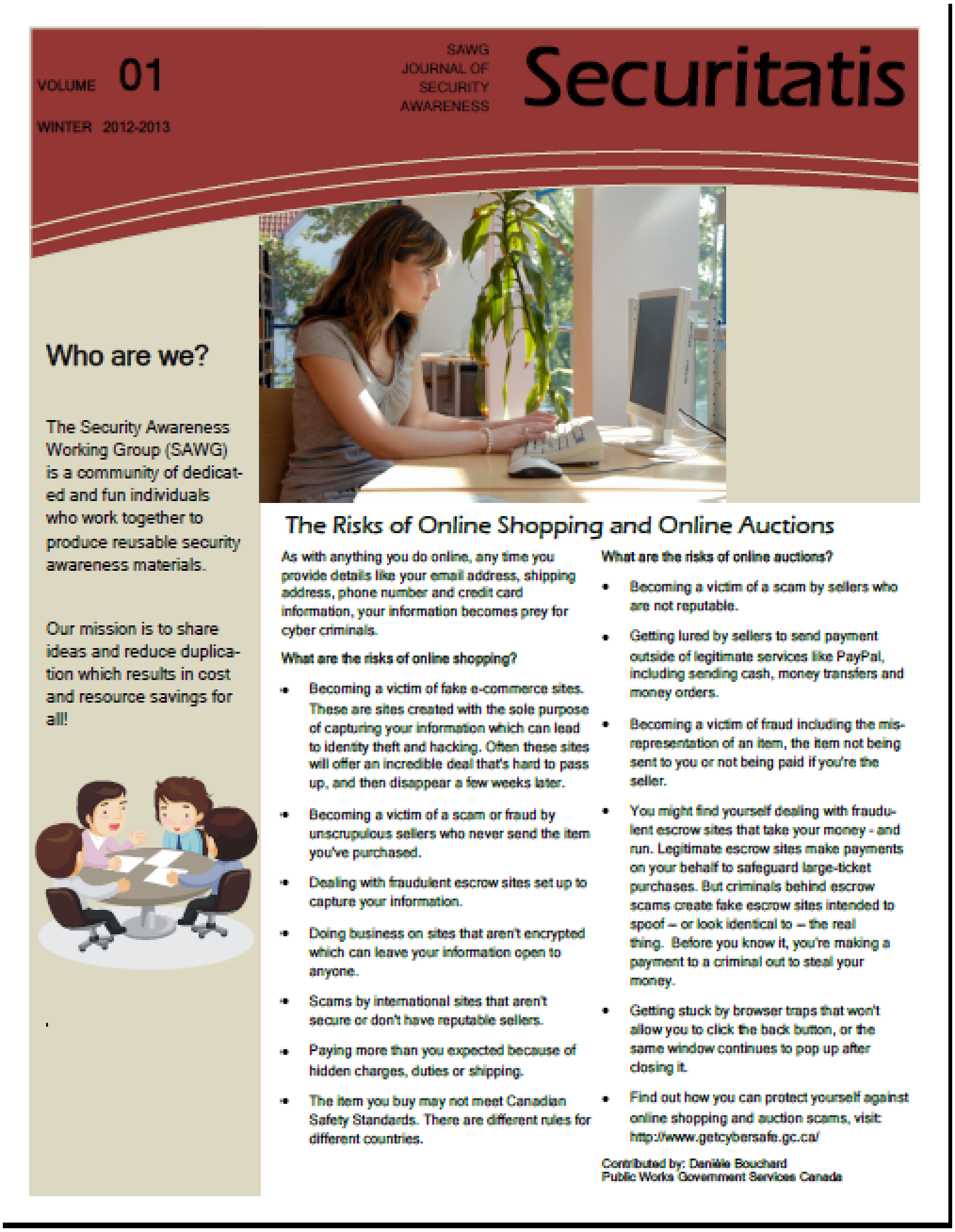
VOLUME 1



VOLUME 01

WINTER 2012-2013

SAWG
JOURNAL OF
SECURITY
AWARENESS

Securitatis

Who are we?

The Security Awareness Working Group (SAWG) is a community of dedicated and fun individuals who work together to produce reusable security awareness materials.

Our mission is to share ideas and reduce duplication which results in cost and resource savings for all!

