



# **Persönliche Sicherheit – Benutzerhandbuch**



**Schütze dich und deine Daten**

# Inhaltsverzeichnis

<b>Unterstützte Lösungssuche</b>	<b>4</b>
Sicherheitsprüfung auf dem iPhone (iOS 16 oder neuer)	4
Checklisten	18
<b>Persönliche Sicherheit auf einen Blick</b>	<b>22</b>
Weitere Sicherheitsressourcen	23
<b>Überprüfen und Maßnahmen ergreifen</b>	<b>24</b>
Sicheres AirDrop und NameDrop	24
Sicher steuern, welche Inhalte über iPhone, iPad und Apple Watch geteilt werden	26
Sicher steuern, mit wem Inhalte vom Mac geteilt werden	32
Verwalten deines Standorts	37
Sicher verwalten, wie Inhalte weitergeleitet werden	52
Ablehnen unbekannter Anmeldeversuche	54
Aufzeichnung verdächtiger Aktivitäten	55
Sicheres Speichern von Daten in iCloud	57
Löschen verdächtiger Inhalte auf deinen Geräten	59
Verwalten von Familienfreigabeeinstellungen	62
Erkennen von betrügerischen Anfragen zum Teilen von Informationen	66
Sicheres Kontrollieren deines Home-Zubehörs	66
Löschen aller Inhalte und Einstellungen	67
Wiederherstellen gesicherter Daten	69

<b>Werkzeuge für Sicherheit und Datenschutz</b>	<b>73</b>
Aktualisieren der Apple-Software	73
Festlegen eines eindeutigen Codes oder Passworts auf Apple-Geräten	76
Schützen des iPhone oder iPad mit Face ID	78
Schützen deiner Geräte mit Touch ID	80
Löschen von unbekanntem Fingerabdrücken vom iPhone oder iPad	82
Hinzufügen oder Löschen von Fingerabdrücken auf dem Mac	83
Schützen deiner Apple-ID	84
Verwenden der Zwei-Faktor-Authentifizierung	87
Verhindern, dass du von deinem Apple-Gerät ausgesperrt wirst	89
Schützen der Geräte-, App- und Website-Passwörter auf dem iPhone und iPad	91
Verwalten geteilter Passwörter und Passkeys	93
Datenschutzfunktionen von Apps in Apple-Produkten	95
Schützen deiner Geräte vor Spionagesoftware mithilfe des Blockierungsmodus	98
Sicherheitseinstellungen in der App „Nachrichten“ verwalten	99
Verwenden der Wegbegleitung für Nachrichten	102
Blockieren von Anrufen und Nachrichten von bestimmten Personen	105
Empfangen von Warnungen zu sensiblen Bildern und Videos auf dem iPhone, iPad und Mac	107
Schützen des Browserverlaufs in Safari und „Karten“	108
Tätigen eines Notrufs oder Senden einer Notfalltextnachricht auf dem iPhone oder der Apple Watch	112
Erhalten eines Nachweises für den Account einer anderen Person	116
<b>Copyright</b>	<b>118</b>

# Unterstützte Lösungssuche

## Sicherheitsprüfung auf dem iPhone (iOS 16 oder neuer)

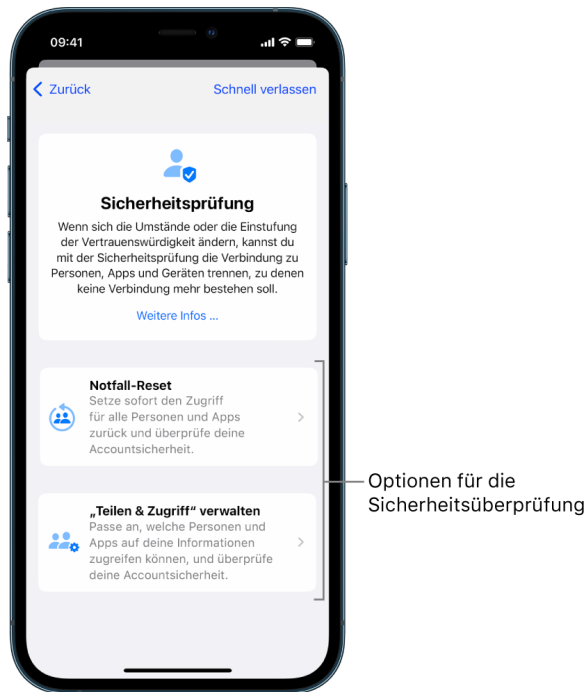
### Verwenden der Sicherheitsprüfung auf dem iPhone, um das Teilen von Informationen zu beenden und deinen Account zu schützen

Wenn deine persönliche Sicherheit gefährdet ist, kannst du die Sicherheitsprüfung auf dem iPhone verwenden, um das Teilen von Informationen schnell zu stoppen oder um zu prüfen, was mit einzelnen Personen und Apps geteilt wird, und dieses ggf. zu aktualisieren. Für die Sicherheitsprüfung ist iOS 16 oder neuer erforderlich. (Um festzustellen, welche Softwareversion auf deinem Gerät installiert ist, wähle „Einstellungen“ > „Allgemein“ und tippe auf „Info“.)

Es gibt zwei Möglichkeiten, wie du mithilfe der Sicherheitsprüfung das Teilen von Informationen stoppen kannst:

- Verwende [Notfall-Reset](#), um sofort das Teilen der Freigabearten zu stoppen, die unter [Funktionsweise der Sicherheitsprüfung](#) genannt sind. „Notfall-Reset“ ermöglicht es dir auch, Einstellungen im Zusammenhang mit deiner Apple-ID zu prüfen und zurückzusetzen.

- Verwende [„Teilen & Zugriff“ verwalten](#), um die Freigabe von Informationen für bestimmte Personen oder Apps zu stoppen. Verwende diese Option, wenn du überprüfen möchtest, was du teilst und mit wem du es teilst.



Bedenke bei der Verwendung von „Notfall-Reset“ und „Teilen & Zugriff“ verwalten“ Folgendes:

- Andere können bemerken, dass du aufgehört hast, Informationen mit ihnen zu teilen.
- Wenn du Freigabebeziehungen beendest, verlierst du möglicherweise den Zugriff auf Daten wie geteilte Fotos und Notizen.

Weitere Informationen zur Sicherheitsprüfung findest du unter [„Funktionsweise der Sicherheitsprüfung auf dem iPhone“](#) weiter unten in diesem Dokument.

### Sicherheitsprüfung schnell verlassen

Wenn du die Sicherheitsprüfung schnell verlassen musst, kannst du die Taste „Schnell verlassen“ verwenden. Änderungen, die du vor dem Verwenden von „Schnell verlassen“ vorgenommen hast, werden gesichert.

- Tippe in einer beliebigen Sicherheitsprüfungsanzeige auf „Schnell verlassen“, um die App „Einstellungen“ sofort zu schließen und zum Home-Bildschirm zurückzukehren.

### Option „Notfall-Reset“ in der Sicherheitsprüfung verwenden

1. Wähle „Einstellungen“ > „Datenschutz & Sicherheit“ > „Sicherheitsprüfung“.
2. Tippe auf „Notfall-Reset“ und befolge die Anleitung auf dem Bildschirm.

Der Fortschritt wird gesichert, während du fortfährst.



3. Wenn du fertig bist, fahre mit **Überprüfen, ob du die Freigabe gestoppt hast** weiter unten in diesem Dokument fort.

*Hinweis:* Wenn du den Schutz für gestohlene Geräte aktiviert hast, funktioniert die Sicherheitsprüfung möglicherweise geringfügig anders. Weitere Informationen über den Schutz für gestohlene Geräte findest du im Apple Support-Artikel [Schutz für gestohlene Geräte für das iPhone](https://support.apple.com/HT212510) (<https://support.apple.com/HT212510>).

## Option „Teilen & Zugriff‘ verwalten“ in der Sicherheitsprüfung verwenden

Wenn du dich detaillierter mit der Freigabe befassen willst, verwende die Option „Teilen & Zugriff‘ verwalten“, um Informationen, die du mit anderen Personen teilst, zu prüfen und zurückzusetzen, um die Informationen, auf die Apps zugreifen können, zu prüfen und zurückzusetzen und um die Sicherheit deines Geräts und deiner Apple-ID zu aktualisieren. Der Fortschritt wird gesichert, während du fortfährst.

1. Wähle „Einstellungen“ > „Datenschutz & Sicherheit“ > „Sicherheitsprüfung“.
2. Tippe auf „Teilen & Zugriff‘ verwalten“.
3. Führe einen der folgenden Schritte aus, um die Freigabe von Informationen für andere Personen zu stoppen:
  - Tippe auf „Personen“, wähle Personen in der Liste aus, prüfe die Informationen, die mit den Personen geteilt werden, und entscheide, welche Informationen du mit ausgewählten Personen nicht mehr teilen willst.
  - Tippe auf „Informationen“, wähle Apps in der Liste aus, prüfe die Informationen, die mit den Personen geteilt werden, und entscheide, welche Informationen du mit ausgewählten Personen nicht mehr teilen willst.
4. Führe einen der folgenden Schritte aus, um die Freigabe von Informationen für andere Apps zu stoppen:
  - Tippe auf „Apps“, wähle Apps in der Liste aus, prüfe die Informationen, die mit diesen geteilt werden, und entscheide, welche Informationen du mit ausgewählten Apps nicht mehr teilen willst.



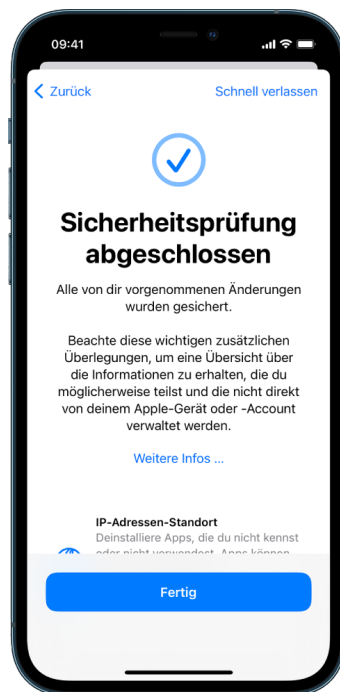
- Tippe auf „Informationen“, wähle die Informationen, die geteilt werden, in der Liste aus, prüfe die Informationen, die mit Apps geteilt werden, und entscheide, welche Informationen du mit ausgewählten Apps nicht mehr teilen willst.

5. Tippe auf „Fortfahren“ und führe einen der folgenden Schritte aus:

*Hinweis:* Du wirst nur zum Prüfen von Inhalten aufgefordert, die du ändern kannst.

- Überprüfe und entferne Geräte, die mit deiner Apple-ID verknüpft sind.
- Überprüfe und aktualisiere Telefonnummern, die zum Bestätigen deiner Identität verwendet werden.
- Aktualisiere dein Apple-ID-Passwort.
- Füge Notfallkontakte hinzu oder aktualisiere sie.
- Aktualisiere deinen Gerätecode oder deine Face ID- oder Touch ID-Informationen.
- Prüfe und entferne synchronisierte Computer. (nur iOS 17 oder neuer)
- Wenn du über iCloud+ verfügst und Privat-Relay noch nicht eingeschaltet hast, kannst du dies jetzt nachholen. (nur iOS 17 oder neuer)

6. Tippe auf „Fertig“.



7. Wenn du fertig bist, fahre mit der nächsten Schritt fort, um zu überprüfen, ob du die Freigabe gestoppt hast.

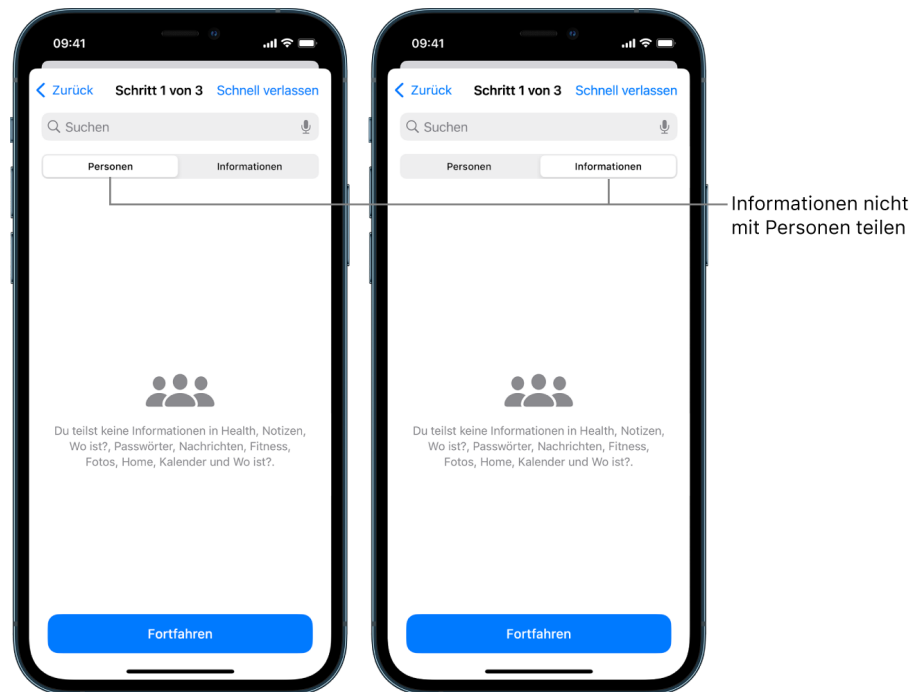
**Wichtig:** Tipps zu Schutzmaßnahmen für deine privaten Informationen, die über die Sicherheitsprüfung hinausgehen, findest du unter [Zusätzliche Überlegungen zum Verwenden der Sicherheitsprüfung](#) weiter unten in diesem Dokument.



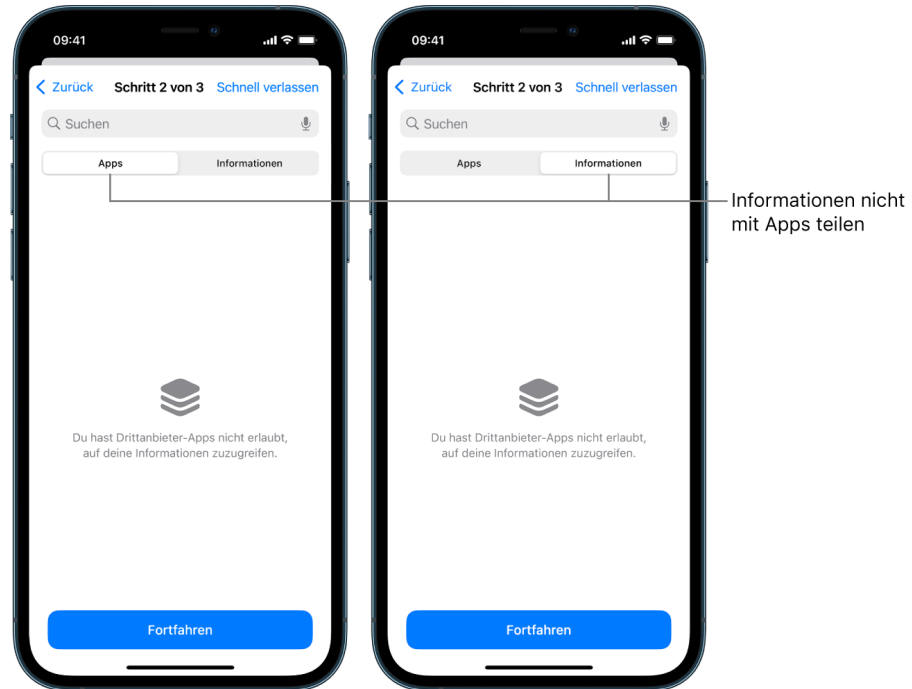
## Überprüfen, ob du die Freigabe gestoppt hast

Nach Verwenden der Sicherheitsprüfung kannst du bestätigen, dass Änderungen vorgenommen wurden. Du kannst überprüfen, ob Freigabe und Informationszugriff gestoppt wurden. Dies geschieht in drei Schritten:

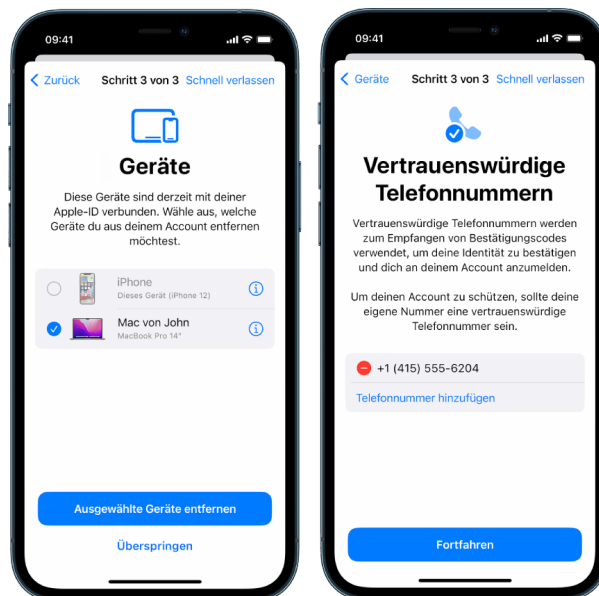
- *Schritt 1:* Stelle sicher, dass die Freigabe von Informationen für alle Personen gestoppt wurde und dass für Personen freigegebene Informationen gestoppt wurden.



- *Schritt 2:* Stelle sicher, dass die Freigabe für Apps gestoppt wurde.



- *Schritt 3:* Überprüfe Änderungen, die du am Account vorgenommen hast:
  - Geräte, die mit deiner Apple-ID verknüpft sind.
  - Telefonnummern, die zum Bestätigen deiner Identität verwendet werden.



- Notfallkontakte, die du hinzugefügt oder geändert hast.



- Synchronisierte Computer, die du entfernt hast.



## Funktionsweise der Sicherheitsprüfung auf dem iPhone

Wenn deine persönliche Sicherheit gefährdet ist, kannst du die Sicherheitsprüfung auf dem iPhone verwenden, um das Teilen von Informationen schnell zu stoppen oder um zu prüfen, was mit einzelnen Personen und Apps geteilt wird, und dieses ggf. zu aktualisieren.

Wenn du das Teilen von Informationen sofort beenden musst, findest du weitere Informationen unter „[Option ‚Notfall-Reset‘ in der Sicherheitsprüfung verwenden](#)“ weiter oben in diesem Dokument.

Wenn du das Teilen von Informationen mit bestimmten Personen oder Apps überprüfen oder stoppen willst, beachte die Hinweise unter „[Option ‚Teilen & Zugriff‘ verwalten](#)“ in der Sicherheitsprüfung verwenden oben im Dokument.



### Was macht die Sicherheitsprüfung?

Du kannst die Sicherheitsprüfung verwenden, um zu prüfen, mit wem du Information teilst, um Nachrichten und FaceTime auf deinem iPhone einzuschränken, um Systemdatenschutzberechtigungen für Apps zurückzusetzen, um deinen Code zu ändern, um dein Apple-ID-Passwort zu ändern und vieles mehr.

Wenn du nach Verwenden der Sicherheitsprüfung die Freigabe für eine Person wieder starten willst, öffnest du einfach die App oder den Dienst, über die bzw. den du Informationen teilen willst, und teilst diese Inhalte erneut.

Wenn du den Schutz für gestohlene Geräte aktiviert hast, funktioniert die Sicherheitsprüfung möglicherweise geringfügig anders. Weitere Informationen über den Schutz für gestohlene Geräte findest du im Apple Support-Artikel [Schutz für gestohlene Geräte für das iPhone](https://support.apple.com/HT212510) (<https://support.apple.com/HT212510>).

*Hinweis:* Wenn auf deinem iPhone Beschränkungen für Bildschirmzeit aktiviert sind oder ein MDM-Profil (Mobile Device Management) installiert ist, kannst du die Sicherheitsprüfung trotzdem nutzen, allerdings sind möglicherweise nicht alle Optionen verfügbar.

## Was benötige ich zur Verwendung der Sicherheitsprüfung?

Die Sicherheitsprüfung ist nur auf iPhones mit iOS 16 oder neuer verfügbar. Für die Nutzung der Sicherheitsprüfung benötigst du eine Apple-ID, die die Zwei-Faktor-Authentifizierung verwendet. Du musst außerdem unter „Einstellungen“ > „[dein Name]“ auf deinem iPhone angemeldet sein. (Um festzustellen, welche Softwareversion auf deinem Gerät installiert ist, wähle „Einstellungen“ > „Allgemein“ und tippe auf „Info“.)












Um auf die Sicherheitsprüfung zuzugreifen, wähle „Einstellungen“ > „Datenschutz & Sicherheit“ > „Sicherheitsprüfung“.



*Hinweis:* Wenn du keinen Zugriff auf die Sicherheitsprüfung hast oder dir die Verwendung dieser Funktion Probleme bereitet, kannst du deine Freigabeeinstellungen und den Zugriff auf dein Gerät und deine Accounts manuell anpassen. Weitere Informationen findest du unter [Beenden der Freigabe für deine iPhone- oder iPad-Inhalte](#) weiter unten in diesem Dokument.
















## Welche Apple-Apps stoppen die Freigabe von Informationen mit Personen bei Verwendung der Sicherheitsprüfung?

Die Sicherheitsprüfung kann die Freigabe von Informationen der folgenden Apple-Apps mit anderen Personen deaktivieren:

App	Information
	Aktivität
	Check-In
	Geteilte Fotos (einschließlich geteilter Mediathek und geteilter Alben)
	Geteilte Kalender
	Geteilte Karten (Ankunftszeit)
	Geteilte Notizen
	Geteilte Objekte in „Wo ist?“
	Geteilte Passwörter
	Health
	Home
	Standortfreigabe mit „Wo ist?“

## Welche Informationen stoppen die Freigabe mit Apps bei Verwendung der Sicherheitsprüfung?

Die Sicherheitsprüfung entfernt von allen Apps auf deinem iPhone Daten, die von folgenden Apps, Netzwerken und Funktionen gesammelt wurden:

	Bluetooth®
	Kalender
	Kamera
	Kontakte
	Dateien und Ordner
	Health
	Lokale Netzwerke
	Ortungsdienste
	Medien und Apple Music
	Mikrofon
	Bewegung & Fitness
	Fotos
	Erinnerungen
	Forschung
	Spracherkennung

## Wie funktioniert die Sicherheitsprüfung mit meiner Apple-ID?

Die Sicherheitsprüfung kann verwendet werden, um Informationen im Zusammenhang mit deiner Apple-ID zu ändern. Du kannst die Sicherheitsprüfung zu folgenden Zwecken verwenden:

- Prüfen und Entfernen von Geräten, die bei deinem Account angemeldet sind
- Prüfen und Aktualisieren von vertrauenswürdigen Telefonnummern
- Ändern deines Apple-ID-Passworts
- Aktualisieren deiner Notrufkontakte
- Aktualisieren deines Gerätecodes und deiner Face ID- oder Touch ID-Informationen

*Hinweis:* Wenn du den Schutz für gestohlene Geräte aktiviert hast, funktioniert die Sicherheitsprüfung möglicherweise geringfügig anders. Weitere Informationen über den Schutz für gestohlene Geräte findest du im Apple Support-Artikel [Schutz für gestohlene Geräte für das iPhone](https://support.apple.com/HT212510) (<https://support.apple.com/HT212510>).

## Was ist der „Notfall-Reset“?

Die Sicherheitsprüfung verfügt über eine Option namens „Notfall-Reset“. Damit kannst du die Freigabe der oben aufgelisteten Objekte sofort beenden, einschließlich Freigaben aller Art. „Notfall-Reset“ ermöglicht es dir auch, Einstellungen im Zusammenhang mit deiner Apple-ID zu prüfen und zurückzusetzen.

Wenn du unsicher bist, welche Informationen du mit wem teilst, findest du weitere Informationen unter „[Verwenden der Option „Teilen & Zugriff“ verwalten](#)“ weiter oben in diesem Dokument.

## Zusätzliche Überlegungen zum Verwenden der Sicherheitsprüfung

Du kannst die Sicherheitsprüfung auf dem iPhone (mit iOS 16 oder neuer) verwenden, um den Zugriff auf deine geteilten oder bereitgestellten Informationen schnell zu stoppen oder um zu prüfen, was mit einzelnen Personen und Apps geteilt wird und dieses ggf. zu aktualisieren.

In einigen Fällen kannst du auch Daten teilen, die von der Sicherheitsprüfung nicht erfasst oder geändert werden können. Beispiele sind Accounts und Passwörter, geteilte Objekte auf Social Media oder einem iPad oder Mac, auf dem sich ebenfalls von dir geteilte Informationen befinden. Überprüfe Folgendes sorgfältig, um bei der Entscheidung mitzuhelfen, welche weitere Schritte du ausführen kannst, um die Menge der geteilten Informationen zu reduzieren.

### IP-Adresse und Apps

Eine IP-Adresse ist eine eindeutige Kennung, die dein Internetanbieter Geräten zuordnet, die mit dem Internet verbunden sind, sodass du das Internet nutzen kannst. IP-Adressen geben deinen Standort nicht exakt, aber grob an und helfen Firmen, die Daten sammeln, mit der Zeit deine Identität zu ermitteln. Auf deinem Gerät installierte Apps können deine IP-Adresse verwenden, um Informationen zu deinem groben Standort zu erfassen. Überprüfe die installierten Apps und lösche die Apps, die du nicht verwendest oder nicht kennst.

Weitere Informationen zum Überprüfen und Löschen installierter Apps findest du unter „[Löschen verdächtiger Inhalte auf deinen Geräten](#)“ weiter unten in diesem Dokument.



## Accounts und Passwörter

Überlege, welche Accounts du verwendest, die möglicherweise vertrauliche persönliche Daten enthalten, die du schützen möchtest. Hierzu gehören beispielsweise Daten für Banken, Einkaufen, E-Mail, Social Media, Bildung und andere. Ändere die Passwörter für diese Accounts, um sicherzustellen, dass niemand außer dir darauf zugreifen kann. Prüfe die Einstellungen für Sicherheit und Datenschutz für jeden Account, um sicherzustellen, dass deine Informationen geschützt sind. Es empfiehlt sich, Accounts, über die du kommunizierst (etwa E-Mail, Telefon und Nachrichten), zu überprüfen, um sicherzustellen, dass keine Informationen ohne deine Erlaubnis weitergeleitet werden.

## Social Media

Vergiss nicht, dass gepostete Fotos und andere persönliche Informationen auf Social Media Details über deinen Standort und deine Privatsphäre preisgeben können. Prüfe deine privaten Einstellungen, deine Verbindungslisten und Follower und bedenke sorgfältig, welche Informationen du postest, um den Grad des von dir benötigten Schutzes deiner Privatsphäre zu gewährleisten.

## Andere Geräte, die du verwendest oder besitzt

Prüfe die Freigabe- und Zugriffseinstellungen für alle anderen Geräte, die du verwendest, um sicherzugehen, dass deine Informationen geschützt sind. Falls sich eine andere Person, etwa ein Kind oder ein:e Freund:in gerade in deiner Nähe befindet, bedenke, dass deren Geräte ebenfalls Informationen teilen können.

## Unerwünschtes Tracking

Die Hinweise über unerwünschtes Tracking wurden erstellt, damit Personen AirTags und andere kleine „Wo ist?“-Accessoires nicht nutzen, um anderen Personen ohne ihr Wissen zu folgen. Um Warnhinweise zu erhalten, wenn sich ein unbekanntes AirTag oder ein anderes „Wo ist?“-Netzwerkzubehör mit dir bewegt, stelle sicher, dass Bluetooth®, Ortungsdienste und Tracking-Mitteilungen aktiviert sind. Um die Tracking-Mitteilungen zu aktivieren, öffne die App „Wo ist?“, tippe auf „Ich“, scrolle zu „Tracking-Mitteilungen anpassen“ und aktiviere dann „Mitteilungen erlauben“.

Weitere Informationen findest du im Apple Support-Artikel [„Wie gehe ich vor, wenn ich eine Benachrichtigung erhalte, dass sich ein AirTag, ‚Wo ist?‘-Netzwerkzubehör oder ein Satz AirPods in meiner Nähe befindet?“](https://support.apple.com/119874) (<https://support.apple.com/119874>).

## Home und HomeKit

Wenn du Mitglied eines Apple-Zuhauses bist und dich selbst entfernen möchtest, denke daran, dass die Person, die das Zuhause verwaltet, weiterhin HomeKit-Geräte wie Kameras verwenden kann, die deine persönliche Sicherheit beeinflussen.

Weitere Informationen findest du unter [„Sicheres Kontrollieren deines Home-Zubehörs“](#) weiter unten in diesem Dokument.

## Apple Wallet

Wenn du Karten oder Schlüssel mit einer anderen Person über Wallet teilst, kann diese Person unter Umständen deinen Transaktions- oder Türschlossverlauf sehen. Wenn du deine letzten Transaktionen prüfen möchtest, öffne die App „Wallet“. Bedenke, dass Einzelheiten von finanziellen Transaktionen auch über geteilte Bankkonten oder Kreditkarten gesehen werden können. Wenn eine andere Person online auf deine Finanz-Accounts hat, kann sie diese ebenfalls einsehen. Denke daran, deine Passwörter zu aktualisieren.

## Mobilfunkplan

Wenn du Mitglied eines geteilten Mobilfunkplans bist, können andere Mitglieder Zugriff auf deinen Standort, deine Anruf- und Nachrichtenaktivität oder Rechnungsdetails haben. Wende dich an deinen Mobilfunkanbieter, um Näheres über deinen Mobilfunkplan zu erfahren und um zu sehen, welche zusätzlichen Sicherheitsmaßnahmen für deinen Account getroffen werden können, etwa ein PIN-Code oder Sicherheitscode, der eingegeben werden muss, bevor Änderungen vorgenommen werden können. Wenn du keinen geteilten Mobilfunkplan hast, eine andere Person jedoch online auf deinen Mobilfunkaccount zugreifen kann, hat diese Person möglicherweise auch Zugriff auf deinen Standort, deine Anruf- und Nachrichtenaktivität oder auf Rechnungsdetails. Denke daran, deine Passwörter zu aktualisieren.

## Familienfreigabe

Wenn du Mitglied einer Apple-Familienfreigabegruppe bist, kann der Organisator der Familienfreigabe möglicherweise deine Käufe sehen und Änderungen an den Geräteeinstellungen eines Kindes vornehmen. Um eine Familiengruppe zu verlassen, wähle „Einstellungen“, tippe auf deinen Namen und öffne die Einstellungen „Familienfreigabe“. Accounts von Kindern können nicht aus der Familienfreigabegruppe entfernt werden. Sie können aber in eine andere Familienfreigabegruppe bewegt oder ihre Apple-ID kann gelöscht werden.

Weitere Informationen zum Verlassen einer Familienfreigabegruppe findest du in Schritt 1 und 2 unter [„Beenden der Freigabe für deinen iPhone- oder iPad-Standort“](#) weiter unten in diesem Dokument.

Ausführlichere Informationen zur Familienfreigabe findest du unter [„Verwalten von Familienfreigabeeinstellungen“](#) weiter unten in diesem Dokument.

# Checklisten

## Zugriffsbeschränkungen für dein iPhone oder iPad

Verwende diese Checklisten, um zu erfahren, wer Zugriff auf deine Geräte oder deine Apple-ID hat, wenn du iOS 15 (oder älter) verwendest. Wenn du mit iOS 16 (oder neuer) arbeitest, findest du Informationen unter „[Funktionsweise der Sicherheitsprüfung auf dem iPhone](#)“ weiter oben in diesem Dokument.





1. Wenn du überprüfen möchtest, welche Geräte bei deiner Apple-ID angemeldet sind, wähle „Einstellungen“  > [dein Name]. Wenn du ein Gerät siehst, das du nicht kennst, tippe auf den Gerätenamen und wähle „Aus dem Account entfernen“.
2. Wenn du überprüfen möchtest, ob unerwartet ein alternatives Erscheinungsbild für Face ID oder zusätzliche Fingerabdrücke für Touch ID auf deinem Gerät eingerichtet sind, befolge diese Anleitungen: [Einrichten von Face ID](#) und [Einrichten von Touch ID auf dem iPhone oder iPad](#).
3. Melde dich auf der [Apple-ID-Website](https://appleid.apple.com) (<https://appleid.apple.com>) an und überprüfe alle persönlichen Informationen und Sicherheitsinformationen in deinem Account, um herauszufinden, ob Informationen von anderen hinzugefügt wurden.
4. Wenn du die Zwei-Faktor-Authentifizierung aktiviert hast, suche in den vertrauenswürdigen Geräten nach Geräten, die du nicht kennst. Wenn du sie nicht aktiviert hast, kannst du sie auf folgende Weise aktivieren: [Einrichten der Zwei-Faktor-Authentifizierung auf dem iPhone oder iPad](#).
5. Überprüfe die Apps, die auf deinem Gerät installiert sind, und achte dabei auf Apps, die du nicht kennst oder die du deiner Erinnerung nach nicht installiert hast. Du kannst für alle Apps im App Store nachsehen, welchen Zweck sie haben.





6. Konfigurationsprofile für die Mobilgeräteverwaltung (Mobile Device Management, MDM) werden für gewöhnlich von Arbeitgebern, Bildungseinrichtungen oder anderen offiziellen Organisationen installiert, um zusätzliche Berechtigungen und Zugriff auf Geräte von Benutzer:innen zu ermöglichen. Weitere Informationen zum Suchen nach unbekanntem MDM-Konfigurationsprofilen auf deinen Geräten findest du unter [Unbekannte Konfigurationsprofile auf deinem iPhone oder iPad löschen](#).
7. Weitere Informationen zum Überprüfen, ob etwas an deinen Freigaben geändert oder zu ihnen hinzugefügt wurde, findest du unter [Beenden der Freigabe für deinen iPhone- oder iPad-Standort](#).

## Beenden der Freigabe für deine iPhone- oder iPad-Inhalte

Wenn du iOS 15 (oder älter) installiert hast, verwende diese Checkliste, um zu erfahren, wie du die Freigabe für Personen beendest, mit denen du Inhalte geteilt hast. Wenn du mit iOS 16 (oder neuer) arbeitest, findest du Informationen unter „[Funktionsweise der Sicherheitsprüfung auf dem iPhone](#)“ weiter oben in diesem Dokument.



