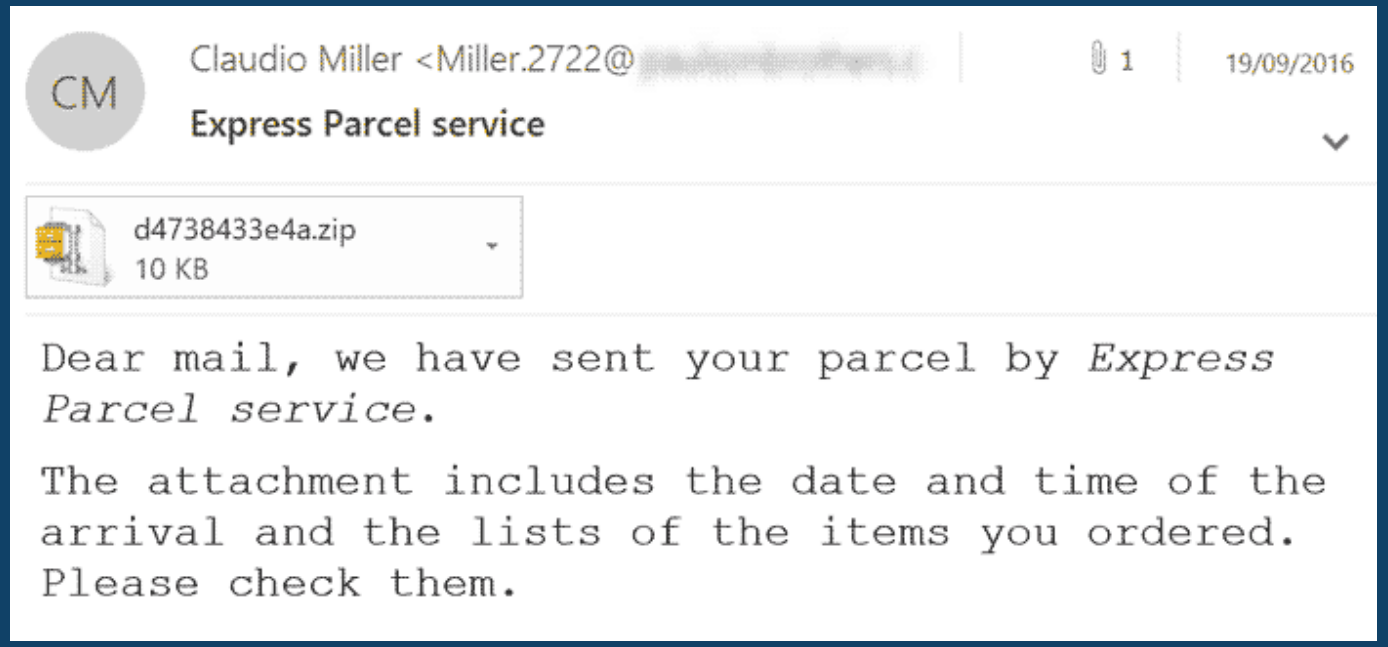
NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

- Les cybercriminels tirent profit de vos données.
- En cas de compromission, vous et vos contacts êtes exposés à des risques.
- Cela peut avoir des répercussions sur votre sécurité financière.

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

Méfiez-vous des pièces jointes!

- Les courriels d'hameçonnage peuvent contenir des virus en pièces jointes.
- Si vous ne faites pas confiance à l'expéditeur, ne les téléchargez pas.

