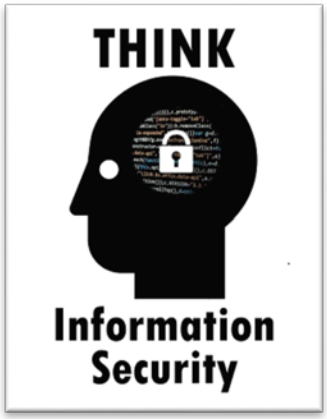
Updated October 2017

Cyber Security Checklist

Stay on track personally & professionally with the latest security requirements by checking off all items on this list.



☐ I use multifactor or two factor authentication whenever possible for accounts with sensitive data.

- ✓ Enable multifactor authentication for all bank accounts, cloud storage and even email.
- ✓ If my password is compromised the second factor provides extra protection.

☐ I use anti-virus & anti-malware software.

- ✓ Use the University's free anti-virus ESET on your home computers.
- ✓ Run a full scan of your computer at least once a month.
- ✓ Set auto updates for virus definitions.
- ✓ Enable anti-virus to on-access scanning.
- ✓ Beware of fake anti-virus software and other rogue programs.
- ✓ Always download software from reputable sources.
- ✓ Acquire anti-virus for your mobile devices too.

☐ I choose strong passwords.

- ✓ Each account should have a unique password. Build your passwords into passphrases. You'll find help in ITS Knowledge Base article (https://www.csusb.edu/kb/36081).
- ✓ Use a password manager like 1Password or KeyPass in creating and protecting your many different passwords.

☐ I use a password-protected screen saver.

- ✓ 'Locking' the screen or using a password-protected screen saver allows you to lock your computer without shutting it down when stepping away from your desk. Press the Windows key + L to lock your Windows computer.
- ✓ Protect your cell phone data, enable a passcode and set it to auto-lock.

☐ I update all software & operating systems on my computers & mobile devices.

- ✓ Regularly update third-party software, especially web browsers, Java, and Adobe products.
- ✓ Enable automatic updates and receive critical patches as soon as they are released to keep my computer's operating system up-to-date and protected.

☐ I protect myself against phishing scams & identity theft

- ✓ Never provide passwords or other sensitive information in response to an email or enter them on an untrusted site.
- ✓ Never respond with personal information nor open attachments from unexpected emails or unsolicited phone calls.
- ✓ Follow appropriate procedures and/or seek independent counsel when unexpected or unusual requests come through.

☐ I clear my private data from Web browsers.

- ✓ Web browsers often store information from Web sites visited (e.g., cookies). Clear this information often, especially if a public or shared computer is used, or set up your browser to do it automatically. Check the browser's help for instructions. Suggest using "anonymous browsing" as an option.
- ✓ Never save passwords in a Web browser.

☐ I only download software from reputable sources.

- ✓ Malware, which includes viruses, spyware, adware, and other malicious software, is often disguised as, or bundled with, legitimate software. Only download software from sources that you trust.

☐ My personal computer has a User Account & an Administrator Account.

- ✓ Create a Limited User Account for everyday use and keep the Administrator access for special tasks (e.g., software installation).

☐ My firewall is turned on.

- ✓ Most computers have a built-in firewall that blocks unauthorized access. Make sure your firewall is on and keep it up-to-date. For more information, check your operating system's Web site.

☐ I use eduroam for wireless when on campus.

- ✓ eduroam is fast, convenient, and secure. Use the setup wizard to configure your computer, then connect automatically from any wireless coverage area on campus. Learn how by reading this article: https://www.csusb.edu/its/support/knowledge-base/28234 or seek assistance from CSUSB Technology Support Center (TSC).

☐ I keep track of sensitive data.

- ✓ Run Identity Finder, a free Campus security tool, to find sensitive data (e.g., Social Security Numbers, credit card numbers) on your Campus computer.
- ✓ Encrypt your sensitive personal data on your home computers.
- ✓ Back up important files to a secure location and delete the files you no longer need.

☐ I don't store sensitive data on USB drives.

- ✓ Any portable storage device can be easily lost or stolen. For grades, finances, and other important data, use a more secure storage space. For University data, talk to your supervisor about recommended storage.

☐ I use digital shredding software or digital cleaner before getting rid of a computer or mobile devices.

- ✓ Manually deleting files on your computer will only remove part of the information. Digital shredding software will completely overwrite your hard drive and make your files irretrievable.
- ✓ Reset mobile devices to "factory" settings to clear out personal information.