1. Überprüfe, ob du Teil einer Familienfreigabegruppe bist. Wähle dazu „Einstellungen“  > [dein Name] > „Familienfreigabe“. Wenn du einer Familienfreigabegruppe angehörst, werden die Namen aller Familienmitglieder angezeigt.
2. Wenn du Teil einer Familienfreigabegruppe bist und deine Informationen nicht mehr teilen möchtest, kannst du dich selbst aus der Gruppe löschen (sofern du mindestens 13 Jahre alt bist). Wenn du die Familienfreigabegruppe eingerichtet hast (in diesem Fall wird das Wort *Organisator:in* unter deinem Namen angezeigt), kannst du alle Personen über 13 Jahre aus der Gruppe entfernen.
3. Tippe in der App „Wo ist?“  auf den Tab „Personen“, um zu sehen, mit wem du deinen Standort teilst. Wenn du deinen Standort nicht mehr mit einer Person teilen willst, wähle die Person aus und tippe auf „Standort nicht mehr teilen“. Wenn du deinen Standort mit niemandem mehr teilen willst, tippe auf „Ich“ und deaktiviere „Standort teilen“.


4. Tippe in der App „Fotos“  auf „Alben“ und wähle „Geteilte Alben“. Wähle ein geteiltes Album aus und tippe auf „Personen“, um zu sehen, wer Eigentümer:in des geteilten Albums ist und mit wem es geteilt wird.
  - Wenn du Eigentümer:in des Albums bist und es nicht mehr teilen willst, tippe auf den Namen des:der Abonnent:in, mit dem:der keine Inhalte mehr geteilt werden sollen, und wähle diese Option aus.
  - Wenn du Abonnent:in bist, kannst du auf „Abo beenden“ am unteren Bildschirmrand tippen. Du kannst außerdem beliebige geteilte Fotos löschen.
5. Tippe in der App „Kalender“  auf „Kalender“. Wähle einen geteilten Kalender aus und tippe auf die Info-Taste , um zu sehen, mit wem der Kalender geteilt wird.
  - Wenn du Eigentümer:in des Kalenders bist und ihn nicht mehr teilen willst, tippe auf den Namen des:der Abonnent:in, mit dem:der keine Inhalte mehr geteilt werden sollen, und wähle diese Option aus.
  - Wenn du Abonnent:in bist, kannst du „Kalender löschen“ am unteren Bildschirmrand auswählen.
6. Wenn du eine Apple Watch hast und deine Aktivitätsringe mit einer anderen Person teilst, kannst du diese Freigabe beenden. Öffne auf deinem iPhone die App „Aktivität“  und tippe auf „Teilen“. Tippe auf den Namen einer Person und wähle entweder „Freund:in entfernen“ oder „Aktivität ausblenden“.
7. Außerdem kannst du Informationen mit anderen über Apps von Drittanbietern teilen. Überprüfe die Apps, die du auf deinem Gerät installiert hast, um herauszufinden, ob sie Informationen teilen. Weitere Informationen findest du unter [Sicher steuern, welche Inhalte über iPhone, iPad und Apple Watch geteilt werden](#).

## Beenden der Freigabe für deinen iPhone- oder iPad-Standort



1. Du kannst die [Sicherheitsprüfung auf dem iPhone \(iOS 16 oder neuer\) verwenden](#), um zu verwalten, welche Personen und Apps auf deinen Standort zugreifen können.
2. Wenn du deinen Standort nicht mehr mit allen Apps und Diensten teilen willst, selbst nur für kurze Zeit, wähle „Einstellungen“  > „Datenschutz“ > „Ortungsdienste“ und deaktiviere die Option „Standortfreigabe“. Daraufhin können alle Apps auf deinem Gerät, wie etwa die App „Karten“, deinen Standort nicht mehr nutzen. Niemand wird benachrichtigt, wenn du die Standortfreigabe deaktivierst, allerdings funktionieren manche Funktionen möglicherweise nicht mehr wie erwartet, wenn sie nicht auf deinen Standort zugreifen können.

*Hinweis:* Außerdem kannst du im selben Tab die Option „Wo ist?“ für dein iPhone vorübergehend deaktivieren, wenn du befürchtest, dass jemand Zugriff auf deinen iCloud-Account hat. Tippe in der Liste der Apps, die deinen Standort nutzen, auf „Wo ist?“ und wähle „Nie“.

3. Um die Freigabe deines Standorts mit bestimmten Apps und Diensten zu stoppen, wähle „Einstellungen“ > „Datenschutz“ > „Ortungsdienste“ und wähle dann die Apps und Dienste aus, für die du das Teilen beenden möchtest. Tippe auf den App-Namen und wähle dann unter „Zugriff auf Standort erlauben“ die Option „Nie“.
4. Um den Standort nicht mehr mit einer bestimmten Person zu teilen, öffne die App „Wo ist?“ , tippe auf „Personen“, wähle eine Person aus. Tippe dann auf „Standort nicht mehr teilen“ unten auf dem Bildschirm.

Wenn du deinen Standort in der App „Wo ist?“ geteilt hast und später nicht mehr teilen willst, wird die jeweilige Person nicht benachrichtigt und kann dich nicht mehr in ihrer Freundesliste sehen. Wenn du die Standortfreigabe für eine Person wieder aktivierst, wird sie darüber benachrichtigt, dass du deinen Standort mit ihr teilst.

5. Um deine voraussichtliche Ankunftszeit in der App „Karten“ nicht mehr zu teilen, öffne die App „Karten“ und wähle die Option „Favoriten“, um ein Fenster zu öffnen, das alle Orte enthält, die du als Favorit angegeben hast. Tippe neben dem jeweiligen Ort, für den du die Einstellungen für das automatische Teilen der voraussichtlichen Ankunftszeit überprüfen möchtest, auf die Infotaste ⓘ. Scrolle dann nach unten zum Bereich zum Teilen der Ankunftszeit und entferne die Person, mit der du nicht mehr teilen möchtest.
6. Um zu überprüfen, welche Geräte und welches Zubehör derzeit unter „Wo ist?“ für die Personen verfügbar sind, die Zugriff auf deine Apple-ID haben, wähle „Wo ist?“ > „Geräte“ und überprüfe die Liste. Wenn sich darin ein unbekanntes Gerät befindet, das du überprüfen möchtest, tippe auf das entsprechende Gerät und dann auf „Dieses Gerät entfernen“.

*Hinweis:* Wenn du zu einer Familienfreigabegruppe gehörst, werden die Mitglieder, die dir erlaubt haben, den Standort ihrer Geräte zu sehen, unten aufgeführt – sortiert nach der Person, der sie gehören.

7. Wenn du Fotos und Videos, die Standortmetadaten enthalten, mit anderen Personen teilst, können diese Personen möglicherweise auf die Standortmetadaten zugreifen und Informationen über den Aufnahmeort erhalten. Wenn du nicht möchtest, dass andere Personen auf die Standortmetadaten zu deinen Fotos oder Videos zugreifen können, [kannst du die aktuellen Metadaten löschen](#) und verhindern, dass in Zukunft Metadaten erfasst werden.

# Persönliche Sicherheit auf einen Blick



Apple macht es dir leicht, mit den Menschen in Verbindung zu bleiben, die dir am nächsten sind, und unterstützt dich dabei, immer genau zu wissen, welche Informationen du mit wem teilst. Wenn du jemandem Zugriff auf deine persönlichen Informationen gegeben hast und dies rückgängig machen möchtest – oder befürchtest, dass jemand mit Zugriff auf deine Geräte oder Accounts ohne dein Einverständnis Änderungen vorgenommen hat – bietet dir dieses Handbuch Strategien und Lösungen, mit denen du die Kontrolle zurückgewinnen kannst.


Diese Ressource gilt überwiegend für Apple-Geräte mit den neuesten Betriebssystemen (iOS 17, iPadOS 17 und macOS Sonoma 14), sie kann jedoch auch auf Apple Watch und HomePod angewendet werden.





In iOS 16 oder neuer kannst du die Sicherheitsprüfung auf dem iPhone verwenden, um schnell zu sehen, was du mit wem teilst. Du kannst dann entscheiden, ob du diese Informationen nicht mehr teilen möchtest. Selbst wenn du noch nicht auf iOS 16 aktualisiert hast, können die Checklisten und ausführlichen Funktionsaufgaben von Apple dich unterstützen, falls du Opfer von technologiebasiertem Missbrauch, Stalking oder Belästigung geworden bist. Diese Aufgaben enthalten Schritt-für-Schritt-Anleitungen dazu, wie du den Zugriff auf Informationen, den du Dritten zu einem früheren Zeitpunkt gewährt hast, widerrufen kannst – darunter Standortinformationen in der App „Wo ist?“, geteilte Meetings in der App „Kalender“ und mehr. Außerdem erfährst du Näheres über Funktionen, die du zur Erhöhung deiner persönlichen Sicherheit nutzen kannst – darunter die Möglichkeit, Freund:innen automatisch darüber zu informieren, dass du sicher zu Hause angekommen bist, und die Aktivierung von „Notruf SOS“.

Dieses Handbuch wird regelmäßig aktualisiert, um dir alle Informationen bereitzustellen, die du brauchst, um dich bei der Verwendung von Apple-Produkten sicher zu fühlen.

 **Tip:** Soweit relevant, werden weitere Details zu anderen Produkten bereitgestellt oder verlinkt, darunter Links zu den Benutzerhandbüchern für Apple-Geräte. Du kannst ein PDF-Dokument dieses Handbuchs laden und ausdrucken, um es jederzeit zur Hand zu haben. Alle Funktionen, Anleitungen und Einstellungen können abhängig von Produktmodell oder Softwareversion variieren. Wenn du Unterstützung für eine bestimmte Funktion benötigst, besuche den Apple Support unter <https://support.apple.com/de-de>.

## Weitere Sicherheitsressourcen


Wenn du annimmst, dass deine Sicherheit nicht gewährleistet ist, können diese zusätzlichen Ressourcen für dich hilfreich sein:

- *USA:* [The Safety Net Project](https://www.techsafety.org/resources-survivors)  
(<https://www.techsafety.org/resources-survivors>)
- *USA:* [National Center for Victims of Crime](https://victimsofcrime.org/getting-help/)  
(<https://victimsofcrime.org/getting-help/>)
- *Vereinigtes Königreich:* [Refuge UK](https://refuge.org.uk/i-need-help-now/how-we-can-help-you/national-domestic-abuse-helpline/)  
(<https://refuge.org.uk/i-need-help-now/how-we-can-help-you/national-domestic-abuse-helpline/>)
- *Australien:* [WESNET Safety Net Australia](https://techsafety.org.au/resources/resources-women/)  
(<https://techsafety.org.au/resources/resources-women/>)

# Überprüfen und Maßnahmen ergreifen

## Sicheres AirDrop und NameDrop

### Was ist AirDrop?

Mit AirDrop  kannst du Bilder, Dokumente und andere Dateien unkompliziert auf verschiedenen Apple-Geräten in der Nähe teilen. Du kannst AirDrop so einrichten, dass alle Personen in deiner Nähe oder nur deine Kontakte Inhalte teilen können oder niemand Inhalte teilen kann.

*Hinweis:* Die Option „Nur Kontakte“ ist auf Geräten mit iOS 10, iPadOS 13.1 und macOS 10.12 oder neuer verfügbar. Wenn deine Geräte eine frühere Softwareversion verwenden und du einschränken möchtest, wer dir Dateien über AirDrop schicken kann, kannst du die Funktion bei Bedarf aktivieren und bei Nichtbenutzung wieder deaktivieren.

### Was ist NameDrop?


NameDrop ist Teil von AirDrop und bietet eine unkomplizierte Möglichkeit zum Teilen deiner Kontaktinformationen mit anderen Personen oder Empfangen der Kontaktinformationen anderer Personen, ohne dass du diesen Personen dein iPhone geben musst. Mit NameDrop können Benutzer:innen auf unkomplizierte Weise Kontaktinformationen teilen, indem sie ihre iPhone-Geräte aneinanderhalten oder ein iPhone und eine Apple Watch aneinanderhalten (Apple Watch Ultra, Apple Watch Series 7 (oder neuer) und Apple Watch SE (2. Generation)).

Außerdem kannst du auswählen, welche Kontaktinformationen du teilen möchtest und, was noch viel wichtiger ist, welche Informationen du *nicht* teilen möchtest. Zum Nutzen von NameDrop müssen beide Geräte iOS 17.1 (oder neuer) oder watchOS 10.1 (oder neuer) verwenden. Weitere Informationen findest du unter [Deine Kontaktkarte prüfen und aktualisieren](#) weiter unten in diesem Dokument.

NameDrop funktioniert automatisch. Wenn du NameDrop deaktivieren musst, findest du Informationen dazu unter [NameDrop deaktivieren](#) weiter unten in diesem Dokument.

*Hinweis:* Beim Teilen deiner Kontaktinformationen mit der App „Kontakte“ oder NameDrop werden deine Pronomen standardmäßig nicht geteilt. Beim Teilen von Kontaktinformationen anderer Personen werden deren Pronomen nie geteilt.

### AirDrop verwalten

- Wähle auf dem iPhone oder iPad „Einstellungen“  > „Allgemein“, tippe auf „AirDrop“ und wähle deine bevorzugte Option aus.


Weitere Informationen findest du unter:

- [Verwenden von AirDrop auf dem iPhone zum Senden von Objekten an Apple-Geräte in der Nähe](https://support.apple.com/guide/iphone/iphcd8b9f0af) im iPhone-Benutzerhandbuch  
(<https://support.apple.com/guide/iphone/iphcd8b9f0af>)
- [Verwenden von AirDrop auf dem iPad zum Senden von Objekten an in der Nähe befindliche Geräte](https://support.apple.com/guide/ipad/ipad46a13d74/ipados) im iPad-Benutzerhandbuch  
(<https://support.apple.com/guide/ipad/ipad46a13d74/ipados>)

### Deine Kontaktkarte prüfen und aktualisieren

Du kannst die Informationen aktualisieren, die du mit NameDrop teilst, indem du deine Kontaktkarte aktualisierst (wenn du beispielsweise nur deinen Vornamen oder deine Initialen teilen möchtest).


*Hinweis:* NameDrop teilt nur deinen Namen, die von dir ausgewählte Telefonnummer oder E-Mail-Adresse und die mit deiner Kontaktkarte verknüpften Informationen deines Kontaktposters. Es teilt keine weiteren Informationen aus deiner Kontaktkarte (z. B. deine Privatadresse oder deinen Geburtstag).

1. Öffne die App „Kontakte“ .
2. Wähle „Meine Karte“ > „Bearbeiten“.
3. Prüfe und aktualisiere deinen Namen, die Telefonnummern und die E-Mail-Adressen, die du mit NameDrop teilen möchtest.

### Teilen deiner Kontaktinformationen mit NameDrop


Du kannst deine Kontaktinformationen mit einer anderen Person teilen.

1. Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad teilen:* Halte dein iPhone wenige Zentimeter über das iPhone oder die Apple Watch einer anderen Person.
  - *Von Apple Watch zu Apple Watch teilen:* Öffne die App „Kontakte“  auf deiner Apple Watch, tippe auf dein Bild oben rechts, tippe auf „Teilen“ und halte deine Uhr an die Apple Watch der anderen Person.
  - Beide Geräte leuchten auf und die Apple Watch vibriert, um anzuzeigen, dass eine Verbindung hergestellt wird.
2. Halte die Geräte weiterhin dicht aneinander, bis NameDrop auf beiden Bildschirmen angezeigt wird.
3. Wähle aus, ob du sowohl deine Kontaktkarte (oder eine bestimmte Telefonnummer oder E-Mail-Adresse) teilen als auch die Kontaktkarte der anderen Person empfangen oder nur die Kontaktkarte der anderen Person empfangen möchtest.

Tippe zum Teilen deiner Kontaktkarte auf , wähle die Felder aus, die geteilt werden sollen, und tippe auf „Sichern“. Bei der nächsten Verwendung von NameDrop werden automatisch dieselben Felder ausgewählt.

Willst du den Vorgang abbrechen, bewege die beiden Geräte voneinander weg oder sperre dein iPhone, bevor die NameDrop-Übertragung abgeschlossen wird.

### NameDrop deaktivieren

1. Öffne die App „Einstellungen“ .
2. Wähle „Allgemein“ > „AirDrop“.
3. Deaktiviere die Option „Geräte aneinanderhalten“.

## Sicher steuern, welche Inhalte über iPhone, iPad und Apple Watch geteilt werden

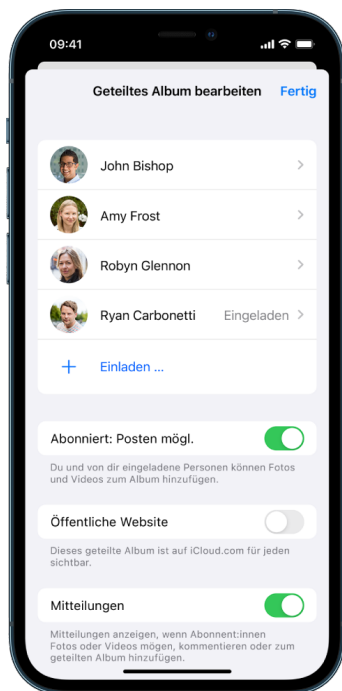
Es gibt verschiedene Möglichkeiten, um auf deinen Apple-Geräten Inhalte sicher mit anderen zu teilen. Mit jeder Methode kannst du die Personen auf deinem Bildschirm sehen, mit denen du Inhalte teilst. Du kannst diese Personen auch von geteilten Inhalten auf deinem iPhone, iPad und deiner Apple Watch entfernen.




Um zu steuern, mit welchen Personen du Inhalte von einem Mac teilst, beachte die Informationen unter „[Sicher steuern, mit wem Inhalte vom Mac geteilt werden](#)“ weiter unten in diesem Dokument.

## Verwalten von Freigabeeinstellungen für geteilte Alben in der App „Fotos“

Mit den geteilten Alben in der App „Fotos“ kannst du Fotos und Videos auswählen, die du teilen möchtest. Außerdem kannst du auswählen, mit welchen Personen du sie teilen möchtest. Du kannst die Freigabeeinstellungen jederzeit ändern. Wenn du die Freigabe für ein Foto oder Album für eine Person beendest, wird die jeweilige Person nicht darüber benachrichtigt und ihr Zugriff auf das geteilte Album und seine Inhalte wird entfernt.



Wenn du Abonnent:in eines geteilten Albums bist, kannst du alle von dir geteilten Fotos löschen. Außerdem kannst du „Abo beenden“ wählen, um das Abonnement des geteilten Albums zu beenden.

1. Wähle ein geteiltes Album auf deinem iPhone oder iPad aus und tippe dann auf die Taste „Abonnenten hinzufügen“ .
2. Führe beliebige der folgenden Schritte aus:
  - *Neue Abonnent:innen einladen:* Tippe auf „Einladen“ und gib die Namen der Abonnent:innen ein, die du hinzufügen möchtest.  
Abonnent:innen können Fotos und Videos zum Album hinzufügen. Deaktiviere die Option „Abonniert: Posten mögl.“, damit nur du Fotos und Videos hinzufügen kannst.
  - *Abonnent:innen entfernen:* Tippe auf den Namen des:der Abonnent:in und dann auf „Abonnent:in entfernen“.
  - *Mitteilungen deaktivieren:* Tippe auf die Taste „Mitteilungen“. Tippe erneut, um Mitteilungen zu aktivieren.

Weitere Informationen findest du unter:

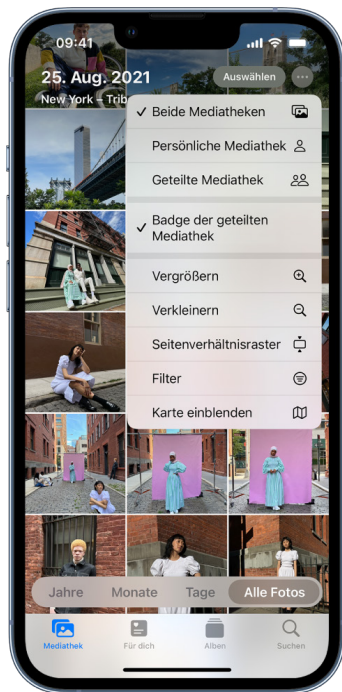
- „[Teilen von Fotos und Videos auf deinem iPhone](https://support.apple.com/guide/iphone/iphf28f17237)“ im iPhone-Benutzerhandbuch (<https://support.apple.com/guide/iphone/iphf28f17237>)
- „[Teilen von Fotos und Videos auf dem iPad](https://support.apple.com/guide/ipad/ipad4f44c78f)“ im iPad-Benutzerhandbuch (<https://support.apple.com/guide/ipad/ipad4f44c78f>)

## Entfernen von Teilnehmern aus einer geteilten Mediathek in der App „Fotos“


Mit „Geteilte iCloud-Fotomediathek“ kannst du Fotos und Videos nahtlos mit bis zu fünf anderen Personen teilen. Wenn du Fotos und Videos zu einer geteilten iCloud-Fotomediathek beiträgst, werden diese aus deiner persönlichen in die geteilte Mediathek verschoben. Bei der geteilten Mediathek kannst du wählen, was du teilen möchtest oder Inhalte automatisch über die Kamera teilen. Alle Teilnehmer können Inhalte in der geteilten Mediathek hinzufügen, bearbeiten und löschen. Und die Person, die die geteilte Mediathek eingerichtet hat, d. h. der Ersteller der Mediathek, stellt iCloud-Speicher für alle Inhalte bereit.

Wenn du der Ersteller der Mediathek bist, kannst du Teilnehmer aus der geteilten Mediathek entfernen oder deine geteilte Mediathek jederzeit löschen. Entfernst du Teilnehmer aus deiner geteilten Mediathek, so erhalten diese eine entsprechende Mitteilung und können alle Objekte in der geteilten Mediathek in ihre persönliche Mediathek kopieren. Teilnehmer verfügen nicht über die Berechtigung, andere Teilnehmer zu entfernen.

*Hinweis:* Für geteilte Mediatheken in der App „Fotos“ ist iOS 16 bzw. iPadOS 16.1 (oder neuer) erforderlich. Wenn du herausfinden möchtest, welche Version der Software auf deinem Gerät installiert ist, wähle „Einstellungen“ > „Allgemein“ und tippe auf „Info“.



### 1. Führe beliebige der folgenden Schritte aus:

- Um Teilnehmer aus einer geteilten Mediathek zu entfernen, wähle „Einstellungen“  > „Fotos“ > „Geteilte Mediathek“ und tippe auf „Teilnehmer löschen“.
- Um eine geteilte Mediathek zu verlassen, wähle „Einstellungen“ > „Fotos“ > „Geteilte Mediathek“ und tippe auf „Geteilte Mediathek verlassen“.

Wenn du eine geteilte Mediathek verlässt, kannst du alles aus der geteilten Mediathek in deine eigene Mediathek kopieren oder wahlweise nur die Inhalte, die du beigesteuert hast.

- Um eine geteilte Mediathek löschen zu können, musst du ihr Organisator sein. Wähle „Einstellungen“ > „Fotos“ > „Geteilte Mediathek“ und tippe auf „Geteilte Mediathek löschen“.
- Alle Teilnehmer werden benachrichtigt, dass die geteilte Mediathek gelöscht wurde.



Weitere Informationen findest du unter:

- „[Einrichten oder Beitreten zu einer geteilten iCloud-Fotomediathek in der App „Fotos“ auf dem iPhone](https://support.apple.com/guide/iphone/iph28ac9ea81)“ im iPhone-Benutzerhandbuch (<https://support.apple.com/guide/iphone/iph28ac9ea81>)
- „[Einrichten oder Beitreten zu einer geteilten iCloud-Fotomediathek in der App „Fotos“ auf dem iPad](https://support.apple.com/guide/ipad/ipad94c5ed43)“ im iPad-Benutzerhandbuch (<https://support.apple.com/guide/ipad/ipad94c5ed43>)

## Verwalten von Kalenderfreigabeeinstellungen

Wenn du bereits eine Person zum Teilen deines Kalenders eingeladen hast, kannst du ihre Bearbeitungsoptionen für diesen Kalender verwalten oder auch die Freigabe des Kalenders für diese Person beenden.

Wenn du Eigentümer:in des Kalenders bist und ihn nicht mehr teilen willst, tippe auf den Namen des:der Abonnent:in, um die Optionen anzuzeigen. Wenn du ein:eine Abonnent:in bist, wähle „Kalender löschen“ aus, um den geteilten Kalender zu entfernen.

1. Tippe auf „Kalender“  auf deinem iPhone oder iPad. Tippe dann auf die Infotaste  neben dem geteilten Kalender, den du bearbeiten möchtest.
2. Tippe auf eine Person und führe einen der folgenden Schritte aus:
  - Aktiviere oder deaktiviere „Bearbeitung zulassen“.
  - Tippe auf „Freigabe stoppen“.



Weitere Informationen findest du unter:

- „[Teilen von iCloud-Kalendern auf dem iPhone](https://support.apple.com/guide/iphone/iph7613c4fb)“ im iPhone-Benutzerhandbuch (<https://support.apple.com/guide/iphone/iph7613c4fb>)
- „[Teilen von iCloud-Kalendern auf dem iPad](https://support.apple.com/guide/ipad/ipadc2a14a22)“ im iPad-Benutzerhandbuch (<https://support.apple.com/guide/ipad/ipadc2a14a22>)

## Verwalten geteilter Tabgruppen in Safari

Du kannst Tabgruppen teilen und mit Personen, die iCloud verwenden, zusammenarbeiten. Eine geteilte Tabgruppe kann bis zu 100 Teilnehmer haben. Teilnehmer können Tabs zur Tabgruppe hinzufügen und Tabs entfernen. Aktualisierungen werden allen Teilnehmern in Echtzeit angezeigt.

Alle, mit denen du zusammenarbeitest, müssen mit ihrer Apple-ID angemeldet sein, Safari in den iCloud-Einstellungen aktiviert haben (<https://support.apple.com/guide/iphone/iphde0f868fd>) und mit aktivierter Zwei-Faktor-Authentifizierung arbeiten.

1. Tippe auf „Safari“  und dann rechts oben auf die Taste „Zusammenarbeiten“ .
2. Tippe auf „Geteilte Tabgruppen verwalten“ und führe einen der folgenden Schritte aus:
  - *Eine Person entfernen:* Tippe erst auf einen Namen und dann auf „Zugriff entfernen“.
  - *Freigabe für alle Personen stoppen:* Tippe auf „Freigabe stoppen“.
  - *Eine Person hinzufügen:* Tippe auf „Mit mehr Personen teilen“ und lade die gewünschten Personen ein.


Weitere Informationen findest du unter:

- [„Personen zu einer geteilten Tabgruppe hinzufügen oder aus ihr entfernen“](https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659) im iPhone-Benutzerhandbuch (https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659)
- [„Personen zu einer geteilten Tabgruppe hinzufügen oder aus ihr entfernen“](https://support.apple.com/guide/ipad/ipad76b9549e#iPad252604e8) im iPad-Benutzerhandbuch (https://support.apple.com/guide/ipad/ipad76b9549e#iPad252604e8)

### Einstellungen für „Mit dir geteilt“ nach Person verwalten

Wenn jemand in den Apps „Musik“, „Apple TV“, „News“, „Fotos“, „Podcasts“ und „Safari“ Inhalte mit dir teilt, zeigt die Option „Mit dir geteilt“ diese Inhalte automatisch im Bereich „Mit dir geteilt“ an, um dir einen einfachen Zugriff auf sie zu ermöglichen.

Inhalte, die mit dir in der App „Nachrichten“ geteilt werden, werden automatisch im Bereich „Mit dir geteilt“ der Apps „Musik“, „Apple TV“, „News“, „Fotos“, „Podcasts“ und „Safari“ angezeigt. Wenn du nicht möchtest, dass in der App „Nachrichten“ geteilte Inhalte in diesen Apps angezeigt werden, kannst du diese Funktion für einzelne Personen deaktivieren.

1. Tippe auf deinem iPhone oder iPad auf „Nachrichten“  und tippe dann auf die Konversation, deren Inhalt nicht in anderen Apps angezeigt werden soll.
2. Tippe in der Konversation auf den Namen der Person oben.
3. Deaktiviere die Option „In ‚Mit dir geteilt‘ anzeigen“ und tippe auf „Fertig“.

Weitere Informationen findest du unter:

- [„Teilen von Inhalten in der App „Nachrichten“ auf dem iPhone“](https://support.apple.com/guide/iphone/iphb66cfeaad) im iPhone-Benutzerhandbuch (https://support.apple.com/guide/iphone/iphb66cfeaad)
- [„Teilen von Inhalten “ in der App „Nachrichten“ auf dem iPad](https://support.apple.com/guide/ipad/ipad5bf3d77b) im iPad-Benutzerhandbuch (https://support.apple.com/guide/ipad/ipad5bf3d77b)

### Einstellungen für „Mit dir geteilt“ für Apps verwalten

Wenn du die Option „Mit dir geteilt“ in der App „Musik“, „Apple TV“, „News“, „Fotos“, „Podcasts“ oder „Safari“ aktivieren oder deaktivieren möchtest, kannst du die entsprechenden Einstellungen anpassen.

- Wähle auf dem iPhone oder iPad „Einstellungen“  > „Nachrichten“ > „Mit dir geteilt“ und deaktiviere „Automatisch teilen“ oder deaktiviere „Mit dir geteilt“ für eine bestimmte App.




## Teilen von Aktivitäten mit der Apple Watch verwalten

Wenn du eine Apple Watch hast und deine Aktivitätsringe mit einer anderen Person geteilt hast, kann diese Person Informationen über dein Aktivitätsniveau und deine Workouts sehen. Die Person erhält keine Informationen über deinen Standort.



Im Tab „Teilen“ der Fitness-App kannst du deine Fortschritte verbergen oder die Freigabe für eine bestimmte Person vollständig beenden. Wenn du deine Aktivität nicht mehr teilen möchtest, wird diese Person nicht benachrichtigt.

1. Öffne die App „Aktivität“  auf deiner Apple Watch.
2. Streiche nach links und drehe die Digital Crown, um zum unteren Bereich des Bildschirms zu scrollen.
3. Um eine Person zu entfernen, mit der du eine Aktivität teilst, tippe auf ihren Namen und dann auf „Entfernen“.

Weitere Informationen findest du unter:

- „[Teilen deiner Aktivität mit der Apple Watch](https://support.apple.com/guide/watch/apd68a69f5c7)“ im Benutzerhandbuch für die Apple Watch (<https://support.apple.com/guide/watch/apd68a69f5c7>)

# Sicher steuern, mit wem Inhalte vom Mac geteilt werden

Es gibt verschiedene Möglichkeiten, um auf deinen Apple-Geräten Inhalte sicher mit anderen zu teilen. Bei jeder Methode kannst du sehen, mit welchen Personen du Inhalte teilst. Außerdem kannst du ihren Zugriff auf geteilte Inhalte auf deinem Mac entfernen.

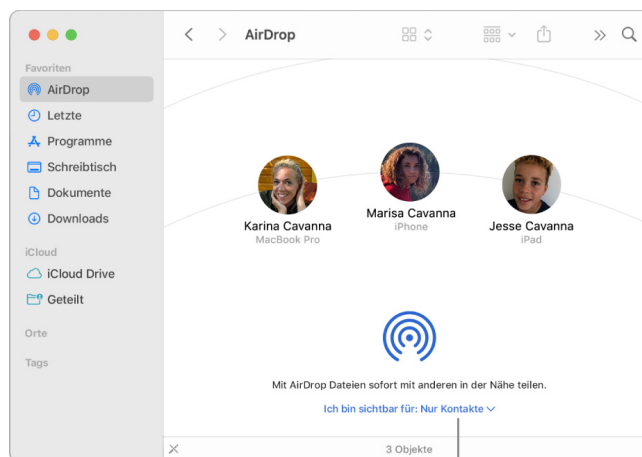


Um zu steuern, welche Inhalte über iPhone, iPad und Apple Watch sicher mit anderen Personen geteilt werden, beachte die Informationen unter [„Sicher steuern, welche Inhalte über iPhone, iPad und Apple Watch geteilt werden“](#) weiter oben in diesem Dokument.

## Dateifreigabeeinstellungen für AirDrop auf dem Mac verwalten


Mit AirDrop kannst du Bilder, Dokumente, und andere Dateien unkompliziert auf verschiedenen Apple-Geräten in der Nähe teilen. Du kannst AirDrop so einrichten, dass alle Personen in deiner Nähe oder nur deine Kontakte Inhalte teilen können oder niemand Inhalte teilen kann.

*Hinweis:* Die Option „Nur Kontakte“ ist auf Geräten mit iOS 10, iPadOS 13.1 und macOS 10.12 oder neuer verfügbar. Wenn deine Geräte eine frühere Softwareversion verwenden und du einschränken möchtest, wer dir Dateien über AirDrop schicken kann, kannst du die Funktion bei Bedarf aktivieren und bei Nichtbenutzung wieder deaktivieren.



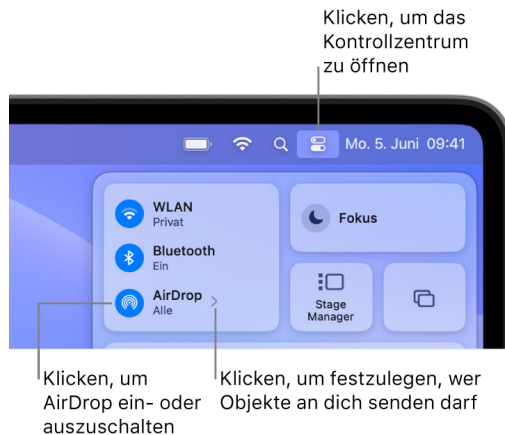
Festlegen, wer Objekte  
an dich senden darf




## AirDrop im Finder verwalten

1. Klicke auf deinem Mac auf das Finder-Symbol  im Dock, um ein neues Finder-Fenster zu öffnen.
2. Klicke in der Finder-Seitenleiste auf „AirDrop“.
3. Klicke im AirDrop-Fenster auf das Einblendmenü „Ich bin sichtbar für“ und wähle deine bevorzugte Option aus.

## AirDrop auf dem Mac im Kontrollzentrum verwalten

Du kannst das Kontrollzentrum auf dem Mac verwenden, um AirDrop schnell ein- oder auszuschalten und auszuwählen, wer dir Objekte mit AirDrop senden kann.



1. Klicke auf deinem Mac auf „Kontrollzentrum“  in der Menüleiste.
2. Führe beliebige der folgenden Schritte aus:
  - *AirDrop ein-/ausschalten*: Klicke auf das AirDrop-Symbol .
  - *Auswählen, wer dir Objekte schicken kann*: Klicke auf die Pfeiltaste  neben AirDrop und wähle deine bevorzugte Option aus.



Weitere Informationen findest du unter:

- „[Verwenden von AirDrop auf deinem Mac zum Senden von Dateien an Geräte in der Nähe](#)“ im macOS-Benutzerhandbuch (<https://support.apple.com/guide/mac-help/mh35868>)

## Verwalten von Freigabeeinstellungen für geteilte Alben in der App „Fotos“ auf dem Mac

Mit den geteilten Alben in der App „Fotos“ auf dem Mac kannst du Fotos und Videos auswählen, die du teilen möchtest. Außerdem kannst du auswählen, mit welchen Personen du sie teilen möchtest. Du kannst auch die Freigabeeinstellungen jederzeit ändern. Wenn du die Freigabe für ein Foto oder Album für eine Person beendest, wird die jeweilige Person nicht darüber benachrichtigt und ihr Zugriff auf das geteilte Album und seine Inhalte wird entfernt.