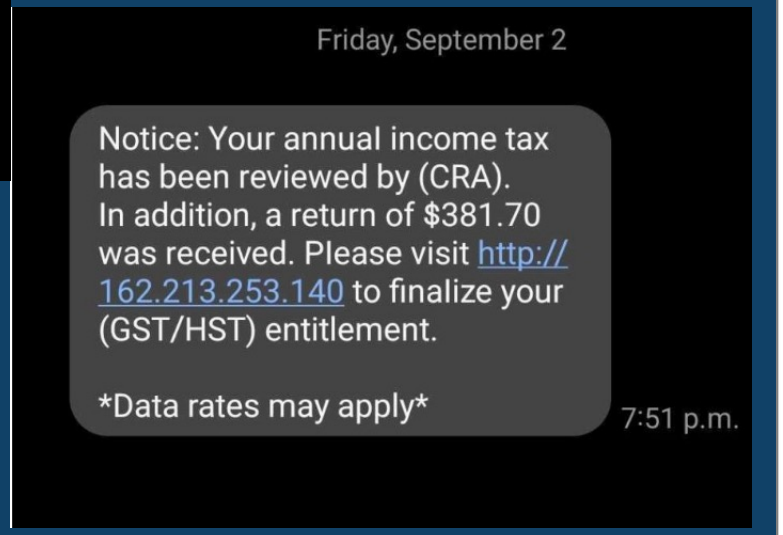


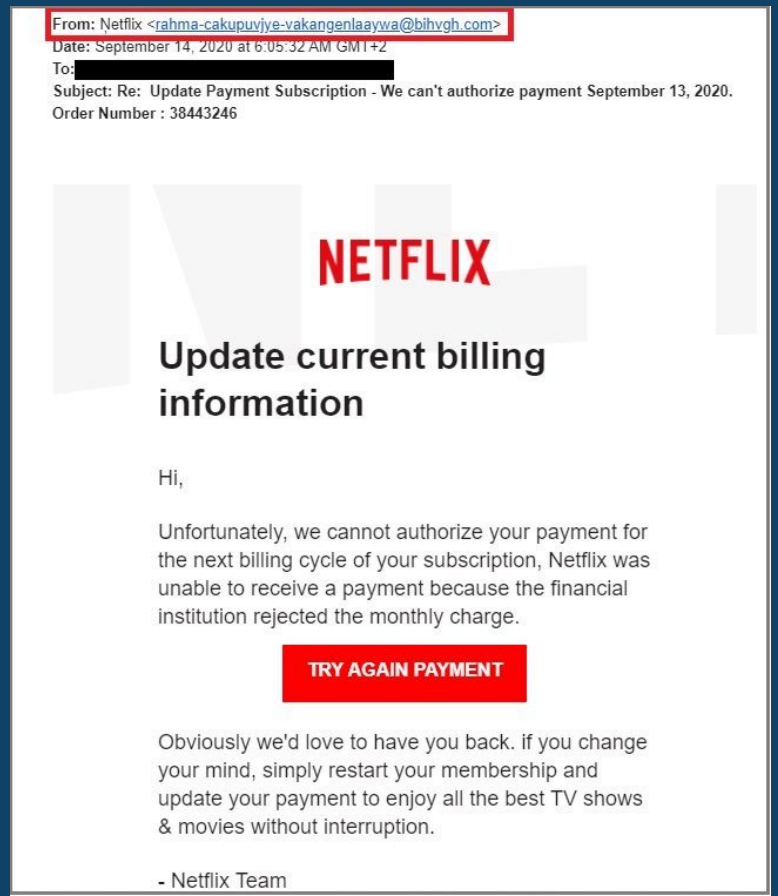
Ces formats de fichiers peuvent contenir des virus!

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

Hameçonnage et hameçonnage par SMS

- Vous avez reçu un message texte étrange concernant votre colis de Postes Canada?
- Ou encore un courriel contenant beaucoup de fautes de frappe de la part d'un « ami » qui vient de gagner à la loterie?

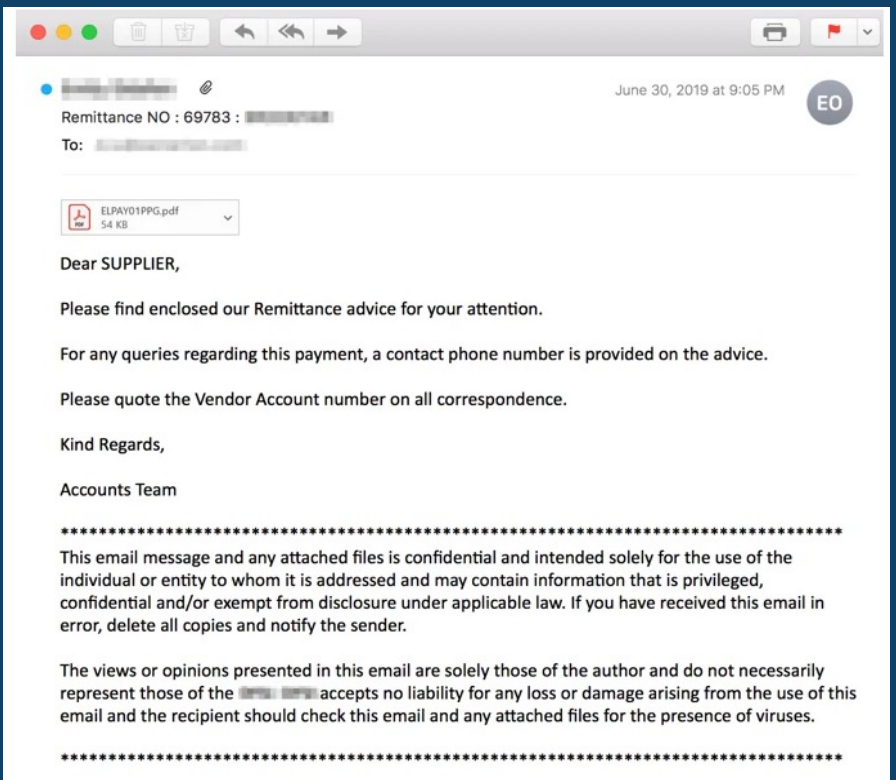




Les professionnels dans le domaine des finances sont des cibles lucratives.

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

- Compromission de courriels d'entreprises
- Fraude liée à une fausse facture de fournisseur
- Fraude liée aux paiements autorisés



June 30, 2019 at 9:05 PM

EO

Remittance NO : 69783 :

To:

ELPAY01PPG.pdf
54 KB

Dear SUPPLIER,

Please find enclosed our Remittance advice for your attention.

