

# CANADIAN CENTRE<sup>FOR</sup> **CYBER** SECURITY

## Reporting Scams

© 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.



# Agenda

## ○ Mandate

- Cyber Centre
- RCMP
- NC3
- Canadian Anti-Fraud Centre
- SPAM Reporting Centre

## ○ Who should you report to

## ○ Scenarios

# CSE Act - CSE's Mandate

*"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

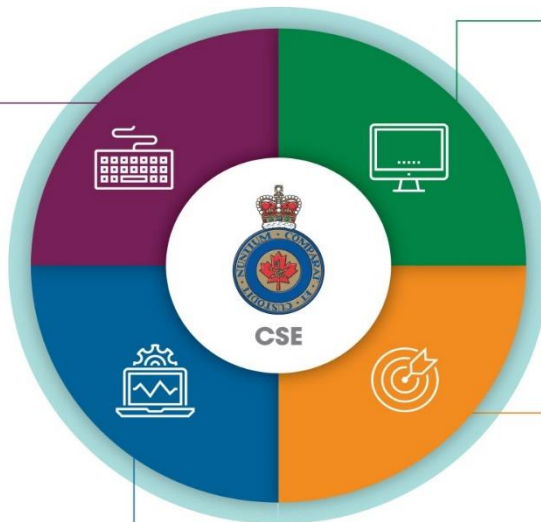


**ASSISTANCE TO DND/CAF INCLUDING CYBER  
OPERATIONS FOR GOVERNMENT-AUTHORIZED  
MILITARY MISSIONS**  
Use advanced techniques to support military campaigns  
and protect military personnel

## 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**

# RCMP Mandate

National, federal, provincial, and municipal policing mandates. From coast to coast to coast, at the community, provincial/territorial and federal levels these are the following mandates:



UNCLASSIFIED



# National Cybercrime Coordination Unit (NC3)

While managed by the RCMP, the NC3 will serve all Canadian police agencies as a National Police Service. Working with Canadian law enforcement agencies, government and private sector partners, the NC3 will:

**Collaborate extensively to coordinate, synchronize and deconflict cybercrime investigations in Canada and work with partners internationally to combat a wide range of cybercrime incidents;**

**Provide digital investigative advice and guidance to Canadian police;**

**Produce cybercrime intelligence for Canadian police, and;**

**Create a national system for individuals and businesses to report cybercrime online.**

# Canadian Anti-Fraud Centre Mandate

*Canada's central repository for information about fraud.*

CAFC is jointly managed by the **RCMP**, the **Competition Bureau Canada**, and the **Ontario Provincial Police**. This organization help citizens and businesses:



report fraud



learn about different types of fraud



recognize the warning signs of fraud



protect themselves from fraud



disrupting crime



strengthening the partnership between the private and public sectors



maintaining Canada's economy

CAFC provides information to law enforcement and governments in Canada and around the world.

# SPAM Reporting Centre - ISED

- Collaborates with **Canadian Radio-television and Telecommunications Commission (CRTC)**, the **Competition Bureau**, and the **Office of the Privacy Commissioner (OPC)**.
- Ensures compliance with **Canada's Anti-Spam Legislation (CASL)**.
- Allows Canadians to report any SPAM they have encountered.

# Who to Contact?

Cybertip.ca

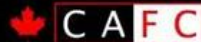
- Child exploitation, trafficking of child porn, sextortion etc.



Royal Canadian Mounted Police  
Gendarmerie royale du Canada

- Cybercrime
- Ransomware, Money Laundering, Identity Theft, Cyberbullying, etc.

Canadian Anti-Fraud Centre



Centre antipour du Canada

- If you receive personal phishing email, telemarketing, tax scam

CENTRE CANADIEN POUR LA  
**CYBERSECURITÉ**

- For urgent cyber incidents, malware sharing. General Advice and Guidance.

SPAM Reporting  
Centre

- Email and web-based spam





# EXAMPLES OF SCAMS



# Scenario 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.

Ref – resourcesforlife.com

# Who to Report to?



## Scenario 2

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 MyRogers account.