Wenn du Abonnent:in eines geteilten Albums bist, kannst du alle von dir geteilten Fotos löschen. Außerdem kannst du „Abo beenden“ wählen, um das Abonnement des geteilten Albums zu beenden.

1. Öffne die App „Fotos“  auf deinem Mac. Klicke dann auf ein geteiltes Album unter „Geteilte Alben“ in der Seitenleiste.
2. Klicke auf die Taste „Personen“  in der Symbolleiste.
3. Führe im Feld „Personen einladen“ einen der folgenden Schritte aus:
  - *Neue Abonnent:innen einladen:* Gib eine E-Mail-Adresse ein.  
Wenn die eingeladene Person iCloud nicht nutzt, kannst du das Markierungsfeld „Öffentliche Website“ auswählen, um eine URL für das geteilte Album zu erzeugen. Jeder, der diese URL erhält, kann die Inhalte des geteilten Albums ansehen und laden.
  - *Abonnent:innen entfernen:* Wähle die E-Mail-Adresse des:der Abonnent:in aus und drücke die Löschtaste.
  - *Abonnent:in erneut einladen:* Klicke auf die Pfeiltaste neben dem Namen des:der Abonnent:in und wähle „Einladung erneut senden“.


Weitere Informationen findest du unter:



- „Was sind geteilte Alben in der App ‚Fotos‘ auf dem Mac?“ im Fotos-Benutzerhandbuch (<https://support.apple.com/guide/photos/pht7a4c765b>)
- „Abonnieren geteilter Alben in der App ‚Fotos‘ auf dem Mac“ im Fotos-Benutzerhandbuch (<https://support.apple.com/guide/photos/pht884a8908>)

## Entfernen von Teilnehmern aus einer geteilten Mediathek in der App „Fotos“ auf dem Mac

Mit „Geteilte iCloud-Fotomediathek“ kannst du Fotos und Videos nahtlos mit bis zu fünf anderen Personen teilen. Wenn du Fotos und Videos zu einer geteilten iCloud-Fotomediathek beiträgst, werden diese aus deiner persönlichen in die geteilte Mediathek verschoben. Bei der geteilten Mediathek kannst du wählen, was du teilen möchtest, oder Inhalte automatisch über die Kamera teilen. Alle Teilnehmer haben die gleichen Berechtigungen zum Hinzufügen, Bearbeiten und Löschen von Inhalten in der geteilten Mediathek, wobei die Person, die die geteilte Mediathek eingerichtet hat, d. h. der Ersteller der Mediathek, iCloud-Speicher für alle Inhalte bereitstellt.

Wenn du der Ersteller der Mediathek bist, kannst du Teilnehmer aus der geteilten Mediathek entfernen oder deine geteilte Mediathek jederzeit löschen. Entfernst du Teilnehmer aus deiner geteilten Mediathek, so erhalten diese eine entsprechende Mitteilung und können alle Objekte in der geteilten Mediathek in ihre persönliche Mediathek kopieren. Teilnehmer verfügen nicht über die Berechtigung, andere Teilnehmer zu entfernen. Ist eine Person seit weniger als 7 Tagen Teilnehmer an der geteilten Mediathek, kann sie nur die Objekte abrufen, die sie selbst beigetragen hat.

*Hinweis:* Geteilte Mediatheken in der App „Fotos“ auf dem Mac erfordern macOS 13 (oder neuer). Um herauszufinden, welche Softwareversion auf deinem Gerät installiert ist, wähle „Über diesen Mac“ aus dem Menü „Apple“  oben links auf deinem Bildschirm.

1. Wähle in der App „Fotos“  auf deinem Mac „Fotos“ > „Einstellungen“ und klicke auf „Geteilte Mediathek“.
2. Klicke auf die Taste „Mehr“  neben der Person, die du entfernen möchtest, und wähle „Entfernen“.
3. Klicke auf „Aus geteilter Mediathek entfernen“.


Weitere Informationen findest du unter:

- [„Was ist die geteilte iCloud-Mediathek in ‚Fotos‘ auf dem Mac?“](https://support.apple.com/guide/photos/pht153ab3a01) im Fotos-Benutzerhandbuch (<https://support.apple.com/guide/photos/pht153ab3a01>)

### **Verlassen oder Löschen einer geteilten Mediathek in der App „Fotos“ auf dem Mac**

Teilnehmer können eine geteilte Mediathek jederzeit verlassen. Wenn du der Organisator einer geteilten Mediathek bist, kannst du diese auch löschen. Wenn du die geteilte Mediathek löschst, erhalten alle Teilnehmer eine Benachrichtigung und haben die Wahl, alle Objekte in der geteilten Mediathek in ihre persönliche Mediathek zu übernehmen.

Wenn du eine geteilte Mediathek nach weniger als 7 Tagen als Teilnehmer verlässt, kannst du nur die Objekte sichern, die du selbst beigetragen hast.

*Hinweis:* Geteilte Mediatheken in der App „Fotos“ auf dem Mac erfordern macOS 13 (oder neuer). Um herauszufinden, welche Softwareversion auf deinem Gerät installiert ist, wähle „Über diesen Mac“ aus dem Menü „Apple“  oben links auf deinem Bildschirm.

1. Wähle in der App „Fotos“  auf deinem Mac „Fotos“ > „Einstellungen“ und klicke auf „Geteilte Mediathek“.
2. Klicke auf „Geteilte Mediathek verlassen“ (wenn du ein Teilnehmer bist) oder auf „Geteilte Mediathek löschen“ (wenn du der Organisator bist).
3. Wähle eine der folgenden Optionen:
  - *Alles behalten:* Füge alle Fotos in der geteilten Mediathek zu deiner persönlichen Mediathek hinzu.
  - *Nur eigene Beiträge behalten:* Füge nur die Fotos, die du selbst zur geteilten Mediathek beigetragen hast, deiner persönlichen Mediathek hinzu.
4. Klicke auf „Geteilte Mediathek löschen“ und dann noch einmal auf „Geteilte Mediathek löschen“, um das Löschen zu bestätigen.


Weitere Informationen findest du unter:

- [„Was ist die geteilte iCloud-Mediathek in ‚Fotos‘ auf dem Mac?“](https://support.apple.com/guide/photos/pht153ab3a01) im Fotos-Benutzerhandbuch (<https://support.apple.com/guide/photos/pht153ab3a01>)
- [„Geteilte Mediathek verlassen oder löschen“](https://support.apple.com/guide/photos/pht4dd77b3aa#pht82b300b22) im Fotos-Benutzerhandbuch (<https://support.apple.com/guide/photos/pht4dd77b3aa#pht82b300b22>)


## Verwalten von Kalenderfreigabeeinstellungen auf dem Mac

Wenn du bereits eine Person zum Teilen deines Kalenders eingeladen hast, kannst du ihre Bearbeitungsoptionen für diesen Kalender verwalten oder auch die Freigabe des Kalenders für diese Person beenden.

Wenn du Eigentümer:in des Kalenders bist und ihn nicht mehr teilen willst, tippe auf den Namen des:der Abonnent:in, um die Optionen anzuzeigen. Wenn du ein/e Abonnent:in bist, kannst du „Kalender löschen“ auswählen, um den geteilten Kalender zu entfernen.

1. Öffne die App „Kalender“  auf deinem Mac.
2. Führe einen der folgenden Schritte aus:
  - Auf einem Mac mit macOS 13 oder neuer: Wähle „Kalender“ > „Einstellungen“.
  - Auf einem Mac mit macOS 12 oder älter: Wähle „Kalender“ > „Einstellungen“.
3. Klicke auf „Accounts“, wähle den Kalenderaccount aus und klicke dann auf „Delegierung“.

In der Liste „Accounts, für die ich Zugriffsrechte habe“ wird ein CalDAV-Account angezeigt.

*Hinweis:* Klicke bei Microsoft Exchange-Accounts auf die Taste „Hinzufügen“  und gib den Namen der Person ein, die dir Zugriffsrechte erteilt hat.



Weitere Informationen findest du unter:

- [„Teilen von Kalenderaccounts auf dem Mac“](https://support.apple.com/guide/calendar/icl27527) im Kalender-Benutzerhandbuch (https://support.apple.com/guide/calendar/icl27527)

## Verwalten geteilter Tabgruppen in Safari auf dem Mac

Du kannst Tabgruppen teilen und mit Personen, die iCloud verwenden, zusammenarbeiten. Eine geteilte Tabgruppe kann bis zu 100 Teilnehmer haben. Teilnehmer können Tabs zur Tabgruppe hinzufügen und Tabs entfernen. Aktualisierungen werden allen Teilnehmern in Echtzeit angezeigt.



Alle, mit denen du zusammenarbeitest, müssen mit ihrer Apple-ID angemeldet sein, Safari in den iCloud-Einstellungen aktiviert haben und mit aktivierter Zwei-Faktor-Authentifizierung arbeiten.

1. Klicke in der App „Safari“  auf deinem Mac auf die Taste „Zusammenarbeiten“  in der Symbolleiste.
2. Klicke auf „Geteilte Tabgruppen verwalten“ und führe einen der folgenden Schritte aus:
  - *Eine Person entfernen:* Klicke auf einen Namen, danach auf „Zugriff entfernen“ und dann auf „Weiter“.
  - *Freigabe für alle Personen stoppen:* Klicke auf „Freigabe stoppen“ und dann auf „Weiter“.
  - *Eine Person hinzufügen:* Klicke auf „Mit mehr Personen teilen“ und dann auf „Nachrichten“, um die gewünschten Personen einzuladen.

Weitere Informationen findest du unter:

- [„Personen zu einer geteilten Tabgruppe hinzufügen oder aus ihr entfernen“](https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659) im Safari-Benutzerhandbuch (https://support.apple.com/guide/iphone/iph4a323d663#iph5f23c7659)

### Auf dem Mac Einstellungen für „Mit dir geteilt“ nach Person verwalten

1. Öffne die App „Nachrichten“  auf dem Mac und wähle die Konversation aus.
2. Klicke auf die Infotaste  in oben rechts in der Konversation und deaktiviere die Option „In ‚Mit dir geteilt‘ anzeigen“, um die geteilten Inhalte aus dem Bereich „Mit dir geteilt“ zu entfernen.


Wenn die Option „Mit dir geteilt“ deaktiviert ist, kannst du weiterhin geteilte Inhalte anheften, um sie in anderen Apps anzuzeigen.

Weitere Informationen findest du unter:

- [„Verfolgen deiner geteilten Inhalte in der App ‚Nachrichten‘ auf dem Mac“](https://support.apple.com/guide/messages/ichtdc9ebc32)  
im Nachrichten-Benutzerhandbuch  
(<https://support.apple.com/guide/messages/ichtdc9ebc32>)

### Auf dem Mac Einstellungen für „Mit dir geteilt“ für Apps verwalten

Wenn du die Option „Mit dir geteilt“ in der App „Musik“, „Apple TV“, „News“, „Fotos“, „Podcasts“ oder „Safari“ aktivieren oder deaktivieren möchtest, kannst du die entsprechenden Einstellungen auf dem Mac anpassen.

1. Öffne die App „Nachrichten“  auf deinem Mac.
  - Auf einem Mac mit macOS 13 oder neuer: Wähle „Nachrichten“ > „Einstellungen“.
  - Auf einem Mac mit macOS 12 oder älter: Wähle „Nachrichten“ > „Einstellungen“.
2. Wähle „Mit dir geteilt“ und führe einen der folgenden Schritte aus:
  - *Alle Apps deaktivieren:* Klicke auf „Deaktivieren“.
  - *Bestimmte Apps deaktivieren:* Deaktiviere die Markierungsfelder neben den entsprechenden Apps.

# Verwalten deines Standorts

## Standort teilen oder Standortfreigabe mit anderen Personen beenden

Mit „Wo ist?“ für iPhone, iPad, Mac und Apple Watch kannst du deine Geräte im Blick behalten. Außerdem ermöglicht die Funktion dir und anderen Personen, eure Standorte miteinander zu teilen.



Wenn du die Familienfreigabe eingerichtet hast und die Standortfreigabe verwendest, werden deine Familienmitglieder automatisch im Tab „Personen“ angezeigt, obwohl sie ihren Standort noch mit dir teilen müssen. Weitere Informationen findest du unter [„Verwalten von Familienfreigabeeinstellungen“](#) weiter unten in diesem Dokument.







### **Informationen zur Standortfreigabe und wo sie angezeigt werden können**

Wenn du mit „Wo ist?“ deinen Standort mit anderen Personen teilst, können diese Personen deinen Standort in den Apps sehen, die in der folgenden Tabelle aufgelistet sind.



Wenn du und die Person, mit der du deinen Standort teilst, ein iPhone mit iOS 15 (oder neuer) verwendet, kannst du außerdem deinen Live-Standort in den unten aufgeführten Apps teilen. Wenn du unterwegs bist, können sich die anderen Personen ein Bild von deiner Bewegungsrichtung und deiner Geschwindigkeit machen.





App	Beschreibung
 Wo ist?	<p>In der App „Wo ist?“ können andere Personen den Tab „Personen“ öffnen und auf deinen Namen tippen, um deinen Standort zu sehen.</p>
 Wo ist?	<p>Wenn du und eine andere Person euren jeweiligen Standort miteinander teilt, ihr beide ein iPhone 15 verwendet und euch in der Nähe voneinander befindet, könnt ihr mit der Funktion „Genaue Suche“ euren genauen Standort bestimmen. Wenn du dich in der Nähe dieser Person befindest, kannst du dich ihr mithilfe der Funktion „Genaue Suche“ nähern, bis du nur wenige Meter von ihr entfernt bist. Wenn eine andere Person dich mit der Funktion „Genaue Suche“ sucht, erhältst du eine Mitteilung darüber, dass diese Person dich sucht.</p> <p>Weitere Informationen findest du unter <a href="https://support.apple.com/de-de/guide/iphone/iph3effd0ed6">Verwenden der Funktion „Genaue Suche“ auf dem iPhone 15, um Bekannte zu treffen</a> im iPhone-Benutzerhandbuch. (<a href="https://support.apple.com/de-de/guide/iphone/iph3effd0ed6">https://support.apple.com/de-de/guide/iphone/iph3effd0ed6</a>)</p>
 Wo ist?	<p>Wenn du die Familienfreigabe eingerichtet hast und die Standortfreigabe verwendest, werden deine Familienmitglieder automatisch im Tab „Personen“ angezeigt. Die Standortfreigabe erfolgt jedoch erst dann, wenn sie deinen Standort mit dir teilen. Weitere Informationen findest du unter <a href="#">Verwalten von Familienfreigabeeinstellungen</a> weiter unten in diesem Dokument.</p>
 Nachrichten	<p>Wenn andere Personen in der App „Nachrichten“ auf dein Kontaktsymbol tippen, wird ihnen die Detailansicht mit deinem aktuellen über „Wo ist?“ geteilten Standort angezeigt.</p>
 Nachrichten	<p>In der App „Nachrichten“ in iOS 17 und iPadOS 17 (oder neuer) können andere Personen außerdem deinen ungefähren Standort oben im Nachrichtenverlauf sehen.</p>
 Karten	<p>Wenn andere deinen Namen in der App „Karten“ suchen, sehen sie deinen aktuellen über „Wo ist?“ geteilten Standort auf der Karte.</p>

## Mitteilungen über dich prüfen und entfernen

Mit der App „Wo ist?“ kannst du [Freund:innen über eine Änderung deines Standorts informieren](https://support.apple.com/guide/iphone/iph9bfec93b1) (<https://support.apple.com/guide/iphone/iph9bfec93b1>). Personen, mit denen du deinen Standort teilst, können außerdem Mitteilungen einrichten, um zu sehen, wenn sich dein Standort ändert.

Du kannst alle Standortänderungsmitteilungen über dich deaktivieren. Das umfasst sowohl alle Mitteilungen, die du festlegst, als auch alle Mitteilungen, die deine Freund:innen erstellen. Weitere Informationen zu Mitteilungen über dich:


1. Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad:* Öffne die App „Wo ist?“  und tippe auf „Ich“.
  - *Auf dem Mac:* Öffne die App „Wo ist?“ , klicke auf „Ich“ und klicke auf die Infotaste ⓘ.

2. Suche den Bereich „Mitteilungen über dich“.
  - Wenn der Bereich „Mitteilungen über dich“ *angezeigt wird*, kannst du einen Namen auswählen, um weitere Details zu sehen.
  - Wenn der Bereich „Mitteilungen über dich“ *nicht* angezeigt wird, erhalten deine Freund:innen keine Mitteilungen, wenn sich dein Standort ändert.
3. Siehst du eine Mitteilung, die du löschen möchtest, wähle zunächst einen Namen und dann eine Mitteilung aus.
4. Lösche die Mitteilung und bestätige, dass du die Mitteilung löschen willst.

### **Teilen des Standorts in der App „Wo ist?“ auf dem iPhone und iPad beenden**



Wenn du das Teilen deines Standorts durch eine der beiden folgenden Methoden beendest, wird dein Standort nicht mehr in der App „Wo ist?“ auf Geräten anderer Personen angezeigt.

*Hinweis:* Wurde die App „Wo ist?“ von deinem Gerät gelöscht, kannst du die Ortungsdienste (unter „Einstellungen“ > „Datenschutz & Sicherheit“ > „Ortungsdienste“) deaktivieren, um sicherzustellen, dass dein Standort nicht geteilt wird. Lade dann erneut die App „Wo ist?“ im App Store.

1. Öffne die App „Wo ist?“ .
2. Führe einen der folgenden Schritte aus:
  - *Teilen mit einer Person beenden:* Wähle den Tab „Personen“ und suche die Person, mit der du deinen Standort nicht mehr teilen möchtest. Tippe auf den Namen der Person, scrolle nach unten und tippe auf „Standort nicht mehr teilen“.
  - *Teilen mit allen Personen beenden:* Wähle den Tab „Ich“ und deaktiviere die Option „Standort teilen“.


### **Teilen des Standorts in der App „Nachrichten“ auf dem iPhone und iPad beenden**

Wenn du das Teilen deines Standorts durch eine der beiden folgenden Methoden beendest, wird dein Standort nicht mehr in der App „Nachrichten“ auf Geräten anderer Personen angezeigt.

1. Öffne die App „Nachrichten“ .
2. Führe einen der folgenden Schritte aus:
  - *Teilen in einer Konversation beenden:* Wähle die Konversation mit der Person aus, mit der du deinen Standort nicht mehr teilen willst, und tippe auf den Namen der Person oben in der Konversation. Tippe dann auf „Freigabe stoppen“.
  - *Teilen durch Löschen der Konversation beenden:* Streiche in der Liste der Konversationen in der App „Nachrichten“ auf der entsprechenden Konversation nach links, tippe auf  und tippe auf „Ja“, um zu bestätigen, dass du deinen Standort nicht mehr mit den Teilnehmer:innen dieser Konversation teilen möchtest.

### Teilen deines Standorts in der App „Kontakte“ auf dem iPhone und iPad beenden

Wenn du das Teilen deines Standorts durch eine der beiden folgenden Methoden beendest, wird dein Standort nicht mehr in der App „Kontakte“ auf Geräten anderer Personen angezeigt.

1. Öffne die App „Kontakte“ .
2. Tippe auf den Namen der Person.
3. Tippe auf „Standort nicht mehr teilen“.


### Wann du „Mein iPhone suchen“ für ein verlorenes oder gestohlenen Gerät deaktivieren solltest

Um Diebstahl vorzubeugen und dir beim Finden deines iPhone zu helfen, wenn du es verloren hast, kannst du die Option „Mein iPhone suchen“ unter „Einstellungen“ > „[dein Name]“ > „Wo ist?“ aktivieren.





Wenn die Option „Mein iPhone suchen“ aktiviert ist, dann ist dein Gerät für 24 Stunden nachdem es ausgeschaltet oder vom Internet getrennt wurde, im „Wo ist?“-Netzwerk auffindbar. Der Standort deines Geräts wird im Tab „Geräte“ in der App „Wo ist?“ auf deinen anderen Geräten und für Personen in der Familienfreigabe angezeigt, mit denen du deinen Standort teilst.

Wenn du einen sicheren Ort erreichen musst und dein Gerät ausschalten möchtest, dir aber Sorgen darüber machst, dass eine andere Person diese Funktion nutzen könnte, um deinen Standort zu ermitteln, kannst du das „Wo ist?“-Netzwerk vorübergehend deaktivieren, wenn du beim Ausschalten auf „iPhone nach dem Ausschalten auffindbar“ (unter dem Schieberegler „Ausschalten“) tippst und die Anleitung auf dem Bildschirm befolgst. Verwende die folgende Aufgabe, wenn du diese Funktion deaktivieren möchtest.

**Wichtig:** Wenn du „Mein [Gerät] suchen“ und das „Wo ist?“-Netzwerk deaktivierst, kannst du dein Gerät nicht finden, sperren oder löschen, wenn es verloren geht oder gestohlen wird.

- Auf iPhone oder iPad: Wähle „Einstellungen“  > „[dein Name]“ > „Wo ist?“ > „Mein iPhone suchen“ > „Wo ist?“-Netzwerk.

Wenn du diese Funktion deaktivierst, kannst du sie nicht nutzen, wenn dein Gerät verloren geht oder gestohlen wurde und ausgeschaltet ist.



- Auf einem Mac mit macOS 13 oder neuer: Wähle „Apple“  > „Systemeinstellungen“, klicke auf „Apple-ID“ , auf „iCloud“ und dann auf „Optionen“ neben „Meinen Mac suchen“.
- Auf einem Mac mit macOS 12 oder älter: Wähle „Apple“  > „Systemeinstellungen“, klicke auf „Apple-ID“ , auf „iCloud“ und dann auf „Optionen“ neben „Meinen Mac suchen“.

## Verwalten der automatischen Freigabe der erwarteten Ankunftszeit in „Karten“

In „Karten“ auf dem iPhone und iPad (WiFi + Cellular-Modelle) kannst du deine erwartete Ankunftszeit an einem Ziel automatisch mit allen in deinen Kontakten teilen. Wenn du diese Option eingerichtet hast, wird deine erwartete Ankunftszeit am diesem Ziel mit den Kontakten geteilt. Während du dich auf der Route befindest, wird unten im Bildschirm angezeigt, ob deine erwartete Ankunftszeit mit anderen Personen geteilt wird.




### Verwalten der Freigabe der erwarteten Ankunftszeit auf dem iPhone und iPad

1. Tippe in der App „Karten“  auf deinem iPhone oder iPad (Wi-Fi + Cellular-Modelle) auf dein Profilsymbol rechts in der Suchleiste.
2. Wähle „Favoriten“, um ein Fenster zu öffnen, das alle Orte enthält, die du als Favorit angegeben hast.
3. Tippe auf die Infotaste  neben der favorisierten Sehenswürdigkeit.
4. Scrolle nach unten zum Abschnitt „Ankunftszeit teilen“, um zu überprüfen, mit wem du deine Ankunftszeit automatisch teilst.
5. Um eine Person zu entfernen, tippe auf die Taste „Entfernen“ neben dem Namen der betreffenden Person.
6. Um eine Person hinzuzufügen, tippe auf „Person hinzufügen“. Wähle dann die Person aus deinen Kontakten, mit der du deine erwartete Ankunftszeit bei dieser Sehenswürdigkeit automatisch teilen möchtest.
7. Wiederhole die Schritte 3 bis 6 für alle Sehenswürdigkeiten in deinen Favoriten.

## Die automatische Freigabe der Ankunftszeit nach Beginn der Routensuche stoppen

Du kannst die automatische Freigabe der erwarteten Ankunftszeit auch stoppen, wenn du bereits die Suche nach einer bevorzugten Sehenswürdigkeit begonnen hast. Wenn du diese Methode zum Stoppen der Ankunftszeitfreigabe verwendest, hat die Person bereits die Mitteilung auf ihrem Gerät erhalten, dass du unterwegs zu dem gewählten Ort bist. Sie kann jedoch nicht mehr auf deine erwartete Ankunftszeit oder Route zugreifen.


**Wichtig:** Mit dieser Methode wird die automatische Freigabe mit dieser Person nicht permanent entfernt. Wenn du das nächste Mal zum selben Ort navigierst, beginnt die automatische Ankunftszeitfreigabe erneut. Um dies zu verhindern, musst du den Kontakt aus „Ankunft teilen“ für den betreffenden Ort entfernen.

1. Tippe in der App „Karten“  auf deinem iPhone oder iPad (Wi-Fi + Cellular) auf die Option „Mit [Name des Kontakts] teilen“ unten im Bildschirm.
2. Suche die Person in der Liste, mit der du deine Ankunftszeit nicht mehr teilen möchtest.
3. Wähle „Zum Beenden tippen“ unter dem Namen der Person.

## Verwalten von Einstellungen für Ortungsdienste

Mit deiner Erlaubnis können die Ortungsdienste es Apps (wie „Karten“, „Kamera“, „Wetter“ und andere) und Websites ermöglichen, Informationen von verschiedenen Netzwerken zur Ermittlung deines ungefähren oder genauen Standorts zu nutzen. Ortungsdienste findest du auf dem iPhone, iPad und Mac.









Wenn eine App die Ortungsdienste nutzt, wird das Symbol „Ortungsdienste“  in der Statusleiste oben auf dem Bildschirm deines iPhone oder iPad oder in der Menüleiste auf deinem Mac angezeigt.

Selbst wenn du die Ortungsdienste deaktivierst, können Apps von Drittanbietern andere Möglichkeiten zur Bestimmung deines Standorts nutzen. Unabhängig davon, ob du die Ortungsdienste ein- oder ausgeschaltet hast, können die Standortinformationen deines Geräts für Notrufe genutzt werden, um Hilfsmaßnahmen zu unterstützen.

## Ortungsdienste deaktivieren







Bei der Einrichtung eines Geräts wirst du gefragt, ob die die Ortungsdienste aktivieren möchtest. Nachdem die Einrichtung abgeschlossen ist, kannst du die Ortungsdienste jederzeit ein- oder ausschalten.

- *Auf iPhone oder iPad:* Wähle „Einstellungen“  > „Datenschutz“ > „Ortungsdienste“ und deaktiviere die Option „Ortungsdienste“.
- *Auf einem Mac mit macOS 13 oder neuer:* Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Datenschutz & Sicherheit“  und auf „Ortungsdienste“. Deaktiviere dann die Ortungsdienste, gib dein Passwort ein und klicke auf „Entsperren“.
- *Auf einem Mac mit macOS 12 oder älter:* Wähle Menü „Apple“  > „Systemeinstellungen“ >, klicke auf „Sicherheit & Datenschutz“  und klicke dann auf „Datenschutz“. Klicke auf „Ortungsdienste“. Wenn das Schloss unten links abgeschlossen ist , klicke darauf, um das Fenster für die Einstellungen zu entsperren. Deaktiviere „Ortungsdienste aktivieren“.

## Ortungsdienste aktivieren

Bei der Einrichtung eines Geräts wirst du gefragt, ob die die Ortungsdienste aktivieren möchtest. Nachdem die Einrichtung abgeschlossen ist, kannst du die Ortungsdienste jederzeit ein- oder ausschalten.

Wenn die Ortungsdienste nicht während der Konfiguration aktiviert wurden:

- *Auf iPhone oder iPad:* Wähle „Einstellungen“  > „Datenschutz & Sicherheit“ > „Ortungsdienste“ und aktiviere die Option „Ortungsdienste“.
- *Auf einem Mac mit macOS 13 oder neuer:* Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Datenschutz & Sicherheit“  und auf „Ortungsdienste“. Aktiviere dann die Ortungsdienste, gib dein Passwort ein und klicke auf „Entsperren“.
- *Auf einem Mac mit macOS 12 oder älter:* Wähle Menü „Apple“  > „Systemeinstellungen“ >, klicke auf „Sicherheit & Datenschutz“  und klicke dann auf „Datenschutz“. Klicke auf „Ortungsdienste“. Wenn das Schloss unten links abgeschlossen ist , klicke darauf, um das Fenster für die Einstellungen zu entsperren. Wähle „Ortungsdienste aktivieren“.

## Apps angeben, die Ortungsdienste auf dem iPhone oder iPad nutzen dürfen

Einige Apps funktionieren möglicherweise nicht ordnungsgemäß, wenn die Ortungsdienste deaktiviert sind. Wenn eine App zum ersten Mal auf die Informationen der Ortungsdienste zugreifen muss, erhältst du eine Mitteilung, in der du deine Erlaubnis erteilen kannst. Wähle eine der folgenden Optionen aus:






- Einmal erlauben
- Beim Verwenden der App erlauben
- Nicht erlauben

Du kannst den Zugriff auf deinen Standort auch für einzelne Apps prüfen und ändern sowie angeben, wie oft sie deinen Standort nutzen können. Es folgen Anleitungen für iPhone und iPad.

1. Wähle „Einstellungen“  > „Datenschutz & Sicherheit“ > „Ortungsdienste“ und prüfe oder ändere die Zugriffseinstellungen einer App.  
Tippe auf die App, um Erläuterungen für die Nutzung der Ortungsdienste zu erhalten.
2. Bestimme, wie genau Apps auf deinen Standort zugreifen dürfen.
  - Wenn du einer App erlauben möchtest, deinen genauen Standort zu verwenden, lasse die Option „Genauer Standort“ aktiviert.
  - Wenn du nur deinen ungefähren Standort teilen möchtest (was für eine App ausreichen kann, die nicht deinen exakten Standort benötigt), kannst du die Option „Genauer Standort“ deaktivieren.


*Hinweis:* Wenn du die Zugriffsoption „Nächstes Mal fragen“ für eine App auswählst, wirst du erneut aufgefordert, die Ortungsdienste zu aktivieren, wenn die App sie das nächste Mal verwenden will.

### Apps bestimmen, die Ortungsdienste auf dem Mac nutzen dürfen

1. Führe einen der folgenden Schritte aus:
  - Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Datenschutz & Sicherheit“  und auf „Ortungsdienste“. Deaktiviere dann die Ortungsdienste, gib dein Passwort ein und klicke auf „Entsperren“.
  - Auf einem Mac mit macOS 12 oder älter: Wähle „Apple“  > „Systemeinstellungen“ > „Sicherheit & Datenschutz“  > „Ortungsdienste, deaktiviere die Option „Ortungsdienste aktivieren“. Eventuell musst du die Systemeinstellungen entsperren, bevor du Änderungen vornehmen kannst. Klicke dazu auf das Schlosssymbol  unten links und gib dein Passwort ein.
2. Aktiviere das Markierungsfeld neben einer App, um ihr die Verwendung der Ortungsdienste zu erlauben. Deaktiviere das Markierungsfeld, um die Ortungsdienste für die App zu deaktivieren.
3. Scrolle zu „Systemdienste“ am Ende der Liste und klicke auf die Taste „Details“, um die Systemdienste anzuzeigen, die deinen Standort verwenden.

Wenn du die Ortungsdienste für eine App deaktivierst, wirst du aufgefordert, sie erneut zu aktivieren, wenn die App das nächste Mal versucht, deine Standortdaten zu verwenden.

Wenn du Siri und Safari erlauben möchtest, den Standort deines Mac für Vorschläge zu verwenden, wähle „Ortsbasierte Vorschläge“.

Wenn du deinem Mac erlauben möchtest, Orte zu erkennen, die für dich von Bedeutung sind, und nützliche Informationen dazu in „Karten“, „Kalender“, „Erinnerungen“ und anderen Apps anzuzeigen, wähle „Wichtige Orte“. Die Informationen für die Option „Wichtige Orte“ werden verschlüsselt und können nicht von Apple ausgelesen werden. Klicke auf „Details“, um eine Liste der erkannten Standorte zu sehen. Um einen Standort aus der Liste zu entfernen, wähle ihn aus und klicke auf die Taste „Entfernen“ — . Um alle Standorte zu entfernen, klicke auf die Taste „Mehr“  und klicke auf „Verlauf löschen“.




## Beenden und Entfernen von Standortmetadaten in der App „Fotos“

Wenn die Ortungsdienste für die App „Kamera“ aktiviert sind, werden Informationen aus dem Mobilfunknetz, aus dem WLAN, aus GPS-Netzwerken und aus Bluetooth® verwendet, um den Standort für Fotos und Videos zu bestimmen. Diese Standortmetadaten werden in jedes Foto und Video eingebettet, sodass du später in der App „Fotos“ auf der Basis des Orts, an dem die Fotos und Videos aufgenommen wurden, nach diesen suchen oder Sammlungen im Album „Orte“ ansehen kannst.

Wenn du Fotos und Videos, die Standortmetadaten enthalten, mit anderen Personen teilst, können diese Personen möglicherweise auf die Standortmetadaten zugreifen und Informationen über den Aufnahmeort erhalten. Wenn du nicht möchtest, dass andere Personen auf die Standortmetadaten zu deinen Fotos oder Videos zugreifen können, kannst du die aktuellen Metadaten löschen und verhindern, dass in Zukunft Metadaten erfasst werden.



### Fotos mit eingebetteten Standortmetadaten auf dem iPhone oder iPad prüfen

Mithilfe des Albums „Orte“ in der App „Fotos“ kannst du sehr einfach die Fotos in deiner Mediathek prüfen, in die Standortmetadaten eingebettet sind.

1. Öffne die App „Fotos“  und tippe auf „Alben“.
2. Tippe auf das Album „Orte“ und führe beliebige der folgenden Schritte aus:
  - Wenn du die Fotos aus einem bestimmten Zeitraum prüfen möchtest, tippst du auf „Raster“, um die Objekte in chronologischer Reihenfolge anzuzeigen.
  - Wenn du die Fotos nach dem Aufnahmeort prüfen möchtest, tippst du auf „Karte“, um die Objekte nach Ort anzuzeigen.



### Fotos mit eingebetteten Standortmetadaten auf dem Mac prüfen

Mithilfe des Albums „Orte“ in der App „Fotos“ kannst du sehr einfach die Fotos in deiner Mediathek prüfen, in die Standortmetadaten eingebettet sind.

1. Wähle in der App „Fotos“  auf deinem Mac die Fotos aus, die du überprüfen möchtest.
2. Klicke auf die Infotaste  und prüfe dann die Ortsinformationen.

