



# **Persönliche Sicherheit – Benutzerhandbuch**



**Strategien und Lösungen**

# Inhaltsverzeichnis

<b>Übersicht</b>	<b>3</b>
Übersicht über die persönliche Sicherheit	3
Neue Funktionen für die persönliche Sicherheit	6
<b>Strategien und Lösungen</b>	<b>7</b>
Handbuch für die derzeitige Sicherheit	7
Handbuch für die geplante Sicherheit	14
Sicherheitsprüfung	17
Checklisten für Geräte mit iOS 15 oder älter	34
<b>Zugriff von Geräten und Accounts begrenzen</b>	<b>40</b>
Apple Account-Zugriff	40
Gerätezugriff	49
Passwörter, Passkeys und Codes	65
<b>Standortinformationen verwalten</b>	<b>75</b>
Wegbegleitung für „Nachrichten“ verwenden	75
AirTags und andere Objekte verwalten	79
„Wo ist?“ und die Standortfreigabe	88
Einstellungen für Ortungsdienste verwalten	93
Automatische Freigabe der erwarteten Ankunftszeit in „Karten“ verwalten	96
Standortmetadaten in der App „Fotos“ verwalten	98
<b>Inhalte verwalten</b>	<b>101</b>
Allgemein	101
Bestimmte Apps und Funktionen	122
<b>Zusätzliche Informationen</b>	<b>167</b>
Sicherheitshinweise	167
Weitere Support-Ressourcen	168
<b>Urheberrechte und Marken</b>	<b>169</b>

# Übersicht

## Übersicht über die persönliche Sicherheit



Wenn du den Zugriff anderer Personen auf deine Apple-Geräte, deinen Account oder deine persönlichen Daten überprüfen, einschränken, stoppen oder verhindern möchtest, kann dir dieses Dokument helfen.



*Hinweis:* Diese Ressource gilt überwiegend für Apple-Geräte mit den neuesten Betriebssystemen (iOS 18, iPadOS 18 und macOS 15), sie kann jedoch auch auf die Apple Watch und den HomePod angewendet werden.

### Du weißt nicht genau, was du brauchst?

- Das [Handbuch für die derzeitige Sicherheit](#) kann dir mit sofortigen Lösungen helfen.
- Das [Handbuch für die geplante Sicherheit](#) kann dir beim Vorausplanen helfen.

## Du suchst nach einer bestimmten Lösung?

- Überprüfe und verwalte, was du teilst (und mit wem du es teilst) mit der Sicherheitsprüfung oder Checklisten (siehe unten).
- Greife auf alle Inhalte dieses Handbuchs mit dem Suchfeld oder dem Inhaltsverzeichnis (oben links auf jeder Seite) zu oder verwende unsere nach Themen sortierten Indexe, um noch mehr Hilfe zu erhalten.

## Sicherheitsprüfung

Die Sicherheitsprüfung bietet einen einfachen Weg, um schnell die Informationen, die du mit Apps und Personen teilst zu überprüfen und zu verwalten. Und das geschieht alles direkt auf deinem iPhone mit iOS 16 oder neuer. Um deine iOS-Version herauszufinden, wähle „Einstellungen“ > „Allgemein“ > „Info“. Weitere Informationen zum Aktualisieren findest du unter [Apple-Software aktualisieren](#) weiter unten.

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

Weitere Informationen zur Sicherheitsprüfung (Anforderungen, Anleitungen, FAQs) findest du weiter unten in diesem Dokument unter [Sicherheitsprüfung](#).

## Checklisten

Viele Personen halten die Verwendung der Sicherheitsprüfung für einfacher, aber Apple bietet außerdem weiter unten in diesem Dokument Checklisten an, mit denen du das, was du teilst, manuell überprüfen und verwalten kannst:

- [Checkliste 1: Zugriff von Geräten und Accounts begrenzen](#)
- [Checkliste 2: Standortinformationen verwalten](#)
- [Checkliste 3: Inhalte verwalten](#)

## Offline-Hilfe

Wenn du später offline auf diese Informationen zugreifen möchtest, kannst du:

- Das vollständige Dokument als PDF über den Link *Dieses Dokument laden* laden (unten links auf jeder Seite) laden.
- Einzelne Seiten mit der Tastenkombination „Command-P“ oder durch Klicken bei gedrückter Control-Taste > „Seite drucken“ drucken. Damit du weiterhin in deinem Download auf Links klicken kannst, wähle „Als PDF sichern“ unten links im PDF-Menü in deinem Druckerfenster aus.

