PRESCOTT MAC USERS GROUP

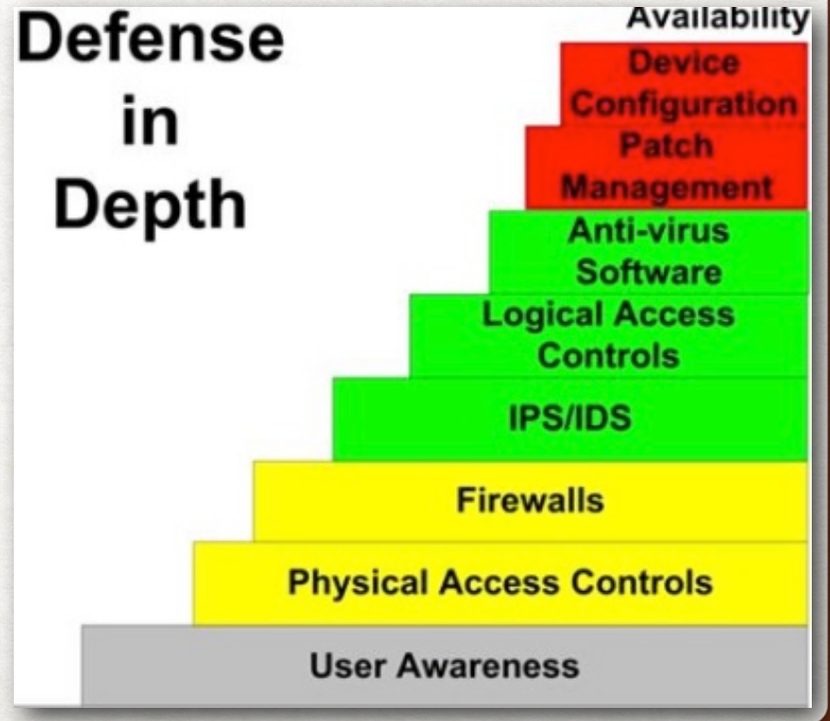
SECURITY ALPHA TO OMEGA

SECURITY OVERVIEW

- What it is
- Components
- Passwords
- 2FA (Two factor authentication)
- Apple solutions built into devices
- Communication issues

FIRST STEPS

- Definitions
  - Security - Freedom from danger or harm - This talk
  - Privacy - freedom from observation or attention
  - Anonymity - Freedom from identification or recognition
- Best defense is a multi-layered defense (not one barrier but many barriers)



RISK LEVEL

- Determine your risk level using the 3 “Ls”
- Likelihood - Probability that someone will violate your security
- Liability - The cost, financial or otherwise, that you would incur if a security breach occurs
- Lost opportunity - what you lose in terms of time and convenience by implementing stronger security

