Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

What kind of information is being collected about me when I'm online?

It's important to know that nothing on the Internet is truly private. All you have to do is visit a web site and, already, information about you is being collected – information like the songs or plug-ins you've downloaded, your computer's technical configurations, addresses of previous sites you've visited, even your e-mail address! Owners of web sites can sometimes view all of these things – and more. If you combine this with information that you've posted about yourself on social networking sites, or information you've submitted to buy things, enter contests, download songs or register for web sites, you'll see that people can find out an awful lot about you if they are so inclined.

How is this information being collected?

In many different ways.

You give it voluntarily: Whether you're playing games on the Internet, or just surfing around, it's easy to forget that others are out there looking for your personal information. Remember this every time you:

- Fill out a registration form to join an online community;
- Create a personal profile to meet others with similar interests;
- Take an online personality test or I.Q. quiz;
- Fill out an online marketing survey that promises points for participating;
- Fill out an entry form for an online contest;
- Fill out a registration form for downloading programs, games or plug-ins;
- Send an e-card;
- Subscribe to a newsletter; or
- Take advantage of "free stuff" being offered – such as audio clips, online quizzes, and discount coupons from online stores or promotional screen-savers.

IP Addresses and Cookies: Many web sites collect personal information – and some are more obvious about it than others. Some web sites ask you for personal information before granting access – you may be asked for your full name, age, address, telephone number, and even about your personal preferences. Others collect information in more subtle ways, such as making a record of your Internet Protocol (IP) address (an address that is unique to your computer or mobile device and can be traced back to you) and of the web pages you visit. They do this by placing "cookies" – small files of text that can collect and store information – on the hard drive of the device you are using. The cookies collect and store information like your IP address ; how many times you visit the site; your preferences, such as preferred language; your user name and password; items in your "shopping cart"; web sites you've visited; your name; and any unique alphanumeric character string that can be linked to your personal information. Check out our fact sheet on cookies, for more information.

Spam: You know those annoying junk e-mails that pop up, unwanted, in your inbox all the time? That is digital spam and you can get it when certain organizations collect, use and disclose your e-mail address without your consent. Sometimes, your address can be gained by web crawling software that mines the Internet for e-mail addresses posted by users in, for example, chat rooms, blogs or social network pages that are unprotected by heightened privacy settings. Spammers can also assemble lists by guessing common names (i.e. John.Smith1) in combination with popular e-mail services (i.e. hotmail.com or gmail.com), hoping to find active accounts. Once you respond to this kind of e-mail, the spammers know the address is in use and can sell this information, along with your profile, to marketers without your consent. All told, when you receive spam, it's best to just delete it rather than open or respond to it. For more information, see our fact sheet Protecting Yourself from Spam.

Phishing: This is an attempt to commit fraud on the Internet, often by someone sending you an e-mail asking for your credit card numbers or passwords. For example, you might get an e-mail from an organization saying that you won the lottery and they need your banking information to deposit the money. The e-mail will ask you to forward them an account number or other personal information that you would never normally give out.

Viruses/worms: This scenario is one everyone wants to avoid: you open an e-mail and it introduces a virus, worm or Trojan into your computer system. These messages may contain attachments that embed malicious code into your computer to corrupt files or hijack your home page or Internet connection. This code can send itself to all the computers in your address book and attack them too. Through these viruses, remote surveillance tools can be installed that monitor and transmit your online behaviour or allow hackers to take control from another computer outside of your home. To protect yourself, run and update antivirus software and don't open e-mails from unknown sources or e-mails that are suspicious.

For more information about how your personal information may be being collected without you knowing about it, check out our Backgrounder on web leakage and the Infographic that illustrates how web leakage can happen.

How is this information being used?

Once information about you has been collected, it can be used, shared – and possibly abused – in countless different ways. Here are just a few:

- It can be used to tailor electronic ads specifically to your habits and interests – and then organizations can use the information they've collected to get those ads to you. For more information on this, check out our fact sheet on behavioural advertising.
- Employers can sometimes access social networking sites to find out more information about the kind of person you are. This is all relatively new, and many companies don't yet have policies about this sort of thing. Right now, the question of whether those party pictures you posted on your favourite site will affect whether you get hired seems to be a case-by-case matter. You might think this is a violation of your privacy, but just think about it for a minute: you are posting pictures on the Internet for all the world to see – you can't really control who sees them so you need to think about what you post.
- Depending on your privacy settings, friends of friends of friends may have access to your online profiles and can find out what you are doing every day. The Internet is such a vast entity, with so many entry points, that it can be difficult to determine what happens to the personal information that is circulating around online. We see media stories everyday about hackers gaining access to supposedly secure web sites and obtaining credit card numbers and other personal information – these stories suggest that few, if any, web sites are completely secure. It can be difficult to predict how a dishonest or disgruntled insider, with legitimate access to your information, could use that information.

What can I do about it?

Fortunately, there is a lot you can do about it! Here are some tips on how you can protect your personal information:

- Make sure that you are dealing with a real company before you give your e-mail address. If you don't know the company, phone and check it out; anything promising instant money is usually a scam.
- Do not open attachments from unknown senders.
- Always read web site privacy policies or statements before submitting personal information, particularly sensitive financial or medical information. If you don't fully understand part of the policy, ask for clarification. Never consent to something you don't understand.
- Install and use anti-spam, firewall, anti-virus and other privacy and security enhancing software, and keep it up to date.
- Download and install critical security patches from your operating system.
- Refuse some or all of the cookies that web sites offer you. Reduce the amount of information you provide and don't provide information that is not required. Check the opt-out provision that limits the use of the information you provide.
- On social networking sites, provide enough information for your friends to identify you – but not so much that someone could use the information to steal your identity. There's no reason to include your entire background, from education to work history.
- Consider making your profile private so people you don't know can't access information and images from it.

- Don’t use the same password for social networking sites that you do for online accounts that have banking and credit card information. Choose strong passwords, in all cases, that include upper- and lower-case letters, along with numbers.
- Use e-mail encryption for particularly sensitive messages.
- Check for updates on privacy policies on the sites you use.
- Use a disposable e-mail address instead of your usual one if you do decide to give contact information to unknown parties on the Internet.
- Always insist on secure, encrypted Web connections to conduct any sensitive transactions, such as online purchases or banking.
- Do not respond to spam in any way. Delete these messages without opening them.
- When forwarding messages, delete the previous recipients’ e-mail addresses.
- Never assume that anything you post online is completely private. Trust your instincts. Remember – ultimately, you are responsible for the information, photos and videos that you post.
- Regularly change your password for accessing your e-mail accounts.
- Be ultra-careful with your Social Insurance Number.