### Standortmetadaten in der App „Fotos“ auf dem iPhone oder iPad entfernen


So entfernst du die Standortmetadaten, die einem bestimmten Foto zugeordnet sind:

1. Öffne die App „Fotos“  und tippe auf „Alben“.
2. Tippe auf das Album „Orte“ und führe einen der folgenden Schritte aus:
  - Wenn du die Fotos aus einem bestimmten Zeitraum prüfen möchtest, tippst du auf „Raster“, um die Objekte in chronologischer Reihenfolge anzuzeigen.
  - Wenn du die Fotos nach dem Aufnahmeort prüfen möchtest, tippst du auf „Karte“, um die Objekte nach Ort anzuzeigen.
3. Öffne das Foto, von dem du Standortmetadaten entfernen möchtest, und tippe dann auf die Infotaste  oder streiche nach oben.

Du siehst auf einem Bild in der App „Karten“, wo das Foto aufgenommen wurde.
4. Tippe zum Entfernen der Standortmetadaten auf „Anpassen“ und dann auf „Standort entfernen“.


## Standortmetadaten in der App „Fotos“ auf dem Mac entfernen

So entfernst du die Standortmetadaten, die Fotos zugeordnet sind:

1. Wähle in der App „Fotos“  auf deinem Mac die Fotos aus, die du ändern möchtest.
2. Wähle „Bild“ > „Standort“ und anschließend „Standort ausblenden“ oder „Ursprünglichen Standort wiederherstellen“.

## Erfassung der Standortmetadaten in der App „Kamera“ auf dem iPhone oder iPad beenden




Standortmetadaten für Fotos und Videos können nur erfasst werden, wenn deine App „Kamera“ Zugriff auf Ortungsdienste hat.

- Öffne die App „Einstellungen“ , tippe auf „Datenschutz & Sicherheit“ > „Ortungsdienste“ > „Kamera“ und tippe dann auf „Nie“.

Wenn du die Erfassung von Standortmetadaten nicht vollständig beenden möchtest, kannst du die Option „Genauer Standort“ deaktivieren, anstatt „Nie“ auszuwählen. Dann kann die App „Kamera“ Daten zu deinem ungefähren Standort anstelle deines genauen Standorts erfassen.

## Standortmetadaten beim Teilen von Fotos in der App „Fotos“ auf dem iPhone oder iPad nicht anzeigen

Du kannst Fotos mit anderen Personen teilen, ohne auch den Aufnahmeort der Fotos zu teilen.

1. Führe beliebige der folgenden Schritte aus:
  - Öffne die App „Kamera“ , wähle „Aufnahmen“ und wähle dann Fotos aus, die du teilen möchtest.
  - Öffne die App „Fotos“  und wähle Fotos aus, die du teilen möchtest.
2. Tippe auf die Freigabeseite („Share Sheet“)  und dann auf „Optionen“.
3. Deaktiviere die Option „Standort“ und tippe auf „Fertig“.
4. Teile die Fotos über eine der Methoden, die auf der Freigabeseite angeboten werden.

## Erkennen von unerwünschten Tracking-Objekten

Apple hat die AirTags und das „Wo ist?“-Netzwerk so konzipiert, dass Benutzer:innen ihr Eigentum orten und – gleichzeitig – unerwünschtes Tracking verhindern können. Um darüber hinaus sicherzustellen, dass niemand von einem Gerät unerwünscht getrackt wird, haben Apple und Google einen Industriestandard geschaffen. Mit diesem Standard können sich Benutzer:innen (von iOS und Android) benachrichtigen lassen, wenn sie getrackt werden.



Wenn du annimmst, dass deine Sicherheit nicht gewährleistet ist, wende dich an die lokalen Strafverfolgungsbehörden. Wenn es sich bei dem Objekt um ein Apple-Produkt handelt, können die Strafverfolgungsbehörden [mit Apple zusammenarbeiten, um die Informationen zum Objekt anzufordern](https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf) (<https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>). Du musst unter Umständen das AirTag, die AirPods, das Zubehör, das sich im „Wo ist?“-Netzwerk befindet, sowie die Seriennummer des Geräts bereitstellen.

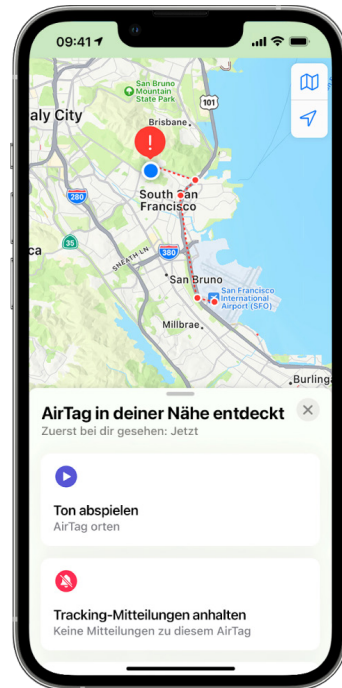
Verfügbarkeit der Software für Hinweise bei unerwünschtem Tracking:

- Hinweise bei unerwünschtem Tracking sind für AirTags und anderes Zubehör, das sich im „Wo ist?“-Netzwerk befindet, auf einem iPhone oder iPad mit iOS 14.5 oder iPadOS 14.5 (oder neuer) verfügbar.
- Hinweise bei unerwünschtem Tracking für unbekannte Bluetooth-Trackinggeräte, die mit der Industriespezifikation [DULT \(Detecting Unwanted Location Trackers\)](https://datatracker.ietf.org/doc/draft-detecting-unwanted-location-trackers/01/) kompatibel sind, sind auf einem iPhone mit iOS 17.5 (oder neuer) verfügbar. (<https://datatracker.ietf.org/doc/draft-detecting-unwanted-location-trackers/01/>)
- Google stellt die Erkennung von unerwünschtem Tracking auf Geräten mit Android 6.0 (oder neuer) bereit.

## Bei Erhalt eines Warnhinweises für unerwünschtes Tracking



Folge den folgenden Schritten, um das Objekt zu suchen:

1. Tippe auf den Hinweis.
2. Tippe auf „Fortfahren“ und dann auf „Ton abspielen“. Du kannst auch (falls verfügbar) auf „In der Nähe suchen“ tippen, um die Funktion „Genaue Suche“ zum Orten des unbekanntes Objekts zu verwenden.



Wenn die Option zum Abspielen eines Tons nicht verfügbar ist oder du das Objekt mit der Funktion „Genaue Suche“ nicht orten kannst, dann befindet sich das Objekt wahrscheinlich nicht mehr in deiner Nähe. Wenn du überzeugt bist, dass sich das Objekt immer noch in deiner Nähe befindet, durchsuche deine Sachen und versuche, das Objekt zu finden. Taste dabei deine Kleidung gründlich ab oder suche überall, wo sich das Gerät befinden könnte. Es könnte sich dort befinden, wo du nicht häufig suchst, z. B. in der Innentasche einer Jacke, in einem Außenfach einer Tasche oder in deinem Fahrzeug. Wenn du das Gerät nicht finden kannst und du dich nicht sicher fühlst, begeben dich an einen sicheren öffentlichen Ort und kontaktiere die Strafverfolgungsbehörden.

## Wenn du zuvor einen Hinweis erhalten hast und die Informationen erneut überprüfen möchtest

1. Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad:* Öffne die App „Wo ist?“ , tippe auf „Objekte“ und dann auf „Bei dir entdeckte Objekte“.
  - *Auf dem Mac:* Öffne die App „Wo ist?“ , klicke auf „Objekte“ und klicke auf „Bei dir entdeckte Objekte“.

Weitere Informationen findest du im Apple Support-Artikel „[Wie gehe ich vor, wenn ich eine Benachrichtigung erhalte, dass sich ein AirTag, ‚Wo ist?‘-Netzwerkzubehör oder ein Satz AirPods in meiner Nähe befindet?](https://support.apple.com/HT212227)“ (<https://support.apple.com/HT212227>).

## Wenn du ein AirTag, „Wo ist?“-Zubehör oder ein kompatibles Bluetooth-Trackinggerät findest

Folge diesen Schritten, um Informationen darüber zu erhalten:

1. Halte die Oberseite des iPhone in die Nähe des Objekts, bis eine Mitteilung erscheint.
2. Tippe auf die Mitteilung. Daraufhin wird eine Website geöffnet, die unter anderem folgende Informationen über das Gerät bereitstellt:
  - Seriennummer oder Geräte-ID
  - Die letzten vier Ziffern der Telefonnummer oder eine unkenntlich gemachte E-Mail-Adresse der Person, die das Objekt registriert hat. Diese Informationen können dir beim Identifizieren der Person helfen, der das Objekt gehört, falls du sie kennst.
3. Wenn das Objekt von der Person, der das Objekt gehört, als verloren markiert wurde, siehst du möglicherweise eine Nachricht mit Informationen, wie du die Person kontaktieren kannst.



### Wenn du beunruhigt bist, dass das Objekt verwendet wird, um dich zu tracken

1. [Erstelle ein Bildschirmfoto](#) des Objekts und der Eigentümerinformationen für deine Unterlagen.
2. Deaktiviere das Gerät und hindere es daran, seinen Standort zu teilen. Tippe dafür auf „Anleitung zum Deaktivieren“ und folge den angezeigten Schritten.
3. Wenn du annimmst, dass deine Sicherheit gefährdet ist, wende dich an die lokalen Strafverfolgungsbehörden. Wenn es sich bei dem Objekt um ein Apple-Produkt handelt, können die Strafverfolgungsbehörden [mit Apple zusammenarbeiten, um die Informationen zum Objekt anzufordern](#). Du musst unter Umständen das AirTag, die AirPods, das Zubehör, das sich im „Wo ist?“-Netzwerk befindetet, sowie die Seriennummer des Geräts bereitstellen.

Weitere Informationen findest du unter <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>.

Nach dem Deaktivieren des Objekts kann die Person, der das Objekt gehört, keine aktuellen Standortinformationen des Objekts mehr abrufen. Außerdem erhältst du ebenfalls keine Hinweise über unerwünschtes Tracking für dieses Objekt mehr.



### AirTags oder „Wo ist?“-Zubehör mit einem Android-Gerät suchen

Weitere Informationen dazu, wie du auf einem Android-Gerät unerwünschtes Tracking identifizierst, findest du auf der Support-Seite [Unbekannte Tracker finden](#). ([https://support.google.com/android/answer/13658562?visit\\_id=638525910154486952-839086324&&hl=de&sjid=4063445914420521927-EU](https://support.google.com/android/answer/13658562?visit_id=638525910154486952-839086324&&hl=de&sjid=4063445914420521927-EU))

## Wenn du einen Ton von einem AirTag hörst

Wenn es bewegt wird, gibt jedes AirTag, das für einen bestimmten Zeitraum von der Person getrennt wird, die es registriert hat, einen Ton aus, um Personen in der Nähe auf sich aufmerksam zu machen. Wenn du ein AirTag findest, das einen Ton ausgegeben hat, kannst du mit jedem Gerät mit Unterstützung für die NFC-Technologie (Near Field Communication), etwa einem iPhone oder Android-Smartphone, herausfinden, ob es als verloren markiert wurde, und dabei helfen, es der Person zurückzugeben, der das Objekt gehört. Wenn du dich in deiner Sicherheit bedroht fühlst, kannst du dich an die lokalen Sicherheitsbehörden wenden, [die dann mit Apple zusammenarbeiten](https://www.apple.com/legal/transparency/government-information.html) (<https://www.apple.com/legal/transparency/government-information.html>). In diesem Fall musst du ggf. das AirTag oder seine [Seriennummer](https://support.apple.com/102170) zur Verfügung stellen. <https://support.apple.com/102170>

## AirTags mit anderen teilen

Mit der Option zum Teilen von Objekten können AirTags mit bis zu fünf Personen geteilt werden. Die Personen, die sich das Objekt ausleihen, haben folgende Möglichkeiten:

- Den Standort des AirTag in der App „Wo ist?“ sehen
- Mit der Funktion „Genaue Suche“ das AirTag orten
- Einen Ton abspielen, wenn das AirTag verloren gegangen ist
- Sich benachrichtigen lassen, wenn eine neue Person der Freigabegruppe beitrifft
- Die Apple-ID oder Kontaktinformationen aller Mitglieder in der Freigabegruppe sehen, wenn die entsprechende Person in ihren Kontakten gesichert ist


*Hinweis:* Die Personen, die sich das AirTag ausgeliehen haben, können nicht sehen, wer das AirTag gerade besitzt.

Da alle Mitglieder einer Freigabegruppe die Position des AirTag sehen können, werden unerwünschte Tracking-Hinweise für das AirTag für alle Gruppenmitglieder unterdrückt. Wenn eine Person die Freigabegruppe verlässt oder die Person, der das Objekt gehört, sie aus der Gruppe entfernt, kann sie die Position des AirTag nicht mehr sehen und die Hinweise bei unerwünschtem Tracking werden wieder gesendet.

Weitere Informationen findest du unter [Teilen eines AirTag oder eines anderen Objekts in der App „Wo ist?“ auf dem iPhone](https://support.apple.com/guide/iphone/iph419cc5f28) im iPhone – Benutzerhandbuch. (<https://support.apple.com/guide/iphone/iph419cc5f28>)


## Dich selbst mithilfe von „Sicherheitsprüfung“ aus einer Freigabegruppe entfernen

*Hinweis:* Nachdem du dich aus der Gruppe entfernt hast, kannst du den Standort des AirTag nicht mehr sehen und die Hinweise bei unerwünschtem Tracking werden wieder aktiviert. Du solltest überprüfen, ob sich das AirTag in deiner Nähe befindet, bevor du dich aus der Freigabegruppe entfernst.


1. Wähle „Einstellungen“  > „Datenschutz & Sicherheit“ > „Sicherheitsprüfung“.
2. Tippe auf „Teilen & Zugriff“ verwalten“.
3. Tippe auf „Objekte“ > „Teilen stoppen“.

### **Dich selbst mithilfe von „Wo ist?“ aus einer Freigabegruppe entfernen**


*Hinweis:* Nachdem du dich aus der Gruppe entfernt hast, kannst du den Standort des AirTag nicht mehr sehen und die Hinweise bei unerwünschtem Tracking werden wieder aktiviert. Du solltest überprüfen, ob sich das AirTag in deiner Nähe befindet, bevor du dich aus der Freigabegruppe entfernst.

1. Öffne die App „Wo ist?“ .
2. Tippe auf „Objekte“ und tippe dann auf das Objekt, bei dem du dich entfernen möchtest.
3. Tippe auf „Entfernen“.

### **Andere Personen mithilfe von „Sicherheitsprüfung“ aus einer Freigabegruppe entfernen**

1. Wähle „Einstellungen“  > „Datenschutz & Sicherheit“ > „Sicherheitsprüfung“.
2. Tippe auf „Teilen & Zugriff verwalten“ > „Fortfahren“.
3. Tippe auf den Namen der Person, mit der du nicht mehr teilen möchtest, und tippe dann auf „Teilen überprüfen“.
4. Tippe auf „Objekte“ und dann auf „Teilen stoppen“.

### **Andere Personen mithilfe von „Wo ist?“ aus einer Freigabegruppe entfernen**

1. Öffne die App „Wo ist?“ .
2. Tippe auf „Objekte“ und tippe dann auf den Namen des Objekts.
3. Tippe auf den Namen der Person, die du entfernen möchtest.
4. Tippe auf „Entfernen“ > „Teilen stoppen“.




# Sicher verwalten, wie Inhalte weitergeleitet werden

Du kannst auf einem iPhone, iPad oder Mac prüfen und verwalten, wie und an wen Inhalte weitergeleitet werden.




## E-Mail-Weiterleitung in Cloud verwalten

Du kannst sehen, ob E-Mails in Mail automatisch an andere E-Mail-Adressen weitergeleitet werden und die Weiterleitung ganz einfach deaktivieren.

1. Melde dich bei iCloud unter <https://www.icloud.com> mit deinem Apple-ID-Benutzernamen und deinem Passwort an. Gib (falls erforderlich) den Code für die Zwei-Faktor-Authentifizierung ein.
2. Klicke auf „Mail“ und dann auf die Taste „Einstellungen“  über der Liste der Postfächer. Wähle danach „Einstellungen“.
3. Prüfe im Tab „Allgemein“, ob die Option „Meine E-Mail weiterleiten“ ausgewählt ist und an wen die Weiterleitung erfolgt. Falls nötig, entferne die Weiterleitungsadresse und beende das Weiterleiten von E-Mails.
4. Prüfe ggf. im Tab „Regeln“ bei welchen Regeln für die Option „dann“ Einstellungen wie „Weiterleiten an“ oder „Weiterleiten an E-Mail-Adresse und als ‚Gelesen‘ markieren“ festgelegt sind und ändere die Regel (falls nötig) entsprechend.
5. Bei iCloud abmelden.


## Weiterleitung von Textnachrichten auf dem iPhone verwalten

Wenn du eine Nachricht an eine Person sendest, die kein iPhone hat, wird deine Nachricht als SMS versendet. Du kannst das iPhone so einrichten, dass beim Senden oder Empfangen einer SMS diese auf anderen Geräten erscheint. Du kannst die Geräteliste prüfen und die Weiterleitung von Textnachrichten an bestimmte Geräte deaktivieren.

1. Wähle auf deinem iPhone „Einstellungen“  > „Nachrichten“.
2. Tippe auf „SMS-Weiterleitung“, um zu sehen, welche Geräte SMS-Nachrichten an dein Gerät senden bzw. von diesem empfangen können.
3. Deaktiviere bestimmte Geräte.

## Anrufweiterleitung auf dem iPhone verwalten

Abhängig von deinem Mobilfunkanbieter kann dein iPhone Anrufe weiterleiten, die du über eine andere Telefonnummer erhältst. Du kannst prüfen, ob empfangene Anrufe von einer anderen Telefonnummer weitergeleitet wurden, und diese Funktion deaktivieren.

1. Wähle auf deinem iPhone „Einstellungen“  > „Telefon“ > „Anrufe“ > „Anrufweiterleitung“.

Wird im Regler grün angezeigt, bedeutet dies, dass die Anrufweiterleitung aktiv ist und du kannst sehen, an welche Telefonnummer deine Anrufe weitergeleitet werden.

*Hinweis:* Wird diese Option nicht angezeigt, ist die Anrufweiterleitung auf deinem iPhone nicht verfügbar. Wenn du weitere Informationen benötigst, wende dich bitte an deinen Mobilfunkanbieter.

2. Deaktiviere ggf. die Anrufweiterleitung.

Durch Deaktivieren der Anrufweiterleitung wird die Telefonnummer nicht benachrichtigt, die bislang die weitergeleiteten Anrufe erhalten hat.

## Ablehnen unbekannter Anmeldeversuche

Wenn du dich auf einem neuen Gerät anmeldest, erhältst du auf deinen anderen vertrauenswürdigen Geräten eine Mitteilung. Diese Mitteilung enthält eine Karte mit Standort des neuen Geräts. Diese Mitteilung kann auf jedem vertrauenswürdigen Gerät angezeigt werden: einem iPhone, iPad oder Mac.



Hierbei handelt es sich um einen ungefähren Standort auf Basis der IP-Adresse oder des Netzwerks, die/das vom Gerät aktuelle genutzt wird. Es ist nicht der exakte Standort des Geräts.

- Wenn du eine Mitteilung darüber erhältst, dass deine Apple-ID für die Anmeldung auf einem neuen Gerät verwendet wird, die nicht von dir ausgeht, tippe auf „Nicht erlauben“, um den Anmeldeversuch zu blockieren. Außerdem kannst du ein Bildschirmfoto von der Mitteilung machen, bevor du sie schließt.

Weitere Informationen findest du unter „[Aufzeichnung verdächtiger Aktivitäten](#)“ weiter unten in diesem Dokument.



Wenn du glaubst, dass deine Apple-ID kompromittiert sein könnte, beachte die Hinweise unter „[Schützen deiner Apple-ID](#)“ (weiter unten in diesem Dokument) und entferne unbekannte Geräte.

# Aufzeichnung verdächtiger Aktivitäten

In manchen Fällen – z. B. wenn du eine Mitteilung darüber erhältst, dass jemand versucht, sich mit deiner Apple-ID auf einem neuen Gerät anzumelden – ist es empfehlenswert, ein Bildschirmfoto oder ein Bildschirmvideo aufzunehmen. Du kannst diese dann als Bild- oder Videodateien auf deinem iPhone, iPad oder Mac sichern.



## Bildschirmfotos oder -videos auf dem iPhone oder iPad aufnehmen

1. Führe einen der folgenden Schritte aus:
  - Auf einem iPhone oder iPad mit Face ID: Drücke gleichzeitig auf die Seitentaste und die Taste „Lauter“ und lasse sie wieder los.
  - Auf einem iPhone oder iPad mit Home-Taste: Drücke gleichzeitig auf die Home-Taste und die Seitentaste oder die Standby-Taste (je nach Modell) und lasse sie wieder los.
2. Tippe auf das Bildschirmfoto unten links und tippe auf „Fertig“.
3. Wähle „In ‚Fotos‘ sichern“, „In ‚Dateien‘ sichern“ oder „Bildschirmfoto löschen“.  
Wenn du „In ‚Fotos‘ sichern“ auswählst, kannst du das Bildschirmfoto im Album „Bildschirmfotos“ in der App „Fotos“ ansehen.

## Bildschirmfotos oder -videos auf dem Mac aufnehmen

1. Drücke die Tastenkombination „Umschalt-Befehl-5“ (oder verwende Launchpad), um die App „Bildschirmfoto“ zu öffnen und die Werkzeuge anzuzeigen.



2. Klicke auf das Werkzeug, das du zum Aufnehmen des Bildschirmfotos oder -videos verwenden möchtest.

Wenn du nur einen Teil des Bildschirms aufnehmen möchtest, bewege den Rahmen an die gewünschte Position oder bewege die Ränder des Rahmens, um die Größe des Aufnahmebereichs anzupassen.


Aktion	Werkzeug
Bildschirmfoto aufnehmen	
Ausgewähltes Fenster aufnehmen	
Bildschirmfoto des Bereichs aufnehmen	
Bildschirmvideo aufnehmen	
Bildschirmvideo des Bereichs aufnehmen	

### 3. Wähle deine gewünschten Optionen aus.

Die verfügbaren Optionen ändern sich abhängig davon, ob du ein Bildschirmfoto oder ein Bildschirmvideo aufnimmst. Du kannst zum Beispiel eine zeitliche Verzögerung festlegen, Mauszeiger oder Klicks anzeigen und festlegen, wo die Datei gesichert werden soll.

Die Option „Schwebende Miniatur anzeigen“ hilft die, leichter mit einem fertigen Foto oder einer fertigen Aufnahmen zu arbeiten. Diese Miniatur wird einige Sekunden lang unten rechts auf dem Bildschirm angezeigt, damit du Zeit hast, sie in ein Dokument zu bewegen, zu markieren oder zu teilen, bevor sie am festgelegten Ort gesichert wird.

### 4. Aufnahme eines Bildschirmfotos oder -videos starten:

- *Zum Aufnehmen eines Bildschirmfotos vom gesamten Bildschirm oder von einem Teil des Bildschirms:* Klicke auf „Aufnehmen“.
- *Zum Aufnehmen eines Fensters:* Bewege den Zeiger zum Fenster und klicke auf das Fenster.
- *Zum Aufnehmen eines Bildschirmvideos:* Klicke auf „Aufnehmen“. Wenn du die Aufnahme beenden möchtest, klicke auf die Taste „Aufnahme stoppen“  in der Menüleiste.

Wenn die Option „Schwebende Miniatur anzeigen“ ausgewählt ist, kannst du beliebige der folgenden Aktionen ausführen, während die Miniatur unten rechts auf dem Bildschirm angezeigt wird:

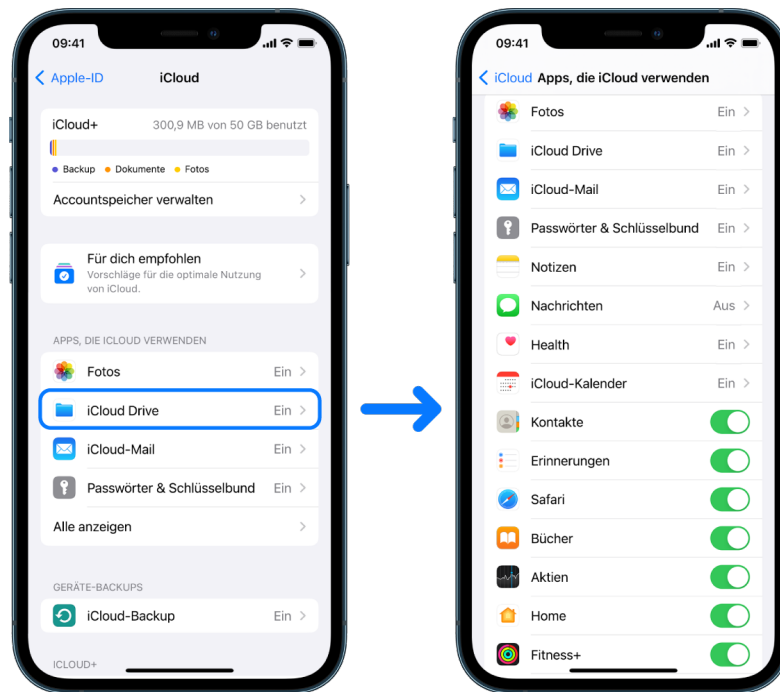
- Streiche nach rechts, um die Datei sofort zu sichern und die Miniatur auszublenden.
- Bewege die Miniatur in ein Dokument, eine E-Mail, eine Notiz oder ein Finder-Fenster.
- Klicke auf die Miniatur, um ein Fenster zu öffnen, in der du das Bildschirmfoto markieren – oder das Video kürzen – kannst, um das Ergebnis anschließend zu teilen.

Je nachdem, welchen Ort du zum Sichern des Bildschirmfotos oder -videos ausgewählt hast, wird möglicherweise ein App geöffnet.

# Sicheres Speichern von Daten in iCloud

iCloud speichert deine Fotos, Videos, Dokumente, Musik, Apps, Gerätebackups und mehr auf sichere Weise und sorgt dafür, dass sie auf allen deinen Geräten aktuell sind. Außerdem ermöglicht dir iCloud, Inhalte mit Freund:innen und Familienmitgliedern zu teilen – z. B. Fotos, Kalender und deinen Standort. Mit deiner Apple-ID kannst du dich auf deinem Gerät oder im Internet bei iCloud anmelden.

Weitere Informationen darüber, was in iCloud gespeichert wird, findest du im [iCloud-Benutzerhandbuch](https://support.apple.com/guide/icloud/) (<https://support.apple.com/guide/icloud/>).



## iCloud-Sicherheitsoptionen






Apple bietet Benutzern zwei Optionen zur Verschlüsselung und zum Schutz der in iCloud gespeicherten Daten:

- *Standardmäßiger Datenschutz (die Standardeinstellung)*: Deine iCloud-Daten werden verschlüsselt, die zugehörigen Schlüssel werden in Apple-Datenzentren gesichert und Apple kann dich bei der Daten- und Accountwiederherstellung unterstützen. Nur bestimmte iCloud-Daten – 14 Datenkategorien, darunter Daten der App „Health“ und Passwörter im iCloud-Schlüsselbund – erhalten eine Ende-zu-Ende-Verschlüsselung.
- *Erweiterter Datenschutz für iCloud*: Eine optionale Einstellung, die dir das höchste Maß an Cloud-Datensicherheit bei Apple bietet. Wenn du dich für die Aktivierung von „Erweiterter Datenschutz“ entscheidest, behalten deine vertrauenswürdigen Geräte für die meisten deiner iCloud-Daten den alleinigen Zugriff auf die Schlüssel der Verschlüsselung und schützen die Daten mittels Ende-zu-Ende-Verschlüsselung. Außerdem steigt mit der Option „Erweiterter Datenschutz“ die Anzahl der Datenkategorien mit Ende-zu-Ende-Verschlüsselung auf 23 und schließt deine Daten aus „iCloud-Backup“, „Fotos“, „Notizen“ und mehr ein.

Weitere Informationen findest du in den Apple Support-Artikeln [So aktivierst du den erweiterten Datenschutz für iCloud](https://support.apple.com/108756) (https://support.apple.com/108756) und [Sicherheitsüberblick – iCloud-Daten](https://support.apple.com/102651) sowie der Tabelle „Datenkategorien und Verschlüsselung“ (https://support.apple.com/102651).






### iCloud-Einstellungen anzeigen und ändern

Du kannst deine iCloud-Einstellungen auf jedem deiner Geräte anzeigen und ändern. Darunter auch, welche Apps (von Apple und Drittanbietern) iCloud, iCloud-Backups usw. verwenden:

- *Auf iPhone oder iPad*: Wähle „Einstellungen“  > „[dein Name]“ > „iCloud“.  
Wenn du diese Funktion deaktivierst, kannst du sie nicht nutzen, wenn dein Gerät verloren geht oder gestohlen wurde und ausgeschaltet ist.
- *Auf einem Mac mit macOS 13 oder neuer*: Wähle „Apple“  > „Systemeinstellungen“, klicke auf „Apple-ID“  und dann auf „iCloud“.
- *Auf einem Mac mit macOS 12 oder älter*: Wähle „Apple“  > „Systemeinstellungen“, klicke auf „Apple-ID“  und dann auf „iCloud“.

### Bei iCloud abmelden

Du kannst dich auf einem Gerät auch vollständig von iCloud abmelden. Wenn du dich von iCloud abmeldest, werden keine Backups der Informationen auf diesem Gerät mehr erstellt.

- *Auf iPhone oder iPad*: Wähle „Einstellungen“  > „[dein Name]“, scrolle nach unten und tippe auf „Abmelden“.
- *Auf einem Mac mit macOS 13 oder neuer*: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Apple-ID“ , auf „Übersicht“ und dann auf „Abmelden“.
- *Auf einem Mac mit macOS 12 oder älter*: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Apple-ID“ , klicke auf „Übersicht“ und dann auf „Abmelden“.



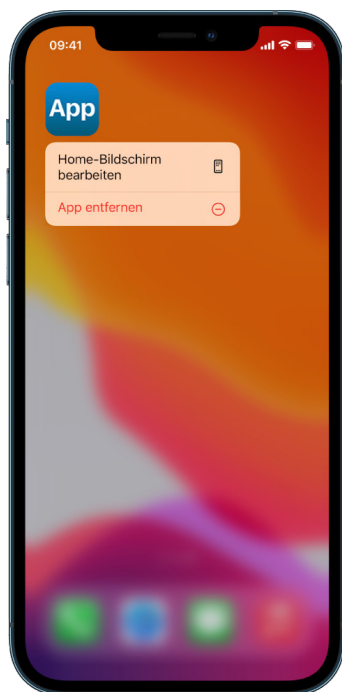
# Löschen verdächtiger Inhalte auf deinen Geräten

Du kannst alle Inhalte löschen, die du für bedenklich hältst oder die dir nicht bekannt vorkommen, darunter unbekannte Apps und Konfigurationsdateien auf deinem iPhone, iPad oder Mac.



## Apps auf dem iPhone oder iPad überprüfen und löschen


Wenn du befürchtest, dass eine Person, der du einmal vertraut hast, ohne dein Einverständnis eine App auf deinem Gerät installiert hat, kannst du eine Liste aller auf dem Gerät installierten Apps durchgehen und überprüfen oder ändern, wie diese Apps auf deine Informationen zugreifen. Wenn dir auffällt, dass eine App auf deine Daten zugreifen kann und du dich nicht erinnern kannst, diese App installiert oder ihr Zugriff auf deine Daten gegeben zu haben, solltest du diese App eventuell entfernen.



- *Eine App aus der App-Mediathek löschen:* Gehe zum Home-Bildschirm und streiche nach links, vorbei an allen deinen Home-Bildschirmseiten, um die App-Mediathek zu erreichen. Tippe als Nächstes in das Suchfeld, finde das Symbol der App und lege den Finger darauf, bis das Menü eingeblendet wird. Tippe zum Löschen auf „App löschen“.
- *Ein App vom Home-Bildschirm löschen:* Lege den Finger auf die App auf dem Home-Bildschirm, tippe auf „App entfernen“ und tippe dann auf „Vom Home-Bildschirm entfernen“, um die App in der App-Mediathek zu behalten, oder auf „App löschen“, um sie zu löschen.

## Apps auf deinem Mac überprüfen und löschen

Du kannst Apps löschen, die aus dem Internet oder von einem Datenträger geladen und installiert wurden.

1. Klicke auf das Finder-Symbol  im Dock und dann auf „Programme“ in der Finder-Seitenleiste.
2. Führe einen der folgenden Schritte aus:
  - *Wenn sich die App in einem Ordner befindet:* Öffne den Ordner der App, um nach einem Deinstallationsprogramm zu suchen. Wenn „[App] deinstallieren“ oder „[App] Uninstaller“ angezeigt wird, doppelklicke darauf und befolge die Anleitung auf dem Bildschirm.
  - *Wenn sich die App nicht in einem Ordner befindet und kein Deinstallationsprogramm vorhanden ist:* Bewege die App aus dem Ordner „Programme“ in den Papierkorb (am Ende des Docks).

**ACHTUNG:** Die App wird dauerhaft von deinem Mac entfernt, sobald der Papierkorb von dir oder dem Finder geleert wird. Wenn du Dateien mit der App erstellt hast, kannst du diese dann möglicherweise nicht mehr öffnen. Wenn du die App doch behalten möchtest, lege sie zurück, bevor du den Papierkorb leerst. Wähle die App im Papierkorb aus und wähle „Ablage“ > „Zurücklegen“.

Verwende Launchpad, um Apps aus dem App Store zu deinstallieren.

## Konfigurationsprofile überprüfen

Möglicherweise nutzen Organisationen (wie Bildungseinrichtungen und Unternehmen) Gerätekonfigurationsprofile, Werkzeuge für die Mobilgeräteverwaltung (Mobile Device Management, MDM) und eigene Apps zur Verwaltung oder Betreuung von Geräten. Diese Werkzeuge können den Zugriff auf Daten oder Standortinformationen auf einem Gerät ermöglichen.

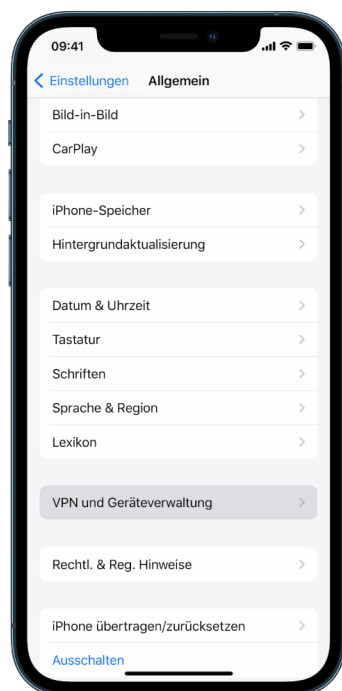
Konfigurationsprofile können Einstellungen für den -E-Mail-Account von Benutzer:innen, WLAN-Einstellungen, VPN-Einstellungen und mehr enthalten. Konfigurationsprofile können auf iPhone und iPad, Mac und Apple TV verwendet werden.