.

The Risks of Online Shopping and Online Auctions

As with anything you do online, any time you provide details like your email address, shipping address, phone number and credit card information, your information becomes prey for cyber criminals.

What are the risks of online shopping?

- Becoming a victim of fake e-commerce sites. These are sites created with the sole purpose of capturing your information which can lead to identity theft and hacking. Often these sites will offer an incredible deal that's hard to pass up, and then disappear a few weeks later.
- Becoming a victim of a scam or fraud by unscrupulous sellers who never send the item you've purchased.
- Dealing with fraudulent escrow sites set up to capture your information.
- Doing business on sites that aren't encrypted which can leave your information open to anyone.
- Scams by international sites that aren't secure or don't have reputable sellers.
- Paying more than you expected because of hidden charges, duties or shipping.
- The item you buy may not meet Canadian Safety Standards. There are different rules for different countries.

What are the risks of online auctions?

- Becoming a victim of a scam by sellers who are not reputable.
- Getting lured by sellers to send payment outside of legitimate services like PayPal, including sending cash, money transfers and money orders.
- Becoming a victim of fraud including the misrepresentation of an item, the item not being sent to you or not being paid if you're the seller.
- You might find yourself dealing with fraudulent escrow sites that take your money - and run. Legitimate escrow sites make payments on your behalf to safeguard large-ticket purchases. But criminals behind escrow scams create fake escrow sites intended to spoof – or look identical to – the real thing. Before you know it, you're making a payment to a criminal out to steal your money.
- Getting stuck by browser traps that won't allow you to click the back button, or the same window continues to pop up after closing it.
- Find out how you can protect yourself against online shopping and auction scams, visit: http://www.getcybersafe.gc.ca/

Contributed by: Danièle Bouchard
Public Works Government Services Canada

Fishing Warfare?

Phishing is largely a criminal activity employing social-engineering tactics to defraud Internet users of sensitive information and steal credentials, money and/or identities.

A Phishing attack is generally characterized by a **lure, hook,** and **catch:**

The Lure: an enticement delivered through email. The email contains a message encouraging the recipient to follow an included hypertext link. The hyperlink often masks a spoofed uniform resource locator (URL) of a legitimate website.

The Hook: a malicious website designed to look and feel like a legitimate website. The authentic-looking website asks the victim to disclose personal information, such as user identification and password. Often the hook is an obfuscated URL that is very close to one the victim finds legitimate and is really a site under the attacker's control.

The Catch: when the originator of the phishing message uses the information collected from the hook to masquerade as the victim and conduct illegal financial transactions.

Spear Phishing is an email spoofing fraud attempt that targets a specific organization and users, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by organized perpetrators out for financial gain, trade secrets, or national security information. As with the email messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source.

Whaling is a spear phishing attempt to target Senior Executives/Leadership (i.e. the big fish).

Thumb Drives

USB thumb drives have become a popular attack vector for injecting malware on computers located within a protected infrastructure. These same mobile devices have also been used to steal sensitive data and have been responsible for the unauthorized disclosure of information either through a malicious user or when an authorized user unintentionally loses a device containing sensitive information.

What are the security concerns?

- These devices can be very small; therefore, they are more easily lost, stolen, or hidden.
- Their popularity and widespread use make them a popular target for cyber criminals to spread malware. They have even been targeted at the production phase, while they are being assembled, meaning that even a brand new device might have been infected.
- They can now hold a very large amount of data, making them attractive to someone who intends to illicitly steal a large amount of data.
- The average user is unaware of the vulnerabilities associated with these devices; and therefore, may be more likely to be careless, store sensitive information, and less vigilant about keeping work and personal information separate.
- If a USB thumb drive is found, typically the first reaction the finder will have is to view the information to attempt to see who the owner is so it may be returned, or to see if there is any "interesting" information.
- A computer can silently run code from a USB Thumb Drive the moment a device is plugged in, without the user's knowledge or permission.
- Cyber criminals have been known to drop several USB thumb drives somewhere public, close to the intended target, and wait for unsuspecting employees to insert it into their work system in order to install malicious software designed to steal personal information.

