

PRESCOTT MAC USERS GROUP

# APPLE SECURITY ALPHA TO OMEGA

1

Alpha - the beginning  
Omega - the end



## iOS SECURITY



- Physical Security
  - Hold on tightly in public and use a lanyard
  - Put into zipped, snapped purse pocket or front pocket of pants/dress/etc
  - Carry purse on side away from road
  - NEVER use belt clips
  - NEVER lay your iPhone down in a public place (bar...)
  - Don't wear AirPods or other sound device in public

## iOS HACKING



- NSO - Israeli spyware maker
- Often cracks iOS code and sells solutions to gov'ts
- Cracked iOS 15 & 16.0-16.3
- Usually targeted attacks
- iOS16.4 and security updates fixed the hole (3 months after it had been exploited...)

According to the report from Citizen Lab, a University of Toronto cyber research center, NSO customers “widely deployed at least three iOS 15 and iOS 16 zero-click exploit chains against civil society” throughout 2022. It had not named the victims when it provided Forbes a look at the report prior to release today, but later confirmed Mexican activists were targeted.

The hacks of HomeKit and Find My iPhone, dubbed “PWNYOURHOME” and “FINDMYPWN,” were used in attempts to compromise Apple devices and install NSO’s Pegasus spyware on target phones from June 2022 onwards. Both attacks also exploited iMessage in what’s known as a “chained” attack, where different parts of an operating system are hacked to get more access to a device. In neither case did the user have to click anything to be infected. The HomeKit attack appeared to work regardless of whether or not a user had configured a smart home with the app before.

## iOS HACKING

- Harder if using Touch ID or FaceID
- Probability of Touch ID being wrong is 1 in 50,000!!
- TouchID - MacOS & iOS - Disabled after:
  - After restart
  - 5 incorrect attempts or
  - 48 hours of a device not being unlocked or
  - Not entering password/code to unlock for 156 hours

Every fingerprint is unique, so it's rare that even a small section of two separate fingerprints are alike enough to register as a match for Touch ID. The probability of this happening is 1 in 50,000 with a single, enrolled finger. And Touch ID allows only five unsuccessful fingerprint match attempts before you must enter your password. By comparison, the odds of guessing a typical 4-digit passcode are 1 in 10,000. Although some codes, like "1234," might be more easily guessed, there is no such thing as an easily guessable fingerprint pattern.

## iOS HACKING

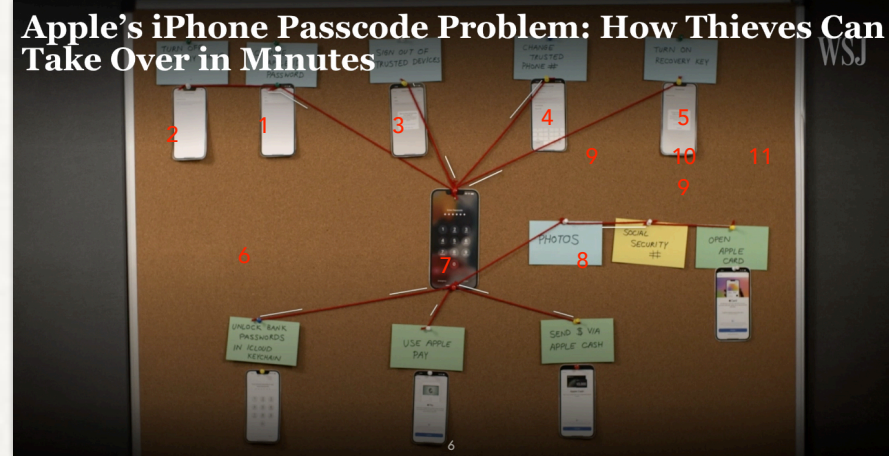
- FaceID more secure (Probability of mis-match is 1 in 1,000,000) than Touch ID. Enter Passcode to turn on if:
  - Device was just turned on or restarted
  - Device has not been unlocked for more than 48 hours
  - Passcode has not been used to unlock in last 6.5 days
  - After 5 unsuccessful attempts to match a face
  - After the device received a "remote lock" command