Thank you,  
Rogers Communication

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](#)

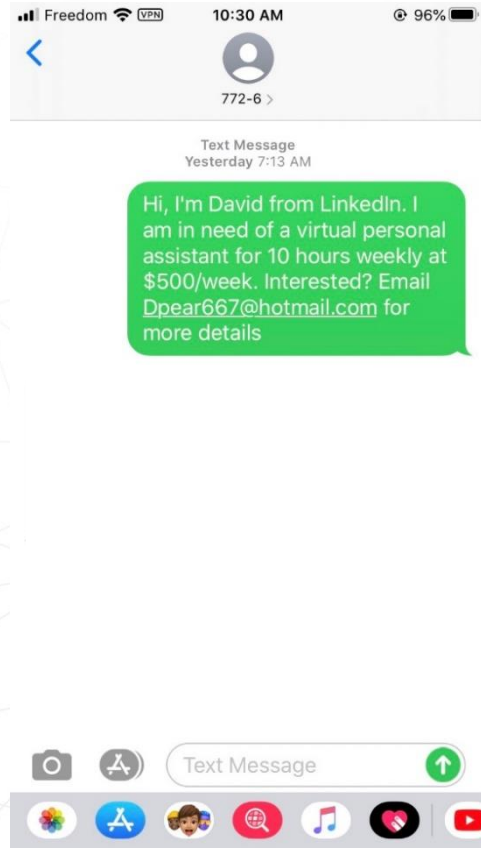
Rogers Communications | 333 Bloor St. E. | Toronto, ON M4W 1G9  
© 2019 Rogers Communications

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

# Who to Report to?



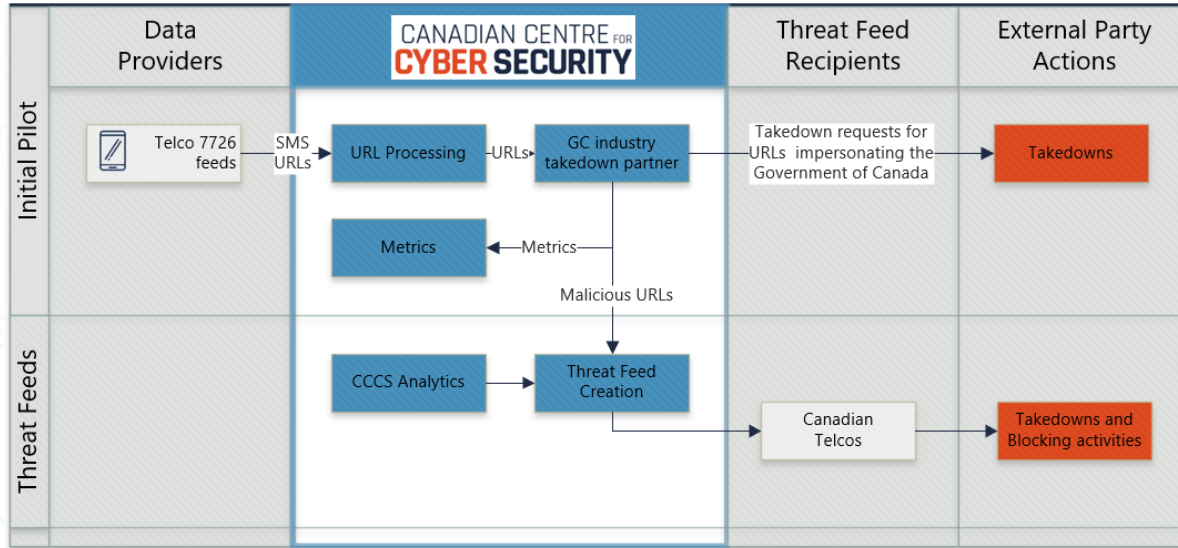
# Scenario 3



Hi, I'm David from LinkedIn. I am in need of virtual personal assistant for 10 hours weekly at \$500/week. Interested? Email [Dpear667@hotmail.com](mailto:Dpear667@hotmail.com) for more details.

# Who to Report to?

Forward to SPAM (7726), most cell phone providers offer the service.



## Scenario 4

- John clicks on an attachment that contains malware.
  - The malware harvests John's email contacts and sends email on his behalf. The malware leads to a Ransomware attack.
  - Joan receives an email from supposed John with an attachment. AV tells that the email contains malware.
  - John contacts Joan and tells her he has been compromised.
- Question: Does Joan need to report her potential compromise?



# Who to Report to?



Royal Canadian Mounted Police  
Gendarmerie royale du Canada

**Local law enforcement**



# Scenario 5

**A cloud tenant account is charged per minute. A review of the logs has identified that an account has been used to rack up a big bill.**



# Who to Report to?

Required by Law



Royal Canadian Mounted Police  
Gendarmerie royale du Canada

Reporting

Canadian Anti-Fraud Centre



C A F C

Centre antip fraude du Canada

Guidance

CENTRE CANADIEN POUR  
LA  
**CYBERSÉCURITÉ**

# Scenario 6

Your network has been penetrated.  
All files on each host in the network have been encrypted with a strong algorithm. No decryption software is available in the public. Do not reset or shutdown as files may be damaged.