Best Practices

- Obtain an approved USB device from your IT branch with encryption and biometric capabilities for all work related activities.
- Never plug an unknown or personal USB device into a work computer - even those that have been offered as a promotional item.
- Always use separate USB devices for work and personal use.

What are the risks associated with Social Media sites?

Identity theft: Posting information such as full name, date of birth, address and phone number can be used by criminals to create a profile in order to access resources or obtain credit and other benefits in that person's name.

Password reuse: Many users of social media sites will use the same password they use for their email, other social media sites, and even their bank accounts. If that password is discovered by computer malware or accidental leak from a website, it provides malicious individuals with a way into all the other sites or even worse a financial institution.

Personal and professional profile overlap: Who you are in the office can be very different from who you are outside of it, and online social networking can focus undesired attention on this distinction.

Scams and hoaxes: Cyber criminals will often attempt to scare or lure social media users in into opening malicious messages in an attempt to extract sensitive information via a malware installation, a phishing attack, or social engineering.

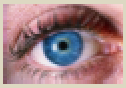
Propagation of malware: Cyber criminals are continually creating new exploits capable of installing malware on a user's computer or social networking account. Real life examples are scripts, which are snippets of computer code that automatically run on your computer when you access a webpage. The objective of malware is often to compromise your account in order to steal your password and other personal information.

Social Media Best Practices

- Familiarize yourself with the social media's policy on security and personal information.
- Never use the same password used for other personal use web services like online banking or email.
- Use secure passwords containing at least 8 alpha-numeric characters and symbols that do not contain names or words to provide more security.
- Make a habit of changing your passwords often, such as every 4 months.
- Never accept the default setting that is typically preconfigured for all new accounts.
- Don't post any information that might cause embarrassment to yourself or others. Remember that once you post a photo or comment, it can't be truly removed. Even if you delete the image or comment, it may have already been downloaded or saved to another user's computer.
- Secure your computer by using up-to-date technical safeguards such as an antivirus and firewall at home.
- Never accept any unsolicited invitations from strangers.
- Avoid sharing personal information, like your phone number, street address, account information, or vacation plans. Consider the risks of becoming a burglar's potential target by posting your full residential address and planned vacation dates.

Contributed by: Michel Lorrain
Senate of Canada

EYE ON:



Social Engineering

Admit it, humans are the weakest link...

Social engineers? The con artists of the electronic age -known for exploiting people's natural desire to help in order to access systems and information. They will use non-technical tactics to obtain passwords, uncover system configurations, and collect any other information that allows hackers to tap into a network.

Some estimates suggest that up to 80 per cent of computer attacks are carried out by insiders. This doesn't mean you should distrust your co-workers, but it does mean you should exercise a degree of caution when asked probing questions about systems and information.

Social engineers are likely to attempt several classic scams: they may pose as a technician on a routine service call or assume the identity of a fellow employee with an urgent problem. Don't be paranoid. But do educate yourself!

Contributed by: Donald Gagnon
Health Canada

Awareness Corner

Privacy Awareness Week:

January 28 - February 1, 2013

Security Awareness Week:

February 11 -15, 2013:

Fraud Prevention Month:

March 2013

Emergency Preparedness Week:

May 5 - 11, 2013

Cyber Security Month:

October 2013

Tips and Tricks

What can I do to protect my Blackberry, PDA, cellphone or laptop?

- Keep your device locked with a strong password.
- Don't store personal information on a handheld device.
- Never use a wireless device to store or send confidential or sensitive information.
- Use data encryption on the device so that data is inaccessible to anyone who finds or steals it.
- Only store corporate information on your handheld device when absolutely necessary.
- Make sure that any corporate information on your handheld device is also stored on the corporate network, where the information is backed up regularly.
- Display your name and phone number on the device so it can easily be returned to you.
- When travelling with your device, store it safely in a secure pocket.
- Use the latest anti-virus software to keep out viruses and malware.