5

The probability that a random person in the population could look at your iPhone or iPad Pro and unlock it using Face ID is less than 1 in 1,000,000 with a single enrolled appearance whether or not you're wearing a mask. As an additional protection, Face ID allows only five unsuccessful match attempts before a passcode is required. The statistical probability is higher—and further increased if using Face ID with a mask—for twins and siblings that look like you, and among children under the age of 13, because their distinct facial features might not have fully developed. If you're concerned about this, we recommend using a passcode to authenticate. You can also use Face ID without enabling Face ID with a mask

## iOS PASSCODE HACKING

- Problem with Apple's Passcode hacking
- <https://www.wsj.com/articles/apple-iphone-security-theft-passcode-data-privacy-a-basic-iphone-feature-helps-criminals-steal-your-digital-life-cbf14b1a>



## iOS SECURITY

- Use biometrics (TouchID or FaceID) in public
- Be conscious of people behind you
- Use AlphaNumeric passcodes with more than 6 digits
- Hide your iPhone face if you must enter a passcode
- NEVER leave your phone on a bar or table in public



7

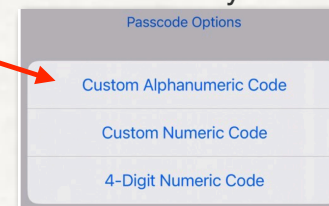
The "hack" involves the thief watching the victim type in their passcode, then steal the iPhone to access their data. In one case, a victim was locked out of her Apple account and lost about \$10,000 from her bank account, according to The Wall Street Journal.

Because the login passcode offers access to most other apps — and system settings — a thief can use it to change the Apple ID password to lock victims out. "Once you get into the phone, it's like a treasure box," said Alex Argiro, who investigated a high-profile theft ring as a New York Police Department detective before retiring last fall.

The thief can also use the device passcode to access iCloud Keychain, which puts a person's entire online life at risk. Argiro said these opportunistic crimes have increased in the past two years in New York. "This is growing," he said. "It is such an opportunistic crime. Everyone has financial apps."

## iOS SECURITY

- Open the Settings app
- Tap the Face ID & Passcode menu
- Enter your current passcode
- Choose Change Passcode
- Verify your old passcode again but don't enter another four-digit code
- Tap on the Passcode Options menu button above the keyboard
- Go for Custom Alphanumeric Code
- Set up a strong password



8

ALWAYS use a custom alphanumeric passcode!!!



## iOS SECURITY



- Extreme security conscious users:
  - Settings>Screen Time>Content & Privacy Restrictions>Turn On
  - Create a new 4 digit passcode ONLY for Screen Time
  - Scroll to Allow Changes> Change Passcode, Account & Cellular to “Don’t Allow”
  - Makes you enter Phone Passcode, then Screen Time Passcode every time you need to change something!
  - Remove checking, savings, credit card account passwords from Keychain

This is the EXTREMELY security conscious people (or ones that frequent bars and other very crowded, populous spaces and events)

## iOS SECURITY

- Use a Recovery Key
- Go to Settings>your name>Password&Security>Recovery Key>On
- Creates a 28 character code you can use to recover your AppleID account
- **WRITE IT DOWN or PUT IT IN A PASSWORD MANAGER!**
- **HOWEVER**, if you use a 4-6 digit numerical Passcode that a thief can see and use after stealing your phone, it is useless!!! **USE ALPHANUMERIC PASSCODE!!**

10

If you forget your Apple ID password, you can try to regain access using your trusted device protected by a passcode. Or you can use your recovery key, a trusted phone number, and an Apple device to reset your password. Make sure the device is running iOS 11 or macOS High Sierra or later, and be sure to enter the complete recovery key including upper-case letters and hyphens. Learn more about what to do if you forget your Apple ID password.

## iOS SECURITY

- Use Screen time which adds another Passcode
- Settings>Screen Time>Use Screen Time Passcode
- Set the passcode, but NOT the iPhone Passcode
- Enter AppleID credentials
- Go to Content & Privacy Restrictions and turn on
- Scroll to Allow Changes Menu & change Account Changes & Passcode Changes to "Don't Allow"

This next trick is likely to prove a headache in the short-term, but the long-term payoff could be the protection of your Apple ID.

As the WSJ notes, you can use a Screen Time Password to add one additional layer of security to your Apple ID. Annoyingly, doing so means you'll have to enter your Screen Time Password any time you want to make innocent changes to your Apple ID, but that's a worthy sacrifice for such a helpful stopgap feature, in our book.