CYBERSECURITY ANALYSIS

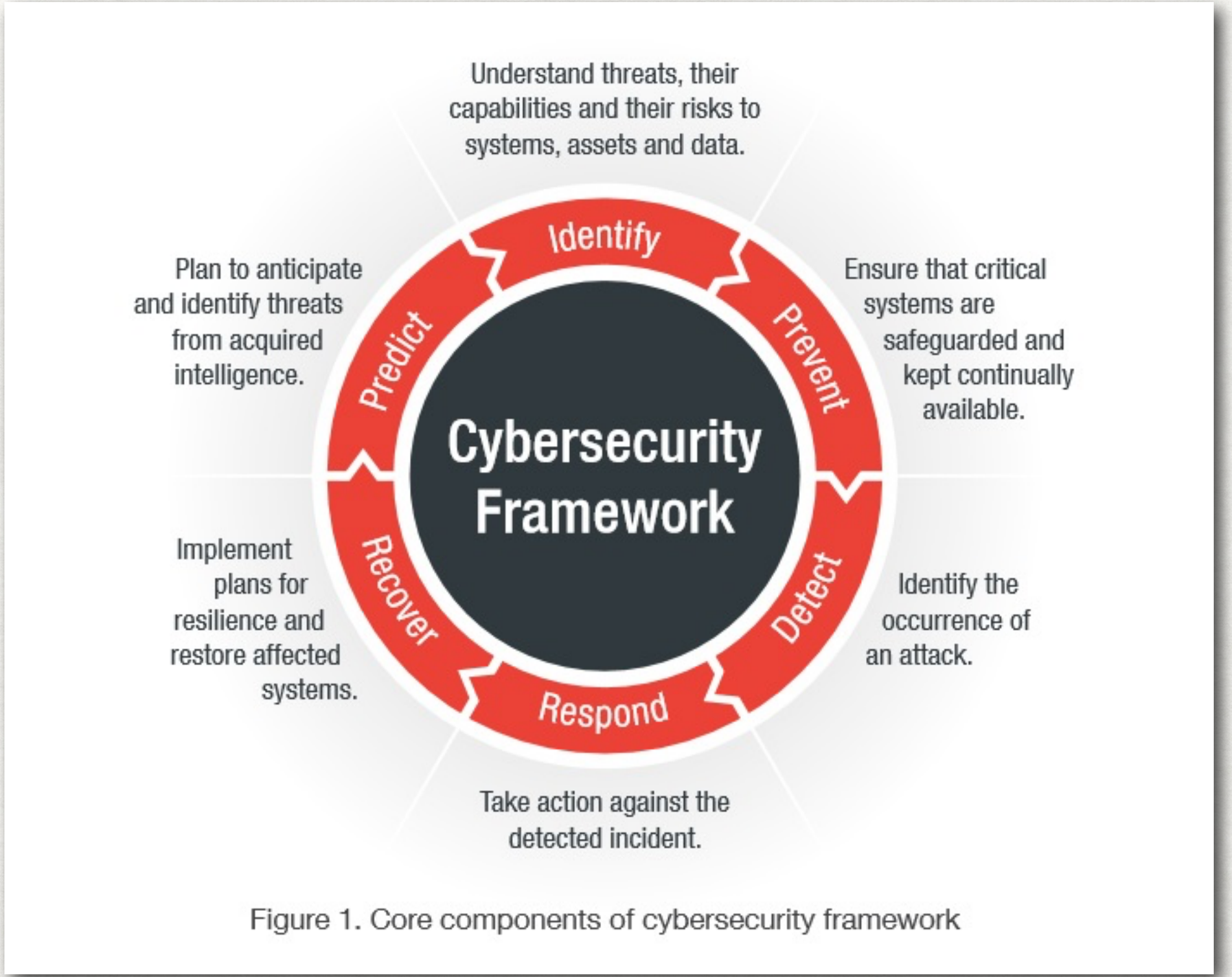
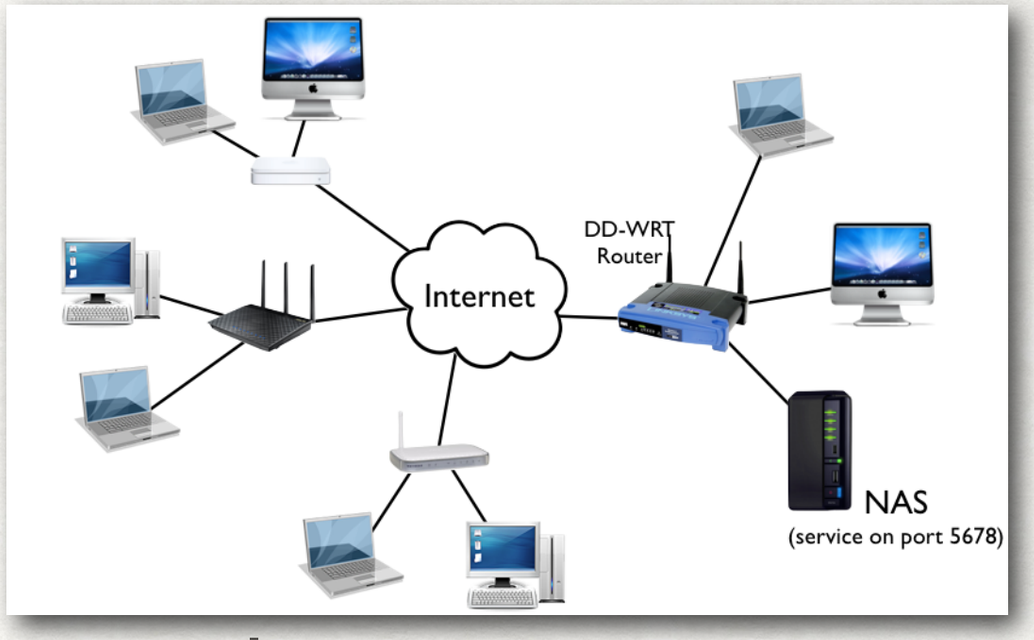