Sites of Interest

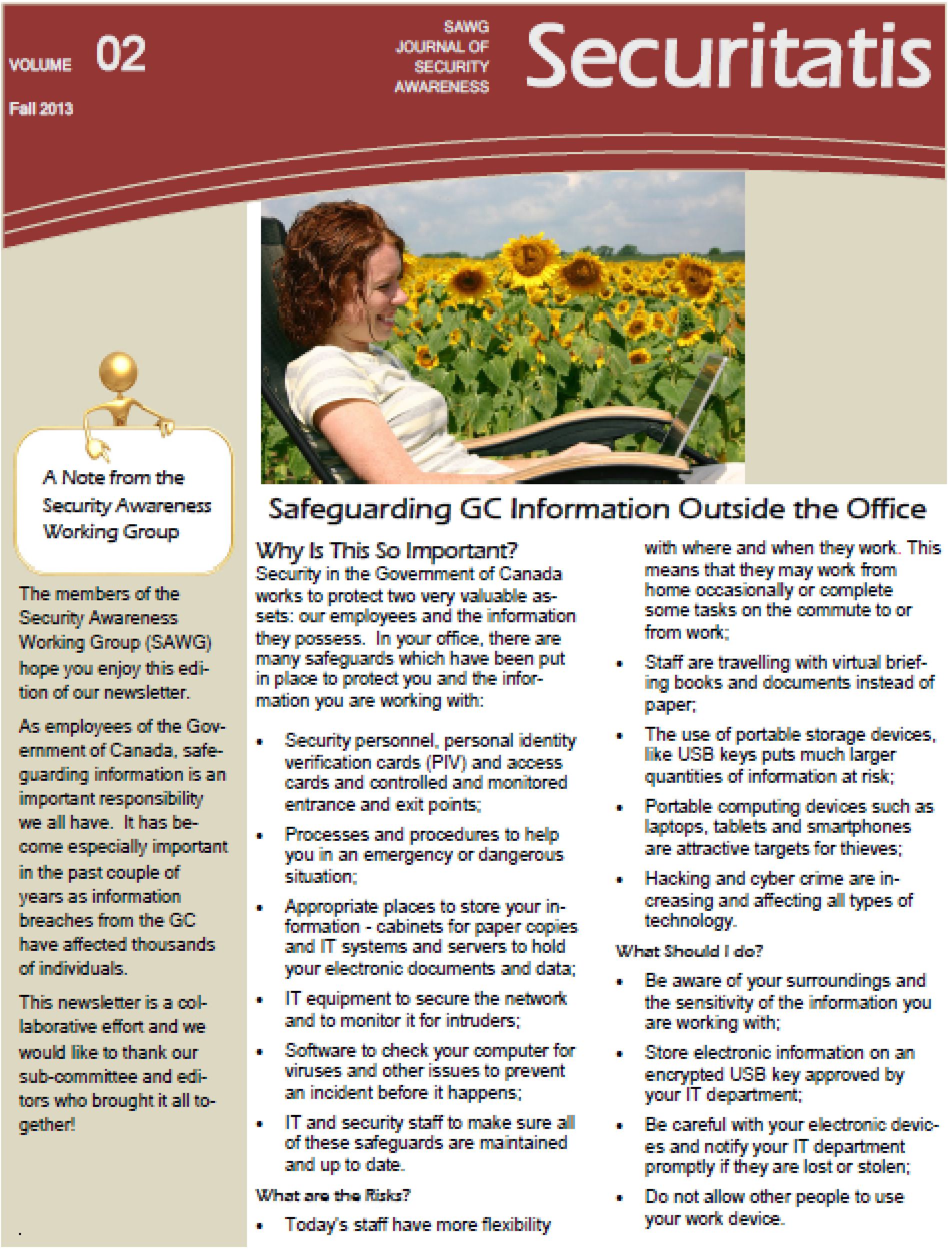
Get Cyber Safe:
http://www.getcybersafe.gc.ca/

Spot Phony Emails:
http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/02607.html

Travel info from the GC:
http://travel.gc.ca/

The Security Awareness Working Group produces reusable security awareness materials while finding innovative ways of bringing awareness to security matters that can impact you in your day to day operations.

VOLUME 2



VOLUME 02

Fall 2013

SAWG
JOURNAL OF
SECURITY
AWARENESS

Securitatis

A Note from the Security Awareness Working Group

The members of the Security Awareness Working Group (SAWG) hope you enjoy this edition of our newsletter.

As employees of the Government of Canada, safeguarding information is an important responsibility we all have. It has become especially important in the past couple of years as information breaches from the GC have affected thousands of individuals.