## iOS SECURITY

- NEVER use public charging cables or USB ports
- These ports are being used to spread malware and monitoring software
- Commonly known as “juice jacking”
- Carry and use your own charger and cable to use with an electrical outlet
- If you must use a public one, use USB data blockers



12

One of the most popular ways people boost their devices' batteries is by using the USB power plugs, usually found at hotels or airports, and other public places. As much as they offer a quick and easy way of charging up your devices, they're not safe. A 2019 travel advisory from the Los Angeles' District Attorney's Office warned travelers about the possible dangers of using USB ports in public places owing to the threat of juice jacking via these USB plugs. That is why you need a USB data blocker to protect your data from hackers who may steal your data through these USB power plugs. “Just by plugging your phone into a [compromised] power strip or charger, your device is now infected, and that compromises all your data” according to FBI.

A USB data blocker is a device that allows you to plug into USB charging ports including charging kiosks, and USB ports on gadgets owned by other people. The main purpose of using one is to eliminate the risk of infecting your phone or tablet with malware, and even prevent hackers to install/execute any malicious code to access your data.

## iOS SECURITY

- Use a Password Manager so passwords can be stronger
  - 1Password, Dashlane, mSecure, etc (not Lastpass!)
- Use strong passwords (>10 letters, numbers, symbols)
- Set your Password Options: Settings>Passwords>
- Manage your Passwords: Settings>Passwords> Security Recommendations



13

From banking sites to dating apps, you need different login information nearly everywhere you go on the internet. Creating unique and strong passwords can get tricky fast. Some people use simple passwords that are easy to remember, and others memorize one complex password and use it everywhere online. Either option is a recipe for disaster in the form of identity theft or an account takeover. A Password Manager solves these issues.

Password managers are apps that generate new, random passwords for all the sites you visit. They store these credentials for you in a secure virtual vault. Then, when you visit a site or open an app where you need to log in, the password manager automatically fills in your login name and password for you.

## iOS SECURITY

- Manage your Passwords: Settings>Passwords
- Since following accounts are ONLY protected by your Passcode, delete following from Passwords:
  - Bank Accounts
  - Credit Cards
  - Cash Apps (Zelle, etc)
- Keep the above passwords ONLY in a Password Manager

14

From banking sites to dating apps, you need different login information nearly everywhere you go on the internet. Creating unique and strong passwords can get tricky fast. Some people use simple passwords that are easy to remember, and others memorize one complex password and use it everywhere online. Either option is a recipe for disaster in the form of identity theft or an account takeover. A Password Manager solves these issues.

Password managers are apps that generate new, random passwords for all the sites you visit. They store these credentials for you in a secure virtual vault. Then, when you visit a site or open an app where you need to log in, the password manager automatically fills in your login name and password for you.

## iOS SECURITY

- Keep your iOS up to date (Settings>General>Software Update On)
- Keep your Apps up to date (automatic)
- Enable “Find My” (Settings>Name>Find My> Find My iPhone On)
- NEVER “jailbreak” your iPhone or iPad
- Never use a public WiFi unless you have an active VPN
- Turn off WiFi when away from home - use Cellular
- Add a hardware “Security Key”



15

All of the above recommendations will keep you as safe as is humanly possible at this date and time.

Jailbreaking turns off all the Apple security features. BAD idea!!!

Cellular connection is inherently secure since it is encrypted. Public WiFi is not encrypted and anyone with the right software can capture everything you transmit over a public WiFi. If you use a VPN with a public WiFi, the VPN creates an encrypted tunnel from your computer through the public WiFi to the VPN servers, thence to your web site.

Security keys are only needed if you have top secret data on your iPhone, and you know someone will try to hack into you...

