

Cyber Security Checkup

Best practices for maintaining security and privacy for you and your family

Passwords and authentication

- PIN- and fingerprint- protect your mobile devices. Longer PINs are more secure
- Use secure passwords. Longer passwords are better. Include numbers and punctuation
- Never use the same password for multiple sites
- Use a password safe to manage your passwords
 - o Keeppass keepass.info/ free open source for PCs and Macs
 - o Lastpass lastpass.com/ free online service - use with multi-factor authentication
 - o Dashlane dashlane.com/ free online service - use with multi-factor authentication
- Use multi-factor authentication (MFA), also known as 2-step authentication, for important accounts
 - o twofactorauth.org/ has a list of services
 - o [UCSB Connect email](#)

System administration and maintenance

- Enable auto-update to get important security fixes
- Regularly update/patch software that does not auto-update
- Install anti-malware software for PC, Mac, and Android devices
 - o Use department supplied software for university computers
 - o Sophos is free for personal use sophos.com/home for PCs and Macs
 - o [Visit the Sophos website to download anti-malware for Androids](#)
- Examine and change default settings
 - o Disable guest accounts
 - o Change default administrator passwords
 - o Disable features that you do not use like file sharing and remote desktop
- Enable encryption
 - o BitLocker full drive encryption in Windows 8 and 10
 - o File Vault full drive encryption in Mac OS X
 - o [Veracrypt for thumb and removable drives](#)
 - o Android device encryption (varies by manufacturer)
 - o iOS devices are encrypted by default
- Enable the built-in firewall
- Back up regularly
 - o Software or services with automatic back up are preferred
 - o Good practice: a second back up to a disconnected removable disk

Wireless and Internet access

- Enable WPA2 on your home wireless router
- Disable universal plug-and-play and device management from the Internet
- [Use web-filtering DNS at home](#)
- [Always use a virtual private network \(VPN\) when connecting to open Wi-Fi hotspots](#)

** Product, services, and websites listed are not endorsements by the University of California.*

General guidelines for online security and privacy

- Check your security and privacy settings periodically. Options and defaults may change
- Use a separate password for each service. Don't use "Log in with..."
- Don't post information that can be used for identity theft
- Don't post information that you use for security questions: pet's name, high school, etc.
- Read privacy policies. Check for data collected, data ownership, and uses of data
- Configure your web browser to send "Do Not Track"
- Use private browsing when accessing sites for which you don't want cookies
- Remember location services and possible consequences of geotagging of photographs
- Use tracking blockers eff.org/privacybadger
- Use SSL/TLS whenever available eff.org/https-everywhere
- Check short URLs at virustotal.com/ before clicking
- Be alert to social engineering including phishing. If it's urgent, it may be a trap
- Check to see if you're a victim: haveibeenpwned.com/
- More information: securityplanner.org/

Privacy settings for products

- Google: privacy.google.com/take-control.html
- Apple: apple.com/privacy/manage-your-privacy
- Microsoft: account.microsoft.com/account/privacy

Privacy settings for LinkedIn

- Click on your picture in the "Me" bar and select "Settings and Privacy," under the "Account" heading
- Review all settings, but pay particular attention to:
 - o The content of your public profile
 - o Who can see your connections (Use "Only you" to respect your contact's privacy)
 - o Profile visibility off of LinkedIn
 - o Sharing with third parties – this can be found under "Manage Your Data and Activity"

Privacy settings for Facebook

- Click the help icon on the top-right side of the screen
- Run the "Privacy Checkup." Pay particular attention to "Your Data Settings on Facebook"
- Review all privacy settings by viewing "Privacy Shortcuts"
- Under "Timeline and Tagging" look at the Review heading and click "View As" to see how your profile appears to non-friends. Look for information you don't want to share
- Review private information in your security settings including passwords for other sites

Privacy settings for Twitter

- Look at the left-hand menu bar and click "More." Select "Settings and privacy" from the menu, then "Privacy and Safety"
- Review all settings, but pay particular attention to:
 - o "Photo tagging," "Protect your tweets," and "Location Information"
 - o Direct messaging settings