Figure 1. Core components of cybersecurity framework

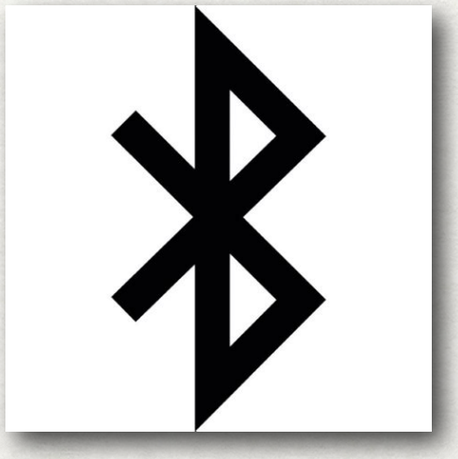
SECURITY COMPONENTS

- Human - PEBKAC
- Computers - Digital & physical access
- iPhone/iPad - losing, dropping, sharing, etc.
- Passwords - EEEEK
- Built in Mac security

SECURITY COMPONENTS



- Communications:
  - BlueTooth & Airdrop
  - WiFi & Router - Set up and control
  - DNS Server - Local or anonymous
  - Internet - IP address shown or VPN



A FEW STATISTICS

- 94% of malware is delivered via email
- Phishing attacks behind 80% of reported incidents
- 60% of breaches due to unpatched software
- Data breaches cost enterprises an average of $3.92 million per breach
- FBI reported hacker attacks increased by 300% last year
- “90-95% of all cyber breaches stemmed from some type of human error of behavior”

A FEW STATISTICS

- “Humans represent the weakest leak in cybersecurity”
- Half of US adults trust public wifi
- Half of US workers share company device with others
- Password reuse and sharing is rampant (⅔ of users)
- “Human intelligence & common sense is best defense against phishing attacks”

HUMAN

- PEBKAC
- Password storage next to computer
- Using short passwords (e.g. 12345)
- Reusing passwords
- Telling a family member or a friend your password(s)
- Letting a family member or a friend on your computer
- Over Sharing on social media (places, times, photos, etc.)

HUMAN

- BE SKEPTICAL - don't trust anyone, any company, any email, any message or any public WiFi
- VERIFY - 2-3 independent sources (Snopes et.al.)
- Do NOT reply to questionable emails or texts
- Do NOT click on unknown links from others
- Do NOT share information about your friends
- Do NOT share information from other social media contacts

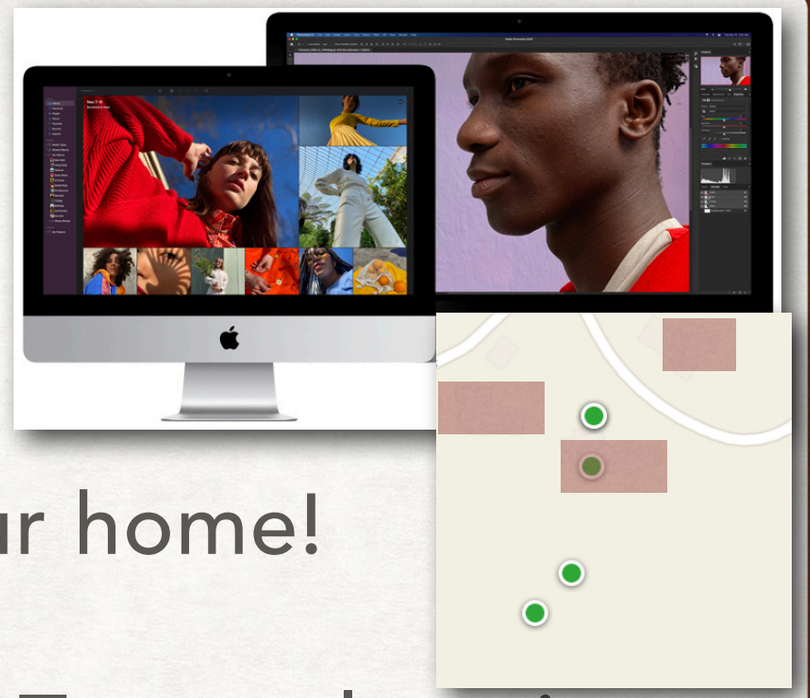
HUMAN

- Lock your system after reboot or wake after sleep
- DO NOT fall for phishing attempts (emails, messages or phone calls)
- NEVER go to unsafe sites (none or bad certificates)
- ALWAYS use intelligence & common sense
- Have a trusted “techie” to run issues by
- ALWAYS do automatic software updates

