

CANADIAN CENTRE^{FOR} **CYBER** SECURITY

Signalement des escroqueries

© 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.



Ordre du jour

○ Mandat

- Centre de cybersécurité
- GRC
- UNCLC
- Centre antifraude du Canada (CAFC)
- Centre de notification des pourriels

○ À qui faire un signalement?

○ Scénarios

Loi sur le Centre de la sécurité des télécommunications et mandat du CSE

"There can be no greater obligation than to protect the security of Canadians at home and abroad. Bill C-59 would provide CSE with the authorities and tools to maintain the highest standards in security protection while adhering to the high standards of accountability and transparency."

—The Honourable Harjit Singh Sajjan,
MINISTER OF NATIONAL DEFENCE

FOREIGN SIGNALS INTELLIGENCE



**MAINTAIN CSE'S ABILITY TO COLLECT
FOREIGN SIGNALS INTELLIGENCE**
Use advanced techniques to access foreign networks
to collect intelligence in support of government priorities

CYBERSECURITY & 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

ASSISTANCE TO FEDERAL SECURITY & INTELLIGENCE PARTNERS



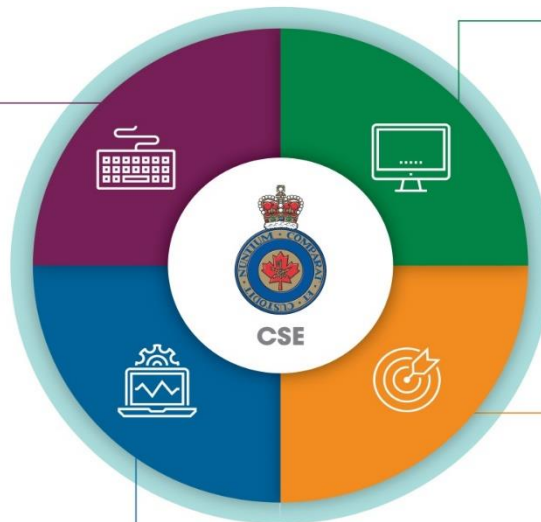
**ASSISTANCE TO DND/CAF INCLUDING CYBER
OPERATIONS FOR GOVERNMENT-AUTHORIZED
MILITARY MISSIONS**
Use advanced techniques to support military campaigns
and protect military personnel

FOREIGN CYBER OPERATIONS



DEFENSIVE CYBER OPERATIONS
Disrupting foreign cyber threats targeting
important Canadian networks

ACTIVE CYBER OPERATIONS
Interfere with foreign online efforts that threaten Canada



INCREASED ACCOUNTABILITY MEASURES

Mandat de la GRC

Ses mandats ont trait aux services de police nationaux, provinciaux et municipaux. D'un bout à l'autre du pays, au niveau communautaire, provincial/territorial et fédéral, ces mandats sont les suivants :



Unité nationale de coordination de la lutte contre la cybercriminalité (UNCLC)

Bien qu'il soit géré par la GRC, l'UNCLC servira tous les services de police canadiens en tant que service national de police. En collaboration avec des partenaires des organismes d'application de la loi, des gouvernements et du secteur privé du Canada, l'UNCLC réalisera les tâches suivantes :

pour coordonner, synchroniser et harmoniser les enquêtes sur la cybercriminalité au Canada et travailler avec des partenaires internationaux pour lutter contre un large éventail d'incidents de cybercriminalité;

fournir aux services de police canadiens des conseils et une orientation sur les enquêtes numériques ;

produire des renseignements sur la cybercriminalité à l'intention des services de police canadiens;

créer un système national permettant aux particuliers et aux entreprises de signaler la cybercriminalité en ligne.

Mandat du Centre antifraude du Canada (CAFC)

Répertoire central du Canada pour les renseignements sur la

fraude
Le CAFC est géré conjointement par la **GRC**, le **Bureau de la concurrence** et la **police provinciale de l'Ontario**. Cet organisme aide les citoyens et les entreprises à faire ce qui suit :



Signaler les fraudes



Se renseigner sur différents types de fraude



Reconnaître les signes de fraude



Se protéger contre la fraude



Combattre le crime



Renforcer le partenariat entre le secteur privé et le secteur public



Maintenir l'économie du Canada

Le CAFC offre des renseignements aux organismes d'application de la loi et aux gouvernements canadiens et mondiaux.

Centre de notification des pourriels — ISDE

- Il collabore avec le **Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)**, le **Bureau de la concurrence** et le **Commissariat de la protection de la vie privée du Canada (CPVPC)**.
- Il assure le respect de la ***Loi canadienne anti-pourriel (LCAP)***.
- Il permet aux Canadiens de signaler tous les pourriels qu'ils reçoivent.

