

# UC SANTA BARBARA

## Cyber Security Checkup

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

---

### Passwords and authentication

- ✓ PIN or 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 more than one site
- ✓ Use a password safe\* to manage your passwords
  - Keepass <http://keepass.info/> free open source for PC's and Mac's
  - Lastpass <https://lastpass.com/> free online service – use with 2-factor authentication
  - Dashlane <https://dashlane.com/> free online service – use with 2-factor
- ✓ Use 2-Factor (2-step) authentication for important accounts
  - <https://twofactorauth.org/> has a list of services

### System administration and maintenance

- ✓ Enable auto-update to get important security fixes
- ✓ Regularly update / patch software that does not have auto-update capability
- ✓ Install anti-malware software for PC's, Mac's, and Android devices
  - Sophos is free for personal use <https://sophos.com/home> for PC's and Mac's
  - Sophos for Android devices is also free <https://www.sophos.com/en-us/products/free-tools/sophos-mobile-security-free-edition.aspx>
- ✓ Examine and change default settings
  - Disable guest accounts
  - Change default administrator passwords
  - Disable features that you do not use like file sharing and remote desktop
- ✓ Enable encryption
  - BitLocker full drive encryption in Windows 8 and 10
  - File Vault full drive encryption in Mac OS X
  - Veracrypt for thumb and removable drives <https://veracrypt.codeplex.com/documentation>
  - Android device encryption (varies by manufacturer)
  - iOS devices are encrypted by default
- ✓ Enable the built-in firewall
- ✓ Backup regularly
  - Automatic backup software or services are preferred
  - A second backup to a disconnected removable disk is a good practice

### 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 <https://www.opendns.com/home-internet-security/>
- ✓ Always use a virtual private network (VPN) when connecting to open Wi-Fi hotspots. Comparison chart at <https://thatoneprivacysite.net/vpn-comparison-chart/>

---

\* Product, services, and web sites listed are not endorsements by the University of California

# UC SANTA BARBARA

## Cyber Security Checkup

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

---

### 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 <https://www.eff.org/privacybadger>
- ✓ Use SSL/TLS whenever available <https://www.eff.org/https-everywhere>
- ✓ Check short URLs at <https://www.virustotal.com/> before clicking
- ✓ Be alert to social engineering including phishing. If it's urgent, it may be a trap.
- ✓ Are you a victim? <https://haveibeenpwned.com/>
- ✓ More information <https://securityplanner.org/>

### Privacy Settings for Products

- ✓ Google: <https://privacy.google.com/take-control.html>
- ✓ Apple: <https://www.apple.com/privacy/manage-your-privacy>
- ✓ Microsoft: <https://account.microsoft.com/account/privacy>

### Privacy settings for LinkedIn

- ✓ Click on your picture in the menu bar and select "Privacy and Settings," then click "Privacy"
- ✓ Review all settings, but pay particular attention to
  - The content of your public profile
  - Who can see your connections (Use "Only you" to respect your contact's privacy)
  - Suggesting you as a connection
  - Sharing with third parties

### Privacy settings for Facebook

- ✓ Click the help icon on the top-right side of the screen
- ✓ Run the privacy checkup. Pay particular attention to application connections.
- ✓ Review all privacy settings
- ✓ View your profile as it appears to others. Look for information you don't want to share.
- ✓ Review private information in your security settings including passwords for other sites.
- ✓ Review linkages with other services like Twitter and Instagram.

### Privacy settings for Twitter

- ✓ Click on your photo and select "Settings." Select "Security and privacy" from the menu.
- ✓ Review all settings, but pay particular attention to
  - Tweet privacy controls whether your tweets can be publically viewed
  - Photo tagging, tweet privacy, and tweet location