For any queries regarding this payment, a contact phone number is provided on the advice.

Please quote the Vendor Account number on all correspondence.

Kind Regards,

Accounts Team

****

This email message and any attached files is confidential and intended solely for the use of the individual or entity to whom it is addressed and may contain information that is privileged, confidential and/or exempt from disclosure under applicable law. If you have received this email in error, delete all copies and notify the sender.

The views or opinions presented in this email are solely those of the author and do not necessarily represent those of the accepts no liability for any loss or damage arising from the use of this email and the recipient should check this email and any attached files for the presence of viruses.

****

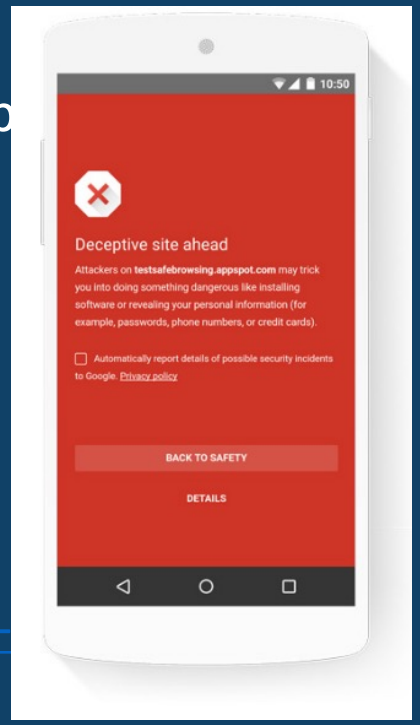
Cyberattacks on the rise for accountancy firms | Naq

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

Principaux conseils de cybersécurité

CIRA Canadian Shield
Free public DNS for Canadians

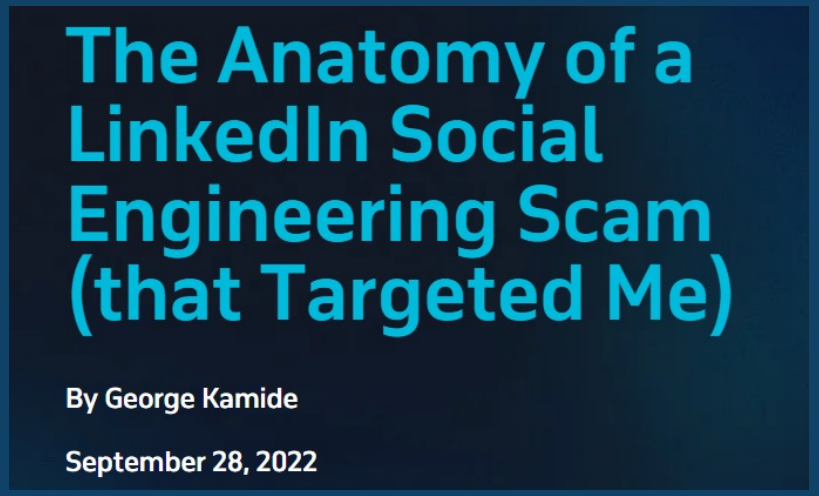
- Utiliser l'authentification multifacteur
- Utiliser des mots de passe robustes et uniques
- Utiliser le Bouclier canadien de CIRA
- Utiliser le mode de navigation sécurisée
- Utiliser des logiciels antivirus et assurer une surveillance du Web clandestin
- Faire des copies de sécurité
- Mettre à jour ses appareils
- Être prudent avec le « Wi-Fi gratuit » – utiliser un RPV
- Se méfier de chaque lien/pièce jointe



