University of Victoria | University Systems

Safe computing guide

Safe computing tips

Update your software promptly.

Operating system and software vendors frequently release updates that patch security flaws. You can use the automatic update features in Windows and macOS to make sure your operating system is up-to-date, but most applications (such as Google Chrome, Microsoft Office, Adobe Reader, and Java) also need regular security updates. Install updates as soon as possible after they're released: your computer will be vulnerable to security threats until you do.

Use computer security software.

Use security software, such as firewalls and anti-malware software, to protect your computer and data from unauthorized access and threats like viruses and spyware. A security suite like Symantec Endpoint Protection (SEP) will protect your data much better than the basic security tools included in Windows and macOS. All computers purchased through the TSC come with SEP installed, and all UVic faculty, staff, and students can download it for free for personal use as well.

Protect sensitive data.

Your computer contains sensitive data—probably your personal information and stored passphrases, and depending on your job, maybe sensitive data of others. Store restricted data on university servers—they're more secure than your local hard drive or device storage. Avoid using cloud storage services like Box, Dropbox, iCloud, OneDrive, and Google Drive for work-related data. Saving data to your local hard drive, printing it, or transferring it to a laptop or USB key risks the security of that data.

Encrypt your devices.

Encrypt your devices using whole disk encryption (WDE) to help mitigate risks to information associated with physical loss or theft. Whole disk encryption will help prevent an unauthorized third party from accessing the data on your device—even if they have physical access to it. iOS, Android, Windows, and macOS all have built-in whole disk encryption support.

BitLocker Whole Disk Encryption is centrally supported by University Systems and provides benefits such as whole disk encryption, central management, policy enforcement, encryption key management, and recovery. This software comes installed on all standard TSC computers. For more information, see https://www.uvic.ca/tsc.

Back up your data frequently.

Make regular copies of important data and store them securely in a geographically separate location. This will help prevent data loss if your computer is attacked by a virus or trojan, or if your computer's hard disk fails. Enterprise backup services (TSM) are available for faculty and staff. UVic's Personal Home File Storage and Departmental File Storage are automatically backed up.

Manage your account credentials.

Managing your account credentials is increasingly important to help keep your personal information, important files and accounts secure. Where possible, use multi-factor authentication. Choose long passphrases that are easy to remember and difficult to guess. Create a unique and strong passphrase for each account and use a password manager like KeePass to help keep track of them. Never give your passphrase to anyone, for any reason, no matter what.

Control physical access to your computer.

Don't leave your computer, tablet, cell phone, or storage media in an unsecured area, or unattended and logged on, especially in public. Use cable locks to secure notebook computers, even in your office. Ensure that your device is set to lock after a period of inactivity and prompt for a username and passphrase to unlock. Set up a login passphrase or passcode for your tablet or smartphone.

Use email and the Internet safely.

Ignore unsolicited emails. Be wary of attachments, links, and forms in emails, instant messaging services, and social networking sites that come from people you don't know or that seem "phishy." For more information, see https://www.uvic.ca/phishing.

When using your browser to transmit sensitive information, ensure the URL address starts with https:// and look for the lock icon in your browser indicating a secure page. Avoid untrustworthy (often free) downloads from freeware or shareware sites.

Whenever your devices are connected to the Internet, your data can be vulnerable while in transit. Assume that public Wi-Fi is not private or secure. Look at secure remote connectivity and file transfer options, such as VPN services, when off campus. UVic offers a free VPN service—download the client by following the instructions at https://uvic.ca/vpn/.

Helpful security websites

- **Secure your data (UVic):** https://www.uvic.ca/secureyourdata
- **Information Security Office (UVic):** https://www.uvic.ca/systems/about/informationsecurity/index.php
- **Get Cyber Safe (Government of Canada):** https://www.getcybersafe.gc.ca/index-en.aspx
- **Office of the Privacy Commissioner of Canada:** https://www.priv.gc.ca/en/
- **Stay Safe Online (National Cyber Security Alliance):** https://www.staysafeonline.org

Questions?

Computer Help Desk staff are ready to answer questions about information security, as well as help you secure your devices, investigate suspicious links and emails, and respond if your device or account is compromised.

Web	https://www.uvic.ca/systems
Email	helpdesk@uvic.ca
Phone	250-721-7687
Building	Clearihue building, room A037