## iOS SECURITY

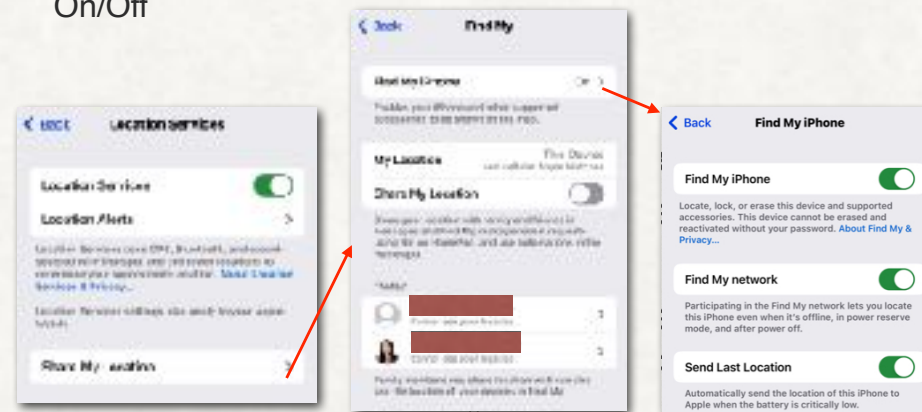
- Review App Tracking permissions:
- Settings>Privacy & Security>Tracking>Allow Apps to Request to Track Off





## iOS SECURITY

- Location Sharing: Settings>Privacy & Security>Location Services>On
- >Share My Location: Find My iPhone On; Share My Location On/Off



Location Services should always be on, Location Alerts>Show Map On

Share My Locations>Find My iPhone On

My Location should say this device (and if you have a watch, then that too!)

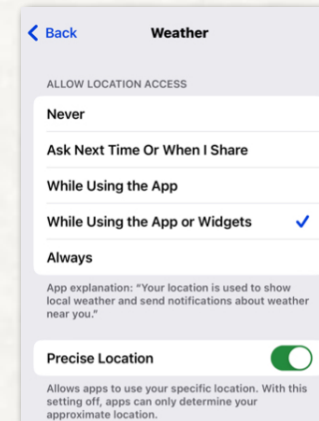
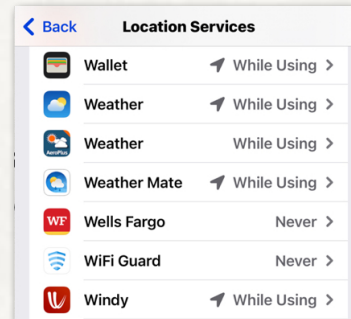
Share My Location on/off depending on your situation.

If you turn a Family member on to share your location, it will send them an email to get agreement.

Find my iPhone all 3 should be on!!

## iOS SECURITY


- Individual Apps to Never, While Using or Always (only trusted apps)
- Precise Location OFF for most apps



18

Note the little arrow meaning my location was used by that app recently. If the app does not need your location, turn it off. If it does, use While Using. I do not let any app have Always. It uses battery, and can set you up to be followed by the App.

I let my weather App use my Precise location since I am 500 feet above and 5 miles away from Prescott - different weather. Most of my apps only use Approximate (about Ten Square Miles which is a circle with a ~3.6 mile diameter). Maps uses Precise.



## iOS SECURITY

- Location Sharing: Settings>Privacy & Security>Location Services - scroll all the way to bottom
- >System Services>Significant Locations>Off
- This file can be read by the same companies that are allowed to write to them, then sold to others on the dark web
- Allows tracking over time!

There are several companies that build libraries for creating smartphone apps where they insert code that records user location data from the apps made using them. While some developers use these libraries for advertising or to track this information themselves, sometimes they aren't aware that the location data of their users is being collected.

Once location data is collected, it's then sold off to third parties who do some work to anonymize it and then resell it themselves. Data brokers also buy location information directly from mobile carriers but these datasets are compiled using data from their cell towers as opposed to from the apps installed on your smartphone.

For instance, The New York Times (opens in new tab) wrote a piece back in 2019 on a dataset that contained over 50 billion location pings from more than 12 million phones that was purchased from a location data company. By analyzing this data, The Times Privacy Project was able to follow the movements of users over a period of several months in 2016 and 2017 to see where they went and how long they stayed at each location.