https://www.cyber.gc.ca/fr/orientation/pratiques-exemplaires-en-cybersecurite

Soyez vigilant dans les médias sociaux

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE



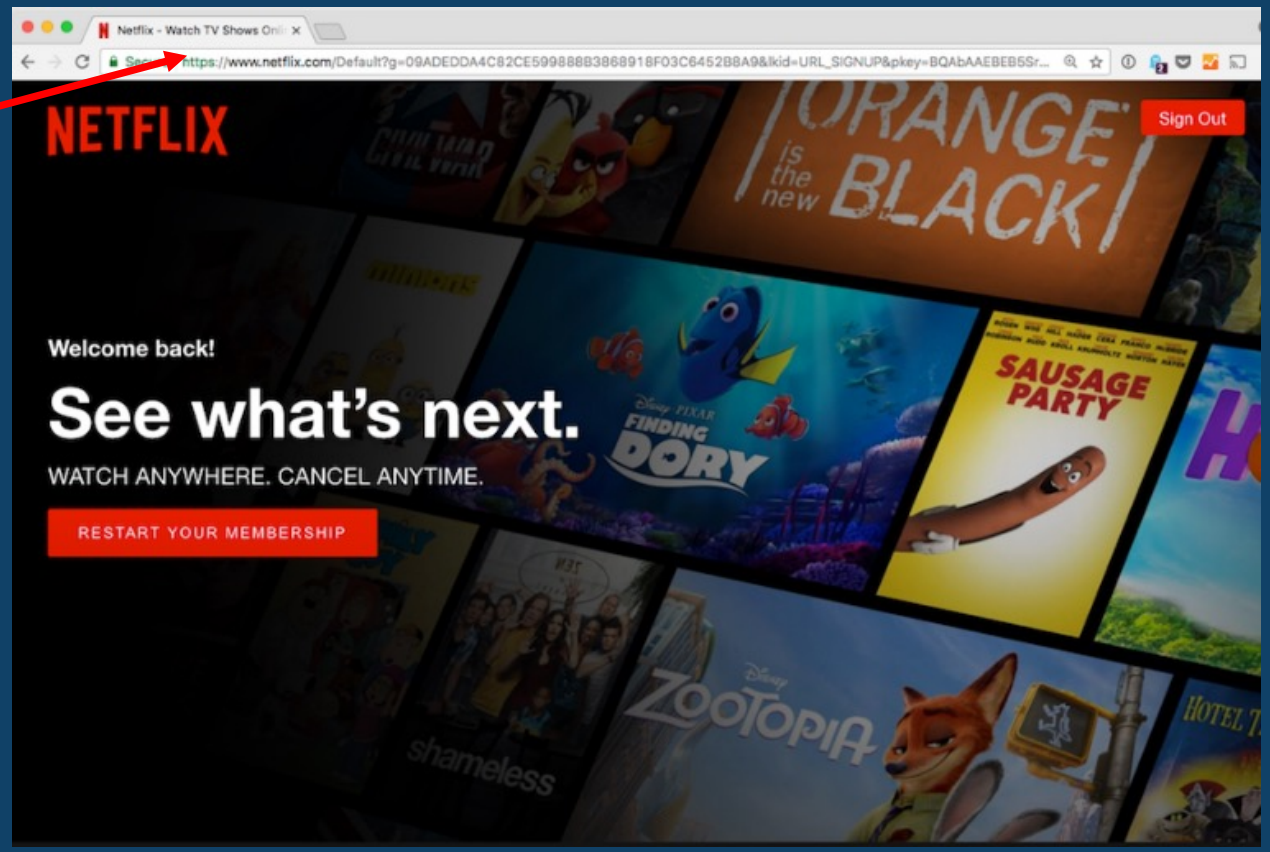
Cinquième question Slido – « Trouvez le leurre »

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

- Quelle est l'adresse URL frauduleuse?
- 1 ou 2?

