Computer and Mobile Device Security

Internet Security

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

Protecting Your Computer and Web-Enabled Devices

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 device. An inadequately protected device can be accessed by an unknown party or malicious software (malware) in a very short period of time, and without your knowledge.

To help reduce risk from damaging malware, we recommend diligent use of the following security practices:

Computer, Laptop, and Tablet

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.

Install Security Patches

Malware programs commonly target security gaps in operating systems such as Windows and Android, and secondary software such as Oracle Java, Adobe Acrobat/Flash, and Internet Explorer. Installing security patches is an important layer of security in addition to the steps below.

- Configure operating system and secondary software to regularly install security patches as soon as they become available, and consider removing secondary software programs that you do not use.

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 remove and detect 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.

Mobile Phones

Protect Your Password
Protect your data from theft - enable the auto-lock function of your mobile phone to ensure that it locks after a short period of dormancy.

- Do not continue using the default factory password – customize your password immediately using a minimum of eight characters including a combination of letters, numbers, and special characters.

Update Your Operating System
Your operating system (OS) is specific to your device, with BlackBerry, Android, iPhone, and Windows Mobile as examples of various OS. Check your mobile provider's website regularly for OS security updates specific to your device make and model, install security patches as soon as they become available.

- Do not 'jailbreak' your device by trying to remove limitations imposed by the manufacturer. This practice will disable or bypass security measures of your mobile OS, making you vulnerable to malware and prevent your mobile from receiving future OS upgrades.

Use Anti-Virus, Anti-Spyware, and Firewall Software
If available for your make and model, install this software on your mobile.

- Configure to run automatic updates and virus scans.

Download Apps Only from Trusted Sources
Apps that seem legitimate can contain malware or be used to collect your personal data for gain. Beware of apps that provide little company, contact, or website information.

- Research app customer reviews and requested permissions carefully before installing – if the data requested does not align with app functionality, do not install.

Avoid Connecting to Unknown or Non-Password Protected Wi-Fi Networks
Wi-Fi predators scan public networks for unsecured devices to target and infiltrate through hacking and malware. Only connect to public Wi-Fi you know and trust, and are confident is secure and password protected.

- Disable settings that automatically search for Wi-Fi networks.

Avoid Activating Bluetooth in Crowded or Public Areas
The moment you set your Bluetooth to discoverable, hackers within range can ‘see’ and possibly hack your device - mobile viruses can also be spread through Bluetooth technology.

- Never connect to unknown, untrusted or suspicious Bluetooth sources and strangers, and never accept files from these devices.
- Immediately delete lost/stolen Bluetooth device pairings from your remaining Bluetooth devices to prevent data compromise.

Online User Tips

- Do not click links in unsolicited email – the link may take you to a counterfeit website that will solicit your sensitive data, known as ‘phishing’ and cause malware infection.
- Never open MMS attachments from unknown or untrusted sources - even if they purport to be coming from your credit union or mobile provider.
- Delete unsolicited email or text messages without opening.
- Be aware of ‘evil twin’ Wi-Fi hotspots that bait unsuspecting users by impersonating legitimate networks - always confirm you are connecting to the correct network.
- Store only data that your require on your mobile and erase everything else.
- Watch for signs of mobile infection: sudden unexplained increase in your phone bill; unexplained messages in your email and social network ‘sent' folders, unexplained user interface change you didn't initiate. Contact your device manufacturer or service provider for instructions to remove malware if you suspect your mobile is infected.
- Verify the legitimacy of free apps, software, tools, online services before you use them – research in your search engine and scan the results.
- 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.
- Do not forget to log off.

For more tips on computer safety and to avoid other kinds of fraud, visit the Government of Canada Get Cyber Safe and Canadian Anti-Fraud Centre websites.