To get info (decrypt your files) contact us at:

[LindaMcCann@protonmail.com](mailto:LindaMcCann@protonmail.com)

You will receive bitcoin address for payment of 2 bitcoins (\$26k CAD) in the reply letter.

You have 72 hours to pay after which your files will be destroyed.

We have made a copy of the data so if you think about not paying it will be posted on the internet.



# Who to Report to?

Required by Law

**Local law enforcement**



Royal Canadian Mounted Police  
Gendarmerie royale du Canada

Guidance

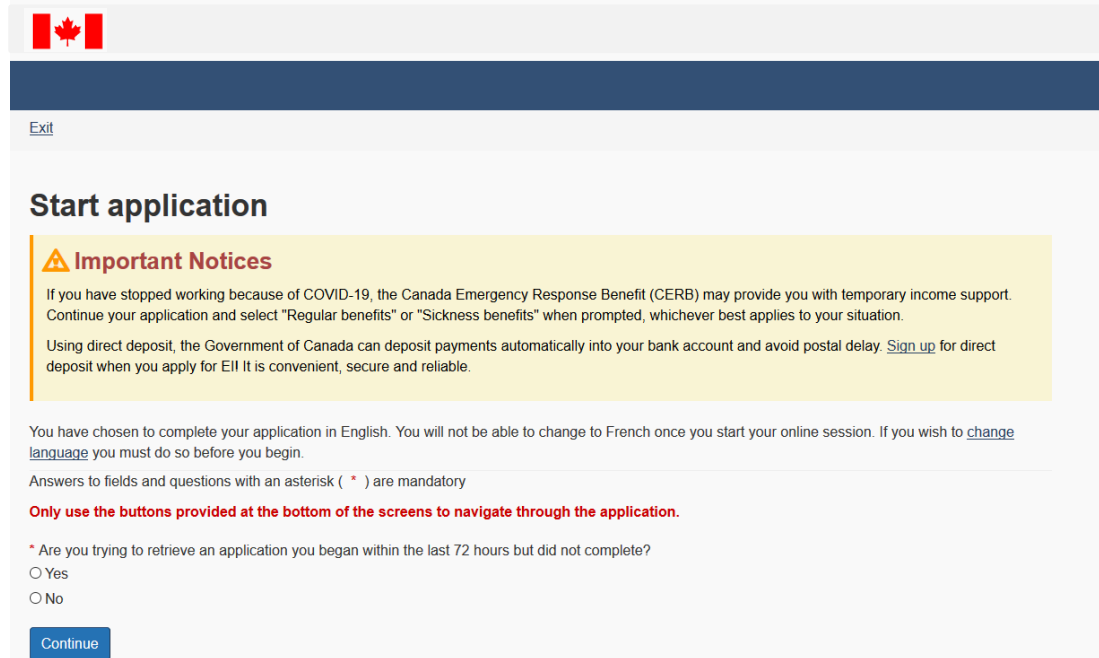
CENTRE CANADIEN POUR LA  
**CYBERSÉCURITÉ**


Support

**MSSP**

# Scenario 7


## ○ Fraudulent website: <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](#)

# Who to Report to?

CENTRE CANADIEN POUR LA  
**CYBERSÉCURITÉ**

## Scenario 8

### ● Fraudulent Call: (Robot call)

The reason behind this call is to notify you that we have registered a criminal case against your name concerning a tax evasion and tax fraud in the federal court house. So if you want any further information about this case, please make sure you give us a call back as quick as possible to our direct hotline number to the Canada Revenue Agency Headquarters. That is 613-927-9919, I will please repeat the number, it is 613-927-9919. If we don't receive a call from your side, please be prepared to face the legal consequences, as the issue of tax is extremely serious and time-sensitive. So have a blessed time.



# Who to Report to?



**Organization who  
supposedly called**

# Scenario 9

- Your organization is a Critical Infrastructure.
  - You are experiencing a cyber incident. Your organization is looking for guidance.
  - You have malware you would like analyzed.


# Who to Report to?



# CONNECT WITH US

 @cse\_cst

 contact@cyber.gc.ca

 www.cyber.gc.ca

 @cybercentre\_ca

To report fraud:

Canadian Anti-Fraud Centre

1-888-495-8501

[www.antifraudcentre-centreantifraude.ca](http://www.antifraudcentre-centreantifraude.ca)

To report a cybercrime:

Local police or

Royal Canadian Mounted Police

[www.rcmp-grc.gc.ca](http://www.rcmp-grc.gc.ca)

To report Spam:

Spam Reporting Centre

[spam@fightspam.gc.ca](mailto:spam@fightspam.gc.ca)

[www.fightspam.gc.ca](http://www.fightspam.gc.ca)