Wenn du ein Konfigurationsprofil auf deinem Gerät entdeckst, das dort nicht vorhanden sein sollte, kannst du es löschen, je nachdem, von wem es installiert wurde. Dadurch werden alle Einstellungen, Apps und Daten gelöscht, die mit dem Konfigurationsprofil verknüpft sind.

**Wichtig:** Wenn dein Gerät einer Bildungseinrichtung oder einem Unternehmen gehört, wende dich an deinen Systemadministrator, bevor du Apps oder Profile löschst.

## Unbekannte Konfigurationsprofile auf deinem iPhone oder iPad löschen

1. Wähle „Einstellungen“  > „Allgemein“ > „VPN und Geräteverwaltung“.







Wenn keine Profile angezeigt werden, sind keine Geräteverwaltungsprofile auf deinem Gerät installiert.

2. Wähle das Profil aus, tippe auf „Profil löschen“ und befolge die Anleitung auf dem Bildschirm. Starte dein Gerät neu.


Wenn du ein Profil entfernst, werden alle seine Einstellungen und Informationen gelöscht. Wenn beispielsweise das Profil Berechtigungen für ein VPN (Virtual Private Network) bereitgestellt hat, um den Zugriff zu einem Schulnetzwerk zu ermöglichen, kann die VPN-Netzwerkverbindung nicht mehr hergestellt werden.

## Unbekannte Konfigurationsprofile auf deinem Mac löschen

1. Führe einen der folgenden Schritte aus:

- Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Einstellungen“ > „Datenschutz & Sicherheit“ und klicke auf „Profile“ .
- Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke auf „Profile“ .

Wenn der Einstellungsbereich „Profile“ nicht angezeigt wird, sind keine Geräteverwaltungsprofile auf deinem Gerät installiert.

2. Wähle ein Profil aus der Liste der Profile aus und klicke auf die Taste „Entfernen“ .

Wenn du ein Profil entfernst, werden alle seine Einstellungen und Informationen gelöscht. Wenn das Profil beispielsweise zu Einrichtung deines E-Mail-Accounts verwendet wurde, werden bei der Entfernung des Profils die Informationen über diesen E-Mail-Account von deinem Mac gelöscht.

## Verwalten von Familienfreigabeeinstellungen

Die Familienfreigabe kann von bis zu fünf Familienmitgliedern genutzt werden, um Abonnements, Käufe, Fotos, Fotoalben, einen Kalender und mehr zu teilen, ohne den eigenen Apple-Account mit anderen Familienmitgliedern zu teilen. Wenn du deinen Familienfreigabestatus ändern möchtest, ist es empfehlenswert, die Funktionen der verschiedenen Rollen in einer Familienfreigabegruppe zu kennen. Du findest die Option „Familienfreigabe“ auf dem iPhone, iPad und Mac.

Wenn du einen iCloud-Speicherplan mit Familienfreigabe nutzt, bleiben Dateien und Dokumente jeder Person privat, während die Menge des von den einzelnen Personen in Anspruch genommenen Speicherplatzes für alle Mitglieder sichtbar ist.



## Arten von Mitgliedern in einer Familienfreigabegruppe

Mitglieder einer Familienfreigabegruppe können je nach Alter verschiedene Rollen haben.

*Hinweis:* Das Alter, in dem eine Person als Erwachsener bzw. als Kind gilt, ist je nach Land oder Region unterschiedlich.



- *Organisator:in:* Eine erwachsene Person, die eine Familienfreigabegruppe einrichtet. Organisator:innen können Familienmitglieder einladen und entfernen und die Gruppe auflösen.
- *Erwachsene:r:* Ein Mitglied einer Familienfreigabegruppe im Alter von mindestens 18 Jahren.
- *Erziehungsberechtigte:r* Ein erwachsenes Familienmitglied der Familienfreigabegruppe, das an der Verwaltung der Kindersicherung für Kinder in der Gruppe teilnehmen kann. Wenn der:die Organisator:in eine erwachsene Person zur Familienfreigabegruppe hinzufügt, kann diese Person als Elternteil oder erziehungsberechtigte Person gekennzeichnet werden.
- *Kind oder Teen:* Ein Mitglied einer Familienfreigabegruppe, das unter 18 Jahre alt ist. Organisator:innen oder Erziehungsberechtigte können eine Apple-ID für Kinder erstellen, die zu jung sind, um diese selber zu erstellen.

In deinem Haushalt wählt eine erwachsene Person, die als *Familienorganisator:in* festgelegt wurde, die Funktionen aus, die die Familie teilt, und kann bis zu fünf weitere Mitglieder einladen. Nachdem die Einladungen angenommen wurde, wird die Familienfreigabe auf allen Geräten automatisch eingerichtet – darunter auch ein geteilter Kalender und ein geteiltes Fotoalbum. Der:die Familienorganisator:in kann alle Personen mit einer Apple-ID zur Familie hinzufügen und alle Personen ab 13 Jahre aus der Familiengruppe entfernen.

Unter Einstellungen > „[dein Name]“ kannst du sehen, ob du bereits Teil einer Familiengruppe bist. Wenn „Familienfreigabe einrichten“ angezeigt wird, verwendest du die Familienfreigabe nicht mit deiner aktuellen Apple-ID. Wenn du das Symbol „Familienfreigabe“ siehst, kannst du auf es tippen, um deine Familienmitglieder und ihre Rollen zu sehen.

## Familienmitglieder entfernen

Der:die Organisator:in einer Familienfreigabegruppe kann andere Mitglieder entfernen.

*Hinweis:* Um mit dem Entfernen von Familienmitgliedern zu beginnen, lies die Informationen zu den beiden Aufgaben „[Mitglieder auf dem iPhone oder iPad aus einer Familiengruppe entfernen](#)“ und „[Mitglieder auf dem Mac aus einer Familiengruppe entfernen](#)“ weiter unten in diesem Dokument.

Alle Familienmitglieder, die älter als 13 Jahre sind, können sich zudem selbst jederzeit aus einer Familiengruppe entfernen. Wähle einfach deinen Namen aus und wähle dann „Familie verlassen“. Du kannst dich auch bei der [Apple-ID-Website](https://appleid.apple.com) (<https://appleid.apple.com>) anmelden und „Account entfernen“ im Bereich „Familienfreigabe“ auswählen.

Aus Sicherheitsgründen können sich Kinder (unter 13 Jahre) nicht aus einer Familie entfernen und die Freigabe von Informationen wie der Bildschirmzeit nicht ohne Eingabe des Bildschirmzeit-Codes beenden. Organisator:innen können auf geteilte Inhalte auf deinem Gerät zugreifen – darunter geteilte Fotoalben und geteilte Kalender – und deine Bildschirmzeit-Aktivitäten einsehen.

*Hinweis:* Organisator:innen können sich selbst nicht aus der Familienfreigabegruppe entfernen. Wenn du den/die Organisator:in ändern möchtest, musst du die Gruppe auflösen und von einem/einer anderen Erwachsenen eine neue Gruppe erstellen lassen.

Wenn ein Mitglied aus der Familienfreigabegruppe entfernt wird oder sie verlässt, behält es die Käufe, die mit der geteilten Kreditkarte getätigt wurden, verliert aber sofort den Zugriff auf andere Objekte, die von den Familienmitgliedern geteilt werden:


- Die Objekte anderer Familienmitglieder werden nicht mehr im Bereich „Käufe“ im iTunes Store, App Store und in Apple Books angezeigt.
- Früher geladene (urheberrechts)geschützte Musiktitel, Filme, TV-Sendungen, Bücher und Apps können nicht mehr genutzt werden, wenn sie ursprünglich von einer anderen Person gekauft wurden. Andere Familienmitglieder können diese aus deiner Sammlung geladenen Inhalte nicht mehr nutzen.
- In-App-Käufe sind nicht mehr nutzbar, wenn du sie in einer App gekauft hast, die ursprünglich von einer anderen Person gekauft wurde. Du kannst diese In-App-Käufe wieder nutzen, wenn du die entsprechende App kaufst.
- Die Gerätestandorte von Familienmitgliedern werden nicht mehr angezeigt, wenn du die App „Wo ist?“ auf iCloud.com oder auf deinen iPhone, iPad oder Mac verwendest.

## Wenn die Familienfreigabe deaktiviert ist

Wenn der:die Familienorganisator:in die Familienfreigabe deaktiviert, werden alle Familienmitglieder gleichzeitig aus der Familiengruppe entfernt. Wenn Kinder unter 13 Jahre Teile der Familiengruppe sind, musst du sie in eine andere Familie übertragen, bevor du deine Familiengruppe auflösen kannst.

### Mitglieder auf dem iPhone oder iPad aus einer Familiengruppe entfernen





Wenn du der:die Familienorganisator:in bist:

1. Wähle „Einstellungen“  > „[dein Name]“ > „Familienfreigabe“.
2. Tippe auf „[Name des Mitglieds]“ und tippe auf „[Name des Mitglieds] aus der Familie entfernen“.

*Hinweis:* Wenn du der:die Familienorganisator:in bist, kannst du dich nicht selbst aus der Familienfreigabe entfernen.

### Mitglieder auf dem Mac aus einer Familiengruppe entfernen


Wenn du der:die Familienorganisator:in bist:

1. Führe einen der folgenden Schritte aus:
  - Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Einstellungen“, klicke auf „Familienfreigabe“  und wähle „Familienfreigabe“ in der Seitenleiste.
  - Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Familienfreigabe“  und wähle „Familienfreigabe“.
2. Wähle ein Mitglied aus der Liste aus und klicke auf die Taste „Entfernen“ —.

*Hinweis:* Wenn du der:die Familienorganisator:in bist, kannst du dich nicht selbst aus der Familienfreigabe entfernen.





### Eine Familienfreigabegruppe auf dem iPhone oder iPad verlassen

Wenn du über 13 Jahre alt und Mitglied einer Familienfreigabegruppe bist:

1. Wähle „Einstellungen“  > „[dein Name]“ > „Familienfreigabe“.
2. Tippe auf „[dein Name]“ und tippe auf „Nutzung der Familienfreigabe beenden“.


## Eine Familienfreigabegruppe auf dem Mac verlassen

Wenn du über 13 Jahre alt und Mitglied einer Familienfreigabegruppe bist:

1. Führe einen der folgenden Schritte aus:
  - Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Einstellungen“, klicke auf „Familienfreigabe“  und wähle „Familienfreigabe“ in der Seitenleiste.
  - Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Familienfreigabe“  und wähle „Familienfreigabe“.
2. Klicke in der Liste der Familienmitglieder auf „Details“ neben deinem Namen, klicke auf „Nutzung der Familienfreigabe beenden“ und befolge die Anleitung auf dem Bildschirm.
3. Klicke auf „Fertig“.





## Familienfreigabe auf dem iPhone oder iPad beenden

Du musst der:die Familienorganisator:in sein, um die Familienfreigabe zu beenden.

1. Wähle „Einstellungen“  > „[dein Name]“ > „Familienfreigabe“.
2. Tippe auf deinen Namen und tippe dann auf „Nutzung der Familienfreigabe beenden“.

## Familienfreigabe auf dem Mac beenden

Du musst der:die Familienorganisator:in sein, um die Familienfreigabe zu beenden.

1. Führe einen der folgenden Schritte aus:
  - Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Einstellungen“, klicke auf „Familienfreigabe“  und wähle „Familienfreigabe“ in der Seitenleiste.
  - Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Familienfreigabe“  und wähle „Familienfreigabe“.
2. Klicke auf die Taste „Details“ neben deinem Namen und klicke auf „Familienfreigabe beenden“.



# Erkennen von betrügerischen Anfragen zum Teilen von Informationen

Sei vorsichtig, wenn du unaufgeforderte Nachrichten erhältst, die dich zum Annehmen von Geschenken, Laden von Dokumenten, Installieren von Software oder Öffnen von verdächtigen Links auffordern. Personen, die auf deine persönlichen Informationen zugreifen wollen, nutzen jedes zur Verfügung stehende Mittel – gefälschte E-Mails und Textnachrichten, irreführende Pop-up-Werbung, falsche Downloads, Spam-Kalender und sogar falsche Telefonanrufe –, um dich zum Teilen deiner Informationen zu bewegen und beispielsweise deine Apple-ID, dein Passwort oder einen Verifizierungscode für die Zwei-Faktor-Authentifizierung (2FA) preiszugeben.

Tipps dazu, wie du verhindern kannst, dass deine Accounts oder persönlichen Informationen kompromittiert werden, findest du im Apple Support-Artikel „[Phishing-Nachrichten, falsche Supportanrufe und andere Betrugsversuche erkennen und vermeiden](https://support.apple.com/102568)“ (<https://support.apple.com/102568>).


*Hinweis:* Unter „Phishing“ versteht man betrügerische Versuche, persönliche Informationen von dir zu erhalten.

## Sicheres Kontrollieren deines Home-Zubehörs

Wenn du Mitglied in einem Zuhause bist, kannst du dein Home-Zubehör leicht und sicher mit der App „Home“ auf deinem iPhone, iPad und Mac oder mit einem HomePod anzeigen und steuern.


*Hinweis:* Home-Zubehör ist sowohl von Apple als auch von Drittanbietern erhältlich. Eine Liste des verfügbaren Home-Zubehörs, das mit der App „Home“ und deinen Apple-Geräten kompatibel ist, findest du unter [Home-Zubehör](https://www.apple.com/de/home-app/accessories/) (<https://www.apple.com/de/home-app/accessories/>).

### Teilen deines Zuhauses mit einer anderen Person beenden

1. Tippe oder klicke auf App „Home“  und wähle „Einstellungen des Zuhauses“. Wenn mehr als ein Zuhause angezeigt wird, wähle das Zuhause, das du verlassen möchtest und wähle „Einstellungen des Zuhauses“.
2. Tippe unter „Personen“ auf den/die Benutzer:in, den/die du aus deinem Zuhause entfernen möchtest und tippe oder klicke auf „Person entfernen“.

## Ein Zuhause verlassen, in das du eingeladen wurdest


Wenn du ein Zuhause verlässt, kannst du die Geräte in diesem Zuhause nicht mehr sehen.

1. Tippe oder klicke in der App „Home“ auf das Home-Symbol  und wähle „Einstellungen des Zuhauses“. Wenn mehr als ein Zuhause angezeigt wird, wähle das Zuhause, das du verlassen möchtest und wähle „Einstellungen des Zuhauses“.
2. Scrolle nach unten, und tippe oder klicke auf „Zuhause verlassen“. Tippe oder klicke auf „Verlassen“.

## Zuhause zurücksetzen

In iOS 16, iPadOS 16.1 und macOS 13 (oder neuer) müssen alle HomeKit-Geräte wieder zu einem neuen Zuhause hinzugefügt werden, wenn du ein Zuhause aus der App „Home“ entfernst. Bevor du ein Zuhause entfernst, vergewissere dich, dass alle Software der Home-Geräte auf ihre neuesten Versionen aktualisiert wurde.

Wenn du dein Betriebssystem nicht aktualisiert hast, solltest du unbedingt Schritt 4 weiter unten komplett ausführen.

1. Tippe oder klicke in der App „Home“ auf das Home-Symbol  und wähle „Einstellungen des Zuhauses“.
2. Tippe oder klicke unten im Dialog auf „Zuhause entfernen“ und tippe oder klicke auf „Entfernen“.
3. Schließe die App „Home“.
4. Suche alle Home-Geräte und setze sie auf die Werkseinstellungen zurück.
5. Öffne die App „Home“ erneut und erstelle ein neues Zuhause.
6. Füge alle Zubehörgeräte zu dem neuen Zuhause hinzu.

## Löschen aller Inhalte und Einstellungen

Wenn du besorgt darüber bist, dass eine andere Person physischen Zugriff auf dein Gerät hatte und die eingebauten Sicherheitsfunktionen des Geräts manipuliert hat, kannst du es auf die Werkseinstellungen zurücksetzen, auch wenn du die neueste Version von iOS, iPadOS und macOS nicht verwendest. Beim Zurücksetzen auf die Werkseinstellungen werden die Informationen und Einstellungen auf deinem Gerät gelöscht. Dabei werden auch alle Apps, die ohne dein Wissen installiert wurden, und deine Datenschutzeinstellungen gelöscht, sodass du deinen Standort nicht mehr mit Personen oder Apps teilst. Außerdem wird dabei die neueste Version des jeweiligen Betriebssystems installiert.




Dieser Vorgang namens „*Alle Inhalte & Einstellungen löschen*“ erfordert Internetzugang und kann eine Weile dauern, stellt allerdings sicher, dass nur du auf dein Gerät zugreifen kannst.

**Wichtig:** Wenn du die Option „Alle Inhalte & Einstellungen“ verwendest, werden alle deine Daten gelöscht.

Wenn du alle Inhalte und Einstellungen auf deinem Mac löschen möchtest, musst du macOS 12.0.1 oder neuer verwenden. Alternativ kannst du auch deinen Mac löschen. Weitere Informationen findest du in den Apple Support-Artikeln „[Einen Mac mit Apple-Chip mithilfe des Festplattendienstprogramms löschen](https://support.apple.com/102506)“ (<https://support.apple.com/102506>) und „[Einen Intel-basierten Mac mithilfe des Festplattendienstprogramms löschen](https://support.apple.com/HT208496)“ (<https://support.apple.com/HT208496>).




## iPhone oder iPad löschen und auf die Werkseinstellungen zurücksetzen

1. Wähle „Einstellungen“  > „Allgemein“ > „Löschen“ und tippe auf „Alle Inhalte & Einstellungen löschen“.



2. Gib deinen Code oder dein Apple-ID-Passwort ein.
3. Warte, bis alle Inhalte sicher von deinem Gerät entfernt wurden.

## Mac löschen und auf die Werkseinstellungen zurücksetzen

1. Führe einen der folgenden Schritte aus:
  - Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Allgemein“ , auf „Übertragen“ oder „Zurücksetzen“ und klicke dann auf „Alle Inhalte und Einstellungen löschen“.
  - Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“. Wähle dann in der Menüleiste „Systemeinstellungen“ > „Alle Einstellungen und Inhalte löschen“.
2. Gib deine Administratordaten (das Passwort, das du für die Anmeldung bei deinem Mac verwendest) im Löschassistenten ein.
3. Überprüfe die Objekte, die zusätzlich zu deinen Inhalten und Einstellungen entfernt werden sollen.

Wenn mehrere Benutzeraccounts auf deinem Mac verwendet werden, klicke auf den Pfeil neben deinem Accountnamen, um die Objekte zu überprüfen.
4. Klicke auf „Weiter“ und befolge die Anleitung auf dem Bildschirm.

# Wiederherstellen gesicherter Daten

Wenn du vor dem Löschen und Wiederherstellen der Werkseinstellungen ein Backup von deinem Apple Gerät erstellt hast, kannst du diese Daten aus dem Backup in iCloud oder auf deinem Computer wiederherstellen. Wenn du befürchtest, dass dein Backup Konfigurationen oder Apps enthält, die du nicht auf deinem Gerät haben möchtest, kannst du nach der Wiederherstellung des Backups die App-Mediathek und Einstellungen überprüfen. Du kannst einen Mac mit Time Machine wiederherstellen. Für ein iPhone oder iPad verwendest du dazu einen Computer oder iCloud.



## iPhone oder iPad aus einem iCloud-Backup wiederherstellen

1. Schalte dein Gerät ein. Daraufhin sollte der Startbildschirm angezeigt werden. (Wenn du dein Gerät bereits eingerichtet hast, musst du alle seine Inhalte löschen, bevor du ein Backup mithilfe dieser Schritte wiederherstellen kannst.)
2. Befolge die Einrichtungsschritte auf dem Bildschirm, bis zum Bildschirm „Apps & Daten“. Tippe dann auf „Aus iCloud-Backup wiederherstellen“.
3. Melde dich mit deiner Apple-ID bei iCloud an.
4. Wähle ein Backup aus.

Sieh dir das Datum und die Größe der einzelnen Backups an und wähle das relevanteste aus. Nachdem du ein Backup ausgewählt hast, beginnt die Datenübertragung. Wenn du in einer Mitteilung darüber informiert wirst, dass eine neuere Softwareversion erforderlich ist, befolge die Aktualisierungsanleitung auf dem Bildschirm.

5. Wenn du dazu aufgefordert wirst, melde dich mit deiner Apple-ID an, um deine Apps und Käufe wiederherzustellen.

Wenn du iTunes- oder App Store-Inhalte mit mehreren Apple-IDs gekauft hast, musst du dich bei jeder von ihnen anmelden. Wenn du ein Passwort vergessen hast, kannst du diesen Schritt überspringen und dich später anmelden. Du kannst die entsprechenden Apps dann nicht verwenden, bis du dich mit deiner Apple-ID anmeldest.

6. Bleib mit dem WLAN verbunden und warte, bis ein Fortschrittsbalken angezeigt wird.

Abhängig von der Größe des Backups und der Netzwerkgeschwindigkeit dauert es einige Minuten bis zu einer Stunde, bis der Fortschrittsbalken die Fertigstellung des Netzwerkprozesses anzeigt. Wenn du die WLAN-Verbindung zu früh unterbrichst, wird der Fortschritt angehalten, bis du die Verbindung erneut herstellst.

7. Dann kannst du die Einrichtung abschließen.

Inhalte wie deine Apps, Fotos, Musik und andere Informationen, werden, abhängig von der Datenmenge, in den nächsten Stunden oder Tagen im Hintergrund wiederhergestellt. Versuche, so oft wie mögliche mit dem WLAN und Stromanschluss verbunden zu sein, damit die Wiederherstellung abgeschlossen werden kann.


Nach Abschluss der Wiederherstellung:

- Öffne die App-Mediathek und überprüfe, welche Apps auf deinem Gerät installiert sind. Wenn du unbekannte Apps von Drittanbietern entdeckst, kannst du sie [löschen](#). Weitere Informationen findest du unter „Apps auf dem iPhone oder iPad überprüfen und löschen“ weiter oben in diesem Dokument.

Weitere Informationen findest du im Apple Support-Artikel „[Organisiere den Home-Bildschirm und die App-Bibliothek auf deinem iPhone](#)“ (<https://support.apple.com/108324>).

- Überprüfe und [lösche die Konfigurationsprofile](#) oder Profile für die Mobilgeräteverwaltung (MDM), die du nicht autorisiert hast. (Konfigurationsprofile werden von Bildungseinrichtungen und Unternehmen verwendet, um eine konsistente Einrichtung aller Geräte zu ermöglichen. Achte darauf, die Profile von deiner Bildungseinrichtung oder deinem Arbeitgeber nicht zu löschen.) Weitere Informationen findest du unter „Löschen verdächtiger Inhalte“ weiter oben in diesem Dokument.

### **iPhone oder iPad aus einem Backup auf deinem Computer wiederherstellen**

1. Öffne auf einem Mac mit macOS 10.15 (oder neuer) den Finder . Öffne iTunes auf einem Mac mit macOS 10.14 oder älter oder auf einem PC.
2. Verbinde dein Gerät über ein USB-Kabel mit deinem Computer. Wenn du einen Code eingeben oder bestätigen musst, dass du dem angeschlossenen Computer vertraust, befolge die Anleitung auf dem Bildschirm.
3. Wähle dein iPhone oder iPad aus, wenn das Gerät im Finder-Fenster oder in iTunes angezeigt wird.
4. Wähle „Backup wiederherstellen“.
5. Sieh dir das Datum der Backups an und wähle das relevanteste aus.
6. Klicke auf „Wiederherstellen“ und warte, bis die Wiederherstellung abgeschlossen ist. Gib den Code für dein verschlüsseltes Backup ein, sobald du dazu aufgefordert wirst.
7. Behalte die Verbindung mit deinem Computer nach dem Neustart bei und warte, bis dein Gerät mit dem Computer synchronisiert wurde. Nach Abschluss der Synchronisation kannst du die Verbindung trennen.

Nach Abschluss der Wiederherstellung:

- Öffne die App-Mediathek und überprüfe, welche Apps auf deinem Gerät installiert sind. Wenn du unbekannte Apps von Drittanbietern entdeckst, kannst du sie [löschen](#). Weitere Informationen findest du unter „Apps auf dem iPhone oder iPad überprüfen und löschen“ weiter oben in diesem Dokument.

Weitere Informationen findest du im Apple Support-Artikel „[Organisiere den Home-Bildschirm und die App-Bibliothek auf deinem iPhone](#)“ (<https://support.apple.com/108324>).

- Überprüfe und [lösche die Konfigurationsprofile](#) oder Profile für die Mobilgeräteverwaltung, die du nicht autorisiert hast. (Konfigurationsprofile werden von Bildungseinrichtungen und Unternehmen verwendet, um eine konsistente Einrichtung aller Geräte zu ermöglichen. Achte darauf, die Profile von deiner Bildungseinrichtung oder deinem Arbeitgeber nicht zu löschen.) Weitere Informationen findest du unter „Löschen verdächtiger Inhalte“ weiter oben in diesem Dokument.

### **Mit Time Machine auf dem Mac gesicherte Objekte wiederherstellen**


Wenn du Time Machine zum Sichern von Dateien auf deinem Mac verwendest, kannst du verlorene Elemente oder ältere Versionen von Dateien leicht wiederherstellen. Du kannst Time Machine mit vielen Apps verwenden.





1. Öffne auf deinem Mac ein Finder-Fenster für das Objekt, das du wiederherstellen möchtest.

Wenn du beispielsweise eine Datei wiederherstellen möchtest, die du versehentlich aus dem Ordner „Dokumente“ gelöscht hast, öffne den Ordner „Dokumente“.

Wenn ein Objekt auf deinem Desktop fehlt, musst du kein Finder-Fenster öffnen.

2. Verwende Launchpad, um die Apps auf deinem Mac anzuzeigen, und öffne Time Machine. Während dein Mac die Verbindung zum Backup-Volumen herstellt, wird möglicherweise eine Nachricht angezeigt.

Du kannst Time Machine auch öffnen, indem du auf das Time Machine-Symbol  in der Menüleiste klickst und „Time Machine öffnen“ wählst. Wird das Symbol „Time Machine“ in der Menüleiste nicht angezeigt, führe einen der folgenden Schritte aus:

- Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Einstellungen“, klicke auf „Time Machine“  und wähle „Time Machine in der Menüleiste anzeigen“.
- Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Einstellungen“, klicke auf „Time Machine“  und wähle „Time Machine in der Menüleiste anzeigen“.

3. Verwende die Pfeile und die Timeline, um lokale Schnappschüsse und Backups zu durchsuchen.



Wenn ein hell bis dunkelgrau blinkendes Häkchen angezeigt wird, weist dies darauf hin, dass das Backup auf dem Backup-Volumen noch geladen oder validiert wird.

4. Wähle ein Objekt oder mehrere Objekte aus, die du wiederherstellen möchtest (dies können auch Ordner oder deine gesamte Festplatte sein), und klicke auf „Wiederherstellen“.

Wiederhergestellte Objekte werden an ihrem ursprünglichen Speicherort wiederhergestellt. So wird zum Beispiel ein Objekt, das im Ordner „Dokumente“ war, im Ordner „Dokumente“ wiederhergestellt.

Nach Abschluss der Wiederherstellung:

- Öffne Launchpad und überprüfe, welche Apps auf deinem Mac installiert sind. Wenn du unbekannte Apps von Drittanbietern entdeckst, kannst du sie löschen, indem du bei gedrückter Wahltaste auf das „X“ auf dem Symbol der App klickst, die du löschen möchtest.
- Überprüfe und [lösche die Konfigurationsprofile](#) oder Profile für die Mobilgeräteverwaltung, die du nicht autorisiert hast. (Konfigurationsprofile werden von Bildungseinrichtungen und Unternehmen verwendet, um eine konsistente Einrichtung aller Geräte zu ermöglichen. Achte darauf, die Profile von deiner Bildungseinrichtung oder deinem Arbeitgeber nicht zu löschen.) Weitere Informationen findest du unter „Löschen verdächtiger Inhalte“ weiter oben in diesem Dokument.



# Werkzeuge für Sicherheit und Datenschutz

## Aktualisieren der Apple-Software

Zur Sicherung deines Geräts und zur Verwaltung des Zugriffs auf deine persönlichen Informationen musst du sicherstellen, dass du das neueste Betriebssystem mit den neuesten Sicherheits- und Datenschutzupdates installiert hast. Sobald deine Geräte auf dem neuesten Stand sind, kannst du lernen, wie du deine Apple-ID verwaltest. Alle Apple-Geräte profitieren von Softwareupdates.




Die Aktualisierung deiner Betriebssystemsoftware gehört zu den wichtigsten Maßnahmen, die du zum Schutz deines Geräts und deiner Daten ergreifen kannst. Apple macht das Laden und Installieren dieser Updates ganz einfach.

Eine Liste der Sicherheitsupdates für Apple-Geräte findest du im Apple Support-Artikel „[Apple-Sicherheitsupdates](https://support.apple.com/HT201222#update)“ (<https://support.apple.com/HT201222#update>).

## iPhone und iPad automatisch aktualisieren

Wenn du die automatischen Updates nicht bereits bei der Ersteinrichtung deines Geräts aktiviert hast, kannst du Folgendes tun:

1. Wähle „Einstellungen“  > „Allgemein“ > „Softwareupdate“ > „Automatische Updates“.
2. Aktiviere beide Optionen: „[iOS oder iPadOS]-Updates laden“ und „[iOS oder iPadOS]-Updates installieren“.

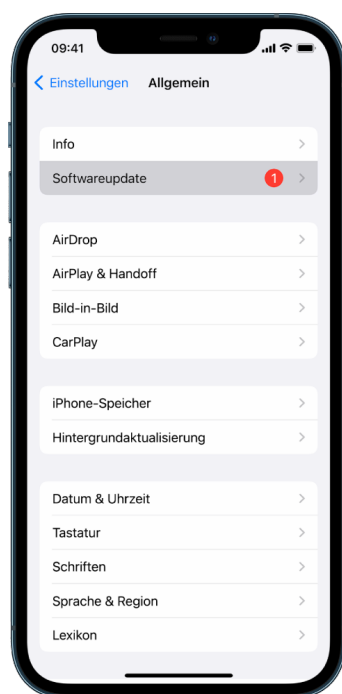
Sobald ein Update verfügbar ist, lädt und installiert das Gerät das Update über Nacht, sofern es am Stromnetz angeschlossen und mit einem WLAN verbunden ist. Bevor ein Update installiert wird, erhältst du eine Mitteilung.

Wenn du die automatischen Updates deaktivieren möchtest, wähle „Einstellungen“ > „Allgemein“ > „Softwareupdate“ > „Automatische Updates“ und deaktiviere beide Optionen.

## iPhone und iPad manuell aktualisieren

Du kannst jederzeit prüfen, ob Softwareupdates verfügbar sind, und sie manuell installieren.

- Wähle „Einstellungen“  > „Allgemein“ > „Softwareupdate“.






Auf dem Bildschirm wird die aktuell installierte Version von iOS sowie ggf. ein Hinweis auf ein verfügbares Update angezeigt.

## **iPhone und iPad mithilfe deines Computers aktualisieren**

1. Stelle sicher, dass du über eines der folgenden Geräte verfügst:
  - Einen Mac mit einem USB-Anschluss und OS X 10.9 oder neuer
  - Einen PC mit einem USB-Anschluss und Windows 7 oder neuer
2. Führe einen der folgenden Schritte aus:
  - Schließe das Gerät mit dem mitgelieferten Lightning-auf-USB-Kabel an deinen Computer an. Wenn dein Computer einen USB-C-Anschluss hat, verwende einen USB-C-auf-USB-Adapter oder ein USB-C-auf-Lightning-Kabel (beide separat erhältlich).
  - Wenn dein Gerät mit einem USB-C-auf-Lightning-Kabel geliefert wurde und dein Computer einen USB-Anschluss hat, verwende ein Lightning-auf-USB-Kabel (separat erhältlich).
  - Wenn dein iPad mit einem USB-C-Ladekabel geliefert wurde und dein Computer einen USB-Anschluss hat, verwende einen USB-C-auf-USB-Adapter und ein USB-A-Kabel (beide separat erhältlich).
  - Wenn dein iPad mit einem Thunderbolt 4/USB-4-Ladekabel geliefert wurde und dein Computer einen USB-Anschluss hat, verwende einen USB-C-auf-USB-Adapter und ein USB-A-Kabel (beide separat erhältlich). Du kannst Thunderbolt- oder USB-Kabel mit Thunderbolt-Geräten wie dem 12,9" iPad Pro (5. Generation) und dem 11" iPad Pro (3. Generation) verwenden.
3. Nachdem du das Gerät erfolgreich mit deinem Computer verbunden hast, führe einen der folgenden Schritte aus:
  - *In der Finder-Seitenleiste auf dem Mac:* Wähle dein Gerät aus und klicke auf „Allgemein“ oben im Fenster.  
  
Wenn du dein Gerät mit dem Finder auf iOS 15 oder iPadOS 15 aktualisieren möchtest, muss macOS 10.15 (oder neuer) auf deinem Computer installiert sein. Wenn du eine ältere Version von macOS hast, [verwende iTunes](#), um das Gerät zu aktualisieren. Weitere Informationen findest du unter „Aktualisieren der Software auf iOS-Geräten in iTunes auf dem Mac“ (<https://support.apple.com/guide/itunes/itns3235/12.9/mac/10.14>).
  - *In der App „iTunes“ auf deinem Windows-PC:* Klicke auf die Taste „iPhone“ oben links im iTunes-Fenster und klicke auf „Übersicht“.
4. Klicke auf „Nach Update suchen“.
5. Klicke auf „Aktualisieren“, um ein verfügbares Update zu installieren.

## Mac automatisch aktualisieren





1. Führe einen der folgenden Schritte aus:
  - Auf einem Mac mit macOS 13 oder neuer: Wähle „Apple“  > „Systemeinstellungen“ und klicke auf „Allgemein“ und dann auf „Softwareupdate“.
  - Auf einem Mac mit macOS 12 oder älter: Wähle „Apple“  > „Systemeinstellungen“ und klicke auf „Softwareupdate“ .
2. Wenn du macOS-Updates automatisch installieren lassen möchtest, wähle „Meinen Mac automatisch aktualisieren“.
3. Wenn du weitere Optionen festlegen möchtest, klicke auf „Weitere Optionen“ und führe beliebige der folgenden Schritte aus:
  - *Wenn dein Mac automatisch nach Updates suchen soll:* Klicke auf „Nach Updates suchen“.
  - *Wenn dein Mac ungefragt Updates laden soll:* Wähle „Neue Updates bei Verfügbarkeit laden“.
  - *Wenn dein Mac automatisch macOS-Updates installieren soll:* Wähle „macOS-Updates installieren“.
  - *Wenn dein Mac automatisch Updates aus dem App Store installieren soll:* Wähle „App-Updates aus dem App Store installieren“.
  - *Wenn dein Mac Systemdateien und Sicherheitsupdates automatisch installieren soll:* Wähle „Sicherheitsmaßnahmen und Systemdateien installieren“.
4. Klicke auf „OK“.

