FISSEA Poster, Website and Security Trinket Contest

Entry Form

PLEASE REVIEW RULES BEFORE COMPLETING ENTRY FORM. **All entries must be received by February 5, 2008.** NO LATE ENTRIES WILL BE ACCEPTED.   E-mail entries to fissea-contest@nist.gov.

Name of submitter: Jane Moser

Organization: Service Canada

Type of entry (poster, website, newsletter, motivational item and/or training/educational exercise/scenario):

> **Website**

Title of Entry:

> **Service Canada IT Security Awareness Program Website**

Description of Entry:

In support of our IT Security Awareness Program, we have a dedicated website. This website is kept current and up-to-date and includes self-study materials, information on course offerings, links to web based training and a password protected trainer's site. Due to the sheer size of our organization (28,000 employees located from coast to coast) this website is a valued communications venue. Let me take you on a quick tour of our site …

Welcome to the Service Canada IT Security Awareness Program Home Page!

- The smiley-face graphic in the top right hand corner tracks the national attendance rate for our End User Awareness sessions, to date we have trained 4,100 employees

- From this page you can access the other sections of the site

IT Security   Sécurité TI de la

Innovation, Information and Technology *Intranet*

Home
IITB Home Page
IT Standards
List of IT Standards

ITSS Home

Contact Us

ITSS Process

Policy, Processes and Governance

IT Security Awareness Program

Perimeter Security Engineering

IT Security Awareness Program

The purpose of this ongoing awareness program is to ensure that all staff better understand IT Security including:

- their roles and responsibilities
- identifying steps they can take to safeguard their environments
- what to do in the event of an IT security breach
- the steps the department already takes to help safeguard the confidentiality, integrity and availability of its IT systems and data.

National Completion Rate End User Awareness Sessions

100%
90%
80%
70%
60%
50%
40%
30%
20%
10%

Registration Information

File   Edit   View   Favorites   Tools   Help

Back   Search   Favorites

IT Standards

List of IT Standards

ITSS Home

Contact Us

ITSS Process

Policy, Processes and Governance

IT Security Awareness Program

Perimeter Security Engineering

Security Engineering

Reference Documents

Other Site Links

FAQ's

Technology Services Directorate
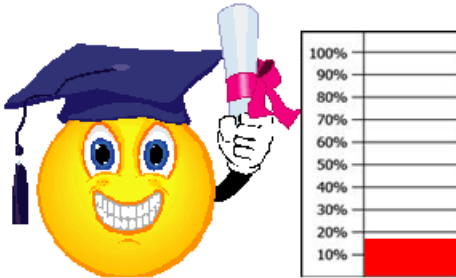
IT Security Awareness Program

The purpose of this ongoing awareness program is to ensure that all staff better understand IT Security including:

- their roles and responsibilities
- identifying steps they can take to safeguard their environments
- what to do in the event of an IT security breach
- the steps the department already takes to help safeguard the confidentiality, integrity and availability of its IT systems and data.

**National Completion Rate
End User Awareness Sessions**

100%
90%
80%
70%
60%
50%
40%
30%
20%
10%

Registration Information

◆ Courses and Other Learning Opportunities
◆ E-Learning - Web Based Training (WBT)
◆ FAQ's (Frequently Asked Questions)
◆ Links
◆ Microsoft Videos
◆ Monthly Tips and Alerts
◆ Newsletters
◆ Posters
◆ Quick Reference Cards and Resource Materials
◆ Roles and Responsibilities
◆ Self-Assessment
◆ Trainers Site

If you have questions or need additional information on IT Security Awareness, please e-mail:

Local intranet

Start   Inbox - Microsoft ...   IT Security Awar...   Microsoft PowerPoi...   EN   12:53 PM   Tuesday

Courses and Other Learning Opportunities

- We have developed awareness materials for 5 audiences: End Users, Managers, Technical Support Staff, New Employees and Executives

- This page identifies the learning opportunities for each audience and links them to related information

