

Simple Steps To Keep Your Computer Secure

Internet Security

Through the use of various techniques and technologies, fraudsters trick unsuspecting Internet users into divulging personal and financial information.

Protecting Your Computer

Internet banking provides convenient access to information and the ability to perform transactions from home, work or other locations. Users must be aware that when you communicate via the Internet, other people and software can also communicate with your computer. An inadequately protected computer can be accessed by an unknown party or malicious software (malware) in a very short period of time, and without your knowledge.

To keep your computer free from damaging malware, we recommend diligent use of the following computer and online security practices:

Use a Firewall

When connected to the Internet, users are particularly vulnerable to computer intrusions and attacks because the internet connection provides "always-on" connection capability. The likelihood of a malicious individual accessing your computer increases significantly the longer your computer is on and connected to the Internet. Remember – you can work offline and only access the Internet when you need it.

Ensure your computing system has an up-to-date firewall to prevent others from accessing your computer and your information through the Internet.

- Always ensure your firewall is enabled and up-to-date.

Use Anti-Virus Software

Anti-virus software can protect you from "trojan horses" or other types of viruses, which are programs that allow others to gain control of your computer system remotely without your knowledge or consent. These programs are used to capture and transmit your personal information.

- Ensure your anti-virus software is enabled and configured to run daily updates and regular virus scans.

Use Anti-Spyware

Spyware monitors internet surfing habits and collects personal information from the computer. Typically, spyware is secretly installed and can be difficult to detect.

- Anti-spyware software can detect and remove spyware, but is most effective when combined with a firewall and anti-virus software. Ensure your anti-spyware is enabled and configured to run daily updates and regular spam scans.

Choose Unique Passwords

Choose passwords that are a minimum of eight characters long and include a combination of letters, numbers and special characters.

- Use a unique password for each login ID.
- Disable the web browser "auto complete" function of your login IDs or passwords to prevent others using your computer from having instant access.
- Keep your passwords confidential.
- Change your password regularly, especially if you might suspect it has been guessed or seen by someone else.

Online User Tips

- Do not open unsolicited or unfamiliar email – spam often contains damaging software.
- Do not click on links within unsolicited email – the link may take you to a counterfeit website that will solicit your personal and financial information – this scam is known as 'phishing'.
- Do not click on pop-ups, windows that say "you're a winner if you *click here*" – these can lead to spyware and malware downloads.
- Be wary of 'freeware' or free services online – even innocent looking screen savers, fun cursors and Internet pets can be contain hidden malware.
- Verify the legitimacy of free software, tools and online services before you use them – research the product, tool or vendor in your search engine and scan the results.
- Always carefully read licensing agreements and privacy agreements prior to installing software.
- Avoid conducting online banking transactions at 'hotspot' (high risk) locations such as Internet cafés and libraries.
- Do not forget to log off.

For more information on computer and Internet safety and on avoid other kinds of fraud, please visit the [RCMP's tips page](#) or [Phonebusters](#).