Personnes-ressources

Cybertip.ca

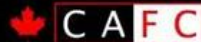
- Exploitation des enfants, trafic de pornographie juvénile, exploitation sexuelle, etc.



Royal Canadian Mounted Police
Gendarmerie royale du Canada

- Cybercrime
- Logiciel de rançon, blanchiment d'argent, vol d'identité, cyberintimidation, etc.

Canadian Anti-Fraud Centre



Centre antifraude du Canada

- Si vous recevez des courriels d'hameçonnage personnels ou une arnaque d'impôt par télémarketing

CENTRE CANADIEN POUR LA
CYBERSÉCURITÉ

- Incidents urgents de cybersécurité, échange de maliciel, conseils et orientation d'ordre général

Centre de notification
des pourriels

- Pourriels par courriel ou sur le Web



EXEMPLES D'ESCROQUERIES



Scénario 1

facebook

Dear Facebook user,

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security.

Before you are able to use the new login system, you will be required to update your account.

Click [here](#) to update your account online now.

If you have any questions, reference our New User Guide.

Thanks,
The Facebook Team

Update your
Facebook account

Update

This message was intended for [REDACTED]
Facebook's offices are located at 1601 S. California Ave., Palo Alto, CA 94304.

Référence — resourcesforlife.com

À qui faire un signalement?



Scénario 2

Cher client,
Nous avons remarqué un solde impayé de 331,71 \$ dans votre compte.

Soyez avisé que si vous ne payez pas ce montant dans les 14 à 25 jours suivant la date de ce courriel, vos services seront suspendus en raison de non-paiement.

Si vos services sont suspendus, des frais de 35 \$ pourraient être ajoutés à votre compte. Pour plus d'information sur ces frais, veuillez consulter le site Web <https://www.rogers.com/signin> et ouvrez une session de votre compte MyRogers.

Dear Customer,

We noticed a balance of \$ 331.71 remains outstanding on your account.

Please be advised if you do not make a payment for the outstanding balance, your service(s) may be suspended for non-payment within 14 to 25 days from the date of this email.

If your service(s) are suspended, a fee of \$35.00 may be applied to your account. For more information on these charges, please visit: <https://www.rogers.com/signin> and log into your MyRogers account.

Thank you,
Rogers Communications



[Contact Us](#) | [Privacy Policy](#) | [Store Locator](#) | [rogers.com](#)

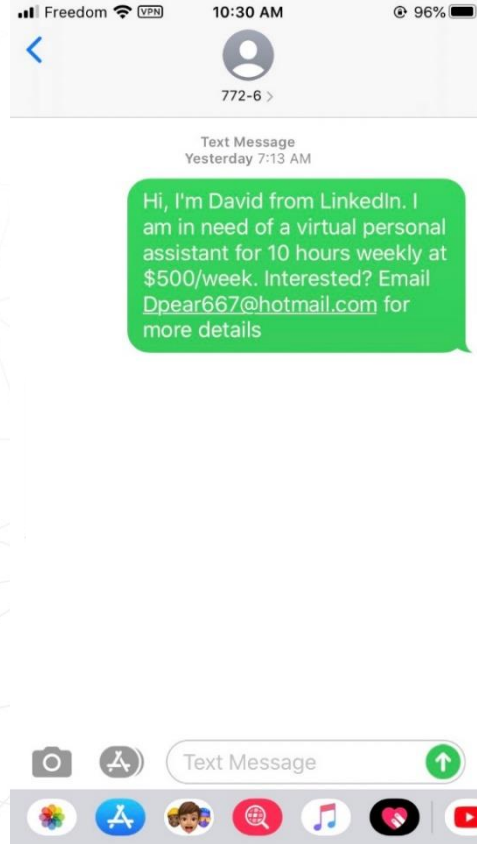
Rogers Communications | 333 Bloor St. E. | Toronto, ON M4W 1G9
© 2019 Rogers Communications

This email is confidential; if you are not the intended recipient, please delete it immediately without keeping a copy.

À qui faire un signalement?