GULLIBLE HUMAN

Trust your anti-virus software, NOT a phone call from "Apple Support"

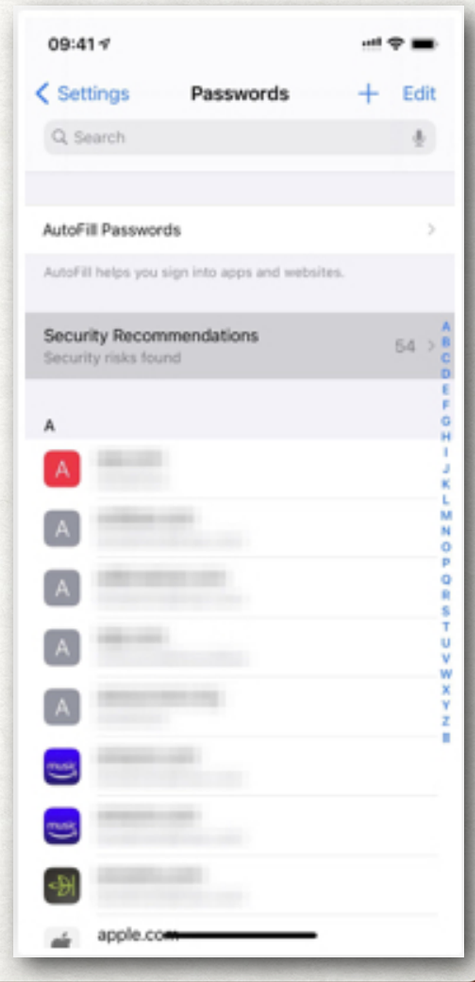
COMPUTER SECURITY



- Physical security of devices - Lock your home!
- Turn on “Find My” on all devices - NOT exact location
- Load & use Virus protection - Sophos recommended
- Load & use Malware protection - Malwarebytes
- Upgrade computer to one with T2 Chip (Intel based computers), or M1 chip - require fingerprint

PASSWORDS

- DO USE a password manager (1Password, Keychain, etc.)
- 12 characters minimum, 16 or longer is better
- Longer Pass Phrases are best (>16 characters)
- DO NOT REUSE your passwords/phrases
- DO USE 2FA in addition to passwords
- iOS - go to Settings/Passwords/Security Recommendations and fix issues



PASSWORD CRACKING

- Brute force - try all possible combinations of numbers, letters, characters
- HSIMP - a web site that tells you how secure your password is
- PA - PassFault Analyzer - much more realistic using today's CPU/GPU speeds and power
- Using a "Pass Phrase" is better - The long ones are best (e.g. "#I lived in Yokohama in 1935#") (29 digits)

