











INITIAL SETUP AND PREFERENCES

- Strong Passwords**
Only use long computer-generated random passwords. 
- Unique Passwords**
Never reuse passwords. Use Keychain or a password manager. 
- Set Up Two-Factor**
Use for your Apple ID, Google, Facebook and everywhere. 
- Disable Automatic Login**
System Preferences, Users & Groups, Login Options. 
- Backup Your Data**
Use Time Machine to back up your drive. Consider online backup too. 
- Enable Find My Mac**
This also allows you to remote wipe your Mac in an emergency. 
- Encrypt Your Drive**
Use FileVault to protect data if Mac is stolen. Optional for desktops. 
- Set Firmware Password**
Locks your Mac to only start from your drive. Optional for desktops. 
- Individual Accounts**
Each person should have their own Mac login and iCloud account. 
- Power Protection**
Use an Uninterruptible Power Supply. Not needed for MacBooks. 

EVERYDAY PRACTICE

- Trust Before Installing**
Only install apps from the Mac App Store or sites you trust. 
- Software Updates**
Install latest macOS updates and of all third-party software. 
- Guest User Account**
Anyone else should only use your Mac as a Guest User. 
- Don't Trust Email, Texts**
Anything in an email/text can be faked. Don't click on links in emails. 
- Don't Trust Ads, Calls**
Ads warning of viruses are fake. No legitimate service will call you. 
- Avoid Online Scams**
Beware of scams involving buying, selling, jobs and offers. 
- Suspect Public Wi-Fi**
Use only https sites and secure services, or install a VPN service. 
- Stay Informed**
Check Mac news sources weekly to keep up with any new threats. 