This newsletter is a collaborative effort and we would like to thank our sub-committee and editors who brought it all together!

Safeguarding GC Information Outside the Office

Why Is This So Important?

Security in the Government of Canada works to protect two very valuable assets: our employees and the information they possess. In your office, there are many safeguards which have been put in place to protect you and the information you are working with:

- Security personnel, personal identity verification cards (PIV) and access cards and controlled and monitored entrance and exit points;
- Processes and procedures to help you in an emergency or dangerous situation;
- Appropriate places to store your information - cabinets for paper copies and IT systems and servers to hold your electronic documents and data;
- IT equipment to secure the network and to monitor it for intruders;
- Software to check your computer for viruses and other issues to prevent an incident before it happens;
- IT and security staff to make sure all of these safeguards are maintained and up to date.

What are the Risks?

- Today's staff have more flexibility with where and when they work. This means that they may work from home occasionally or complete some tasks on the commute to or from work;
- Staff are travelling with virtual briefing books and documents instead of paper;
- The use of portable storage devices, like USB keys puts much larger quantities of information at risk;
- Portable computing devices such as laptops, tablets and smartphones are attractive targets for thieves;
- Hacking and cyber crime are increasing and affecting all types of technology.

What Should I do?

- Be aware of your surroundings and the sensitivity of the information you are working with;
- Store electronic information on an encrypted USB key approved by your IT department;
- Be careful with your electronic devices and notify your IT department promptly if they are lost or stolen;
- Do not allow other people to use your work device.

Telework?

Flexibility in the workplace to accommodate work, personal and family needs can result in benefits to organizations such as:

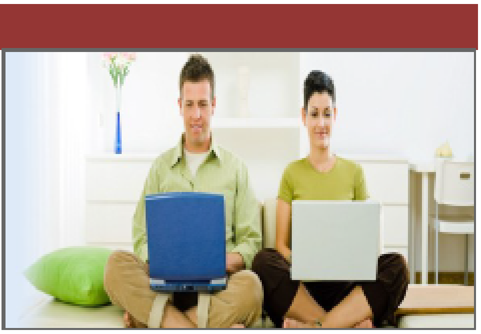
- A competitive edge for attracting and retaining highly skilled individuals;
- Reduced stress levels; Higher levels of productivity and reduced absenteeism;
- Ability to accommodate employment related needs for employment equity designated group members;
- Higher levels of employee satisfaction and motivation;
- A more satisfying work environment;

Both managers and employees are responsible to ensure that operational needs of the organization are met and that neither productivity nor costs are negatively impacted by the application of this policy.

The impact of flexible work arrangements can also reach beyond the benefits derived by the organization and contribute to the development of a sustainable society. For example, opportunities for reducing traffic congestion and air pollution and for supporting regional economic development can be realized at the same time the employer's objectives are met.

Telework Policy – TBS

Working from home? The do's and the don'ts



When you are using a departmental device at home, you are solely responsible for the information you are processing, and should be taking a proactive approach and exercising due caution:

- GC information has been entrusted to you. Do not let anyone have access to the corporate material given to you.
- No other person should have access to your departmental computer/laptop. This includes family members, friends and guests. If maintenance is required take the device in to your department for support.
- Work from an appropriate location like a den or a home office and be aware of your surroundings while you are working.
- Departmental equipment must be used **exclusively** to process departmental sensitive information up to Protected B.
- If you are keeping sensitive material in electronic format on a portable medium (CD's, USB keys, etc.), you must identify this portable medium according to the Government of Canada standards and encrypt the information, if necessary.
- If you are not sure about the standards, check your Service desk for departmental specific info.
- If you have not been given the tool to encrypt information, take the initiative and ask for it! (ex: Entrust, myKey)
- Exercise caution if you have to print sensitive information. Such material must be destroyed, kept, stored and/ or transported in accordance with Government of Canada standards. If you are not sure about the standards, check your departmental-specific information.
- Ensure that your departmental computer is running the latest fixes/ patches and anti-virus updates.
- Make sure that no one can overhear sensitive information, if you are participating in phone calls or teleconferences.

Remember!

Abide by your department's policies regarding the use of department-issued equipment to access personal e-mail systems (examples: Hotmail, GMail or Sympatico).