PASSWORD CRACKING

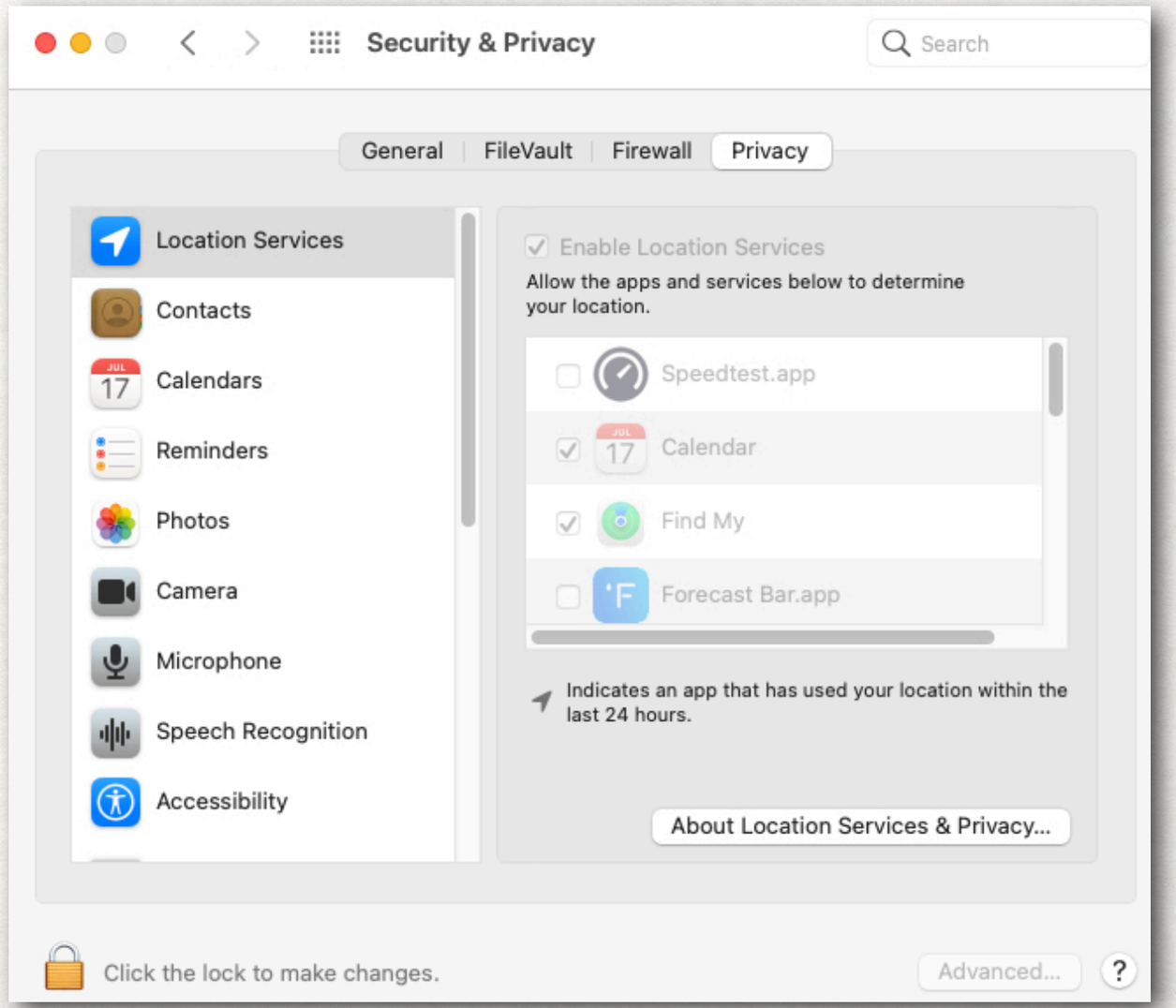
Type	Password	Time (HSIMP)	Time (PA)	Security Level
8 character common word	required	52 seconds	<1 day	Useless
8 random characters	qkcrmztd	52 seconds	<1 day	Useless
8 random chars w/numbers	kqwbv832	11 minutes	<1 day	Useless
8 random chars w/mixed case, symbols, & numbers	J5bZ>9p!	20 days	<1 day	Risky

PASSWORD STRING CRACKING

Type	Password	Time (HSIMP)	Time (PA)	Security Level
Passphrase 1	i own 2 dogs and 1 cat	1 sextillion years	330130 centuries	Secure forever
Passphrase 2	I own 2 dogs and 1 cat!	30 octillion years	8594846 centuries	Secure forever
Passphrase 3	#I own 2 dogs and 1 cat!?	285 nonillion years	1220882818 centuries	Secure forever

MAC SECURITY

- Many capabilities built into MacOS
- Open System Preferences/Security & Privacy
  - General
  - FileVault
  - Firewall
  - Privacy