## iOS SECURITY

- Set up your biometrics (face or fingers) - more secure than passcodes
- Use Passkeys, or if not available, passwords with 2FA.
- 2FA REQUIRES that you always have your phone when you login!!
- Turn iCloud Backup On: Settings>name>iCloud>iCloud Backup On
- iCloud Backup happens every night when your iPhone is connected to your WiFi AND power

20

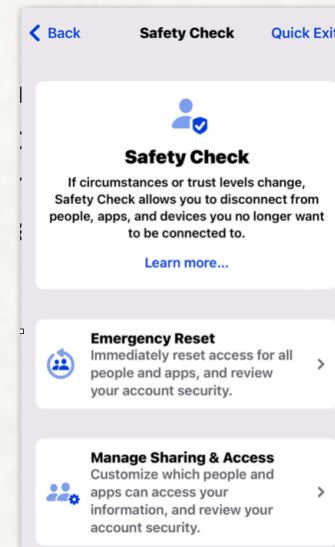
I use two different fingers for touch ID, and two different looks (with/without glasses, or with/without beard). However, the more biometric measurements you make, the less secure your iPhone is.

If you are using 2FA, make sure you keep your iPhone with you!!

If your iPhone is not backing up (Settings>AppleID>iCloud>iCloud Backup under Back Up Now is the when the last successful backup was done), check your WiFi bars at the place you plug it in. It could be too weak a signal to backup (at least 2 bars). You can also do a Back Up Now when you have bars!!

## iOS SECURITY

- If you suspect you have been hacked, do an Emergency Reset - Settings>Privacy & Security>Emergency Reset
- Do the Safety Check at least once a year - Settings>Privacy & Security>Safety Check>Manage Sharing & Access



21

Safety Check allows you to quickly check who you've shared information with. The feature also allows you to restrict Messages and FaceTime to your iPhone, reset system privacy permissions, and change passcodes and passwords associated with your iPhone and Apple ID.

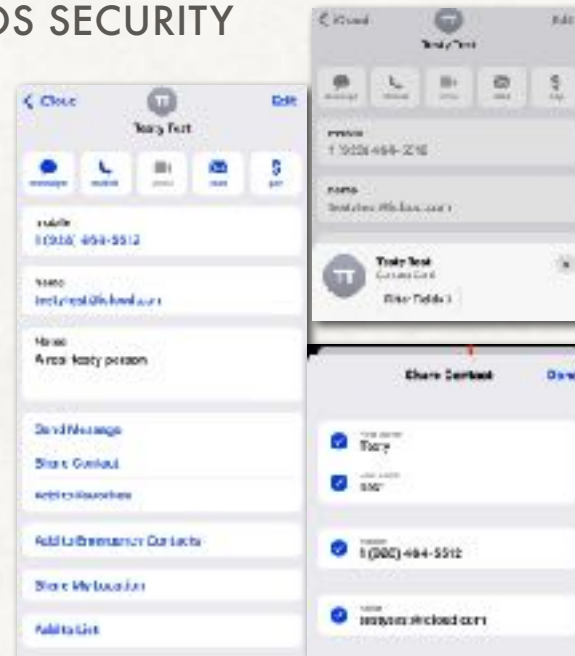
Safety Check can quickly halt information sharing with others in the following apps:

- Health - shared health information
- Home
- Calendar - shared calendars
- Find My - shared location via Find My
- Notes - shared notes
- Photos - shared photos albums

Safety Check can also remove all data gathered by the following apps and features: Bluetooth, Camera, Contacts, Files & Folders, Local Network, Location Services, Apple Music, Motion and Fitness, Reminders, Research and Speech Recognition

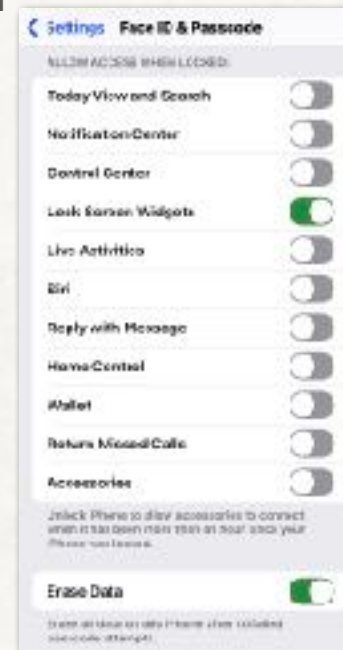
## iOS SECURITY

- When you Share Contact (at bottom of contact) with someone else, make sure you “Filter Fields” to restrict some of the data in the contact



## iOS SECURITY

- Review data seen on lock screen:
- Settings>Face ID & Passcode - scroll to bottom, and turn off Access When Locked items
- After you confirm you did an iCloud backup the previous night, Turn on Erase Data



23

Most of these are up to you depending on how you use your iPhone. If you have FaceID, there is no need to have any of them on since as soon as you raise the iPhone to view any of them, you unlock it as well! If they are turned on, then anyone who picks up your phone can see them (who needs to see your wallet or Today View???)