1. www.Netflix.com/login

2. www.Netflìx.com/login

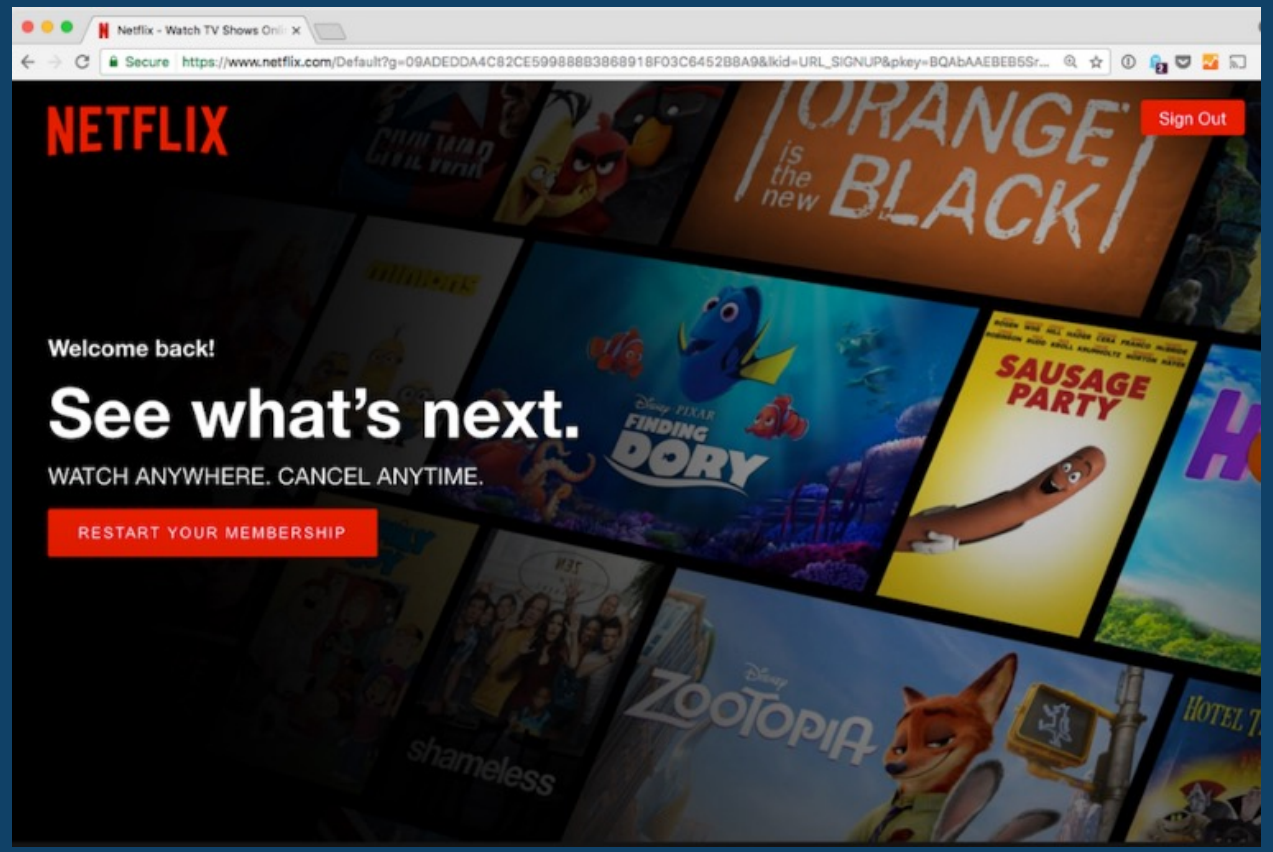


Cinquième question Slido – « Trouvez le leurre »

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

- Quelle est l'adresse URL frauduleuse?
- La bonne réponse est 2

1. www.Netflix.com/login
2. www.Netflix.com/login



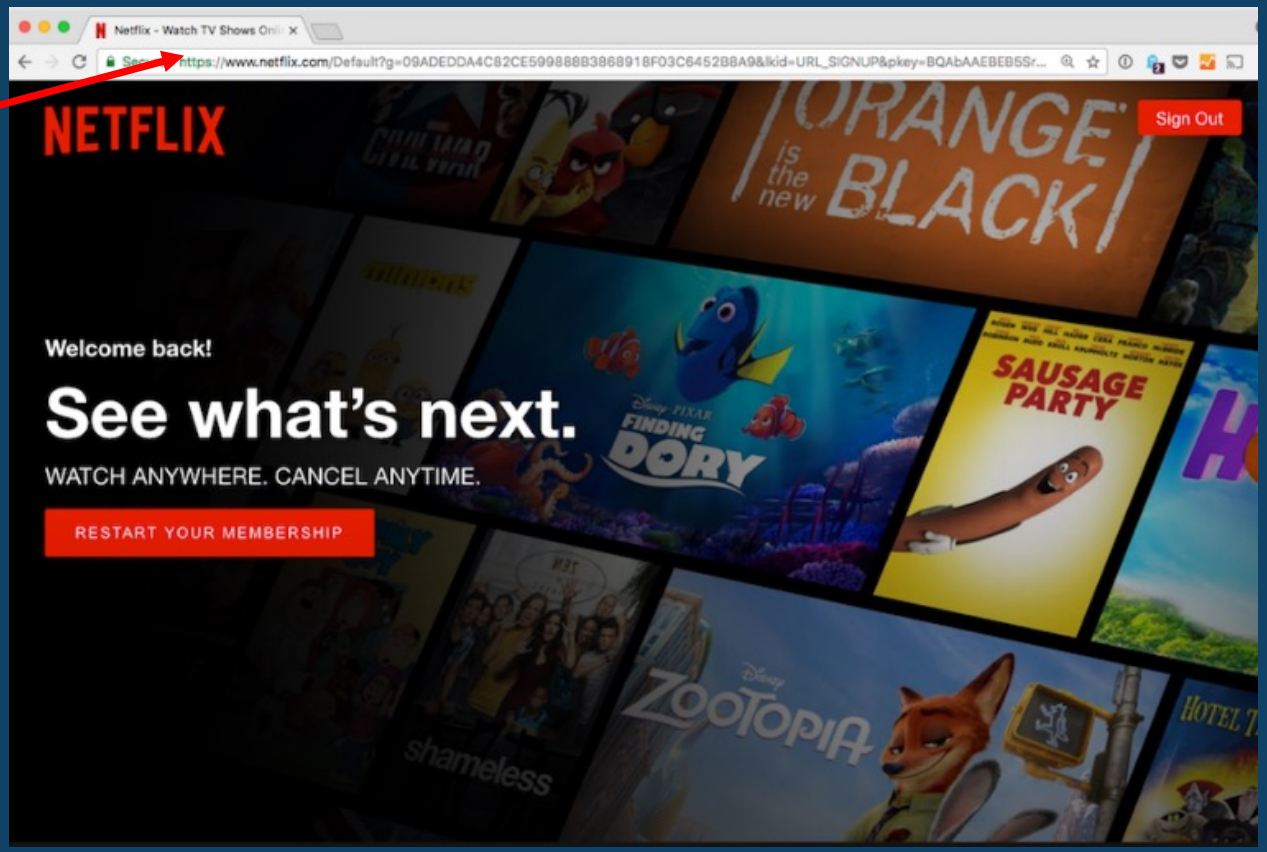
Sixième question Slido – « Trouvez le leurre »

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

- Quelle est l'adresse URL frauduleuse? (**plus difficile**)
- 1 ou 2?