Wenn du automatisch die neuesten Updates erhalten möchtest, solltest du „Nach Updates suchen“, „Neue Updates bei Verfügbarkeit laden“ und „Systemdateien und Sicherheitsupdates installieren“ wählen.

*Hinweis:* MacBook-, MacBook Pro- und MacBook Air-Computer müssen am Stromnetz angeschlossen sein, um Updates automatisch zu laden.

## Mac manuell aktualisieren

Du kannst das Betriebssystem deines Mac und Software, die du im App Store geladen hast, manuell aktualisieren.

- Führe einen der folgenden Schritte aus:
  - Auf einem Mac mit macOS 13 oder neuer: Wähle „Apple“  > „Systemeinstellungen“ und klicke auf „Allgemein“ und dann auf „Softwareupdate“.
  - Auf einem Mac mit macOS 12 oder älter: Wähle „Apple“  > „Systemeinstellungen“ und klicke auf „Softwareupdate“ .
- Wenn du im App Store geladene Software aktualisieren möchtest, wähle „Apple“. Soweit verfügbar, wird die Anzahl der verfügbare Updates neben „App Store“ angezeigt. Wähle „App Store“, um in der App „App Store“  fortzufahren.

# Festlegen eines eindeutigen Codes oder Passworts auf Apple-Geräten

Wenn du verhindern möchtest, dass andere deine Geräte verwenden oder auf deine Informationen zugreifen, lege einen eindeutigen, nur dir bekannten Code oder ein entsprechendes Passwort fest. Wenn du ein Gerät mit anderen teilst oder andere deinen Code oder dein Passwort kennen, solltest du bedenken, dass sie die Informationen auf deinem Gerät oder in deinem Account sehen und die Einstellungen des Geräts ändern können.


Wenn du denkst, dass eine andere Person deinen Gerätecode oder dein Passwort kennt, und du einen nur dir bekannten Code oder ein entsprechendes Passwort festlegen möchtest, kannst du den Code oder das Passwort je nach Gerät unter „Einstellungen“ oder „Systemeinstellungen“ zurücksetzen. Dein Mac-Passwort muss aus mindestens acht Zeichen mit Groß- und Kleinbuchstaben sowie mindestens einer Zahl bestehen. Außerdem kannst du Sonderzeichen und Interpunktionszeichen verwenden, um es noch sicherer zu machen.



## Gerätecode auf dem iPhone oder iPad festlegen

Aus Sicherheitsgründen kannst du einen Gerätecode festlegen, der jedes Mal eingegeben werden muss, wenn das iPhone oder iPad eingeschaltet wird oder den Standby-Modus verlässt, damit das Gerät entsperrt wird. Durch das Festlegen eines Gerätecodes wird außerdem der Datenschutz aktiviert, der die Daten auf deinem iPhone und iPad verschlüsselt, sodass nur Personen, die deinen Code kennen, auf diese zugreifen können.


*Hinweis:* Dein *Gerätecode* ist nicht identisch mit deinem *Apple-ID-Passwort*, mit dem du auf den iTunes Store, den App Store, Apple Books, iCloud und andere Dienste von Apple zugreifst.

- Wähle „Einstellungen“  und führe einen der folgenden Schritte aus:
  - Auf einem iPhone oder iPad mit Face ID: Tippe auf „Face ID & Code“ und dann auf „Code aktivieren“ oder „Code ändern“.
  - Auf einem iPhone oder iPad mit Home-Taste: Tippe auf „Touch ID & Code“ und dann auf „Code aktivieren“ oder „Code ändern“.

Um Optionen zum Erstellen eines Codes zu sehen, tippe auf „Codeoptionen“. Codes bestehen standardmäßig aus sechs Ziffern. Die Optionen reichen von vierstelligen Codes, die die geringste Sicherheit haben, bis hin zu alphanumerischen Codes, die am sichersten sind.

## Gerätecode auf dem iPhone oder iPad ändern und vorherigen Code ungültig machen

Wenn du befürchtest, dass eine andere Person Zugriff auf deinen Gerätecode hat, und du dein iPhone schützen möchtest, kannst du den Code ändern und den vorherigen Code ungültig machen, um deine Privatsphäre zu schützen. Führe zum Ändern des Gerätecodes die folgenden Schritte aus.

1. Wähle „Einstellungen“  und führe einen der folgenden Schritte aus:
  - Auf einem iPhone oder iPad mit Face ID: Tippe auf „Face ID & Code“ und gib den Code ein.
  - Auf einem iPhone oder iPad mit Home-Taste: Tippe auf „Touch ID & Code“ und gib den Code ein.
2. Tippe auf „Code ändern“ und gib deinen aktuellen Code ein.
3. Wenn du die Sicherheit erhöhen möchtest, tippe auf „Codeoptionen“, um das Format für deinen zukünftigen Code auszuwählen.

Die verfügbaren Formate umfassen einen vierstelligen numerischen Code, einen sechsstelligen numerischen Code, einen eigenen alphanumerischen Code und einen eigenen numerischen Code.

4. Gib deinen neuen Code zweimal ein.






**Wichtig:** Nachdem du in iOS 17 oder iPadOS 17 deinen Code geändert hast, kannst du noch 72 Stunden lang deinen alten Code verwenden, um deinen Code zurückzusetzen. Dies ist als Sicherheitsmaßnahme gedacht, falls du den neuen Code vergisst. Wenn du deinen alten Code vollständig deaktivieren möchtest, nachdem du ihn geändert hast, tippe auf der Seite „[Face ID]/[Touch ID] & Code“ unter den Einstellungen auf „Vorherigen Code jetzt ungültig machen“.

## Ändern des Anmeldepassworts auf dem Mac

Wenn du befürchtest, dass eine andere Person Zugriff auf dein Passwort hat, und du deinen Mac schützen möchtest, kannst du das Benutzerpasswort ändern, um deine Privatsphäre zu schützen.

*Hinweis:* Dein Anmeldepasswort ist das Passwort, das du zum Entsperren deines Mac verwendest, wenn du ihn einschaltest oder aus dem Ruhezustand weckst. Da du das Passwort selbst erstellt hast, kann es identisch mit deinem Apple-ID-Passwort sein, mit dem du auf den iTunes Store, den App Store, Apple Books, iCloud und andere Dienste von Apple zugreifst.


1. Führe einen der folgenden Schritte aus:

- Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Allgemein“, auf „Benutzer:innen & Gruppen“  und klicke auf die Infotaste .
- Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“ >, klicke auf „Benutzer:innen & Gruppen“  und klicke dann auf „Passwort ändern“.

2. Klicke auf „Passwort ändern“.

3. Gib dein altes Passwort im Feld „Altes Passwort“ ein.

4. Gib dein neues Passwort im Feld „Neues Passwort“ und noch einmal im Feld „Bestätigen“ ein.

Wenn du Hilfe bei der Wahl eines sicheren Passworts brauchst, klicke auf die Schlüsseltaste  neben dem Feld „Neues Passwort“.


5. Gib eine Merkhilfe ein, die dir hilft, dich an dein neues Passwort zu erinnern.

Die Merkhilfe wird angezeigt, wenn du dreimal in Folge das falsche Passwort eingibst. Alternativ kannst du auch auf das Fragezeichen im Passwortfeld auf dem Anmeldebildschirm klicken.

6. Klicke auf „Passwort ändern“.

## iPhone oder iPad automatisch sperren

Um den Schutz deiner Daten noch weiter zu erhöhen, kannst du dein Gerät so einrichten, dass es automatisch gesperrt wird, wenn eine bestimmte Zeit lang keine Aktivität stattgefunden hat.

- Wähle „Einstellungen“  > „Anzeige & Helligkeit“ > „Automatische Sperre“ und lege eine Dauer fest.


# Schützen des iPhone oder iPad mit Face ID

Face ID lässt sich von allen nutzen, die ihr iPhone oder iPad mit einer zusätzlichen Sicherheitsstufe sichern möchten. Face ID stellt sicher, dass niemand auf die Informationen auf deinem Gerät zugreifen kann. Wenn du Face ID verwenden möchtest, musst du zunächst einen Code auf deinem iPhone oder iPad einrichten.

Eine Liste der unterstützten Geräte findest du im Apple Support-Artikel „[iPhone- und iPad-Modelle, die Face ID unterstützen](https://support.apple.com/102854)“ (<https://support.apple.com/102854>).



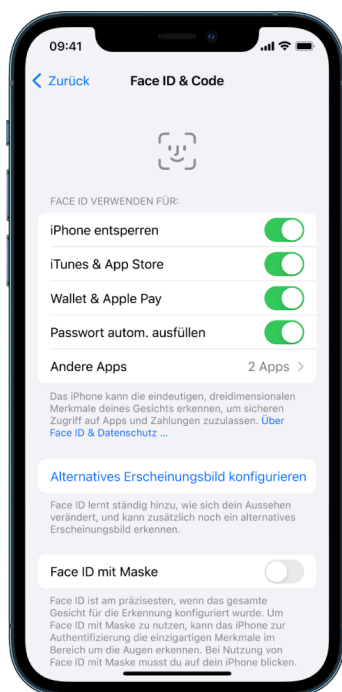
## Einrichten von Face ID

- Wenn du Face ID nicht bei der Ersteinrichtung deines iPhone oder iPad eingerichtet hast, wähle „Einstellungen“  > „Face ID & Code“ > „Face ID einrichten“ und befolge die Anleitung auf dem Bildschirm.

Wenn du körperlich eingeschränkt bist, kannst du während der Einrichtung von Face ID auf „Optionen für Bedienungshilfen“ tippen. Wenn du das tust, ist für die Einrichtung der Gesichtserkennung nicht der volle Umfang der Kopfbewegung erforderlich. Face ID ist auch dann sicher, erfordert aber mehr Genauigkeit beim Blick auf das iPhone oder iPad.




Face ID verfügt auch über eine Bedienungshilfe, die du verwenden kannst, wenn du blind bist oder eine Sehschwäche hast. Wenn du willst, dass du Face ID nicht mit geöffneten Augen verwenden musst, wähle „Einstellungen“ > „Bedienungshilfen“ und deaktiviere „Aufmerksamkeitsprüfung für Face ID“. Diese Funktion wird automatisch deaktiviert, wenn du bei der Ersteinrichtung deines iPhone oder iPad VoiceOver aktivierst.



Weitere Informationen findest du unter „Ändern der Einstellungen für Face ID und Aufmerksamkeit auf dem iPhone“ (<https://support.apple.com/guide/iphone/iph646624222>) im iPhone-Benutzerhandbuch oder unter „Ändern der Einstellungen für Face ID und Aufmerksamkeit auf dem iPad“ im iPad-Benutzerhandbuch (<https://support.apple.com/guide/ipad/ipad058b4a31>).

### Zurücksetzen von Face ID

Wenn ein alternatives Erscheinungsbild eingerichtet ist, dass du nicht mehr behalten möchtest, oder denkst, dass jemand ohne deine Erlaubnis ein alternatives Erscheinungsbild auf deinem Gerät hinzugefügt hat, kannst du Face ID zurücksetzen und erneut einrichten.

1. Wähle „Einstellungen“  > „Face ID & Code“ und tippe auf „Face ID zurücksetzen“.
2. Lies die Anleitung oben, um Face ID erneut einzurichten.


# Schützen deiner Geräte mit Touch ID

Du kannst Touch ID verwenden, um dein iPhone oder iPad sicher und bequem zu entsperren, Einkäufe und Zahlungen zu autorisieren und dich bei vielen Apps von Drittanbietern anzumelden, indem du einen Finger oder deinen Daumen auf die Home-Taste legst.

Wenn du Touch ID verwenden möchtest, musst du zunächst einen Code auf deinem iPhone oder iPad einrichten.



## Einrichten von Touch ID auf dem iPhone oder iPad

1. Wenn du die Fingerabdruckerkennung nicht bei der Ersteinrichtung deines iPhone oder iPad aktiviert hast, wähle „Einstellungen“  > „Touch ID & Code“.
2. Aktiviere beliebige der Optionen und befolge die Anleitung auf dem Bildschirm.





Wenn bereits Fingerabdrücke eingerichtet sind und du dich nicht daran erinnern kannst, diese hinzugefügt zu haben, siehe [„Löschen von unbekanntem Fingerabdrücken vom iPhone oder iPad“](#) weiter unten in diesem Dokument.

*Hinweis:* Wenn du keinen Fingerabdruck hinzufügen oder dein iPhone oder iPad nicht mit Touch ID entsperren kannst, findest du weitere Informationen im Apple Support-Artikel [„Wenn Touch ID auf deinem iPhone oder iPad nicht funktioniert“](#) (<https://support.apple.com/101612>).

## Einrichten von Touch ID auf dem Mac oder Magic Keyboard

Wenn du Touch ID verwenden möchtest, musst du zunächst ein Passwort auf deinem Mac einrichten.

1. Führe einen der folgenden Schritte aus:

- Auf einem Mac mit macOS 13 oder neuer: Wähle „Apple“  > „Systemeinstellungen“ und klicke auf „Touch ID“ .
- Auf einem Mac mit macOS 12 oder älter: Wähle „Apple“  > „Systemeinstellungen“ und klicke auf „Touch ID“ .

2. Klicke auf „Fingerabdruck hinzufügen“, gib dein Passwort ein und befolge die Anleitung auf dem Bildschirm.

Wenn dein Mac oder Magic Keyboard über Touch ID verfügt, befindet sich der Sensor oben rechts auf der Tastatur. Du kannst bis zu drei Fingerabdrücke zu deinem Benutzeraccount hinzufügen (und kannst insgesamt fünf Fingerabdrücke auf deinem Mac speichern).


3. Klicke auf die Markierungsfelder, um festzulegen, wie du Touch ID verwenden möchtest:

- *Deinen Mac entsperren:* Verwende Touch ID, um den Mac zu entsperren, wenn du ihn aus dem Ruhezustand weckst.
- *Apple Pay:* Verwende Touch ID, um Einkäufe abzuschließen, die du mit Apple Pay auf dem Mac machst.
- *iTunes Store, App Store & Apple Books:* Verwende Touch ID, um Einkäufe abzuschließen, die du auf dem Mac in Apple Online-Stores machst.
- *Passwort automatisch ausfüllen:* Verwende Touch ID, um Benutzernamen und Passwörter sowie Kreditkartendaten automatisch auszufüllen, wenn du in Safari und anderen Apps dazu aufgefordert wirst.
- *Touch ID-Sensor für schnellen Benutzerwechsel verwenden:* Verwende Touch ID, um zwischen Mac-Benutzeraccounts zu wechseln.

# Löschen von unbekannten Fingerabdrücken vom iPhone oder iPad

Wenn mehrere Fingerabdrücke auf deinem iPhone oder iPad vorhanden sind und du vermeiden möchtest, dass andere über einen zusätzlichen Fingerabdruck auf dein Gerät zugreifen können, kannst du die Fingerabdrücke zurücksetzen, damit nur deine Fingerabdrücke auf dem Gerät verfügbar sind.






1. Wähle „Einstellungen“  > „Touch ID & Code“.
2. Wenn mehr als ein Fingerabdruck verfügbar ist, lege einen Finger auf die Home-Taste, um seinen Abdruck zu bestimmen.
3. Tippe auf den Fingerabdruck und führe einen der folgenden Schritte aus:
  - Gib einen Namen ein (z. B. „Daumen“).
  - Tippe auf „Fingerabdruck löschen“.

# Hinzufügen oder Löschen von Fingerabdrücken auf dem Mac

Wenn mehrere Fingerabdrücke auf deinem Mac oder Magic Keyboard mit Touch ID vorhanden sind und du befürchtest, dass einer oder mehrere von ihnen nicht deiner ist, kannst du die Fingerabdrücke löschen und erneut deinen eigenen Fingerabdruck hinzufügen.



1. Führe einen der folgenden Schritte aus:
  - Auf einem Mac mit macOS 13 oder neuer: Wähle „Apple“  > „Systemeinstellungen“ und klicke auf „Touch ID“ .
  - Auf einem Mac mit macOS 12 oder älter: Wähle „Apple“  > „Systemeinstellungen“ und klicke auf „Touch ID“ .
2. Führe beliebige der folgenden Schritte aus:
  - *Einen Fingerabdruck hinzufügen:* Klicke auf „Fingerabdruck hinzufügen“, um einen neuen Fingerabdruck hinzuzufügen, und wähle, mit welchen Optionen du Touch ID verwenden möchtest.
  - *Einen Fingerabdruck löschen:* Klicke auf einen Fingerabdruck, gib dein Passwort ein, klicke auf „OK“ und dann auf „Löschen“.

## Schützen deiner Apple-ID

Deine Apple-ID ist der persönliche Account, mit dem du dich auf deinen Geräten anmeldest und Dienste von Apple wie den App Store, iCloud, Nachrichten, FaceTime und „Wo ist?“ nutzt. Er enthält außerdem persönliche Informationen, die du bei Apple hinterlegst und geräteübergreifend teilst, darunter Kontakte, Zahlungsinformationen, Fotos, Gerätebackups und vieles mehr. Wenn andere Personen Zugriff auf deine Apple-ID haben, können sie Informationen sehen, die geräteübergreifend synchronisiert werden, wie z. B. Nachrichten und dein Standort. Erfahre hier, wie du deine Apple-ID auf dem iPad, iPhone und Mac schützen kannst.



Im Folgenden findest du einige wichtige Maßnahmen, die du ergreifen kannst, damit deine Apple-ID sicher und deine Privatsphäre geschützt bleibt.

## Deine Apple-ID sichern

1. Teile deine Apple-ID nicht mit anderen Personen – auch nicht mit Familienmitgliedern, Partner:innen und engen Freund:innen. Wenn du deine Apple-ID teilst, gibst du einer anderen Person Zugriff auf alle deine persönlichen Daten und Inhalte. Wenn eine andere Person deine Apple-ID und dein Passwort für dich eingerichtet hat oder Zugriff auf dein Passwort hatte, solltest du dein Passwort ändern.
2. Verwende die Zwei-Faktor-Authentifizierung für deine Apple-ID. Die Zwei-Faktor-Authentifizierung stellt sicher, dass du die einzige Person bist, die auf deinen Account zugreifen kann – selbst wenn jemand dein Passwort kennt. Bei der Zwei-Faktor-Authentifizierung musst du sowohl dein Passwort als auch einen sechsstelligen Verifizierungscode eingeben, der automatisch auf deinen vertrauenswürdigen Geräten angezeigt wird, wenn du dich erstmalig auf einem neuen Gerät anmeldest.

Um dich für die Zwei-Faktor-Authentifizierung zu registrieren, musst du mindestens eine vertrauenswürdige Telefonnummer verifizieren, über die du Verifizierungscodes per Textnachricht oder einen automatisierten Anruf erhalten kannst.






3. Achte auf Mitteilungen zu deiner Apple-ID. Apple benachrichtigt dich per E-Mail, Textnachricht oder Push-Mitteilung, wenn Änderungen an deinem Account vorgenommen wurden, z. B. bei der ersten Anmeldung auf einem neuen Gerät oder wenn dein Passwort geändert wurde. Deshalb ist es wichtig, dass deine Kontaktinformationen immer aktuell sind.

Weitere Informationen findest du unter „[Ablehnen unbekannter Anmeldeversuche](#)“ weiter oben in diesem Dokument.

4. Wenn du eine Mitteilung über einen Anmeldeversuch oder Änderungen an deinem Account erhältst, die du nicht autorisiert hast, ist es möglich, dass jemand auf deinen Account zugegriffen hat oder versucht, auf deinen Account zuzugreifen.

## Deine Apple-ID-Sicherheitsinformationen überprüfen und aktualisieren

So stellst du sicher, dass die persönlichen Informationen, die mit deiner Apple-ID verknüpft sind, auch von dir stammen:

1. Führe einen der folgenden Schritte aus:
  - Auf iPhone oder iPad: Wähle „Einstellungen“  > [dein Name].
  - Auf einem Mac mit macOS 13 oder neuer: Wähle „Apple“  > „Systemeinstellungen“ und klicke auf „Apple-ID“ .
  - Auf einem Mac mit macOS 12 oder älter: Wähle „Apple“  > „Systemeinstellungen“ und klicke auf „Apple-ID“ .
  - In einem Webbrowser auf deinem Mac oder PC: Gehe zur [Apple-ID-Website](https://appleid.apple.com) (<https://appleid.apple.com>).
2. Aktualisiere im Bereich für Name, Telefonnummern und E-Mail-Adressen alle Informationen, die nicht stimmen oder die dir nicht bekannt vorkommen, darunter deinen Namen sowie die Telefonnummern und E-Mail-Adressen, unter denen du erreichbar bist.



3. Führe einen der folgenden Schritte aus:
  - Wenn du die Zwei-Faktor-Authentifizierung aktiviert hast, überprüfe deine vertrauenswürdigen Geräte. Wenn du Geräte entdeckst, die du aus deinem Account entfernen möchtest, befolge die Anleitung im nächsten Abschnitt.
  - Wenn du die Zwei-Faktor-Authentifizierung nicht eingerichtet hast, findest du weitere Informationen unter „[Verwenden der Zwei-Faktor-Authentifizierung](#)“ weiter unten in diesem Dokument.













## Deinen Account sichern und unbekannte Geräte entfernen

Wenn Geräte mit deiner Apple-ID verknüpft sind, die du nicht kennst oder nicht für die Verwendung mit deinem Account autorisiert hast, kannst du deinen Account sichern und sie anhand der folgenden Schritte entfernen. Wenn du ein unbekanntes Gerät entfernst, wird sichergestellt, dass keine Verifizierungs-codes mehr auf ihm angezeigt werden können und dass der Zugriff auf iCloud (und andere Dienste von Apple auf dem Gerät) blockiert ist, bis du dich erneut mit der Zwei-Faktor-Authentifizierung anmeldest.

Außerdem kannst du ein Bildschirmfoto zur Dokumentation machen, bevor du deinen Account sicherst.

Befolge diese Schritte, um deine Accountinformationen zu überprüfen und deinen Account zu schützen:


1. Wenn du dein Passwort ändern möchtest:
  - *Auf iPhone oder iPad:* Wähle „Einstellungen“  > [dein Name] > „Passwort & Sicherheit“ > „Passwort ändern“. Wähle ein sicheres Passwort (mindestens acht Zeichen mit Groß- und Kleinbuchstaben sowie mindestens eine Zahl).
  - Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke auf Apple-ID  > „Passwort & Sicherheit“ > „Passwort ändern“. Wähle ein sicheres Passwort (mindestens acht Zeichen mit Groß- und Kleinbuchstaben sowie mindestens eine Zahl).
  - Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke auf Apple-ID  > „Passwort & Sicherheit“ > „Passwort ändern“. Wähle ein sicheres Passwort (mindestens acht Zeichen mit Groß- und Kleinbuchstaben sowie mindestens eine Zahl).
  - Wenn du Geräte entfernen möchtest, die nicht mit deinem Account verknüpft sein sollen, wähle „Einstellungen“ > Apple-ID. Scrolle in der Geräteliste nach unten, tippe auf das Gerät, das du entfernen möchtest, und tippe auf „Aus dem Account entfernen“.
2. Wenn du für mehr Sicherheit die E-Mail-Adresse ändern möchtest, die mit deiner Apple-ID verknüpft ist, öffne Safari  und melde dich auf der [Apple-ID-Website](https://appleid.apple.com) (<https://appleid.apple.com>) an. Wähle „Account“ und wähle unter deiner aktuellen Apple-ID „Apple-ID ändern“. Gib dann die neue E-Mail-Adresse ein, die du verwenden möchtest.
3. Wenn du Geräte entfernen möchtest, die nicht mit deinem Account verknüpft sein sollen:
  - *Auf iPhone oder iPad:* Wähle „Einstellungen“ > [dein Name], scrolle in der Geräteliste nach unten, tippe auf das Gerät, das du entfernen möchtest, und tippe auf „Aus dem Account entfernen“.
  - Auf einem Mac mit macOS 13 oder neuer: Wähle „Apple“  > „Systemeinstellungen“, klicke auf Apple-ID , scrolle in der Geräteliste nach unten, tippe auf das Gerät, das du entfernen möchtest, und tippe auf „Aus dem Account entfernen“.
  - Auf einem Mac mit macOS 12 oder älter: Wähle „Apple“  > „Systemeinstellungen“, klicke auf Apple-ID , scrolle in der Geräteliste nach unten, tippe auf das Gerät, das du entfernen möchtest, und tippe auf „Aus dem Account entfernen“.

# Verwenden der Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung stellt eine zusätzliche Sicherheitsstufe für deine Apple-ID dar und stellt sicher, dass du die einzige Person bist, die auf deinen Account zugreifen kann – selbst wenn jemand dein Passwort kennt. Du kannst die Zwei-Faktor-Authentifizierung auf deinem iPhone, iPad und Mac einrichten.



## Einrichten der Zwei-Faktor-Authentifizierung auf dem iPhone oder iPad

1. Wähle „Einstellungen“  > [dein Name] > „Passwort & Sicherheit“.
2. Tippe auf „Zwei-Faktor-Authentifizierung aktivieren“ und dann auf „Fortfahren“.
3. Gib eine vertrauenswürdige Telefonnummer ein. Über diese Nummer erhältst du die Verifizierungs-codes für die Zwei-Faktor-Authentifizierung. Es kann die Nummer von deinem iPhone sein.

Du kannst wählen, ob du diese Codes per Textnachricht oder automatisiertem Anruf erhalten möchtest.

4. Tippe auf „Weiter“.
5. Gib den Verifizierungscode ein, der an deine vertrauenswürdige Telefonnummer gesendet wurde.

Wenn der Verifizierungscode erneut gesendet werden soll, tippe auf „Keinen Bestätigungscode erhalten?“.

Anschließend musst du keinen weiteren Verifizierungscode auf deinem iPhone mehr eingeben, es sei denn, du meldest dich vollständig ab, löschst dein iPhone, meldest dich in einem Webbrowser auf der Apple-ID-Accountseite an oder musst aus Sicherheitsgründen dein Apple-ID-Passwort ändern.

Nachdem du die Zwei-Faktor-Authentifizierung aktiviert hast, kannst du sie zwei Wochen lang wieder deaktivieren. Nach diesem Zeitraum kannst du sie nicht mehr deaktivieren. Wenn du sie deaktivieren möchtest, öffne die E-Mail-Bestätigung und klicke auf den Link zur Wiederherstellung deiner alten Sicherheitseinstellungen. Denke daran, dass die Deaktivierung der Zwei-Faktor-Authentifizierung deinen Account weniger sicher macht und zur Folge hat, dass du keine Funktionen verwenden kannst, die ein höheres Maß an Sicherheit erfordern.

## Einrichten der Zwei-Faktor-Authentifizierung auf dem Mac

1. Führe einen der folgenden Schritte aus:
  - Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Systemeinstellungen“ > Apple-ID  und wähle „Passwort & Sicherheit“ in der Seitenleiste.
  - Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“ > Apple-ID  und wähle dann „Passwort & Sicherheit“.
2. Klicke auf „Zwei-Faktor-Authentifizierung einrichten“ und dann auf „Fortfahren“.
3. Beantworte die Verifizierungsfragen und klicke auf „Verifizieren“.
4. Gib deine Telefonnummer für die Verifizierung ein, wähle eine Verifizierungsmethode aus und klicke auf „Weiter“.
5. Sobald du dazu aufgefordert wirst, verifiziere deine Identität mit dem sechsstelligen Verifizierungscode, der an dein vertrauenswürdigen Telefon gesendet wird. Anschließend musst du keinen weiteren Verifizierungscode auf deinem Mac mehr eingeben, es sei denn, du meldest dich vollständig von deiner Apple-ID ab, löschst deinen Mac oder musst aus Sicherheitsgründen dein Passwort ändern.

## Sicherheitsschlüssel für die Apple-ID

Ein Sicherheitsschlüssel ist ein kleines externes Gerät, das wie ein USB-Stick oder ein Anhänger aussieht und zur Verifizierung verwendet werden kann, wenn du dich mit deiner Apple-ID über die Zwei-Faktor-Authentifizierung anmeldest. Sicherheitsschlüssel für Apple-ID ist eine optionale erweiterte Sicherheitsfunktion für Personen, die zusätzlichen Schutz vor gezielten Angriffen wie Phishing oder Social-Engineering-Betrug wünschen. Da du anstelle des sechsstelligen Codes einen physischen Schlüssel verwendest, stärkst du den Zwei-Faktor-Authentifizierungsprozess und verhinderst, dass dein zweiter Authentifizierungsfaktor abgefangen oder von einem Angreifer angefordert werden kann.

Weitere Informationen zu Sicherheitsschlüsseln findest du im Apple Support-Artikel „[Informationen zu Sicherheitsschlüsseln für Apple-IDs](https://support.apple.com/HT213154)“ (<https://support.apple.com/HT213154>).

# Verhindern, dass du von deinem Apple-Gerät ausgesperrt wirst

Kontakte für die Accountwiederherstellung sind vertrauenswürdige Personen, die dir dabei helfen können, wieder Zugriff auf deinen Account zu erhalten, wenn du dein Passwort oder deinen Gerätecode vergessen hast oder diese ohne dein Einverständnis geändert wurden. Kontakte für die Accountwiederherstellung können nicht auf deinen Account zugreifen; sie können dir lediglich einen Wiederherstellungscode für deinen Account senden, wenn du ihn benötigst. Du kannst einen Kontakt für die Accountwiederherstellung auf deinem iPhone, iPad oder Mac einrichten, damit du den Zugriff auf deine Daten wiedererhältst, wenn du einmal ausgesperrt wirst.








*Hinweis:* Neben einem Wiederherstellungskontakt ist ein *Nachlasskontakt* die einfachste und sicherste Methode, einer vertrauenswürdigen Person nach deinem Tod Zugriff auf die in deinem Apple-Account gespeicherten Daten zu erteilen. Weitere Informationen findest du im Apple Support-Artikel „[Einen Nachlasskontakt für deine Apple-ID hinzufügen](https://support.apple.com/102631)“ (<https://support.apple.com/102631>).

Kontakte für die Accountwiederherstellung müssen mindestens 13 Jahre alt sein, ein Gerät mit iOS 15, iPadOS 15 oder macOS 12 (oder neuer) besitzen, die Zwei-Faktor-Authentifizierung für ihre Apple-ID aktiviert und einen Code auf ihrem Gerät eingerichtet haben.








## Einrichten eines Wiederherstellungskontakts

Wenn du befürchtest, dass jemand den Zugriff auf deinen Account nutzen könnte, um dein Passwort zu ändern und dich aus deinem Account auszusperrt, kannst du einen vertrauenswürdigen Kontakt für die Accountwiederherstellung festlegen, damit du in diesem Fall deinen Zugriff wiedererhältst.

1. Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad:* Wähle „Einstellungen“  > [dein Name] und tippe auf „Passwort & Sicherheit“.
  - Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Systemeinstellungen“ > Apple-ID  und wähle „Passwort & Sicherheit“ in der Seitenleiste.
  - Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“ > Apple-ID  und wähle dann „Passwort & Sicherheit“.
2. Wähle „Account-Wiederherstellung“, füge einen Wiederherstellungskontakt hinzu und authentifiziere dich mit Face ID, Touch ID, deinem Code oder deinem Passwort.
3. Wenn du einer Familienfreigabegruppe angehörst, werden die Mitglieder dieser Gruppe als Kontakte empfohlen. Du kannst auch einen anderen deiner Kontakte auswählen.
4. Wenn du ein Familienmitglied auswählst, wird es automatisch hinzugefügt. Wenn du einen anderen Kontakt auswählst, muss dieser eine entsprechende Anfrage bestätigen.
5. Nachdem der Kontakt die Anfrage bestätigt hat, wirst du in einer Nachricht darüber informiert, dass er als dein Kontakt für die Accountwiederherstellung hinzugefügt wurde.

## Wiederherstellungskontakt anzeigen und entfernen

Wie gehst du vor, wenn du deinen Wiederherstellungskontakt anzeigen oder entfernen möchtest?

1. Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad:* Wähle „Einstellungen“  > [dein Name] und tippe auf „Passwort & Sicherheit“.
  - Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Systemeinstellungen“ > Apple-ID  und wähle „Passwort & Sicherheit“ in der Seitenleiste.
  - Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“ > Apple-ID  und wähle dann „Passwort & Sicherheit“.
2. Unter „Wiederherstellungshilfe“ wird eine Liste deiner Wiederherstellungskontakte angezeigt.
3. Wähle den Wiederherstellungskontakt aus, den du entfernen möchtest, und entferne ihn.


# Schützen der Geräte-, App- und Website-Passwörter auf dem iPhone und iPad

Auf deinem iPhone oder iPad kannst du deine Passwörter in „Einstellungen“, in der Spotlight-Suche oder mit Siri verwalten. Du kannst auch die Sicherheitsempfehlungen für Passwörter verwenden, um schwache oder anfällige Passwörter zu identifizieren. Gesicherte Passwörter erscheinen in alphabetischer Reihenfolge sortiert nach der Website oder Plattform, auf der sie gesichert wurden.




## Passwörter verwalten

Du kannst deine Passwörter in „Einstellungen“, in der Spotlight-Suche oder mit Siri verwalten.

1. Wähle „Einstellungen“  > „Passwörter“ und führe einen der folgenden Schritte aus:
  - Tippe oben rechts auf „Hinzufügen“, um ein neues Passwort manuell hinzuzufügen.
  - Tippe zum Bearbeiten oder Löschen eines Passworts oben rechts auf „Bearbeiten“, auf „Gesicherte Passwörter auswählen“ und dann auf „Bearbeiten“ oder „Löschen“.  
**Wichtig:** Ein gelöscht Passwort kann nicht wiederhergestellt werden.
2. Wenn du ein neues Passwort hinzugefügt hast, teste es, um sicherzustellen, dass du es korrekt eingegeben hast.


## Sicherheitsempfehlungen für Passwörter verwenden

Wenn du deine eigenen Passwörter für Websites und Apps erstellst und speicherst, kannst du die Funktion für Sicherheitsempfehlungen für Passwörter nutzen, um schwache oder anfällige Passwörter zu identifizieren (etwa, wenn diese leicht zu erraten sind oder häufig verwendet wurden). Du kannst diese Funktion auch verwenden, um deine Passwörter sicher zu überwachen und um dich warnen zu lassen, wenn sie durch ein bekanntes Datenleck kompromittiert wurden.