Accessories & Control Center MUST BE TURNED OFF ALWAYS - that is how hackers can break into your iPhone in minutes using specialized hardware from an Israeli company.

A thief can use this to their advantage by using Control Center to switch your iPhone to Airplane Mode and stop it connecting to the internet, so the security conscious should turn it off. Turning off Accessories also stops any nefarious plug in devices being used on the phone while locked to control and even unlock it.

## iOS SECURITY

- Prevent Cross-Site Tracking On
- Clear Browser History and Website Data regularly
- Settings>Safari>Clear History and Website Data
- Clears all data from iPhone and iCloud and other devices signed into iCloud!
- Still have all your Bookmarks from the iCloud!

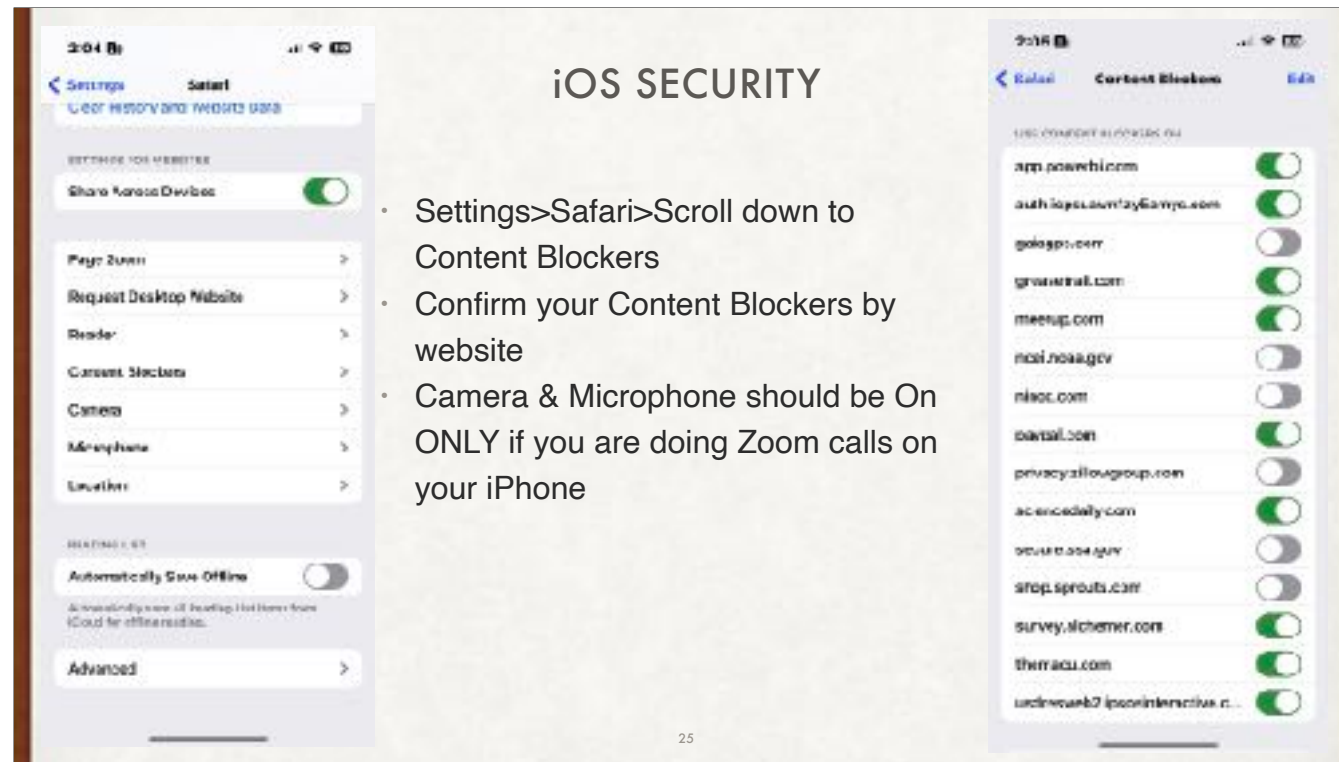


24

Most of these are up to you depending on how you use your iPhone. If you have FaceID, there is no need to have any of them on since as soon as you raise the iPhone to view any of them, you unlock it as well! If they are turned on, then anyone who picks up your phone can see them (who needs to see your wallet or Today View???)