1. www.Netflix.com

2. www.Netflix.com



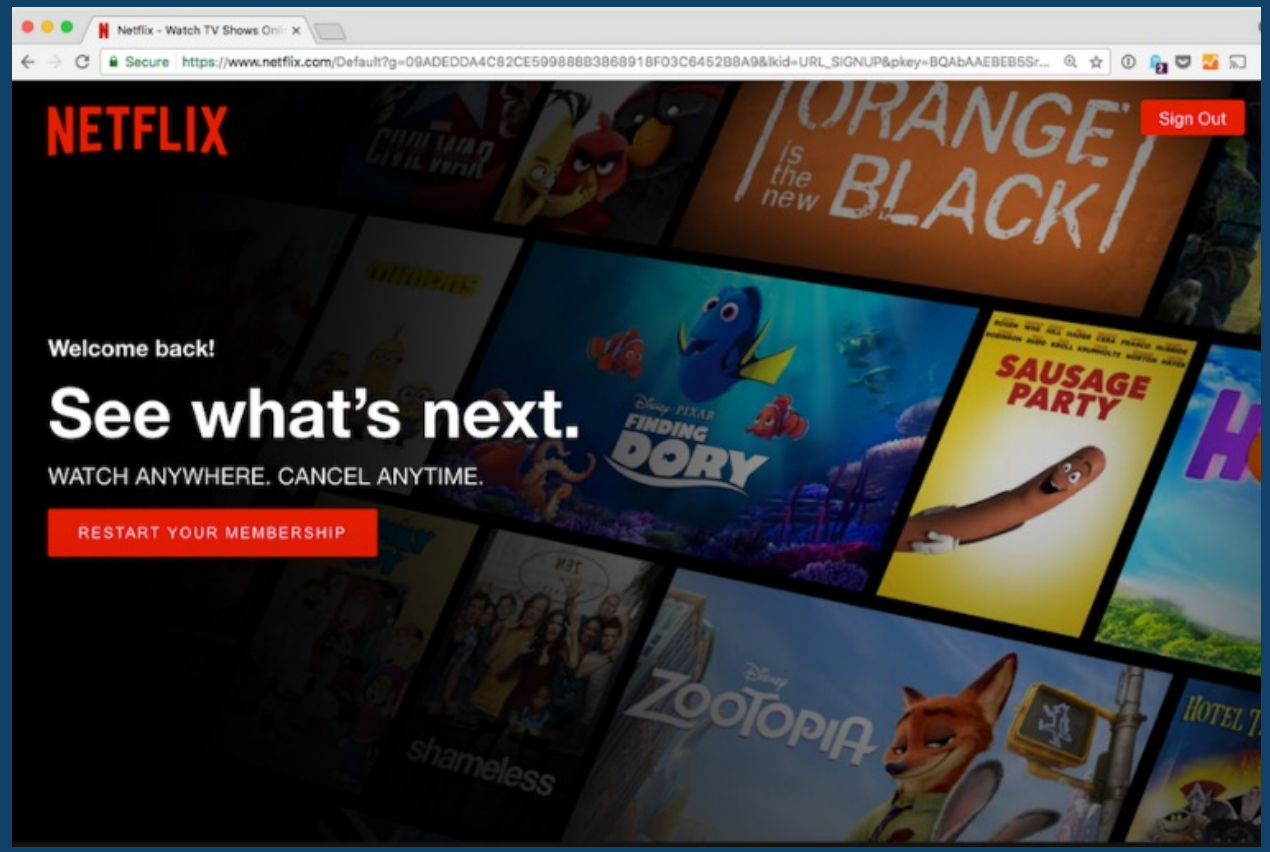
Sixième question Slido – « Trouvez le leurre »

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

- Quelle est l'adresse URL frauduleuse? (**plus difficile**)
- La bonne réponse est 1