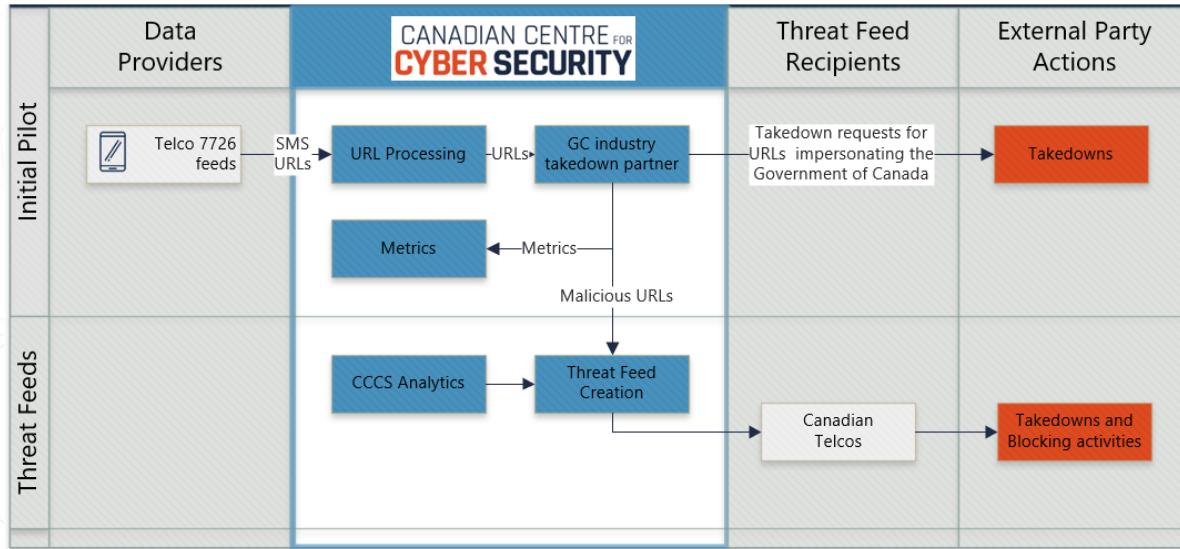
Scénario 3



Bonjour, c'est David de LinkedIn. Je suis à la recherche d'un assistant personnel virtuel, qui pourrait me consacrer 10 heures par semaine. Le salaire serait de 500 dollars par semaine. Vous êtes intéressé? Envoyez un courriel à Dpear667@hotmail.com pour plus de détails.

À qui faire un signalement?

Transférez le message à SPAM (7726). La plupart des fournisseurs de services de



Scénario 4

- John clique sur une pièce jointe qui comprend un maliciel.
- Le maliciel récupère les contacts de courriel de John et leur envoie un courriel en son nom. Il s'agit d'une attaque par logiciel rançonneur.
- Joan reçoit un courriel avec une pièce jointe de l'adresse de John. La protection anti virus signale la présence d'un maliciel.
- John communique avec Joan pour lui dire qu'il a été compromis.

○ Question : Joan doit-elle signaler sa compromission potentielle?

À qui faire un signalement?



Royal Canadian Mounted Police
Gendarmerie royale du Canada

**Services de police
locaux**

Scénario 5

Un compte locataire dans le nuage est facturé à la minute. Un examen des journaux nous a permis de constater que le compte a été utilisé de façon à accumuler une facture salée.

À qui faire un signalement?

Requis par la loi



Royal Canadian Mounted Police
Gendarmerie royale du Canada

Rapport

Canadian Anti-Fraud Centre



C A F C

Centre antip fraude du Canada

Orientation

CENTRE CANADIEN POUR
LA
CYBERSÉCURITÉ

Scénario 6

Votre réseau a été infiltré.
Les fichiers de tous les hôtes du réseau ont été chiffrés à l'aide d'un algorithme robuste. Aucun logiciel de déchiffrement offert au public ne sera efficace. Ne redémarrez pas votre ordinateur et ne le fermez pas puisque vos fichiers pourraient être endommagés.

Pour obtenir des renseignements (décrypter vos fichiers),
communiquez avec nous à l'adresse suivante :
LindaMcCann@protonmail.com.

Vous recevrez une adresse bitcoin dans le courriel de réponse et vous devrez payer deux bitcoins (26 000 CAD).
Vous avez 72 heures pour payer sinon vos fichiers seront détruits.
Nous avons copié les données. Si vous ne payez pas, elles seront publiées sur Internet.

À qui faire un signalement?