Social Engineering - It comes in many forms.

GPS:

A fan had their car broken into while they were at a football game. Their car was parked on the green which was adjacent to the football stadium and specially allotted to football fans. Things stolen from the car included a garage door remote control, some money and a GPS which had been prominently mounted on the dashboard. When the victims got home, they found that their house had been ransacked and just about everything worth anything had been stolen. The thieves had used the GPS to guide them to the house. They then used the garage remote control to open the garage door and gain entry to the house. The thieves knew the owners were at the football game, they knew what time the game was scheduled to finish and so they knew how much time they had to clean out the house. It would appear that they had brought a truck to empty the house of its contents.

***Consider this:** If you have a GPS, don't store your home address in it. Use a nearby address like a store or a gas station so you can still find your way home if you need to.*

MOBILE PHONES:

A woman's handbag, which contained her cell phone, credit card, wallet... etc...was stolen. 20 minutes later when she called her husband from a pay phone telling him what had happened, he says, 'I received your text asking about our PIN number and I replied a little while ago.'

The thief had actually used the stolen cell phone to text 'hubby' in the contact list and ask for the pin number. Within 20 minutes he had withdrawn a lot of money from their bank account.

Moral of the story:

Do not disclose the relationship between you and the people in your contact list. Avoid using names like Home, Honey, Hubby, Sweetheart, Dad, Mom, etc.... And very importantly, when sensitive info is being asked through texts, CONFIRM by calling back.

Also, when you're being texted by friends or family to meet them somewhere, be sure to call back to confirm that the message came from them. If you don't reach them, be very careful about going places to meet 'family and friends' who text you.

Tips for Travellers

Before you Leave:

- Review country specific information on the DFAIT website (travel.gc.ca)
- Minimize the number of electronic devices you take with you and remove as much information as possible from them.
- Check with your IT department to see if you can borrow a device while travelling instead of bringing your regular device with you
- Verify costs for blackberry roaming – a calling card may be a more cost-effective solution

While you are Away:

- Be careful with your electronics—don't check them in your baggage and don't leave them unattended.
- Be aware of who might overhear your conversations (taxi drivers, other passengers).
- Remember that internet connections in hotels are not safe and don't have protection from malware.

Awareness Corner

October is **Cyber Security Awareness** Month. The themes for this year are as follows:

- Week 1 – General Online Safety (October 1-5)
- Week 2 – Being Mobile: Online Safety and Security (October 6-12)
- Week 3 – Media Literacy (October 13-19)
- Week 4 – Cyber Crime / Small and Medium Business (October 20-26)
- Week 5 – Cyber Security and Critical Infrastructure (October 27 -31)

Fire Prevention Week 2013 will be observed from Sunday, October 6th through to Saturday, October 12th. The theme for this year is "PREVENT KITCHEN FIRES"

Survey of Canadians and Privacy

The Office of the Privacy Commissioner of Canada commissioned Phoenix Strategic Perspectives Inc. to conduct a survey of Canadians on privacy-related issues. The purpose of the survey was to explore Canadians' awareness, understanding and perceptions of privacy-related issues.

Canadians' knowledge about their privacy rights under Canada's privacy laws is limited, although improving. While one-third (35%) rated their knowledge relatively highly (scores of 5-7 on a 7-point scale), a clear majority (63%) rated their knowledge low on the scale or in the neutral range.

For the full report go to:

http://www.priv.gc.ca/information/por-rop/2013/

Sites of Interest

Get Cyber Safe: http://www.getcybersafe.gc.ca/

Telework Policy: http://publiservice.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12559&section=text#cha1

Spot Phony Emails: http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/02607.html

Travel info from the GC: http://travel.gc.ca/

Privacy Breach http://www.priv.gc.ca/resource/pb-avp/pb-avp_intro_e.asp

Helping youth protect their online reputations

http://www.priv.gc.ca/newsletter-bulletin/2011-9/index_e.asp#privacypreoccupations

The Security Awareness Working Group produces reusable security awareness materials while finding innovative ways of bringing awareness to security matters that can impact you in your day to day operations.

This newsletter reflects security best practices. For specific guidance, contact your Departmental Security Unit.