1. www.Netflix.com → I = i majuscule

2. www.Netflix.com → l = L minuscule



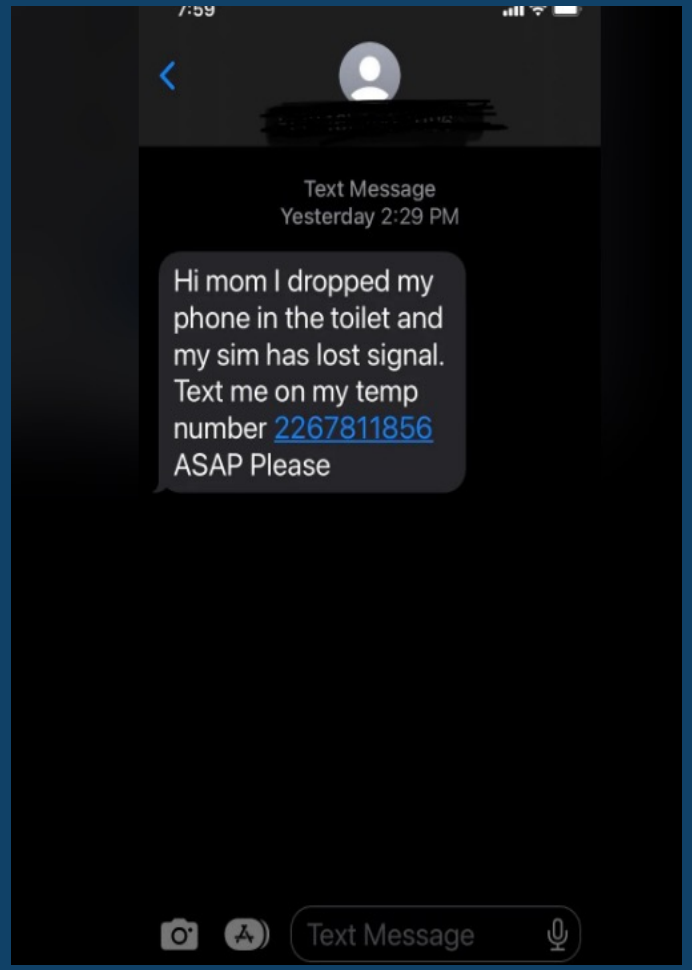
Outils de manipulation psychosociale des cybercriminels

- Mystification
- Sentiment d'urgence
- Manipulation émotionnelle
- Menaces
- Usurpation d'identité
- RÉACTION À AVOIR : Prenez quelques instants pour réfléchir!
  - Le temps joue en votre faveur
  - Faites confiance à votre intuition!

Septième question Slido : Honnêtement, qui serait tombé dans le panneau?

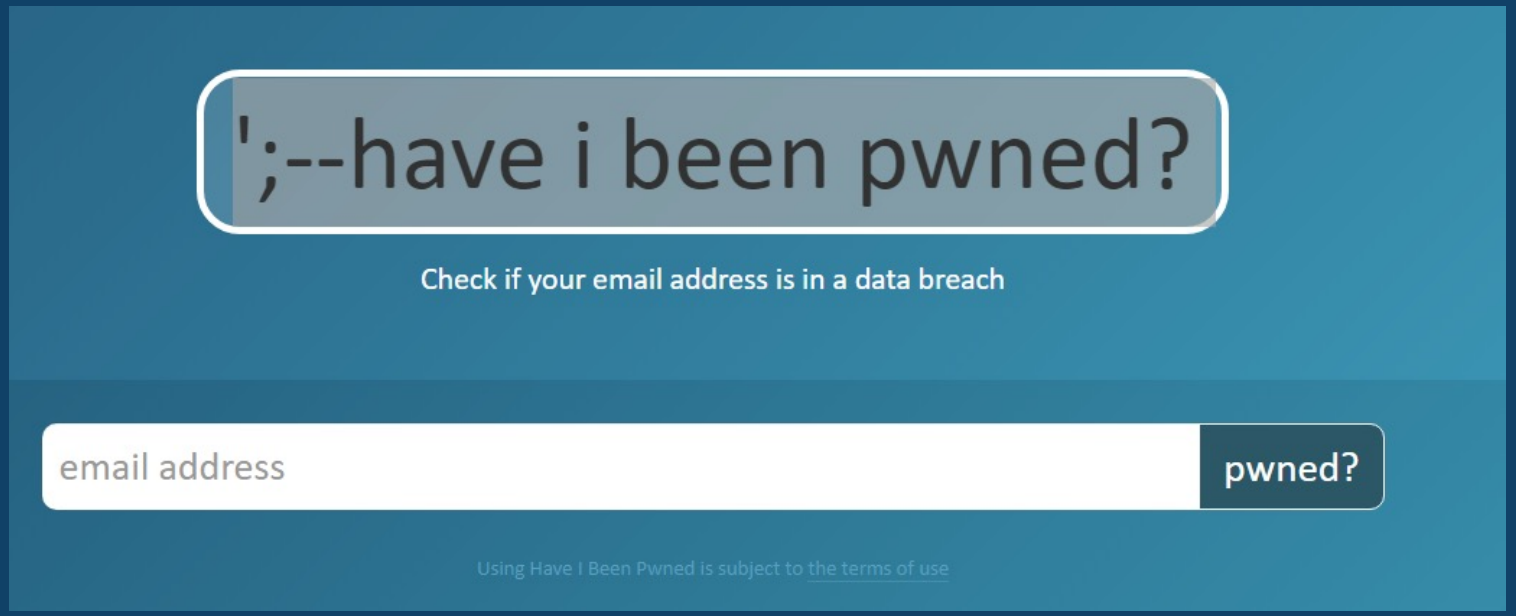
NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