File   Edit   View   Favorites   Tools   Help

Back   Search   Favorites

Address http://intracom.hq-ac.prv/sys/dst-tsd/snvd-nvds/itsec/security_awareness/learning_e.shtml

ITB Home Page

IT Standards

List of IT Standards

ITSS Home

Contact Us

ITSS Process

Policy, Processes
and Governance

IT Security
Awareness Program

Perimeter Security
Engineering

Security Engineering

Reference
Documents

Other Site Links

FAQ's

**Technology Services
Directorate**

IT Security Awareness Program

Courses and Other Learning Opportunities

End User

If you work in the **National Capital Region**, you can register to attend a session using the IT Security Awareness Learning Portal.

If you work in one of the **other Regions**, please contact your Regional Coordinator to find out when awareness sessions will be offered in your location.

Portal Login Procedures (NOTE: If you require an alternate method of registration due to accessibility issues, we invite you to register by e-mail at hlor@nexientlearning.com or by phone at 613-288-0451 extension 244.)

Course Description

By the end of this 3.5 hour awareness session you will be able to:

- Recognize your roles and responsibilities in IT security
- Recognize the difference between the levels of sensitive information and how to handle, store and destroy these materials
- Identify existing threats from the "outside world" such as viruses and phishing
- Create a strong password
- Identify steps you can take to safeguard your environment
- Understand what are acceptable and non-acceptable uses of our electronic network
- List some e-mail best practice guidelines
- Identify tips to ensure the confidentiality, integrity, availability of IT systems and data.

Local intranet

Start   Inbox - Microsoft ...   Courses and Oth...   Microsoft PowerPoi...   12:53 PM   Tuesday

Manager

This 3 hour presentation covers:

1. IT Security Awareness Program
2. Manager responsibilities for IT security
3. IT security measures
4. Extra IT security measures – outside premises
5. Security threats – electronic devices
6. IT issues – Cessation of Employment

Recommended add-on training (logicial flow)

- E-Learning - Web Based Training (WBT)
- End user training session (1/2 day)
- RCMP - Security Awareness Training (2 hrs)
- CSE - IT Security Learning Centre
- Introduction to Information Technology Security (IITS)
- IT Security Awareness Tutorial (ITSAT)
- Manager Resource Guide

Technical

Course Description

During this two day course you will learn more about your roles and responsibilities, security basics, risk management, anti-virus applications, incidents, protective measures and much more!

Recommended add-on training (logicial flow)

E-Learning

- Two web based training products have been developed – one for End Users (all staff) and one for Managers

- This page provides links to the WBT's along with information on how to make E-Learning more effective for the learner

IT Standards

List of IT Standards

ITSS Home

Contact Us

ITSS Process

Policy, Processes and Governance

IT Security Awareness Program

Perimeter Security Engineering

Security Engineering

Reference Documents

Other Site Links

FAQ's

Technology Services Directorate

IT Security Awareness Program

E-Learning - Web Based Training

These e-Learning courses are housed on the departmental Online Learning Campus. This user-friendly portal has a Help function which will answer any questions you have about creating an account, logging in and completing a course. *The courses can be found under Departmental Online Courses, Online Learning Campus Curriculum, IT Security Awareness.*

◆ Manager WBT

This web based training can be used as a refresher or reference after attending one of the facilitator-led sessions **or**, as an alternate to attending a Manager's IT Security Awareness Session.

◆ End User WBT

This web based training is to be used as a refresher or reference **after** attending one of the facilitator-led End User IT Awareness Sessions.

