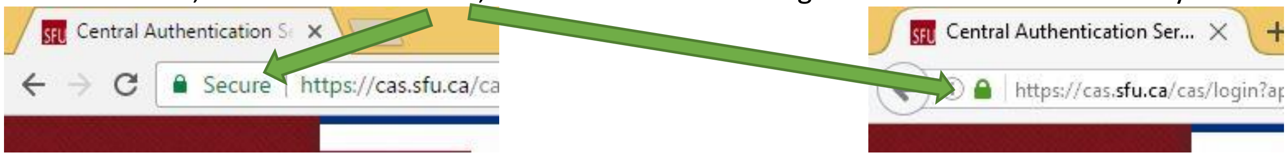
FHS Computing Security Best Practices Guide

Online

Protecting your SFU Computing Account	• Under no circumstances will SFU or FHS ever request our users to provide or confirm their computing ID and password via email. You should never divulge your SFU password to anyone. • If you receive an email message asking for your SFU Computing ID and password : **<u>DO NOT RESPOND</u>**, no matter how official the request seems.
Secure Web Browsing	• Before entering personally identifiable information (eg. Login id, passwords, addresses, birthdates, and payment information), ensure you see HTTPS:// in the address field. The "s" stands for secure. • In addition, look for a visual cues, such as a lock icon or a green bar. This is another way to convey the connection is secured.  Central Authentication S Secure https://cas.sfu.ca/ca Central Authentication Ser... https://cas.sfu.ca/cas/login?ap • Also, double check every web address to ensure you are entering information directly to the first-party.
Email Ransomware	• Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. • Don't open any email attachment you were not expecting or have come from unknown people or from known people that contain suspicious text. **On FHS PCs** – We employ an additional security measure to screen the running of unauthorized programs.
Email Phishing	• Phishing is a type of attack carried out in order to steal usernames, passwords, credit card information, and other sensitive data by masquerading as a trustworthy entity. • Emails indicating your email account is about to run out of space or the account is about to be suspended unless action is taken are not legitimate and not issued by SFU. All SFU faculty and employees will never run out of email storage. Storage is automatically increased with no action on your part. • Don't open links that you are not expecting or are sent by unknown people or known people that are in any weird form.
Tech Support Scams	• Cybercriminals might call you on the telephone and claim to be from Microsoft or Apple. They might also setup websites with persistent pop-ups displaying fake warning messages and a phone number to call and get the "issue" fixed. They might offer to help solve your computer problems or sell you a software license. • Microsoft or Apple will never proactively reach out to you to provide unsolicited PC or technical support. Any communication they have with you must be initiated by you. **On FHS PCs** – Only FHS IT Staff are to provide technical support on FHS PCs. To ensure the integrity and security of information on your PC, do not allow anyone to provide support or install applications to your computer, unless directed by FHS IT Staff.
Mobile Device Security	Regularly check and apply updates to Mobile Device (Smartphone, tablet) System Software and Apps • iOS - https://support.apple.com/en-us/HT204204 • Android - https://support.google.com/android-one/answer/4457705?hl=en

FHS Computing Security Best Practices Guide

Desktop/Laptop

	Purpose	What we do on FHS PCs	What you can do on your home computer
Computer Login	A computer username and password prevents the unauthorized use of your computer.	• SFU Computing ID and Password is required to log on • Screen Saver is enabled • Requiring password to exit screensaver is initially set • Automatic login on computer startup is disabled	• Create a password for your computer login. • If necessary, create separate accounts for different users sharing the same computer • Enable both the screen saver and requiring the password to exit the screensaver • Disable the automatic login on computer startup feature
Antivirus	Windows and Mac computers are susceptible to viruses, malware, and spyware. Enabling and frequently updating antivirus is a must. Do not install more than one antivirus solution as they may interfere with each other.	• Trend Micro OfficeScan is installed on all PCs and is frequently updated automatically	We recommend the following antivirus software • Windows 7 – Microsoft Security Essentials • Windows 8 and 10 – Built-in Windows Defender • Mac - Purchase or download well-recognized free anti-virus or anti-spyware solution
Operating System and Application Updates	Operating system and Application updates often address security vulnerabilities that have been discovered or not previously disclosed. If updates are not installed in a timely manner it can lead to unauthorized access, theft of personal or confidential Information, or the destruction of data.	• PCs are set to check and apply updates to PCs and Software everyday during the overnight hours	Ensure your computer is set to automatically check for updates and apply downloaded updates as soon as possible. • Windows - https://support.microsoft.com/en-us/help/12373/windows-update-faq • Mac – https://support.apple.com/en-us/HT201541 Equally important, ensure third-party software are set to check automatically for updates and have them regularly applied. These include, • Web Browsers (Firefox, Chrome) • Web Plugins (Adobe Flash) • Adobe PDF (Adobe Reader, Adobe Acrobat) • Java • Microsoft Office