Accessories **MUST BE TURNED OFF ALWAYS** - that is how hackers can break into your iPhone in minutes using specialized hardware from an Israeli company.





Most of these are up to you depending on how you use your iPhone. If you have FaceID, there is no need to have any of them on since as soon as you raise the iPhone to view any of them, you unlock it as well! If they are turned on, then anyone who picks up your phone can see them (who needs to see your wallet or Today View???)

Accessories **MUST BE TURNED OFF ALWAYS** - that is how hackers can break into your iPhone in minutes using specialized hardware from an Israeli company.

## APPLE PAY INSTEAD OF CREDIT CARD



- More privacy
- Secure connection
- Merchant never sees card number
- Easy to use with NFC scanner
- Can use out of touch of internet
- No hidden charges
- Can pay using iPhone or Apple Watch

### 1. Payment Made Easy

You can store your debit or credit card in the Apple Wallet for purchases. To make payments via Apple Pay, simply move the phone close to an NFC scanner, and use the iPhone's Touch ID to accept or make purchases. It's as easy as that. You may no longer need to carry debit/credit cards anymore, as most stores accept Apple Pay.

### 2. Secured Connection

Since you don't need a physical debit/credit card, there's a reduced risk of someone stealing your card(s) or their information. In fact, Apple Pay doesn't use your card number to make a purchase; rather, it uses a token called a "device account number" to complete the transaction. This significantly decreases the likelihood of information theft or a security breach.

### 3. You Can Use It Offline

People love the fact that you don't need an internet connection to make payments. With Apple Pay, you can make purchases even when you're offline, including while your phone is in airplane mode.

### 4. No Additional or Hidden Charges

Apple Pay deducts approximately 0.15% from each purchase, which results in less money for a merchant. But because Apple worked with major credit card companies and banks to give their users a convenient experience, there are no other hidden or additional charges for using the app.

### 5. Privacy

Apple doesn't monitor your purchases or store details, so you can make payments with confidence. Also, using device account numbers instead of the credit/debit card or number itself helps prevent cyberattacks.

### 6. Availability

Apple Pay is accepted nearly everywhere today, with more stores jumping on the bandwagon every day.

### 7. Apple Watch

You don't even need to take out your phone. One of the many conveniences is using your Apple watch. How?

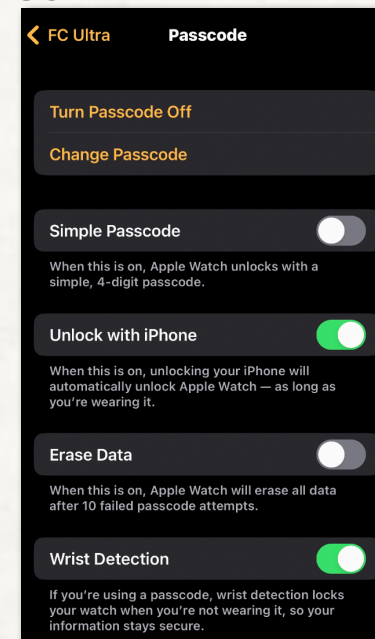
Double-click the side button to open your default card

Scroll down if you want to choose another card.

Hold the display of your watch near the contactless reader until you hear a beep.

## APPLE WATCH SECURITY

- Activation Lock: Watch can only be paired with one iPhone at a time
- 6+ digits for Passcode recommended
- Turn on Wrist Detection



27

Apple Watch only supports numeric passcodes. If you require an iPhone passcode that uses letters or special characters, you can't set an Apple Watch passcode. Instead, you must unlock your iPhone to unlock their Apple Watch. Open the Apple Watch app on the paired iPhone, tap the My Watch tab, then tap Passcode > Unlock with iPhone.

Wrist Detection is the other way to keep your data safe. As soon as it no longer detects your nice warm wrist (1-2 seconds), it locks. Turn it on!!