iPad Security Guide

Use the built-in privacy and security protections of iPad

iPad is designed to protect your data and your privacy. Built-in privacy features minimize how much of your information is available to anyone but you, and you can adjust what information is shared and where you share it. Built-in security features help prevent anyone but you from accessing the data on your iPad and in iCloud.

To take maximum advantage of the privacy and security features built into iPad, follow these practices.

Protect access to your iPad

- *Set a strong passcode:* Setting a passcode to unlock iPad is the most important thing you can do to safeguard your device.
- *Use Face ID or Touch ID:* Face ID (supported models) or Touch ID (supported models) provides a secure and convenient way to unlock your iPad, authorize purchases and payments, and sign in to many third-party apps. See Set up Face ID on iPad or Set up Touch ID on iPad.
- *Turn on Find My iPad:* Find My helps you find your iPad if it's lost or stolen and prevents anyone else from activating or using your iPad if it's missing.
- *Control what features are available without unlocking your iPad:* Disallow or allow access to some commonly used features, such as Control Center and USB connections, when your device is locked.

Keep your Apple ID secure

Your Apple ID provides access to your data in iCloud and your account information for services like the App Store and Apple Music. To learn how to protect the security of your Apple ID, see Keep your Apple ID secure on iPad.

Make account sign-ins safer and easier

For participating websites and apps, there are multiple ways to make sign-in more convenient and secure.

- *Sign in with passkeys:* Passkeys let you sign in to website and app accounts with Face ID or Touch ID instead of a password. Because a passkey doesn't leave the devices where you're signed in with your Apple ID, and because it's specific to the website or app you create it for, it's protected from leaks and phishing attempts. And unlike a password, you don't have to create, guard, or remember it.
- *Use Sign in with Apple:* You can use your Apple ID instead of creating and remembering user names and passwords for signing in to accounts. Sign in with Apple also provides the security of two-factor authentication, and it limits the information shared about you.
- *Let iPad create strong passwords:* If passkey support or Sign in with Apple isn't available when you sign up for a service, let iPad automatically create a strong password that you don't have to remember.

For all your website and app passwords, there are many other ways to make sign-in safer and easier.

- *Replace weak passwords:* If you create any weak or compromised passwords, iPad automatically identifies them for you to fix.
- *Share passkeys and passwords securely:* Use AirDrop to securely share a passkey or password with someone using their iPhone, iPad, or Mac.
- *Use the built-in authenticator for two-factor authentication:* For websites and apps that offer two-factor authentication, fill in automatically generated verification codes without relying on SMS messages or additional apps.
- *Keep passkeys and passwords up to date on all your devices:* iCloud Keychain automatically keeps your credentials up to date across your other devices.

Manage the information you share with people and apps

- *Control app tracking:* All apps are required to ask your permission before tracking you or your iPad across websites and apps owned by other companies for advertising or to share your information with a data broker. You can change permission later, and you can stop all apps from requesting permission.
- *Control what you share with apps:* You can review and adjust the data you share with apps, the location information you share, the hardware you share, and how Apple delivers advertising to you in the App Store, Apple News, and Stocks.

- *Review the privacy practices of apps:* Go to the app's product page in the App Store for a developer-reported summary of the app's privacy practices, including what data is collected. For the apps that you download, review the App Privacy Report, which shows you how apps are using the permissions you granted them.

Protect your email privacy

- *Protect your Mail activity:* Turn on Mail Privacy Protection to make it harder for senders to learn about your Mail activity. Mail Privacy Protection hides your IP address so senders can't link it to your other online activity or use it to determine your exact location. Mail Privacy Protection also prevents senders from seeing whether you've opened the email they sent you.

- *Hide your personal email address:* When you subscribe to iCloud+, Hide My Email allows you to generate unique, random email addresses that forward to your personal email account. You don't have to share your personal email address when filling out forms or signing up for newsletters on the web, or when sending email.

Protect your web browsing

- *Use the internet more privately with iCloud Private Relay:* When you subscribe to iCloud+, you can use iCloud Private Relay to help prevent websites and network providers from creating a detailed profile about you.

- *Manage your privacy, and help protect yourself against malicious websites:* Safari helps prevent trackers from following you across websites. You can review the Privacy Report to see a summary of trackers that have been encountered and prevented by Intelligent Tracking Prevention on the current webpage you're visiting. You can also review and adjust Safari settings to keep your browsing activities private from others who use the same device, and help protect yourself from malicious websites.
  See Browse privately in Safari on iPad.

Lock down your iPad if it’s facing a sophisticated cyberattack

If you find your iPad and personal accounts are targeted by sophisticated remote attacks, you can also help protect yourself with Lockdown Mode. Lockdown Mode offers an extreme level of security for the very few users who, because of who they are or what they do, may be personally targeted by some of the most sophisticated digital threats, such as those from private companies developing state-sponsored mercenary spyware. Lockdown Mode automatically protects Safari, Messages, Home, and many other Apple services and apps. Webpages and internet communications continue working, but with reduction in performance and usability. See Harden your iPad from a cyberattack with Lockdown Mode.