



SPAM

HOW TO **RECOGNIZE IT** AND
BETTER **PROTECT YOURSELF**

What is Spam?

Spam is considered to be any unsolicited commercial electronic message. It is often a source of scams, computer viruses and offensive content that takes up valuable time and increases costs for consumers, business and governments.



There are many things you can do to prevent spam and manage the amount you receive. It is important to do what you can to protect yourself, but also to know how to properly manage the spam you do receive.

The key to preventing and managing spam is to protect:

- *your computer*
- *your email*
- *yourself*

The following guidelines can help you best prevent and manage spam.

Protect your Computer

Never open email attachments from someone you don't know or trust.

An attachment may contain software that could put your computer's performance and your personal information at risk. Malicious software can corrupt your computer or hijack your email account to send viruses to other people. Be aware that spammers can make messages look like they come from people you know - this is called "spoofing." If you are in doubt about an attachment, check with the sender before opening it.

Install anti-spam, anti-virus and firewall software.

Spam often includes harmful programs such as viruses. It is recommended that you use the following three types of protection:

- 1) **Anti-spam software** scans emails before they reach your computer and automatically gets rid of known spam. Most Internet Service Providers (ISPs) offer this service, sometimes for a monthly fee. Many free email services also offer anti-spam services.
- 2) **Anti-virus software** can help protect your computer from computer viruses. It can also help remove known viruses from an infected computer system. Make sure you choose anti-virus software that is up-to-date so that it recognizes current and old viruses.
- 3) A **personal firewall** is a software package that helps you control information that is received and sent from your computer. Make sure to choose a firewall that provides protection for information you receive (incoming) and information you send (outgoing).

Many Internet Service Providers (ISPs) in Canada provide security software to their customers for free. Check with your ISP to find out if they have software available for you to install.

Update your anti-virus program and personal firewall regularly.

New computer viruses are found every day. Many software packages allow you to check for viruses and download updates automatically (auto-update). You may be able to find more details on how to update your software in the information available with each software package.

Disconnect and shut down your computer when you are not using it.

New spam programs and other threats can appear at any time, and no security package is totally safe. Many spammers are using complicated programs which find and take advantage of unprotected computers that have been left turned on and connected to the Internet. If you turn off your computer and disconnect it from the Internet, you'll prevent harmful programs from connecting to and entering your computer system.

Update your Web browser regularly.

Make sure you regularly check for updates to your Web browser. The companies that design Web browsers are always looking for ways to make their software safer in order to protect their customers.

Protect your Email

Delete spam email messages without opening them.

Spam can often have an invisible programming code that allows spammers to validate an email address when a message is opened. A validated email address is more likely to receive spam than one that isn't validated, so be sure to delete the email before opening it. If however, you are receiving emails from a legitimate organization that you have registered your email address with and no longer wish to receive emails from them, you may use their "unsubscribe" service, rather than deleting the messages. Legitimate organizations are happy to keep the amount of unwanted email down.

Turn off the preview pane in your email software.

The preview pane is a window that allows you to preview the contents of an email message without having to open it. The invisible programming code that spammers often use can be activated through the preview pane. Most email programs give you the option of turning off the preview pane. You will find more information on this issue in the documentation for your email program.

Set up filtering options in your email software.

By setting up filtering options in your email software you have a better chance of controlling the spam that you receive. Consult your software's documentation for additional information.

Create an "alphanumeric" email address.

Creating an email address that includes both numbers and letters makes it more difficult for spammers to guess your address. (Example: john72robert@ ____.ca)

Have more than one email address.

It's a good idea to have one email address that you only use for friends and family, a second one that you use for dealing with trusted businesses and a third for other activities such as subscriptions, message board postings, social networking sites and other online services that require an email address. Having a third email account for the other activities may lower the amount of spam received in your email accounts used for dealing with trusted businesses and for communicating with friends and family. Check with your Internet Service Provider (ISP) to find out how you can setup additional email addresses. A number of free email services are also available on the Internet.



Protect Yourself

Never respond to an email asking for your personal information.

Phishers often send authentic looking messages that appear to come from legitimate companies to request personal information or ask you to confirm personal information which is then used for fraudulent purposes. Do not respond to email claiming to be from, for example, your financial institution or other legitimate organizations, asking you to provide your passwords, financial information or other personal information. Your bank should never send you an email asking you to provide this information. Even though your bank may call you if they suspect fraudulent activity on your bank account or credit card, they should never ask you to provide your passwords or account numbers verbally or via the telephone keypad.

If you are asked for this type of information, phone the organization to verify that the request is valid, but **do not** use the email address or telephone contact information provided in the email as it could be false as well. Instead, look up the contact information for the organization on their website, in the phone book or on printed correspondence you may have from them.

Never call a long distance number that you receive through unsolicited email.

Some spammers will send you an email message promoting a service or product that you never asked for. The message may contain a phone number for you to call in order to be removed from the mailing list. Do not call the number as fraudsters may be trying to steal your long distance service, which is known as “toll fraud.”

Beware that 1-900 telephone numbers are connected to pay-per-call services. Pay-per-call services include live

and pre-recorded services such as adult chat lines, vote casting, psychic consultations, horoscopes, soap opera updates, games, donations processing, sports scores, weather forecasts, translation, and media, legal or government services. Understand that you must pay for all calls originating from or charged to your telephone no matter who made the calls or accepted the charges. This also means that if you are the victim of toll fraud, you are liable for the costs.

Create passwords made up of mixed characters and numbers.

The more complex a password is, the harder it is for others to figure out. When possible create passwords of at least eight characters that combine numbers, letters and special characters.

Change your passwords.

This reduces the risk of your passwords being discovered.

Memorize your passwords.

Unless you use secure password management software, storing passwords in a file on your computer is not safe. Your computer could be hacked into or stolen. Memorizing your passwords provides you with the best protection. If you decide to write your passwords down on paper, store the paper in a secure place and do not:

- Store your user name and passwords in the same document or in the same place.
- Include obvious headings on the page such as “my password” or “my user names.”
- Place this information near your computer.