APPLE BUILT IN DEFENSES

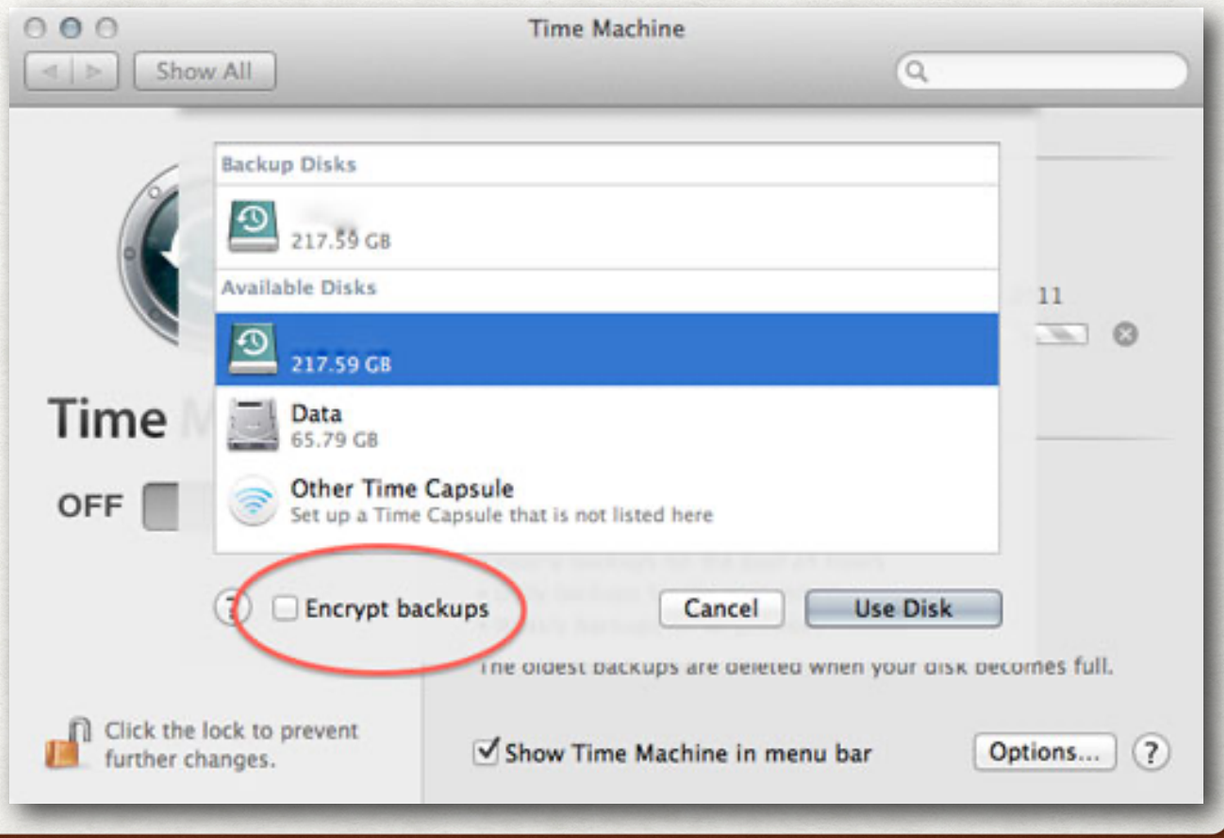
- Gatekeeper - MacOS - Prevents loading software by “unsigned” software companies
- Recovery Key - MacOS - Prevents password change without the key or another device logged into iCloud
- Download ALL Security Updates to software - MacOS & iOS
- TouchID - MacOS & iOS - Disabled after:
  - 5 incorrect attempts or
  - 48 hours of a device not being unlocked or
  - Not entering password/code to unlock for 156 hours

APPLE BUILT IN DEFENSES

- Encryption of iOS backups - MacOS
- Encryption of TimeMachine Backups - MacOS
- Encryption of main disk using FileVault - MacOS
- Apple Pay - MacOS & iOS - merchant NEVER sees the credit card number
- 2FA - MacOS & iOS - Two Factor Authentication - ***requires smartphone*** and to be on you

ENCRYPT YOUR BACKUP DISK

- On your Mac, click on Apple> System Preferences, then click Time Machine.
- Click Select Disk or Add or Remove Backup Disk (if you have multiple backup disks).
- Select your backup disk, then click Remove Disk.
- Set up the disk again as an encrypted backup disk.



ENCRYPT YOUR IOS BACKUP

- Open **iTunes** or **Finder** and connect your iPhone or iPad to your computer.
- Click your device in iTunes or Finder.
- Select **Summary** from the options on the left or at the top in Finder.
- On the right pane, you'll see an option that says **Encrypt local backup**. Tick this option.
- iTunes or Finder will prompt you to set a password for encryption. Enter a password in both fields and click **Set Password**. Save this password somewhere safe as you won't be able to restore your backups without it.
- iTunes or Finder will start backing up your device.

COMMUNICATIONS

- BlueTooth - Check your BlueTooth settings regularly
- Airdrop - Contacts only or none
- WiFi - Good long password - change default
- Router - Changing password more advanced
- IOT - TV, baby monitors, security cameras, video doorbells, garage door openers, thermostats, etc.
- Internet - Use Cloudflare DNS & Reputable VPNs

NEED FOR IOT HOME SECURITY