To assist you:

Step-by-Step WBT Usage Instructions

E-Learner at Work Sign

Getting the Most out of E-Learning

Don't forget to complete a Learning Report (HRB2791B) following any IT Security Awareness learning event (self-study, course, presentation). The training code is 00577. For more information on how to complete a Learning Report, visit: http://hr.hq-ac.prv/hrb/training/report.asp

Tips and Alerts

- IT Security alerts to staff are posted here after distribution via e-mail or internal communication newsletters
- Various tips and messages are also included for reference

File   Edit   View   Favorites   Tools   Help

Back | Search   Favorites

Address   http://intracom.hq-ac.prv/sys/dst-tsd/snvd-nvds/itsec/security_awareness/monthly_tips_e.shtml   Go   Links

Home

IITB Home Page

IT Standards

List of IT Standards

ITSS Home

Contact Us

ITSS Process

Policy, Processes
and Governance

IT Security
Awareness Program

Perimeter Security
Engineering

Security Engineering

Reference
Documents

Other Site Links

FAQ's

**Technology Services
Directorate**

IT Security Awareness Program

Monthly Tips and Alerts

- Protection of Government Information - November 2007
- Facebook and MySpace - November 2007
- Laptop Incident - October 2007
- Suspicious Telephone Calls - CCIRC Alert - October 2007
- E-Card Spam and Virus Attack Alert - August 2007
- CCIRC Alert - July 2007
- Notice to Remote Users, February 2007
- Spam Update - IITB News, November 27, 2006
- Email Attachment Deletion
- Top 10 Security Pointers
- Password Best Practices
- Your password is like a toothbrush
- Security Vulnerability - WinAmp

Done   Local intranet

Start   Inbox - Microsoft ...   Monthly Tips an...   Microsoft PowerPoi...   EN   12:55 PM   Tuesday

Resource Materials

- Well visited and popular, this page houses:
  - quick reference cards
  - self-study guides
  - checklists
  - IT Security related policies and forms

File   Edit   View   Favorites   Tools   Help

Back   Search   Favorites

Address http://intracom.hq-ac.prv/sys/dst-tsd/snvd-nvds/itsec/security_awareness/ref_card_e.shtml   Go   Links

IT Standards
List of IT Standards

ITSS Home

Contact Us

ITSS Process

Policy, Processes
and Governance

IT Security
Awareness Program

Perimeter Security
Engineering

Security Engineering

Reference
Documents

Other Site Links

FAQ's

**Technology Services
Directorate**

IT Security Awareness Program

Quick Reference Cards and Resource Materials

For Everyone

- Computer Security Terminology W
- E-mail Best Practices Guide
- How do I create a strong password - and, remember it? W
- Information Classification Guide
- IT Security Quick Reference Card W
- I think I have a virus! What do I do? W
- National Security Functions W
- NCR End User Version
- Policy on the Use of the Electronic Network
- Protect Yourself - Internet Safety
- Protect Your Family - Internet Safety
- Protecting Your Home Computer System W

For Managers

- Blackberry Reference Guide
- Delegation and Permissions W
- Manager's After Course Checklist W
- Manager's Checklist for Security Walkabout's W
- Manager's "TO DO" List When Employee Leaves W
- MOU Telework W
- Remote Network Access (RNA) Worker Agreement W
- Threat and Risk Assessment (TRA) Checklist

Local intranet

Start   Inbox - Microsoft ...   Quick Reference ...   Microsoft PowerPoi...   EN   12:55 PM   Tuesday

Self-Assessment

- We are very proud of this self-assessment tool

- We have three different self-assessments: End User, Manager and Technical

- Employees are asked to complete the questionnaire, add up their score and rate themselves against the scale

- We are recommending that all staff be at Level 5

File Edit View Favorites Tools Help

Back | Search Favorites

Address http://intracom.hq-ac.prv/sys/dst-tsd/snvd-nvds/itsec/security_awareness/security-assessment_e.shtml | Go Links

IT Standards
List of IT Standards

ITSS Home

Contact Us

ITSS Process

Policy, Processes and Governance

IT Security Awareness Program

Perimeter Security Engineering

Security Engineering

Reference Documents

Other Site Links

FAQ's

Technology Services Directorate

IT Security Awareness Program

IT Security Awareness Self-Assessment

All employees have a role to play when it comes to IT security. A continuous education program has been established which includes instructor led courses and various other learning materials.

The purpose of this ongoing awareness program is to ensure that all staff better understand IT Security including:

- their roles and responsibilities
- identifying steps they can take to safeguard their environments
- what to do in the event of an IT security breach
- the steps the department already takes to help safeguard the confidentiality, integrity and availability of its IT systems and data.

