

FISSEA Contest Entry - 2017 &

Name of Submitter: **Gilles Thériault**

Organization: **Employment and Social
Development Canada (ESDC)**

Type of Entry: **Website**

Title of Entry: **ESDC iService Security Portal**

The Home Page %

Departmental Security

Topics

Physical Security
Securing Information
Reporting Security Incidents
Personnel Security
Securing Computers & Devices
Phishing and Spam
Reporting Allegations of Employee Wrongdoing
Emergency Management and Business Continuity

Tools and Resources

E-Learning
Posters and On-the-Job Tools
Easy Action Toolkit for Employees and Managers
Handling of Information and Required Safeguards (PDF, 194 KB)
Information Classification Guide (PDF, 81 KB)
Security Videos

Key Links

Contact Us

Regional Security Offices (RSO)
IT Security Centre of Expertise
NHQ Security Contacts
Branch USB/SDCS/SPOC Coordinators

Departmental Security

Employees and managers all have a role to play in keeping our workplace, our technology, our information and ourselves safe.

Securing our workplace, technology and information				
 Physical Security	 Securing Information	 Reporting Security Incidents	 Personnel Security	 Securing Computers and Devices
 Phishing and Spam	 Reporting Allegations of Employee Wrongdoing	 Emergency Management and Business Continuity	 E-Learning	 Posters and On-the-Job Tools

A Closer Look at the Icons %

Departmental Security

Employees and managers all have a role to play in keeping our workplace, our technology, our information and ourselves safe.

Securing our workplace, technology and information				
 Physical Security	 Securing Information	 Reporting Security Incidents	 Personnel Security	 Securing Computers and Devices
 Phishing and Spam	 Reporting Allegations of Employee Wrongdoing	 Emergency Management and Business Continuity	 E-Learning	 Posters and On-the-Job Tools

Drilling Down One Level %



Securing Information

Securing information not only concerns the proper handling and protection of information but also safeguarding information from creation and storage to disposal. Employees must protect all information, whether it is in a physical form or electronic form.

Do you...

- Store Protected or Classified information and departmental assets securely to ensure they are properly safeguarded?
- Adjust your computer screen or use a closed room when working with sensitive information?
- Understand the "Need-to-know principle"?
- Regularly review and update your user profile, passwords and access privileges?
- Know how to securely store, transmit and dispose of electronic information?

Do you know...

- The sensitivity level of the information you are creating/working with and how to classify that information?
- The type of approved containers to safeguard Protected or Classified information?
- Where and how to share information securely to ensure it is not at risk, including who is authorized to view the information and how it is to be shared?
- How to safely dispose of information based on its level of sensitivity?

Handling of Information and Required Safeguards

The following safeguards and security measures represent the minimum measures that should be applied for each activity related to the handling of information (mailing, faxing, transporting, etc).

Select the level of protection or classification to find what safeguards apply to the securing, transporting, transmitting and storing information.

Protected Information	Classified Information
Protected A	Confidential
Protected B	Secret
Protected C	Top Secret


Dedicated Spam and Phishing Page %

Phishing and Spam






Spam and Phishing are two types of e-mail which are widely used by cyber criminals to compromise personal or business information for the purposes of fraud or theft.

Check out this video and see how employees can [Put a Halt to Phishing!](#) (MP4, 144 MB)

A look at the implications of phishing, and what employees can do to be sure that they do not get "hooked".

 [Transcript](#) (DOCX, 29 KB)

DO...

- Understand the differences between  [spam and phishing](#) (DOCX, 28 KB) and  [recognize clues](#) (DOCX, 166 KB) that can help you
- Know  [what to do with spam or phishing e-mail](#) (DOCX, 28 KB)
- Be suspicious of unexpected e-mail attachments or links from any source
- Be aware of  [targeted attacks](#) (DOCX, 17 KB)
- Remember to  [HALT](#) (DOCX, 17 KB)

DON'T...

- Click on links or open attachments from suspicious e-mails
- Reply to the e-mail
- Provide any personal or business information
- Click "Unsubscribe" on spam e-mails as doing so will validate your e-mail address; simply delete spam e-mail
- Ignore phishing e-mails as you must report it by clicking on the fishhook icon on the [National Service Desk](#) webpage as soon as possible.




Email feels Phish-y? Access the the [Email template to report phishing](#).

ESDC Mock Phishing Exercise Messages

A number of Mock Phishing Exercises were conducted in ESDC to increase awareness of cybercriminal phishing email attacks, which will help to improve the security of our network and information. Below are the messages that were used in our exercises. Each message was based on real-life examples used by cybercriminals. To demonstrate how the message appeared to employees, the e-mails have not been translated. Tips have been added in red to point out the clues that each message was suspicious.

2016

 [December 2016](#) (DOCX, 77 KB)

 [...](#) (DOCX, 22 KB)

2015

 [November 2015](#) (DOCX, 57 KB)

Security Video's Page %

Security



Date: March 2, 2016

Telephone Security: It's in your hands

Passport employees can [view the video here](#) (WMV, 36.5 MB)

(2:59) A look at the implications of telephone scams and what employees can do to protect themselves.

↓ [Transcript](#) (DOCX, 36 KB)



Date: February 2, 2015

Put a Halt to Phishing

Passport employees can [view the video here](#) (MP4, 144 MB)

(2:52) A look at the implications of phishing, and what employees can do to be sure that they do not get "hooked".

↓ [Transcript](#) (DOCX, 29 KB)



Date: January 29, 2015

Physical Security: It starts with you

Passport employees can [view the video here](#) (MP4, 111 MB)

(3:27) Check out the latest video from ESDC – a light-hearted look at the implications of physical security and what employees can do to ensure everyone's safety.

↓ [Transcript](#) (DOCX, 24.7 KB)

Reporting Security Incidents %

Consistent Use of Icons %

Reporting Security Incidents

Security incidents are...

incidents or situations that affect, or have the potential to affect, the department, its assets and/or its employees.

Reporting a Security Incident... Knowing what to do

1. Employee

- Take necessary measures to protect individuals, information and assets
- Call Emergency Services / 911 if necessary and advise your Team Leader / Manager immediately *
- Report the incident to your Team Leader / Manager as soon as possible








2. Team Leader / Manager

- Report the incident immediately to your [Regional Security Office](#) (RSO)
- Call Emergency Services / 911 if necessary and advise your RSO immediately *
- Complete and send the [Security Incident Report \(ADM 3061\)](#) (*opens new window*) form to your RSO as soon as possible

* Only Managers with delegated authority can disclose personal information to the police

As needed, consult the [How to Report Security Incidents for ESDC Employees](#) (PDF, 22 KB) decision making diagram to quickly determine the course of action.

Refer to the table below for more information and guidance on the types of Security Incidents:

Types of Security Incidents		
 Violence or threats of violence Threats or acts of violence	 Involving information	 Loss or theft of public assets and public goods
 User Compromise	 Denial of Service Attack	 Malicious Code
 Loss, Damage or Theft of Departmental Device	 Phishing Attack	 Spam