Requis par la loi

**Services de police
locaux**



Royal Canadian
Mounted Police

Gendarmerie royale
du Canada

Orientation

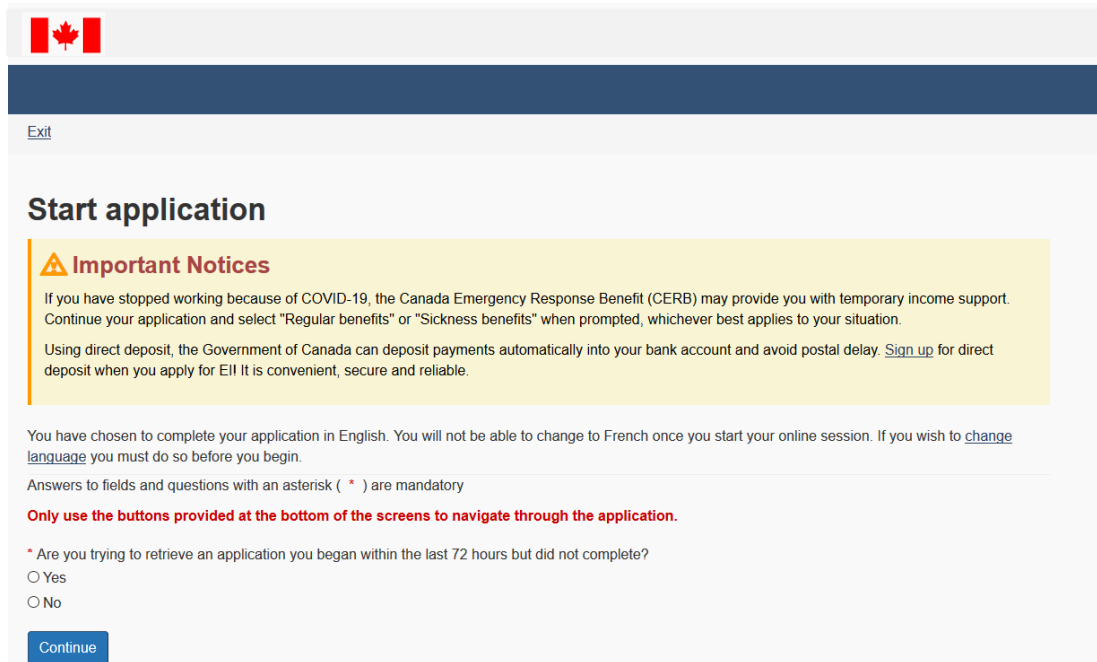
CENTRE CANADIEN POUR LA
CYBERSÉCURITÉ


Aide

**Fournisseur de
services gérés de
sécurité (MSSP)**

Scénario 7


Site Web frauduleux : <https://hrdc-dhrc.ca>





[Exit](#)

Start application

 **Important Notices**

If you have stopped working because of COVID-19, the Canada Emergency Response Benefit (CERB) may provide you with temporary income support. Continue your application and select "Regular benefits" or "Sickness benefits" when prompted, whichever best applies to your situation.

Using direct deposit, the Government of Canada can deposit payments automatically into your bank account and avoid postal delay. [Sign up](#) for direct deposit when you apply for EII It is convenient, secure and reliable.

You have chosen to complete your application in English. You will not be able to change to French once you start your online session. If you wish to [change language](#) you must do so before you begin.

Answers to fields and questions with an asterisk (*) are mandatory

Only use the buttons provided at the bottom of the screens to navigate through the application.

* Are you trying to retrieve an application you began within the last 72 hours but did not complete?

☐ Yes

☐ No

[Continue](#)

À qui faire un signalement?

CENTRE CANADIEN POUR
LA
CYBERSÉCURITÉ

Scénario 8

● Appel frauduleux : (appel automatisé)

La raison du présent appel est de vous aviser que nous avons engagé une procédure pénale à votre encontre pour évasion fiscale et fraude fiscales auprès de la Cour fédérale. Si vous voulez plus de renseignements sur cette procédure, veuillez nous rappeler le plus vite possible à la ligne directe de l'administration centrale de l'Agence du revenu du Canada. Le numéro est 613-927-9919. Je répète 613-927-9919. Si nous ne recevons pas d'appel de votre part, vous devrez vous préparer à faire face aux conséquences juridiques puisqu'il s'agit d'un problème sérieux et urgent. Bonne journée.

À qui faire un signalement?



**Le prétendu
organisme**

Scénario 9

- Votre organisme est une infrastructure essentielle.
 - Vous faites face à un cyberincident. Votre organisme a besoin d'orientation.
 - Vous souhaitez faire analyser un maliciel.

À qui faire un signalement?



COMMUNIQUEZ AVEC NOUS

 @cse_cst

 contact@cyber.gc.ca

 www.cyber.gc.ca

 @cybercentre_ca

Signaler une fraude
Centre antifraude du Canada

1-888-495-8501

www.antifraudcentre-centreantifraude.ca

Signaler un cybercrime
Police locale ou Gendarmerie
royale du Canada

www.rcmp-grc.gc.ca

Signaler des pourriels
Centre de notification des pourriels
spam@fightspam.gc.ca
www.fightspam.gc.ca