This assessment has been developed to help you gage your knowledge of IT Security. It is recommended that all staff maintain a skill level of 5.

Stage I: Determine Your Current Skill Level

When you have completed the self-assessment, you will be able to identify if you need to improve your knowledge of IT Security.

IT Security - Self Assessment - End Users
IT Security - Self Assessment - Technical
IT Security - Self Assessment - Managers

▲ Back to Top

Done Local intranet

Start Inbox - Microsoft... IT Security Awar... Microsoft PowerPoi... 12:56 PM Tuesday

File   Edit   View   Favorites   Tools   Help

Back   Search   Favorites

Address http://intracom.hq-ac.prv/sys/dst-tsd/snvd-nvds/itsec/security_awareness/security_e.shtml   Go   Links

IT Standards
List of IT Standards

ITSS Home

Contact Us

ITSS Process

Policy, Processes
and Governance

IT Security
Awareness Program

Perimeter Security
Engineering

Security Engineering

Reference
Documents

Other Site Links

FAQ's

**Technology Services
Directorate**

IT Security Awareness

IT Awareness Self-Assessment

For each question, please select the number from 0 to 5 that best corresponds to your own level of ability. **Please print off a hard copy of the questionnaire, complete the questions and tabulate the results manually.** The scoring table is below.

1. **I understand the scope of my responsibility regarding IT security.**
   (No Knowledge) 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ (Expert Competency)

2. **I understand the possible consequences of breached IT security.**
   (No Knowledge) 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ (Expert Competency)

3. **I know the proper ways of handling and storing sensitive information.**
   (No Knowledge) 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ (Expert Competency)

4. **I am familiar with the various forms of environmental security threats.**
   (No Knowledge) 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ (Expert Competency)

5. **I am familiar with the various forms of human IT security threats.**
   (No Knowledge) 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ (Expert Competency)

6. **I know the basic means by which a virus may infiltrate my computer.**
   (No Knowledge) 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ (Expert Competency)

7. **I know how to respond if a virus is detected on my computer.**
   (No Knowledge) 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ (Expert Competency)

Done   Local intranet

Start   Inbox - Microsoft ...   IT Security Awar...   SERVICE CANADA ...   EN   1:14 PM   Tuesday

13. **I understand the risks of transferring data between home and work.**
(No Knowledge) 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ (Expert Competency)

14. **I know the guidelines for the acceptable use of the electronic network.**
(No Knowledge) 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ (Expert Competency)

15. **I am familiar with the Email Best Practices Guide and create emails that follow the best practices outlined therein.**
(No Knowledge) 0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ (Expert Competency)

Add your score:

TOTAL POINTS	0-14	15-29	30-44	45-59	60-68	69-75
SKILL LEVEL	0	1	2	3	4	5

Add your total score:

69 to 75

Congratulations!:
You have achieved the target skill level for IT Security Awareness

0 to 68

Your Current Skill Level is less than the identified Target Skill Level of 5. It is recommended that you add IT Security Awareness to your Personal Learning Plan

Your Current Skill Level is less than the identified Target Skill Level of 5. It is recommended that you add IT Security Awareness to your Personal Learning Plan

Assessment Scale Defined

0 = No knowledge or experience:
Completely unfamiliar with roles and responsibilities concerning IT Security.

1 = Some familiarity:
Recognizes what is required but doesn't know how to do it.

2 = Basic proficiency:
Knows some of the policies and procedures that are in place but needs a refresher.

3 = A working knowledge:
Understands and performs all or most of what is required but is inconsistent in approach.

4 = Easily and regularly follows the proper procedures:
Knows roles and responsibilites and follows procedures as required with little hesitation.

5 = Expert competency in this area:
Is fully aware of IT Security issues and possible problem areas and reacts accordingly.