1. Wähle „Einstellungen“  > „Passwörter“ > „Sicherheitsempfehlungen“.
2. Aktiviere „Kompromittierte Passwörter erkennen“, damit das iPhone deine Passwörter sicher überwacht und dich warnt, wenn Passwörter in bekannten Datenlecks erschienen sind.
3. Prüfe diese Empfehlungen für die Passwörter, die du erstellt hast:
  - Passwörter, die als *wiederholt verwendet* markiert werden, sind in verschiedenen Domains verwendet worden. Wird dasselbe Passwort für mehrere Dienste verwendet, macht dies die betreffenden Accounts anfällig für Angreifer, die deine Anmeldedaten entdeckt haben.
  - Passwörter, die als *schwach* markiert werden, können von Angreifern leicht erraten werden.
  - Passwörter werden als *kompromittiert* gekennzeichnet, wenn die Funktion für die Passwortüberwachung sie in einem bekannten Datenleck identifiziert hat.
4. Um ein wiederholt verwendetes, schwaches oder kompromittiertes Passwort zu aktualisieren, tippe auf das Objekt und befolge die angezeigten Anleitungen.



## Erkennung kompromittierter Passwörter aktivieren

Das iPhone und iPad kann (unter iOS 17, iPadOS 17 oder neuer) deine Passwörter überwachen und dir mitteilen, wenn sie von bekannten Datenlecks betroffen sind.

- Wähle „Einstellungen“  > „Passwörter“ > „Sicherheitsempfehlungen“ und aktiviere die Option „Kompromittierte Passwörter erkennen“.

## Einmalige BestätigungsCodes automatisch löschen

In iOS 17, iPadOS 17 und macOS Sonoma 14 oder neuer werden einmalige BestätigungsCodes automatisch ausgefüllt, sodass du die App oder Website, bei der du dich anmeldest, nicht verlassen musst. Du kannst festlegen, dass die BestätigungsCodes nach der Eingabe mit „Automatisch ausfüllen“ automatisch gelöscht werden, oder du behältst sie.

- Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad:* Wähle „Einstellungen“  > „Passwort“, wähle „Passwortoptionen“ und aktiviere die Option „Automatisch löschen“.
  - *Auf dem Mac:* Wähle „Apple“  > „Systemeinstellungen“ > „Passwort“ in der Seitenleiste, wähle „Passwortoptionen“ und aktiviere die Option „Automatisch löschen“.



# Verwalten geteilter Passwörter und Passkeys





In iOS 17, iPadOS 17 und macOS Sonoma 14 oder neuer kannst du eine Gruppe von vertrauenswürdigen Kontakten erstellen oder einer solchen Gruppe beitreten, um Passwörter und Passkeys geräteübergreifend zu teilen. In Gruppen für geteilte Passwörter gibt es zwei verschiedene Benutzerrollen: Gruppeneigentümer:in und Gruppenmitglied. Die Benutzerrolle bestimmt die Aufgaben, die du ausführen kannst.

- *Gruppeneigentümer:in:* Der:die Gruppeneigentümer:in ist das Gruppenmitglied, das die Gruppe erstellt hat. Der:die Eigentümer:in ist die einzige Person, die andere Mitglieder hinzufügen oder entfernen kann.
- *Gruppenmitglied:* Jede Person, die eine Einladung von dem:der Eigentümer:in erhalten und angenommen hat, ist ein Gruppenmitglied. Alle Gruppenmitglieder können jederzeit Passwörter hinzufügen, anzeigen, bearbeiten oder löschen. Gruppenmitglieder können jederzeit eine Gruppe verlassen.



*Hinweis:* Wenn du ein Passwort oder einen Passkey löschst, das/den du mit einer Gruppe geteilt hast, kannst du es/ihn 30 Tage lang wiederherstellen. Wenn du ein Passwort oder einen Passkey löschst, das/den eine andere Person mit der Gruppe geteilt hat, wird diese Person darüber informiert, dass sie es/ihn 30 Tage lang wiederherstellen kann. Weitere Informationen findest du unter „[Wiederherstellen eines zuletzt gelöschten Passworts oder Passkeys auf dem Mac](https://support.apple.com/guide/mac-help/mchlee73013a)“ (<https://support.apple.com/guide/mac-help/mchlee73013a>) im macOS-Benutzerhandbuch.





## Deine Rolle in einer Gruppe für geteilte Passwörter ermitteln

- Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad:* Wähle „Einstellungen“  > „Passwort“, suche nach einer Gruppe für geteilte Passwörter , wähle die Gruppe aus und stelle fest, ob du der:die Eigentümer:in oder ein Mitglied der Gruppe bist.
  - *Auf dem Mac:* Wähle „Apple“  > „Systemeinstellungen“ > „Passwort“ in der Seitenleiste, suche nach einer Gruppe für geteilte Passwörter  und wähle die Gruppe aus. Klicke dann auf „Verwalten“ und stelle fest, ob du der:die *Eigentümer:in* oder ein *Mitglied* der Gruppe bist.







## Person aus einer von dir erstellten Gruppe für geteilte Passwörter entfernen

Wenn du eine andere Person aus einer Gruppe für geteilte Passwörter entfernst, hat diese Person möglicherweise weiterhin Zugriff auf die Accounts und Passwörter, die du geteilt hast, als die Person sich in der Gruppe befand. Nach dem Entfernen einer Person musst du auch die Passwörter für deine Accounts ändern, auf die diese Person keinen Zugriff mehr haben soll.

- Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad:* Wähle „Einstellungen“  > „Passwort“, suche nach einer Gruppe für geteilte Passwörter , wähle die Gruppe aus und entferne das Mitglied.
  - *Auf dem Mac:* Wähle Menü „Apple“  > „Systemeinstellungen“ > „Passwort“ in der Seitenleiste, suche nach einer Gruppe für geteilte Passwörter  und wähle die Gruppe aus. Klicke dann auf „Verwalten“ und entferne das Mitglied.

## Als Mitglied eine Gruppe für geteilte Passwörter verlassen






Wenn du dich selbst aus einer Gruppe für geteilte Passwörter entfernst, haben die Mitglieder dieser Gruppe möglicherweise weiterhin Zugriff auf die Accounts und Passwörter oder Passkeys, die du geteilt hast, als du ein Mitglied der Gruppe warst. Nach dem Verlassen einer Gruppe musst du auch die Passwörter oder Passkeys für deine Accounts ändern, auf die die Gruppenmitglieder keinen Zugriff mehr haben sollen.

- Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad:* Wähle „Einstellungen“  > „Passwort“, suche nach einer Gruppe für geteilte Passwörter , wähle die Gruppe aus und entferne dich aus der Gruppe.
  - *Auf dem Mac:* Wähle Menü „Apple“  > „Systemeinstellungen“ > „Passwort“ in der Seitenleiste, suche nach einer Gruppe für geteilte Passwörter  und wähle die Gruppe aus. Klicke dann auf „Verwalten“ und entferne dich aus der Gruppe.

## Passwort oder Passkey aus einer Gruppe für geteilte Passwörter löschen

Wenn du Passwörter oder Passkeys aus einer Gruppe für geteilte Passwörter löschst, haben die Mitglieder der Gruppe möglicherweise weiterhin Zugriff auf die Accounts und Passwörter oder Passkeys, die du mit der Gruppe geteilt hast. Nach dem Löschen dieser Objekte musst du auch die Passwörter oder Passkeys für deine Accounts ändern, auf die die Gruppenmitglieder keinen Zugriff mehr haben sollen.

*Hinweis:* Wenn du ein Passwort oder einen Passkey löschst, das/den du mit einer Gruppe geteilt hast, kannst du es/ihn 30 Tage lang wiederherstellen. Wenn du ein Passwort oder einen Passkey löschst, das/den eine andere Person mit der Gruppe geteilt hat, wird diese Person darüber informiert, dass sie es/ihn 30 Tage lang wiederherstellen kann. Weitere Informationen findest du unter [„Wiederherstellen eines zuletzt gelöschten Passworts oder Passkeys auf dem Mac“](#) im macOS-Benutzerhandbuch (<https://support.apple.com/guide/mac-help/mchlee73013a>).

- Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad:* Wähle „Einstellungen“  > „Passwort“ in der Seitenleiste aus, suche nach einer Gruppe für geteilte Passwörter , wähle die Gruppe aus und stelle fest, ob du der:die Eigentümer:in oder ein Mitglied der Gruppe bist.
  - *Auf dem Mac:* Wähle „Apple“  > „Systemeinstellungen“, klicke auf „Passwörter“  in der Seitenleiste und klicke auf die Infotaste  neben dem Account mit dem du das löschende Passwort oder Passkey. Klicke dann auf „Passwort löschen“ oder „Passkey löschen“ und klicke (erneut) auf „Passwort löschen“ oder „Passkey löschen“.

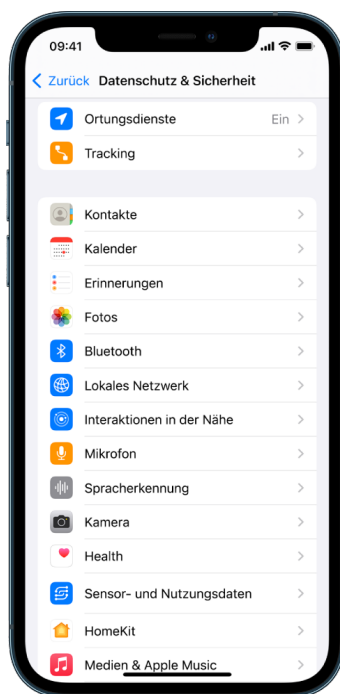
# Datenschutzfunktionen von Apps in Apple-Produkten





Apple bietet Einstellungen, Funktionen und Steuerelemente, mit denen du die Daten, die du mit Apps teilst, überprüfen und verwalten kannst.



## Datenschutzeinstellungen von Apps auf Apple-Geräten überprüfen und aktualisieren

Die Datenschutzeinstellungen auf deinem Gerät wurden entwickelt, um dir die Kontrolle über deine Daten zu geben. Du kannst beispielsweise einer Social-Media-App erlauben, deine Kamera zu verwenden, damit du Fotos aufnehmen und in dieser App hochladen kannst. Ein Grund für die Überprüfung dieser Einstellung kann sein, dass eine andere Person dein Gerät eingerichtet hat oder Zugriff auf es hatte und deinen Code kennt. Du solltest sicherstellen, dass diese Person keine Änderungen an deinen Einstellungen vorgenommen hat.




1. Führe einen der folgenden Schritte aus:
  - Auf iPhone oder iPad: Wähle „Einstellungen“  > „Datenschutz & Sicherheit“ .
  - Auf einem Mac mit macOS 13 oder neuer: Wähle „Apple“  > „Systemeinstellungen“, wähle „Datenschutz & Sicherheit“ in der Seitenleiste aus und klicke dann auf „Datenschutz“.
  - Auf einem Mac mit macOS 12 oder älter: Wähle „Apple“  > „+Systemeinstellungen“, wähle „Datenschutz & Sicherheit“ und klicke dann auf „Datenschutz“.
2. Überprüfe die Liste der Datenarten (z. B. Kalender, Kontakte, Fotos, Erinnerungen usw.).
3. Wähle eine Datenart in der Liste aus, um festzustellen, welche Apps auf deinem Gerät auf sie zugreifen können.

Apps werden nicht in der Liste angezeigt, wenn sie keinen Zugriff angefordert haben. Du kannst jeder App den Zugriff erteilen oder entziehen, die ihn angefordert hat. Für Fotos kannst du auch den Zugriff ändern, der Apps erteilt wird. Eine App kann die Datenart in der entsprechenden Einstellung nur nutzen, wenn du ihr Zugriff erteilt hast.

*Hinweis:* Das Ändern der Datenschutzeinstellungen auf deinem Apple-Gerät ändert nur, wie diese Apps auf deine Daten zugreifen können. Wenn du die Einstellungen für „Datenschutz & Sicherheit“ bei einer App von einem Drittanbieter (d. h. Apps, die nicht von Apple erstellt wurden) ändern möchtest, musst du dich (in der App oder in einem Webbrowser) bei deinem Account von diesem Drittanbieter anmelden und die Einstellungen dort aktualisieren.

### Transparenz beim App-Tracking verwenden


Über die Transparenz beim App-Tracking kannst du entscheiden, ob eine App übergreifend über Apps und Websites eines anderen Unternehmens deine Aktivitäten per Tracking protokollieren darf. Du kannst die Berechtigungen zur Protokollierung deiner Aktivitäten jederzeit zurückziehen. Wenn du „Apps erlauben, Tracking anzufordern“ deaktivierst, werden keine Aufforderungen von Apps mehr angezeigt, die deine Aktivitäten erfassen möchten. Jede App, die eine Berechtigung für das Tracking einholt, während diese Einstellung deaktiviert ist, wird so behandelt, als ob du auf „App-Tracking ablehnen“ getippt hättest.

- Führe einen der folgenden Schritte aus:
  - Auf iPhone oder iPad: Wähle „Einstellungen“  > „Datenschutz & Sicherheit“ > „Tracking“ und deaktiviere dann „Apps erlauben, Tracking anzufordern“.
  - Auf deinem Apple TV-Gerät: Wähle „Einstellungen“ > „Allgemein“ > „Datenschutz & Sicherheit“ > „Tracking“ und deaktiviere dann „Apps erlauben, Tracking anzufordern“.

## Über den App-Datenschutzbericht feststellen, wie Apps auf deine Daten zugreifen

Wenn du befürchtest, dass jemand in deiner Nähe ohne dein Einverständnis Apps auf deinem iPhone oder iPad installiert oder die Einstellungen von Apps geändert hat, die du installiert hast, kannst du den App-Datenschutzbericht aktivieren.

Der Bericht enthält nähere Informationen darüber, wie oft jede App auf deine Daten (wie etwa deinen Standort oder deine Kamera und dein Mikrofon) zugreift.

1. Wähle „Einstellungen“  > „Datenschutz“.
2. Scrolle nach unten und tippe auf „App-Datenschutzbericht“.
3. Aktiviere „App-Datenschutzbericht“.

Du kannst den App-Datenschutzbericht auch jederzeit unter „Einstellungen“ > „Datenschutz & Sicherheit“ > „App-Datenschutzbericht“ deaktivieren. Dadurch wird auch der Bericht von deinem Gerät gelöscht.

*Hinweis:* Nachdem du ihn aktiviert hast, beginnt der App-Datenschutzbericht mit der Sammlung von Daten. Es kann also eine Weile dauern, bis die Informationen angezeigt werden. Im Laufe der weiteren Nutzung der Apps auf deinem Gerät werden mehr Informationen angezeigt. Die Daten in deinem App-Datenschutzbericht sind verschlüsselt und werden nur auf deinem Gerät gespeichert. Der Bericht zeigt an, wie oft – und wann – eine App in den vorherigen 7 Tagen auf datenschutzrelevante Daten oder deine Gerätesensoren zugegriffen hat. Du kannst auf die einzelnen Apps und Arten von Daten tippen, um genauere Informationen zu erhalten.

# Schützen deiner Geräte vor Spionagesoftware mithilfe des Blockierungsmodus

Der Blockierungsmodus ist eine extreme, optionale Schutzfunktion für iPhone, iPad und Mac (mit iOS 16, iPadOS 16.1 und macOS 13 oder neuer), die nur verwendet werden sollte, wenn du denkst, dass du das Ziel eines komplexen Cyberangriffs bist – z. B. von privaten Unternehmen, die staatlich geförderte Spionageprogramme entwickeln.

*Hinweis:* Die meisten Menschen werden niemals Ziel eines derartigen Angriffs.






Wenn sich ein Gerät im Blockierungsmodus befindet, funktioniert es nicht wie gewohnt. Apps, Websites und Funktionen sind aus Sicherheitsgründen stark eingeschränkt und einige Benutzererlebnisse sind überhaupt nicht verfügbar. Der Blockierungsmodus umfasst die folgenden Schutzfunktionen:

- *Nachrichten:* Die meisten Arten von Nachrichtenanhängen außer Bildern sind blockiert. Einige Funktionen, wie beispielsweise Link-Vorschauen, sind deaktiviert.
- *Surfen im Web:* Bestimmte komplexe Webtechnologien, wie die Just-in-Time (JIT) JavaScript-Kompilierung, sind deaktiviert, es sei denn, Nutzer:innen schließen eine vertrauenswürdige Website vom Blockierungsmodus aus.
- *Apple-Dienste:* Eingehende Einladungen und Serviceanfragen, einschließlich FaceTime-Anrufe, werden blockiert, wenn Nutzer:innen den:die Initiator:in zuvor nicht angerufen oder eine Anfrage gesendet haben.
- *Kabelgebundene Verbindungen:* Verbindungen mit einem Computer oder Zubehör werden blockiert, wenn das Gerät gesperrt ist.
- *Konfigurationsprofile:* Konfigurationsprofile können nicht installiert werden und das Gerät kann sich nicht bei einer MDM-Lösung (Mobile Device Management) anmelden, wenn der Blockierungsmodus aktiviert ist. Alle MDM-Profile, die vor der Aktivierung des Blockierungsmodus aktiviert waren, verbleiben jedoch auf dem Gerät.

## Blockierungsmodus aktivieren/deaktivieren

Der Blockierungsmodus muss auf dem iPhone, iPad und Mac jeweils separat aktiviert werden. Beim Aktivieren des Blockierungsmodus auf dem iPhone aktiviert das iPhone automatisch den Blockierungsmodus auf allen gekoppelten Apple Watch-Geräten mit watchOS 10 (oder neuer). Du kannst den Blockierungsmodus nicht direkt auf einer Apple Watch ein- oder ausschalten.

- Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad:* Wähle „Einstellungen“  > „Datenschutz & Sicherheit“ > „Blockierungsmodus“, tippe auf „Blockierungsmodus aktivieren“, dann auf „Aktivieren und neu starten“ und gib deinen Gerätecode ein.
  - *Auf dem Mac:* Wähle „Apple“  > „Systemeinstellungen“ > „Datenschutz & Sicherheit“  > „Blockierungsmodus“, wähle „Aktivieren“, gib bei Aufforderung dein Passwort ein und wähle „Aktivieren und neu starten“.

# Sicherheitseinstellungen in der App „Nachrichten“ verwalten

In der App „Nachrichten“  hast du zwei Möglichkeiten, um Textnachrichten zu senden:

- Mit iMessage über WLAN oder Mobilfunknetze an andere Personen, die ebenfalls iMessage auf einem iPhone, iPad oder Mac verwenden. Deine iMessage-Texte werden in blauen Sprechblasen angezeigt.
- Mit SMS/MMS-Nachrichten, die von deinem iPhone an andere Geräte versendet werden. Deine SMS/MMS-Nachrichten werden in grünen Sprechblasen angezeigt.



Du kannst mit iMessage Nachrichten, Fotos oder Videos über WLAN oder Mobilfunknetze an ein anderes iPhone oder iPad oder an einen anderen Mac senden. Diese Nachrichten sind immer verschlüsselt und erscheinen in blauen Textblasen auf deinem iPhone, iPad und Mac.



## Nachrichten auf ein Gerät einschränken


Wenn du Nachrichten auf ein Gerät einschränken möchtest, musst du den Account auf den Geräten, auf denen keine Nachrichten mehr empfangen werden sollen, bei der App „Nachrichten“ abmelden und Nachrichten in iCloud deaktivieren.

1. Führe einen der folgenden Schritte aus:

- *Auf iPhone oder iPad:* Wähle „Einstellungen“  > „Nachrichten“ und aktiviere oder deaktiviere dann iMessage.
- *Auf dem Mac:* Wähle in der App „Nachrichten“  „Nachrichten“ > „Einstellungen“, klicke auf iMessage und dann auf „Abmelden“. Bestätige, dass du dich abmelden möchtest, und klicke erneut auf „Abmelden“.


## Nachrichten in iCloud auf dem iPhone oder iPad deaktivieren

Wenn du Nachrichten in iCloud verwendest, werden alle Nachrichten, die du sendest, empfängst und löschst, auf allen deinen Apple-Geräten automatisch aktualisiert.

1. Auf *iPhone* oder *iPad*: Wähle „Einstellungen“  > [dein Name] und tippe auf „iCloud“.
2. Tippe auf „Alle anzeigen“ unter „Apps, die iCloud verwenden“.
3. Tippe auf „Nachrichten“ und deaktiviere dann „Dieses [*iPhone*]/[*iPad*] synchronisieren“.
4. Wiederhole diesen Vorgang auf jedem Gerät, um die Nachrichten aus iCloud zu entfernen.

## Nachrichten in iCloud auf dem Mac deaktivieren

Wenn du Nachrichten in iCloud verwendest, werden alle Nachrichten, die du sendest, empfängst und löschst, auf allen deinen Apple-Geräten automatisch aktualisiert.

1. Wähle in der App „Nachrichten“  auf deinem Mac „Nachrichten“ > „Einstellungen“ und klicke dann auf „iMessage“.
2. Klicke auf „Einstellungen“ und deaktiviere dann Nachrichten in iCloud.
3. Wähle eine der folgenden Optionen aus:
  - *Alle deaktivieren*: Deaktiviert Nachrichten in iCloud auf allen deinen Geräten. Die Nachrichten werden nicht mehr in iCloud, sondern auf jedem Gerät gespeichert.
  - *Dieses Gerät deaktivieren*: Deaktiviert Nachrichten in iCloud nur auf deinem Mac. Die Nachrichten auf deinem Mac werden nicht mehr in iCloud gespeichert; auf Geräten, auf denen die Option „Nachrichten in iCloud“ aktiviert ist, werden Nachrichten aber weiterhin in iCloud gespeichert.

## iMessage aktivieren und deaktivieren

iMessage nutzt die Ende-zu-Ende-Verschlüsselung, um deine Nachrichten auf allen Geräten zu schützen, sodass niemand ohne Code darauf zugreifen kann – noch nicht einmal Apple. Da iMessage-Konversationen über WLAN und Mobilfunknetze erfolgen, erscheinen Informationen darüber, an welche Person du die Nachrichten sendest, nicht auf deiner Telefonrechnung. iMessages können gesichert werden, sodass du auch bei Verlust oder Diebstahl deines Geräts wichtige Nachrichtenverläufe wiederherstellen kannst.

**Wichtig:** Damit Nachrichten in iCloud gesichert werden können, musst du die Backup-Funktion aktiviert haben. Wenn dies nicht der Fall ist, lassen sich deine Nachrichten nicht wiederherstellen. Weitere Informationen findest du unter „[iCloud für ‚Nachrichten‘ auf all deinen Geräten einrichten](#)“ im iCloud-Benutzerhandbuch (<https://support.apple.com/guide/icloud/mm0de0d4528d>).






### Wenn iMessage aktiviert ist

Du kannst eine iMessage über eine WLAN-Verbindung senden, wenn kein Mobilfunkdienst verfügbar ist. Die Funktion „Zuletzt gelöscht“ bewahrt gelöschte Nachrichten für bis zu 30 Tage auf. Wenn du befürchtest, dass jemand Nachrichten von deinem Gerät gelöscht hat, sind diese Nachrichten möglicherweise noch über diesen Tab verfügbar.

### Wenn iMessage deaktiviert ist

Wenn iMessage deaktiviert ist, stehen Funktionen wie das Bearbeiten von Nachrichten, das Senden noch nicht gesendeter Nachrichten und das Lesen von Lesebestätigungen nicht zur Verfügung. Nachrichten werden stattdessen via SMS/MMS gesendet.

**Wichtig:** Bei Verwendung von SMS/MMS erscheinen Aufzeichnungen dieser Nachrichten möglicherweise auf deiner Telefonrechnung und können vom Mobilfunkanbieter an den Accountinhaber für diese Telefonnummer weitergegeben werden.




- Auf iPhone oder iPad: Wähle „Einstellungen“  > „Nachrichten“ und aktiviere oder deaktiviere dann iMessage.
- Auf einem Mac mit macOS 13 oder neuer: Öffne die App „Nachrichten“ , wähle „Nachrichten“ > „Einstellungen“, klicke auf iMessage und dann auf „Abmelden“. Bestätige, dass du dich abmelden möchtest, und klicke erneut auf „Abmelden“.
- Auf einem Mac mit macOS 12 oder älter: Öffne die App „Nachrichten“ , wähle „Nachrichten“ > „Einstellungen“, klicke auf iMessage und dann auf „Abmelden“. Bestätige, dass du dich abmelden möchtest, und klicke erneut auf „Abmelden“.

### Lesebestätigungen aktivieren und deaktivieren

Durch iMessage-Lesebestätigungen erfahren iMessage-Benutzer:innen, wann ihre Nachrichten gelesen wurden. Wenn Lesebestätigungen aktiviert sind, erhält die Person, die dir die iMessage gesendet hat, einen „Gelesen“-Hinweis unter der Nachricht, nachdem du sie gelesen hast. Sind Lesebestätigungen deaktiviert, sieht die Person nur, dass die Nachricht zugestellt wurde.

Du kannst Lesebestätigungen für alle Konversationen oder nur für bestimmte Konversationen senden. Wenn du Lesebestätigungen für alle Konversationen aktiviert hast, kannst du sie dennoch für einzelne Konversationen deaktivieren – und umgekehrt.

*Hinweis:* Lesebestätigungen werden für SMS-Nachrichten und Gruppentextnachrichten nicht unterstützt.



- Auf iPhone oder iPad: Wähle „Einstellungen“  > „Nachrichten“ und aktiviere oder deaktiviere „Lesebestätigungen“.
- Auf einem Mac mit macOS 13 oder neuer: Öffne „Nachrichten“ , wähle „Nachrichten“ > „Einstellungen“, klicke auf den Tab „iMessage“ und aktiviere oder deaktiviere „Lesebestätigungen senden“.
- Auf einem Mac mit macOS 12 oder älter: Öffne „Nachrichten“ , wähle „Nachrichten“ > „Einstellungen“, klicke auf den Tab „iMessage“ und aktiviere oder deaktiviere „Lesebestätigungen senden“.

## Gesendete Nachricht bearbeiten

In iOS 16, iPadOS 16.1 und macOS 13 oder neuer kannst du eine kürzlich gesendete Nachricht bis zu 5-mal innerhalb von 15 Minuten nach dem Senden bearbeiten. So kannst du Schreibfehler korrigieren. Die Empfänger sehen, dass die Nachricht bearbeitet wurde, und können sich den Bearbeitungsverlauf ansehen.

*Hinweis:* SMS-Nachrichten lassen sich nicht bearbeiten.



Wenn deine Empfänger Apple-Geräte mit früheren Versionen von iOS, iPadOS oder macOS haben, erhalten sie Folgenachrichten mit der Einleitung „Geändert in“ und deine neue Nachricht erscheint in Anführungszeichen.

- *Auf iPhone oder iPad:* Tippe auf „Nachrichten“ , lege den Finger auf die Nachrichtenblase, tippe auf „Bearbeiten“, bearbeite die Nachricht und sende sie anschließend erneut.
- *Auf einem Mac mit macOS 13:* Öffne „Nachrichten“ , klicke bei gedrückter Taste „ctrl“ auf die Nachrichtenblase, wähle „Bearbeiten“, bearbeite die Nachricht und sende sie anschließend erneut.

## Nachricht zurückrufen

In iOS 16, iPadOS 16.1 und macOS 13 oder neuer kannst du eine kürzlich gesendete Nachricht innerhalb von 2 Minuten nach dem Senden zurückrufen. Eine Nachricht, die versehentlich an die falsche Person gesendet wurde, kannst du so zurückrufen. Die Empfänger können sehen, dass eine Nachricht zurückgerufen wurde.

*Hinweis:* SMS-Nachrichten lassen sich nicht zurückrufen.

- *Auf iPhone oder iPad:* Tippe auf „Nachrichten“ , lege den Finger auf die Nachrichtenblase und tippe auf „Senden widerrufen“.  
Ein Hinweis, der das Widerrufen der Nachricht bestätigt, erscheint in beiden Konversationstranskripten – in deinem und in dem des:der Empfänger:in.
- *Auf einem Mac mit macOS 13 oder neuer:* Öffne „Nachrichten“ , klicke bei gedrückter Taste „ctrl“ auf die Nachrichtenblase und wähle „Senden widerrufen“.  
Ein Hinweis, der das Widerrufen der Nachricht bestätigt, erscheint in beiden Konversationstranskripten – in deinem und in dem des:der Empfänger:in.

# Verwenden der Wegbegleitung für Nachrichten

Du kannst die Funktion „Wegbegleitung“ auf dem iPhone verwenden, um Freund:innen mitzuteilen, dass dein iPhone an einem Ziel eingetroffen ist. Außerdem kannst du festlegen, welche Informationen sie sehen können, wenn du dein Ziel nicht erfolgreich erreichst.

Ebenso kannst du, wenn Freund:innen die Funktion „Wegbegleitung“ mit dir verwenden, aber ihr iPhone nicht wie erwartet am Ziel eintrifft, den Standort des Geräts, die Batterieladung, das Mobilfunksignal und mehr sehen.

*Hinweis:* Zum Nutzen der Funktion „Wegbegleitung“ müssen sowohl Absender:in als auch Empfänger:in iOS 17 (oder neuer) verwenden. Die Standortfreigabe wird in Südkorea nicht unterstützt und kann aufgrund lokaler Gesetzgebungen in anderen Regionen nicht verfügbar sein.

Beim Starten einer *reisebasierten* Wegbegleitung wird dein Kontakt über Folgendes informiert:

- Dein Ziel und deine ungefähre Ankunftszeit
- Was er:sie erwarten kann, wenn du nicht auf Aufforderungen reagierst, „Notruf SOS“ während einer aktiven Wegbegleitung verwendest oder dein Telefon nicht wie erwartet am Ziel eintrifft

Beim Starten einer *timerbasierten* Wegbegleitung wird dein Kontakt über Folgendes informiert:

- Zu welchem Zeitpunkt du den Timer gestartet hast
- Zu welchem Zeitpunkt der Timer endet
- Was dein Kontakt erwarten kann, wenn du nicht auf Aufforderungen des Timers reagierst oder „Notruf SOS“ während einer aktiven Wegbegleitung verwendest

## Welche Informationen werden zu welchem Zeitpunkt geteilt?

Beim Einrichten der Wegbegleitung kannst du festlegen, welche Informationen du mit deinem Kontakt teilen möchtest, wenn die Wegbegleitung nicht wie erwartet beendet wird. Nach der Einrichtung der Wegbegleitung kannst du unter „Einstellungen“ > „Nachrichten“ > „Wegbegleitung“ > „Daten“ ändern, welche Arten von Daten du sendest.

Du kannst die folgenden Informationsstufen auswählen:

- *Begrenzter Datenbereich:* Beinhaltet deinen aktuellen Standort und Informationen über die Batterieladung und das Netzsignal von iPhone und Apple Watch.
- *Vollständiger Datenbereich:* Beinhaltet alle Daten der Informationsstufe „Begrenzter Datenbereich“ und die Position, an der dein iPhone zuletzt entsperrt und deine Apple Watch entfernt wurde.

Dein Kontakt erhält in den folgenden Situationen automatisch einen Link mit den von dir geteilten Informationen:

- Dein iPhone trifft nicht an deinem Ziel ein.
- Du bist erheblich verspätet und reagierst nicht auf die Aufforderung, den Timer zu verlängern.
- Du hast „Notruf SOS“ verwendet und reagierst nicht auf die anschließende Aufforderung der Wegbegleitung.
- Du reagierst nicht auf die Aufforderung am Ende deiner timerbasierten Wegbegleitung.

**Wichtig:** Wenn du dein iPhone verlierst, während eine Wegbegleitung aktiv ist, erhält dein Kontakt Mitteilungen, als ob du nicht antworten würdest.

## Während einer aktiven Wegbegleitung

Während einer aktiven reisebasierten Wegbegleitung wird die folgende Nachricht auf deinem Sperrbildschirm angezeigt: „Wegbegleitung: Zum Anzeigen der Details entsperren.“ Durch Tippen auf diese Nachricht entsperrst du das Gerät und siehst das von dir festgelegte Ziel, deine erwartete Ankunftszeit, die auf der Grundlage von Verkehrs- und Fahrbedingungen automatisch aktualisiert wird, und die Daten, die mit deinem Kontakt geteilt werden, wenn die Wegbegleitung nicht erfolgreich beendet wird („Beschränkt“ oder „Vollständig“). Außerdem kannst du die Wegbegleitung abbrechen.



### Timerbasierte Wegbegleitung starten

Wenn du dich an einem Ort befindest, an dem du dich nicht sicher fühlst, und dir Unterstützung von einem vertrauenswürdigen Kontakt wünschst, kannst du eine timerbasierte Wegbegleitung starten. Die timerbasierte Wegbegleitung informiert deinen vertrauenswürdigen Kontakt, wenn du nicht auf die Aufforderung reagierst, die bei Ablauf des Timers erfolgt.

Während einer aktiven timerbasierten Wegbegleitung wird die folgende Nachricht auf deinem Sperrbildschirm angezeigt: „Wegbegleitung: Zum Anzeigen der Details entsperren.“ Durch Tippen auf diese Nachricht entsperrst du das Gerät und siehst die folgenden Informationen:

- Die verbleibende Zeit für die Wegbegleitung
- Den für die Wegbegleitung ausgewählten Kontakt
- Die mit deinem Kontakt geteilten Daten:
  - „Beschränkt“ oder „Vollständig“

Timerbasierte Wegbegleitung starten:



1. Öffne die App „Nachrichten“  und wähle eine Person aus, die du benachrichtigen möchtest.
2. Tippe auf „Neue Nachricht“ oben auf dem Bildschirm und füge eine:n Empfänger:in hinzu oder wähle eine vorhandene Konversation aus.
3. Tippe auf , tippe auf „Wegbegleitung“ und dann auf „Bearbeiten“.  
Möglicherweise musst du auf „Mehr“ tippen, um die Option „Wegbegleitung“ zu sehen.
4. Wähle „Nach einem Timer“.
5. Wähle einen Zeitraum für den Timer aus.

Wenn die timerbasierte Wegbegleitung endet, erhältst du die Aufforderung, auf „Wegbegleitung beenden“ oder „Zeit hinzufügen“ zu tippen. Beim Beenden der Wegbegleitung wird dein Kontakt darüber informiert, dass die Wegbegleitung erfolgreich beendet wurde. Außerdem kannst du „Zeit hinzufügen“ wählen, um den Timer um 15, 30 oder 60 Minuten zu verlängern. Dein Kontakt wird über die aktualisierte Ablaufzeit des Timers informiert.

## Reisebasierte Wegbegleitung starten

Bist du mit dem Auto, öffentlichen Verkehrsmitteln oder zu Fuß unterwegs, kannst du eine Wegbegleitung starten, um automatisch eine:n Freund:in zu benachrichtigen, sobald du an deinem geplanten Ziel eintriffst.