1. J’aurais probablement répondu
2. Jamais



Royal Canadian Mounted Police | Gendarmerie royale du Canada

Vérifiez si votre adresse courriel est vulnérable



https://haveibeenpwned.com/ (en anglais seulement)

2. Vous pouvez aider en signalant les incidents…

Impact of Fraud

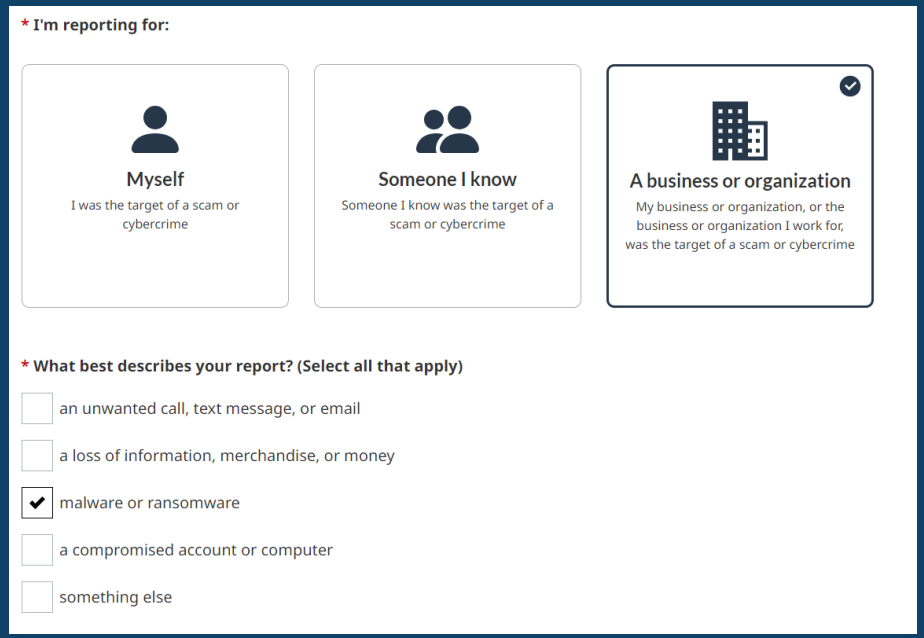
Why victims don't report?

- 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



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

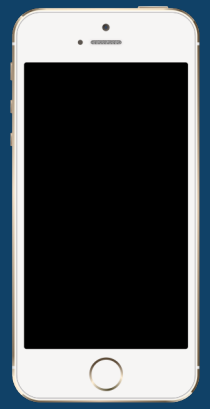
Où signaler les tentatives d'hameçonnage par SMS

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

Lutter contre les messages textes indésirables en transférant ces messages au 7726!

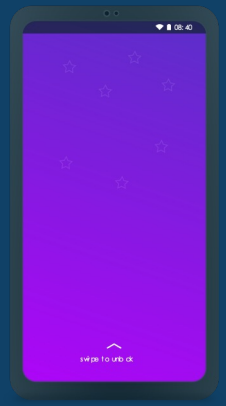
iPhone

1. Maintenez votre doigt appuyé sur le message
2. Appuyez sur « Plus… »
3. Sélectionnez le message à transférer et appuyez sur la flèche dans le coin inférieur droit
4. Inscrivez **7726**
5. Appuyez sur le bouton d'envoi



Android

1. Maintenez votre doigt appuyé sur le message (faites attention de ne pas activer un lien)
2. Choisissez « Transférer » (dans le menu)
3. Inscrivez **7726**
4. Appuyez sur « Envoyer »



3. Passez le mot…

Arnaque des grands-parents

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**

Dites à vos proches…

- Ne divulguez jamais de renseignements à l'interlocuteur, y compris le nom de la personne qu'il prétend être, avant qu'il ne s'identifie lui-même.
- Posez à l'interlocuteur des questions personnelles auxquelles seule la personne concernée pourrait répondre.
- Raccrochez et tentez de communiquer avec un autre membre de votre famille pour confirmer l'endroit où se trouve votre proche.
- N'envoyez jamais de l'argent pour des paiements au moyen de cartes-cadeaux.
- APPELEZ LA POLICE IMMÉDIATEMENT!

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

CNC3 – Sport d'équipe – Aidez-nous à lutter contre la cybercriminalité

Prévention

Réduction des risques

Perturbation

Appréhension

En savoir plus

NC3 | NATIONAL CYBERCRIME COORDINATION CENTRE

Signalez une fraude au CAFC
https://www.antifraudcentre-centreantifraude.ca/report-signalez-fra.htm

Pour obtenir de plus amples renseignements
Visitez le https://www.rcmp-grc.gc.ca/fr/gnc3#wb-info
Site Web du CAFC : https://www.antifraudcentre-centreantifraude.ca/index-fra.htm

Merci!


NATIONAL CYBERCRIME COORDINATION UNIT
GROUPE NATIONAL DE COORDINATION CONTRE LA CYBERCRIMINALITÉ