Trainer's Site

- Last but not least, we have a password protected Trainer's site

- As we have trainers from across the country, all materials and handouts they require for delivering the awareness sessions can be found and printed from here

- In addition, the various reporting forms are also available

IT Standards
List of IT Standards

ITSS Home

Contact Us

ITSS Process

Policy, Processes and Governance

IT Security Awareness Program

Perimeter Security Engineering

Security Engineering

Reference Documents

Other Site Links

FAQ's

Technology Services Directorate

IT Security Awareness Program

Security Awareness Website for Trainers

Reporting

- Coordinator Monthly Report
- Instructor Report
- ITSS Quarterly Report
- Manager Session Updates
- End User Session Updates

Technical

1. Workshop for Technical Staff - January 11-12, 2006 (NCR)
   a. PowerPoint Presentations with Speaking Notes, Exercises, Handouts
      - presented in module format (same as at the workshop)
      - content based on materials developed by Don Wood from IPC
      - participants to be provided copy of Resource Guide below

2. Material developed by Don Wood, IPC Team
   a. Instructor Guide
      - includes key speaking points for each powerpoint slide
   b. PowerPoint Presentation
      - 100 slides in length (+7 glossary slides), see Instructor Guide for speaking notes and Resource Guide as reference
   c. Resource Guide
      - intended for distribution to all participants
      - includes references from different sources and additional materials which supplement course delivery

File   Edit   View   Favorites   Tools   Help

Address http://intracom.hq-ac.prv/sys/dst-tsd/snvd-nvds/itsec/security_awareness/locked/trainers_e.shtml

- quiz developed to evaluate the knowledge of the participants about various IT Security topics

New Employee Orientation

- PowerPoint Presentation with Speaking Notes
- Information Classification Guide
- IT Security Quick Reference Card

End User

- PowerPoint Presentation with Speaking Notes
- Handouts and Reference Materials
- Resource Guide
- Information Classification Guide - ITLS Version

Manager

- PowerPoint Presentation October 2006
- PowerPoint Presentation with Speaking Notes
- Handouts and Reference Materials

Executives

- PowerPoint Presentation with Speaking Notes

Portable Media

- PowerPoint Presentation with Speaking Notes

Done   Local intranet

Start   Inbox - Microsoft ...   Security Awaren...   Microsoft PowerPoi...   EN   12:57 PM   Tuesday

File   Edit   View   Favorites   Tools   Help

Back   Search   Favorites

Address http://intracom.hq-ac.prv/sys/dst-tsd/snvd-nvds/itsec/security_awareness/locked/end_user_handouts_ref_material.shtml   Go   Links »

Innovation, Information and Technology Intranet

IT Security   Sécurité de la TI

Home

IITB Home Page

IT Standards

List of IT Standards

ITSS Home

Contact Us

ITSS Process

Policy, Processes and Governance

IT Security Awareness Program

Perimeter Security Engineering

Security Engineering

Reference Documents

Other Site Links

IT Security Awareness Program

Handouts and Reference Materials - End User

- ◆ Acceptable Use Guidelines
- ◆ Computer Security Terminology
- ◆ End User Self-Assessment
- ◆ E-Mail Best Practices Guide
- ◆ Evaluation Form
- ◆ Evaluation Form V2 (Includes Self-Assessment Information)
- ◆ How do I create a strong password – and, remember it?
- ◆ Information Classification Guide
- ◆ I think I have a virus! What do I do?
- ◆ IT Security Quick Reference
- ◆ Learning Report (HRB 2791)
- ◆ National Security Functions
- ◆ Protect Yourself - Internet Safety
- ◆ Protect Your Family - Internet Safety
- ◆ Protecting Your Home Computer System
- ◆ Regional Roles and Responsibilities

http://intracom.hq-ac.prv/sys/dst-tsd/snvd-nvds/itsec/security_awareness/locked/documents/email_best_pra   Local intranet

Start   Inbox - Microsoft ...   Handouts and R...   SERVICE CANADA ...   EN   1:24 PM   Tuesday

I hope you enjoyed this quick tour of our website!

As our motto states:

IT Security IS everybody's business!

Jane Moser, Service Canada