Während einer aktiven reisebasierten Wegbegleitung wird die folgende Nachricht auf deinem Sperrbildschirm angezeigt: „Wegbegleitung: Zum Anzeigen der Details entsperren.“ Durch Tippen auf diese Nachricht entsperrest du das Gerät und siehst das von dir festgelegte Ziel, deine erwartete Ankunftszeit, die auf der Grundlage von Verkehrs- und Fahrbedingungen automatisch aktualisiert wird, und die Daten, die mit deinem Kontakt geteilt werden, wenn die Wegbegleitung nicht erfolgreich beendet wird. Außerdem kannst du die Wegbegleitung abbrechen.

1. Öffne die App „Nachrichten“  und wähle eine Person aus, die du benachrichtigen möchtest.
2. Tippe auf „Neue Nachricht“ oben auf dem Bildschirm und füge eine:n Empfänger:in hinzu oder wähle eine vorhandene Konversation aus.
3. Tippe auf , tippe auf „Wegbegleitung“ und dann auf „Bearbeiten“.  
Möglicherweise musst du auf „Mehr“ tippen, um die Option „Wegbegleitung“ zu sehen.
4. Wähle „Bei Ankunft“.
5. Tippe auf „Ändern“ und gib dein Ziel in der Suchleiste ein.
6. Tippe zum Festlegen des Ankunftsradius für dein Ziel auf „Klein“, „Mittel“ oder „Groß“ unten auf dem Bildschirm. Dein:e Freund:in erhält eine Ankunftsmitteilung, wenn du dich innerhalb dieses Radius befindest.
7. Tippe auf „Fertig“.
8. Tippe auf „Fahren“, „ÖPNV“ oder „Gehen“ und dann bei Bedarf auf „Zeit hinzufügen“.  
Wenn dein Gerät sich nicht dem Ziel nähert, erhältst du eine Aufforderung und hast 15 Minuten Zeit, um auf sie zu reagieren. Wenn du nicht reagierst, wird dein Kontakt automatisch benachrichtigt.

Wenn dein iPhone am Ziel einer reisebasierten Wegbegleitung eintrifft, wird die Wegbegleitung beendet und dein Kontakt wird in einer Mitteilung darüber informiert, dass du angekommen bist.

# Blockieren von Anrufen und Nachrichten von bestimmten Personen

Wenn du Anrufe, FaceTime-Anrufe, Nachrichten oder E-Mails von einer Person erhältst, mit der du keinen Kontakt haben möchtest, kannst du zukünftige Kontaktversuche von dieser Person blockieren. Wenn du eine Person auf einem Gerät blockierst, wird sie auf allen Geräten blockiert, die mit derselben Apple-ID angemeldet sind.


**Wichtig:** Die blockierte Person wird nicht darüber benachrichtigt, dass sie blockiert wurde. Du kannst einen blockierten Kontakt weiterhin anrufen und ihm Nachrichten oder E-Mails schicken, ohne dass die Blockierung aufgehoben wird. Wenn du jedoch deinen Standort mit diesem Kontakt geteilt hast, *wird* die entsprechende Person darüber informiert, dass du deinen Standort nicht mehr mit ihr teilst, sobald du sie blockierst.


Wenn du einen Kontakt in Telefon, FaceTime, Nachrichten oder Mail blockierst, wird er in allen vier Apps blockiert.



## Sprachanrufe, FaceTime-Anrufe, Nachrichten und E-Mails von bestimmten Personen blockieren

- *In der App „Telefon“ auf dem iPhone:* Tippe in der App „Telefon“ auf „Favoriten“, „Anrufliste“ oder „Voicemail“, tippe auf die Infotaste ⓘ neben dem Namen, der Telefonnummer oder der E-Mail-Adresse des Kontakts, den du blockieren möchtest, scrolle nach unten, tippe auf „Anrufer blockieren“ und tippe auf „Kontakt blockieren“.
- *In der App „FaceTime“ auf iPhone oder iPad:* Tippe in deiner FaceTime-Anrufliste auf die Infotaste ⓘ neben dem Namen, der Telefonnummer oder der E-Mail-Adresse des Kontakts, den du blockieren möchtest, scrolle nach unten, tippe auf „Anrufer blockieren“ und tippe auf „Kontakt blockieren“.
- *In der App „FaceTime“ auf dem Mac:* Klicke in deiner FaceTime-Anrufliste bei gedrückter Taste „ctrl“ auf den Namen, die Telefonnummer oder die E-Mail-Adresse des Kontakts, den du blockieren möchtest und wähle „Anrufer blockieren“.
- *In der App „Nachrichten“ auf iPhone oder iPad:* Tippe in der App „Nachrichten“ auf eine Konversation, tippe auf den Namen oder die Nummer oben auf dem Bildschirm, tippe auf die Infotaste ⓘ, scrolle nach unten und tippe auf „Anrufer blockieren“.

- *In der App „Nachrichten“ auf dem Mac:* Wähle im Nachrichtenverlauf der App „Nachrichten“ den Namen, die Telefonnummer oder die E-Mail-Adresse der Person aus, die du blockieren möchtest. Wähle „Person blockieren“ im Menü „Konversationen“ aus und klicke auf „Blockieren“.
- *In der App „Mail“ auf iPhone oder iPad:* Tippe auf „Mail“ , wähle eine E-Mail von einer Person aus, die du blockieren möchtest, tippe auf ihren Namen oben in der E-Mail, wähle „Diesen Kontakt blockieren“ und tippe auf „Diesen Kontakt blockieren“.
- *In der App „Mail“ auf dem Mac:* Öffne die App „Mail“, wähle eine E-Mail von einer Person aus, die du blockieren möchtest, klicke auf ihren Namen oben in der E-Mail und wähle „Kontakt blockieren“ aus dem Einblendmenü aus.

Das Symbol „Blockiert“  wird in der Nachrichtenliste neben dem Namen der absendenden Person angezeigt. Außerdem werden die Nachrichten dieser Person mit einem Banner versehen, aus dem ersichtlich ist, dass sie blockiert wurde. Das Banner umfasst außerdem einen Link zum Bereich „Blockiert“ in den Einstellungen der App „Mail“, in dem du blockierte Absender:innen verwalten kannst.

*Hinweis:* Absender:innen, die du in der App „Mail“ zu den VIPs hinzugefügt hast, musst du zunächst aus den VIPs entfernen, bevor du sie blockieren kannst.

### **Blockierte Kontakte verwalten**

Du kannst deine blockierten Kontakte in allen vier Apps verwalten, die das Blockieren von Kontakten ermöglichen: Telefon, FaceTime, Nachrichten und Mail. Wenn du eine Blockierung in einer App entfernst, wird sie in allen vier Apps entfernt. Führe einen der folgenden Schritte aus, um eine Liste der Nummern zu sehen, die du blockiert hast:

- *In der App „Telefon“ auf dem iPhone:* Wähle „Einstellungen“  > „Telefon“ und tippe auf „Blockierte Kontakte“.
- *In der App „FaceTime“ auf iPhone oder iPad:* Wähle „Einstellungen“ > „FaceTime“ und tippe auf „Blockierte Kontakte“.
- *In der App „FaceTime“ auf dem Mac:* Öffne die App „FaceTime“, wähle „FaceTime“ > „Einstellungen“ und klicke auf „Blockiert“.
- *In der App „Nachrichten“ auf iPhone oder iPad:* Wähle „Einstellungen“ > „Nachrichten“ und tippe auf „Blockierte Kontakte“ unter „SMS/MMS“.
- *In der App „Nachrichten“ auf dem Mac:* Öffne die App „Nachrichten“, wähle „Nachrichten“ > „Einstellungen“, klicke auf „iMessage“ und dann auf „Blockiert“.
- *In der App „Mail“ auf iPhone oder iPad:* Wähle „Einstellungen“ > „Mail“ und tippe auf „Blockiert“.
- *In der App „Mail“ auf dem Mac:* Öffne die App „Mail“, wähle „Mail“ > „Einstellungen“, klicke auf „Spam“ und dann auf „Blockiert“.

## Empfangen von Warnungen zu sensiblen Bildern und Videos auf dem iPhone, iPad und Mac

Mit der Warnung vor sensiblen Inhalten können Erwachsene verhindern, dass sie nicht erwünschte Nacktdarstellungen in Bildern und Videos sehen, die sie in der App „Nachrichten“, in AirDrop, in einer FaceTime-Videonachricht und in der App „Telefon“ beim Erhalten eines Kontaktposters empfangen. Alle diese Apps und Funktionen verwenden dieselbe Datenschutztechnologie als zentrales Element der Kommunikationssicherheit. Die Funktion ist optional und kann von Benutzer:innen in den Einstellungen unter „Datenschutz & Sicherheit“ aktiviert werden.







Du erhältst eine Warnung (oder deine Familienmitglieder erhalten eine Warnung), bevor sexuell explizite Fotos empfangen oder gesendet werden. Außerdem kannst du bei der Verwendung der Funktion „Bildschirmzeit“ sensible Inhalte blockieren und Einschränkungen für Käufe einrichten. Weitere Informationen findest du unter [Kommunikation auf dem Gerät eines Familienmitglieds erlauben oder blockieren](#) im iPhone-Benutzerhandbuch.





## Konfigurieren der Warnung vor sensiblen Inhalten auf dem iPhone, iPad oder Mac

1. Führe einen der folgenden Schritte aus:

- Auf iPhone oder iPad: Wähle „Einstellungen“  > „Datenschutz & Sicherheit“  und tippe auf „Warnung vor sensiblen Inhalten“.
- Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“ , klicke auf „Systemeinstellungen“, klicke auf „Datenschutz & Sicherheit“  und dann auf „Warnung vor sensiblen Inhalten“.
- Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“ > „Datenschutz & Sicherheit“  und klicke dann auf „Warnung vor sensiblen Inhalten“.



2. Scrolle nach unten, tippe auf „Warnung vor sensiblen Inhalten“ und aktiviere dann „Warnung vor sensiblen Inhalten“.
3. Deaktiviere oder aktiviere die Erlaubnis zum Erkennen von sensiblen Inhalten, bevor sie angezeigt werden können, und erhalte Hinweise, die dich beim Treffen einer sicheren Wahl unterstützen.

# Schützen des Browserverlaufs in Safari und „Karten“

Suchverläufe und Caches für Browser und andere Apps regelmäßig zu prüfen und zu löschen, ist eine nützliche Maßnahme, wenn du befürchtest, dass jemand auf dein Gerät zugreift. Viele Apps speichern Informationen darüber, wonach du gesucht hast, sodass du diese in Zukunft auf einfache Weise wiederfinden kannst. Wenn du beispielsweise die App „Karten“ verwendest, kann ein Verlauf der Orte, nach denen du gesucht hast oder zu denen du navigiert bist, die Rückkehr zum kürzlich besuchten Ort vereinfachen.



Wenn du dich in einer unsicheren persönlichen Situation befindest und online Sicherheitsstrategien recherchieren musst, aber nicht möchtest, dass Safari Informationen über die von dir besuchten Webseiten speichert, kannst du auf dem [iPhone](#), [iPad](#) und [Mac](#) ein Fenster für privates Surfen öffnen. Wenn du den Modus „Privates Surfen“ verwendest werden deine Surfaktivitäten nicht gespeichert und nicht mit deinen anderen Geräten geteilt. Wenn du deine Geräte auf iOS 17, iPadOS 17 oder macOS Sonoma 14 aktualisiert hast, sperrt Safari außerdem die Tabs für privates Surfen nach einem Zeitraum ohne Aktivität. Sie können dann nur mit deinem Passwort, deinem Gerätecode, deiner Face ID oder deiner Touch ID geöffnet werden. So sind deine Daten geschützt, wenn du nicht in der Nähe deines Geräts bist. Du kannst den Browserverlauf löschen und ein Fenster für privates Surfen auf dem iPhone, iPad und Mac öffnen.

Wie du auf einem iPhone, iPad oder Mac ein Fenster für privates Surfen öffnest, erfährst du weiter unten in diesem Dokument.



## Löschen des Browserverlaufs



Wenn du online Informationen über Sicherheitsstrategien recherchiert hast und befürchtest, dass andere deinen Browserverlauf sehen können, kannst du alle Daten deiner Surfaktivitäten löschen, die in der App „Safari“ erfasst werden.

- *Auf iPhone oder iPad:* Wähle „Einstellungen“  > „Safari“ > „Verlauf und Websitedaten löschen“.
- *Auf dem Mac:* Öffne die App „Safari“ , wähle „Verlauf“ > „Verlauf löschen“, klicke auf das Einblendmenü und wähle aus, für welchen Zeitraum der Verlauf gelöscht werden soll.


Wenn du den Verlauf löschst, werden alle Daten deiner Surfaktivitäten gelöscht, die in der App „Safari“ gespeichert werden, darunter:

- Verlauf der Webseiten, die du besucht hast
- Liste der vorherigen und nächsten Seiten für geöffnete Webseiten
- Liste oft besuchter Seiten
- Aktuelle Suchanfragen
- Symbole von Webseiten
- Gespeicherte Schnappschüsse von geöffneten Webseiten
- Liste der Downloads (geladene Dateien werden nicht gelöscht)
- Websites, für die du die schnelle Website-Suche aktiviert hast
- Websites, die die Nutzung deines Standorts angefordert haben
- Websites, die dich um Erlaubnis zum Senden von Mitteilungen gefragt haben

## Benutzte Routen und Favoriten in der App „Karten“ auf iPhone und iPad löschen

1. Öffne die App „Karten“  und scrolle im Suchfeld nach unten zu „Zuletzt“.
2. Führe einen der folgenden Schritte aus:
  - Streiche auf einer benutzten Route nach links.
  - Tippe auf „Mehr“ direkt über der Liste und streiche auf einer benutzten Route nach links. Tippe zum Löschen einer Route über der betreffenden Route auf „Löschen“.
3. Wenn du einen Ort aus den Favoriten entfernen willst, scrolle zu „Favoriten“ und tippe auf „Mehr“. Streiche auf dem Favoritenort, der gelöscht werden soll, von rechts nach links oder tippe auf „Bearbeiten“ und dann auf die Taste „Entfernen“ , um mehrere Favoriten zu entfernen.

## Benutzte Routen und Favoriten in der App „Karten“ auf dem Mac löschen



1. Öffne die App „Karten“  und scrolle in der Seitenleiste zu „Zuletzt“.
2. Klicke unter „Zuletzt“ auf „Verlauf löschen“.
3. Wenn du einen Ort aus den Favoriten löschen willst, klicke bei gedrückter Taste „ctrl“ auf einen Ort (in der Seitenleiste unter „Favoriten“) und wähle „Aus Favoriten entfernen“.


## Fenster für privates Surfen auf dem iPhone öffnen

1. Öffne die App „Safari“.
2. Tippe auf die Taste „Tabs“ .
3. Tippe auf die Taste „Tabgruppen“  in der Mitte der Tableiste am unteren Bildschirmrand und tippe auf „Privat“.


Der Tab wird automatisch zu einer Tabgruppe mit der Bezeichnung „Privat“ hinzugefügt. Du kannst mehrere private Tabs in der Gruppe öffnen.

Du kannst einfach überprüfen, ob du dich im Modus „Privates Surfen“ befindest, indem du nachsiehst, ob das Suchfeld grau ist oder das Wort „Privat“ anzeigt.


Um die Webseiten auszublenden und den Modus „Privates Surfen“ zu verlassen, tippe auf die Taste „Tabs“  und tippe auf die Taste „Tabgruppen“ , um eine andere Tabgruppe über das Menü am unteren Bildschirmrand zu öffnen. Die privaten Webseiten werden wieder angezeigt, wenn du das nächste Mal den Modus „Privates Surfen“ verwendest.

Wenn du die privaten Tabs schließen möchtest, tippe auf die Taste „Tabs“  und streiche auf den Tabs, die du schließen möchtest, nach links.


## Privates Fenster auf dem iPad öffnen

- Tippe in der App „Safari“ auf die Taste „Seitenleiste einblenden“  und dann auf „Privat“.

Wenn der Modus „Privates Surfen“ aktiviert ist, hat das Suchfeld keinen schwarzen, sondern einen weißen Hintergrund. Die Webseiten, die du besuchst, werden nicht im Verlauf auf dem iPad oder in der Tabliste auf anderen Geräten angezeigt. Du kannst mehrere private Tabs in der privaten Tabgruppe öffnen.

Wenn du die Webseiten ausblenden und den Modus „Privates Surfen“ beenden möchtest, tippe auf die Taste „Seitenleiste einblenden“  und wechsele zu einer anderen Tabgruppe. Die Tabs werden wieder angezeigt, wenn du das nächste Mal den Modus „Privates Surfen“ verwendest.

## Privates Fenster auf dem Mac öffnen


1. Wähle in der App „Safari“  „Ablage“ > „Neues privates Fenster“ oder wechsele zu einem Safari-Fenster, das bereits den Modus „Privates Surfen“ verwendet.

Fenster, die den Modus „Privates Surfen“ verwenden, haben ein dunkles intelligentes Suchfeld mit weißem Text.







2. Du kannst so surfen wie gewohnt.

## Fenster immer im Modus „Privates Surfen“ auf dem Mac öffnen

1. Wähle in der App „Safari“  „Safari“ > „Einstellungen“ und klicke auf „Allgemein“.
2. Klicke auf das Einblendmenü „Safari öffnen mit:“ und wähle „Neuem privaten Fenster“.

Wenn diese Option nicht angezeigt wird, führe einen der folgenden Schritte aus:

- Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Schreibtisch & Dock“  und vergewissere dich, dass „Fenster beim Beenden eines Programms schließen“ ausgewählt ist.
- Auf einem Mac mit macOS 12 oder älter: Wähle „Apple“  > „Systemeinstellungen“ klicke auf „Allgemein“  und stelle sicher, das „Fenster beim Beenden eines Programms schließen“ ausgewählt ist.

## Weitere Datenschutzoptimierungen in Safari

- Lösche im Ordner „Downloads“ alle Elemente, die du während der Verwendung des Modus „Privates Surfen“ geladen hast.
- Schließe alle anderen noch geöffneten privaten Fenster, damit andere nicht die Tasten zum Öffnen der vorherigen und nächsten Seite verwenden und die von dir geöffneten Seiten sehen können.

# Tätigen eines Notrufs oder Senden einer Notfalltextnachricht auf dem iPhone oder der Apple Watch

Bei einem Notfall kannst du mit dem iPhone oder der Apple Watch schnell über einen Anruf oder eine Textnachricht Hilfe anfordern.




Wenn du deinen Notfallpass teilst, sendet dein iPhone deine Gesundheitsinformationen an den Rettungsdienst, wenn du ihn per Telefon oder Textnachricht kontaktierst oder „Notruf SOS“ verwendest (nur USA). Weitere Informationen über den Notfallpass findest du unter „[Hinterlegen deiner Gesundheitsinfos in der App ‚Health‘ auf dem iPhone](#)“ im iPhone-Benutzerhandbuch (<https://support.apple.com/guide/iphone/iph08022b194/#iphbcea12902>).

*Hinweis:* In einigen Gebieten kannst du auch eine Textnachricht an 911 senden, um die Notfallhilfe anzufordern. Wo dies nicht angeboten wird, erhältst du eventuell eine Nachricht, die dich darauf hinweist, dass deine Textnachricht nicht zugestellt werden konnte. Weitere Informationen findest du im Apple Support-Artikel „[Eine SMS an 911 auf dem iPhone oder der Apple Watch senden](#)“ (<https://support.apple.com/101996>).

Mit „Notruf SOS“ kannst du schnell und unkompliziert Hilfe anfordern und deine Notfallkontakte informieren. Deshalb ist es besonders wichtig, dass du den Personen, die du zu deinen Notfallkontakten gemacht hast, vertraust.




## Einstellungen für „Notruf SOS“ auf dem iPhone ändern

1. Wähle „Einstellungen“  > „Notruf SOS“.
2. Führe beliebige der folgenden Schritte aus:
  - *„Durch Halten anrufen“ aktivieren oder deaktivieren:* Drücke und halte die Seiten- und Lautstärketasten, um einen Countdown zu starten und den Rettungsdienst anzurufen.
  - *„Durch 5-mal Drücken anrufen“ aktivieren oder deaktivieren:* Drücke die Seitentaste schnell 5-mal, um einen Countdown zu starten und den Rettungsdienst anzurufen.
  - *Notrufkontakte verwalten:* Tippe in der App „Health“ auf „Notfallkontakte konfigurieren“ oder „Notfallkontakte bearbeiten“. Weitere Informationen findest du unter [„Einrichten und Anzeigen deines Notfallpasses“](#) im iPhone-Benutzerhandbuch (<https://support.apple.com/guide/iphone/iph08022b192>).


## Notfallkontakte auf dem iPhone einrichten oder ändern

Notfallkontakte lassen sich so einrichten, dass sie im Falle eines Notrufs von deinem iPhone über den Notruf informiert werden. Außerdem teilt dein iPhone deinen Standort mit diesen Kontakten und informiert sie, wenn sich dieser ändert. Wenn du eine Person als Notfallkontakt hinzugefügt hast und wieder entfernen möchtest, kannst du sie einfach löschen.

Hinzufügen oder Löschen von Notfallkontakten:

1. Öffne die App „Health“  und tippe auf dein Profilbild.
2. Tippe auf „Notfallpass“.
3. Tippe auf „Bearbeiten“ und scrolle zu „Notfallkontakte“.
4. Füge einen Kontakt hinzu oder lösche ihn.
  - *Kontakt hinzufügen:* Tippe auf die Taste „Hinzufügen“ , um einen Notfallkontakt hinzuzufügen. (Der Rettungsdienst kann nicht als Notfallkontakt festgelegt werden.)
  - *Kontakt löschen:* Tippe auf die Taste „Löschen“  neben dem Kontakt, den du löschen möchtest, und tippe auf „Löschen“.
5. Tippe auf „Fertig“, um die Änderungen zu sichern.

## Notruf tätigen, wenn das iPhone gesperrt ist


1. Tippe auf dem Bildschirm für die Codeeingabe auf „Notfall“.
2. Wähle die Notrufnummer – z. B. 911 in den USA – und tippe auf die Anruftaste .

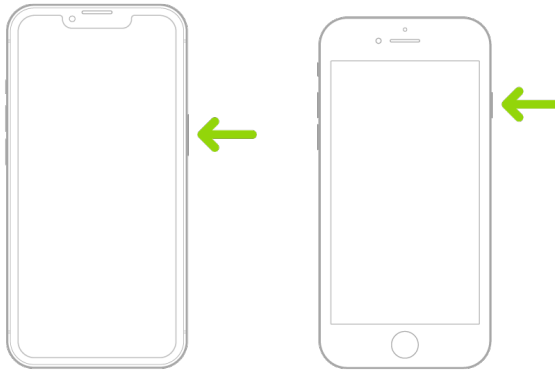
## „Notruf SOS“ auf dem iPhone verwenden (alle Länder und Regionen außer Indien)

Verwende in einem Notfall dein iPhone, um schnell und einfach nach Hilfe zu rufen und deine Notfallkontakte zu informieren (falls der Mobilfunkdienst verfügbar ist). Nach Beendigung eines Notrufs sendet dein iPhone eine Textnachricht an deine Notfallkontakte, es sei denn, du brichst den Vorgang ab. Dein iPhone sendet deinen aktuellen Standort (sofern verfügbar) und – für einen gewissen Zeitraum, nachdem du im SOS-Modus bist – deine Notrufkontakte werden informiert, wenn sich dein Standort ändert.

*Hinweis:* Wenn du ein iPhone 14 oder neuer hast (beliebiges Modell), kannst du den Rettungsdienst möglicherweise über Satellit kontaktieren, wenn kein Mobilfunkdienst verfügbar ist. Weitere Informationen findest du unter [„Notruf SOS“ via Satellit auf deinem iPhone verwenden](#) weiter unten in diesem Dokument.

- Halte gleichzeitig die Seitentaste und eine der Lautstärketasten gedrückt, bis die Schieberegler eingeblendet werden und der Countdown für „Notfall SOS“ endet. Lasse dann die Tasten wieder los.

Alternativ kannst du festlegen, dass das iPhone „Notruf SOS“ startet, wenn du die Seitentaste schnell 5-mal drückst. Wähle dazu „Einstellungen“  > „Notruf SOS“ und aktiviere „Durch 5-mal Drücken anrufen“.



## „Notruf SOS“ auf dem iPhone verwenden (Indien)

- Drücke die Seitentaste schnell 3-mal, bis die Schieberegler eingeblendet werden und der Countdown für „Notfall SOS“ endet.
- Wenn du den Bedienungshilfen-Kurzbefehl aktiviert hast, halte gleichzeitig die Seitentaste und eine der Lautstärketasten gedrückt, bis die Schieberegler eingeblendet werden und der Countdown für „Notfall SOS“ endet. Lasse dann die Tasten wieder los.

Das iPhone gibt standardmäßig einen Warnton aus, startet einen Countdown und ruft dann den Rettungsdienst.

Nach Beendigung eines Notrufs sendet dein iPhone eine Textnachricht an deine Notfallkontakte, es sei denn, du brichst den Vorgang ab. Dein iPhone sendet deinen aktuellen Standort (sofern verfügbar) und – für einen gewissen Zeitraum, nachdem du im SOS-Modus bist – deine Notrufkontakte werden informiert, wenn sich dein Standort ändert.





## Rettungsdienst mit der Apple Watch kontaktieren

- Führe einen der folgenden Schritte aus:
  - Halte die Seitentaste gedrückt, bis die Schieberegler eingeblendet werden, und bewege den Regler „Notruf“ nach rechts.

Deine Apple Watch ruft den Rettungsdienst in deiner Region an, z. B. die Nummer 112. (In einigen Regionen musst du möglicherweise eine Zahl im Ziffernblock drücken, um den Anruf durchzuführen.)
  - Halte die Seitentaste gedrückt, bis deine Apple Watch einen Warnton ausgibt und einen Countdown startet. Sobald der Countdown endet, ruft die Apple Watch den Rettungsdienst an. Die Apple Watch erzeugt das Warnsignal auch im Stummmodus. Deshalb kannst du in Notsituationen, in denen du keine Geräusche machen solltest, den Regler „Notruf“ verwenden, um den Rettungsdienst ohne Countdown anzurufen.




Soll deine Apple Watch nicht automatisch den Notrufcountdown starten, wenn du die Seitentaste gedrückt hältst, kannst du die Option „Automatisches Wählen“ deaktivieren. Öffne die App „Einstellungen“ auf deiner Apple Watch, tippe auf „SOS“, dann auf „Seitentaste gedrückt halten“ und deaktiviere die Option „Seitentaste gedrückt halten“. (Du kannst auch die Apple Watch-App auf dem iPhone öffnen, auf „Meine Watch“ tippen, auf „Notruf SOS“ tippen und anschließend die Option „Zum Wählen Seitentaste gedrückt halten“ deaktivieren.) Du kannst trotzdem mit dem Regler „Notruf“ einen Notruf tätigen.
  - Sage „Siri, rufe 112“.

## Textnachricht mit dem iPhone an den Rettungsdienst senden (nicht in allen Ländern oder Regionen verfügbar)

1. Öffne die App „Nachrichten“  und gib 112 oder die Nummer deines lokalen Rettungsdienstes in das Feld „An“ ein.
2. Gib in das Feld für die Textnachricht Informationen zu dem Notfall ein.
3. Tippe auf die Taste „Senden“ .

**Wichtig:** Nachdem du eine Textnachricht an die Notrufnummer gesendet hast, befindet sich das iPhone 30 Minuten lang im Notfallmodus. Starte dein iPhone neu, um den Notfallmodus zu beenden.

## Textnachricht mit der Apple Watch an den Rettungsdienst senden (nicht in allen Ländern oder Regionen verfügbar)

1. Öffne die App „Nachrichten“  und tippe auf „Neue Nachricht“.
2. Tippe auf „Kontakt hinzufügen“.
3. Tippe auf die Taste für den Ziffernblock , gib 112 ein und tippe auf „OK“.
4. Tippe auf „Nachricht erstellen“ und dann auf „SMS“.
5. Schreibe eine Nachricht mit deinem Finger, tippe auf die Taste „Mikrofon“ , um eine Nachricht zu diktieren, oder tippe eine Nachricht über die Tastatur.
6. Tippe auf „Fertig“ und danach auf „Senden“.

**Wichtig:** Nachdem du eine Textnachricht an die Notrufnummer gesendet hast, befindet sich die Apple Watch 30 Minuten lang im Notfallmodus. Starte deine Apple Watch neu, um den Notfallmodus zu beenden.

## „Notruf SOS“ via Satellit auf deinem iPhone verwenden

Auf dem iPhone 14 oder neuer (beliebiges Modell) mit iOS 16.1 oder neuer kannst du „Notruf SOS“ via Satellit verwenden, um eine Textnachricht an den Rettungsdienst zu senden, wenn du dich außerhalb der Reichweite von Mobilfunk- und WLAN-Netzen befindest. Weitere Informationen findest du im Apple Support-Artikel [„Notruf SOS via Satellit‘ auf dem iPhone 14 verwenden“](https://support.apple.com/HT213426) (https://support.apple.com/HT213426).

Du kannst auch die App „Wo ist?“ verwenden, um deinen Standort via Satellit mit anderen Personen zu teilen. Weitere Informationen findest du unter [„Teilen des Standorts via Satellit in der App ‚Wo ist?‘ auf dem iPhone“](https://support.apple.com/guide/iphone/iph2aac8ae20) im iPhone-Benutzerhandbuch (https://support.apple.com/guide/iphone/iph2aac8ae20).

## Wichtige Informationen über Notrufe auf dem iPhone

- Einige Mobilfunknetze akzeptieren möglicherweise keinen Notruf vom iPhone, wenn das iPhone nicht aktiviert ist, wenn das iPhone mit einem bestimmten Mobilfunknetz nicht kompatibel oder für dieses nicht konfiguriert ist oder (sofern zutreffend), wenn das iPhone keine SIM-Karte hat oder die SIM-Karte mit einer PIN gesperrt ist.
- In bestimmten Ländern oder Regionen können die Anbieter von Rettungsdiensten auf deine Ortsinformationen (sofern feststellbar) zugreifen, wenn du einen Notruf tätigtst.
- Ziehe die Notrufinformationen deines Anbieters zurate, um mehr über die Beschränkungen von Notrufen via WLAN zu erfahren.
- Wenn bei CDMA ein Notruf endet, wird das iPhone für einige Minuten in den *Notrufmodus* versetzt, um einen Rückruf von den Rettungsdiensten zu ermöglichen. Während dieses Zeitintervalls sind Datenübertragungen und Textnachrichten blockiert.
- Nachdem ein Notruf abgesetzt wurde, werden bestimmte Anruffunktionen, die eingehende Anrufe blockieren oder stummschalten, möglicherweise für kurze Zeit deaktiviert, um einen Rückruf der Rettungsdienste zu ermöglichen. Hierzu gehören „Nicht stören“, „Unbekannte Anrufer stummschalten“ und „Bildschirmzeit“.
- Wenn du auf einem iPhone mit Dual SIM (iPhone SE 2. Generation oder neuer und iPhone X-Modelle oder neuer) WLAN-Anrufe für eine Leitung nicht aktivierst, werden eingehende Anrufe auf dieser Leitung (einschließlich Anrufe von Rettungsdiensten) direkt an die Voicemail weitergeleitet (sofern bei deinem Anbieter verfügbar), wenn die andere Leitung belegt ist; du erhältst keine Mitteilungen über verpasste Anrufe.

Wenn du die bedingte Rufweiterleitung konfiguriert hast (sofern bei deinem Anbieter verfügbar), sodass Anrufe von einer Leitung zu einer anderen geleitet werden, wenn eine Leitung besetzt oder außer Dienst ist, werden die Anrufe nicht in die Voicemail geleitet. Informationen zur Konfiguration erhältst du bei deinem Anbieter.

## Erhalten eines Nachweises für den Account einer anderen Person

Apple hat sich verpflichtet, die Sicherheit und Privatsphäre der Benutzer:innen zu schützen. Wende dich an die lokalen Vollzugsbehörden, wenn du Opfer von technologiebasiertem Missbrauch, Stalking oder Belästigung geworden bist und einen Nachweis für den Account einer anderen Person beantragen willst. Apple ist sich des zunehmenden Bedarfs an digitalen Nachweisen von Vollzugsbehörden bewusst und hat ein Team von Fachkräften in der Rechtsabteilung damit betraut, alle rechtlichen Anfragen von Behörden weltweit zu verwalten und zu bearbeiten.

Alle anderen Anfragen nach Informationen bezüglich Apple-Kund:innen, einschließlich Kundenfragen zur Offenlegung von Informationen sind an <https://www.apple.com/privacy/contact/> zu richten.

## Apple-Richtlinien für Anfragen von Behörden

Richtlinien für Anfragen von Behörden innerhalb und außerhalb der USA:

- *Innerhalb der USA:* [Legal Process Guidelines](https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf)  
(<https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>)
- *Außerhalb der USA:* [Legal Process Guidelines](https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf)  
(<https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf>)

# Copyright

© 2024 Apple Inc. Alle Rechte vorbehalten.

Die Verwendung des über die Tastatur erzeugten Apple-Logos (Wahl-Umschalt-+) für kommerzielle Zwecke ohne vorherige schriftliche Einwilligung von Apple kann als Markenmissbrauch und unlauterer Wettbewerb gerichtlich verfolgt werden.

Apple, das Apple-Logo, AirDrop, AirPods, AirTag, Apple Books, Apple Music, Apple Pay, Apple TV, Apple Watch, Digital Crown, Face ID, FaceTime, FileVault, Finder, Find My, HomeKit, HomePod, iMac, iMessage, iPad, iPadOS, iPad Pro, iPhone, iTunes, Launchpad, Lightning, Mac, MacBook Air, MacBook Pro, macOS, Magic Keyboard, OS X, Safari, Siri, Time Machine und Touch ID sind Marken der Apple Inc., die in den USA und weiteren Ländern und Regionen eingetragen sind.

App Store, iCloud und iTunes Store sind Dienstleistungsmarken der Apple Inc., die in den USA und weiteren Ländern und Regionen eingetragen sind.

Apple  
One Apple Park Way  
Cupertino, CA 95014  
[apple.com](https://apple.com)

IOS ist eine Marke oder eingetragene Marke von Cisco in den USA und weiteren Ländern und wird in Lizenz verwendet.

Die Bluetooth®-Wortmarke und -Logos sind Marken und Eigentum der Bluetooth SIG, Inc., und die Verwendung solcher Marken durch Apple Inc. erfolgt in Lizenz.

Andere hier genannte Produkt- und Herstellernamen sind möglicherweise Marken ihrer jeweiligen Rechtsinhaber.

Es wurden alle Anstrengungen unternommen, um die Richtigkeit der Informationen in diesem Handbuch sicherzustellen. Apple übernimmt keine Verantwortung für Druck- oder Schreibfehler.

Einige Apps sind nicht in allen Regionen verfügbar. Änderungen bei der Verfügbarkeit von Apps sind vorbehalten.

D028-00788