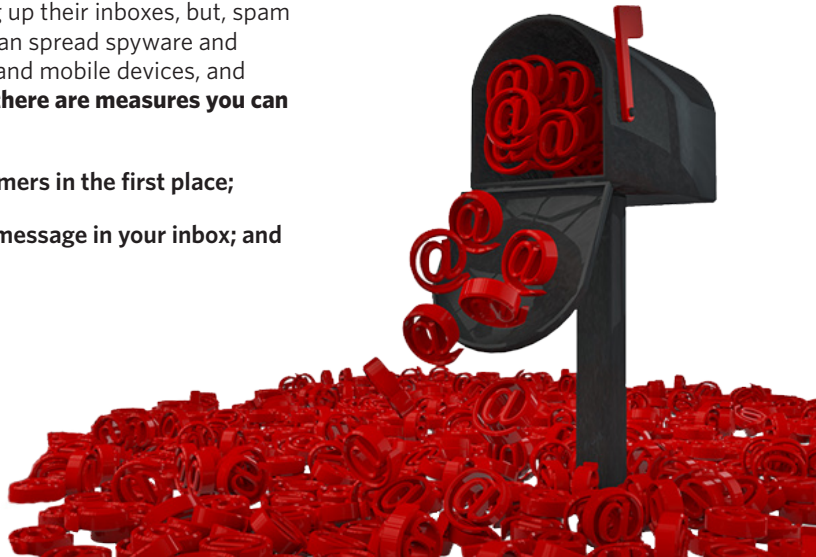
TOP 10 TIPS

to protect your inbox, computer and mobile device

Office of the Privacy Commissioner of Canada

To some people, spam messages are simply a nuisance cluttering up their inboxes, but, spam messages can actually pose a real threat to your privacy. They can spread spyware and other types of malware, which can compromise your computer and mobile devices, and collect your personal information without your knowledge. **However, there are measures you can take to reduce the risk of:**

- **Your email address being collected and targeted by spammers in the first place;**
- **Inadvertently launching malicious software from a spam message in your inbox; and**
- **Your computer or device being compromised.**



Protect your e-mail address from being harvested

Spam starts with a practice called "address harvesting," where computer programs indiscriminately collect email addresses that are sold to spammers. And so, your first line of defence is protecting your email address. Here are some ways to do this:

1. **If posting your email address to a website, do not use the "@" or "." symbols**. Instead, use a format such as "jane **at** myDomain **dot** com". This can help prevent "spambot" software, often used to seek out and extract email addresses online, from recognizing it.

2. Use a **primary email address for your trusted contacts and consider creating additional addresses for use in online activities**, such as filling out forms or joining communities. These addresses can be easily changed if they are harvested and you start receiving spam.

Protect your inbox from being a launchpad for spyware and other types of malware

While address harvesting leads to spam, spam may spread spyware, which can transmit your personal information to unauthorized parties. In some cases, your key strokes can be monitored, revealing sensitive information like account passwords. To help avoid this:

3. First and foremost, **don't open e-mails** from an unfamiliar person or organization. Deleting mail from unknown senders can avoid a host of future problems.

4. But, if you do, **don't reply to spam** as that can confirm your address as being active and cause you to receive more spam. For the same reason, never click on a "remove" or "unsubscribe" link in a suspicious spam message. You may be unwittingly "subscribing" to receiving even more spam.

5. And **don't click on links or attachments** in an e-mail if the message is suspicious. They may be harbouring malware, which, if unleashed from your inbox, can jeopardize your privacy or compromise your device.

6. Malware can even come from the accounts of your friends or other known sources if their computers have been hijacked. So, **if you are in doubt about an attachment,** don't reply to the email itself and before opening it **check with the sender** by phone or in person. In other words, if an email from a trusted source seems out of character it may indeed be from an altogether different character.

7. **Report unsolicited e-mail containing suspicious attachments** or content to the Spam Reporting Centre at **www.fightspam.gc.ca**. By analyzing accumulated reports and identifying trends gathered by the Centre, the Office of the Privacy Commissioner of Canada is working with its enforcement partners to identify address harvesters and sources of spyware for investigation.

Protect your device or computer

Think of these next steps as a sort of insurance policy for your device in the event your first two lines of defence fail:

8. **Install security software from a reliable company on your computer**. Security software should include features like anti-spam, anti-virus, anti-malware and a firewall.

9. Ensure your operating system and other software suites, including security software, are **set to automatically update.** If you're not sure how, use your "Help" function and search for "Automatic Updates."

10. Don't acquire security software in response to unexpected calls, messages or pop-ups. This type of marketing is commonly used for malicious purposes. Instead, **only download security software from web sites you know and trust**. Free software might sound appealing but can hide malware. In the same vein, apps for your mobile device should only be downloaded from reputable marketplaces.

To find out more about the Office of the Privacy Commissioner of Canada's responsibilities under Canada's anti-spam legislation or "CASL", Canada's law against spam and other electronic threats, visit www.priv.gc.ca/casl or call 1-800-282-1376.

For information about CASL overall, visit www.fightspam.gc.ca