## Andere Anliegen

- [Apple Support](https://support.apple.com/) (https://support.apple.com/): Zugriffslösungen für all deine Apple-Produkte und -Dienste, einschließlich Benutzerhandbücher, Hilfe bei vergessenen Passwörtern und mehr.
- [Weitere Support-Ressourcen](#) (weiter unten in diesem Dokument) – Wenn du befürchtest, dass deine Sicherheit nicht gewährleistet ist, können diese zusätzlichen Ressourcen für dich hilfreich sein.

Dieses Handbuch wird regelmäßig aktualisiert, um dir alle Informationen bereitzustellen, die du brauchst, um dich bei der Verwendung von Apple-Produkten sicher zu fühlen. Weitere Informationen findest du weiter unten unter [Neue Funktionen](#).

# Neue Funktionen für die persönliche Sicherheit

## Namensänderung der Apple ID

Apple ID heißt nun Apple Account. Hierbei handelt es sich um ein globales Update bei allen Apple-Diensten.

## Updates für das Persönliche Sicherheit – Benutzerhandbuch

Apple hat umfassende Änderungen an diesem Handbuch vorgenommen, einschließlich:

### Neuer Inhalt

- [Teilen eines AirTag beenden](#) und [Teilen des Standorts eines verloren gegangenen AirTag beenden](#) helfen dir dabei zu steuern, wer Zugriff auf den Standort deines AirTag erhält.
- [Anruf auf dem iPhone aufnehmen und transkribieren](#) erklärt, wie du die Anrufaufnahme während eines Telefonats verwendest oder sie stoppst.
- [iPhone-Synchronisierung verwalten](#) hilft dir dabei zu sehen, welche Mac-Computer für die iPhone-Synchronisierung eingerichtet sind, den Zugriff zu widerrufen und Einstellungen anzupassen.
- [Apps sperren oder ausblenden](#) bietet dir Beruhigung, wenn du nicht möchtest, dass andere Personen Zugriff auf bestimmte Apps erhalten.
- [„Bildschirmfreigabe“ und „Bildschirmsteuerung“ verwalten](#) hilft dir dabei zu verstehen, was eine Person für Rechte erhält, wenn sie deinen Bildschirm sieht oder steuert.

### Verbesserungen

- [Apple Account schützen](#) enthält eine neue Aufgabe dazu, wie du dich auf allen Browsern von iCloud.com abmeldest und den Web-Zugriff deaktivierst.
- [Notruf oder Notrufnachricht auf dem iPhone oder der Apple Watch absetzen](#) enthält eine neue Aufgabe dazu, wie Videos und Bilder mit Rettungsdiensten geteilt werden können.
- [Sicherheitsprüfung](#) enthält einen neuen Abschnitt zur iPhone-Synchronisierung.
- [Checkliste 1: Geräte- und Account-Zugriff begrenzen](#) enthält neue Schritte zur iPhone-Synchronisierung und dem Ändern deines Codes und Passworts.

# Strategien und Lösungen

## Handbuch für die derzeitige Sicherheit

Wenn du (oder eine Person, die du kennst) befürchtest, dass du Opfer von technologiebezogenem Stalking oder Belästigung auf einem Apple-zugehörigen Produkt geworden bist oder du alle digitalen Verbindungen mit einer Person abbrechen willst, können dir die folgenden Strategien helfen. Weitere Informationen zur Verbindung mit Organisationen, die Unterstützung bei Belästigung, häuslicher Gewalt, Stalking oder anderen Problemen bieten, findest du auf der Webseite [Here to Help](https://learn.appleservices.apple/here-to-help) (<https://learn.appleservices.apple/here-to-help>).

Wenn du nach proaktiven Wegen suchst, dich gegen zukünftige technologiebasierte Probleme zu schützen, findest du weitere Informationen im [Handbuch für die geplante Sicherheit](#) weiter unten in diesem Dokument.

## Strategien für mehr Sicherheit

In den folgenden Schritten wird dir beim Verwalten deiner Freigaben und beim Schützen deiner Geräte und Accounts geholfen.

### Schritt 1. Sicher ist sicher

🚩 **WICHTIG:** Bevor du Änderungen vornimmst oder Informationen löschst, solltest du dir über die [potenziellen Auswirkungen auf deine Sicherheit](#) bewusst sein.

Du kannst dieses Dokument im X für später laden oder ausdrucken, indem du bei gedrückter Control-Taste klickst und entweder „Seite sichern unter“ oder „Seite drucken“ auswählst.

### Schritt 2. Apple-Software aktualisieren

Um dich beim Schützen deines Geräts zu unterstützen, stelle sicher, dass all deine Geräte das neueste Betriebssystem mit den neuesten Sicherheits- und Datenschutzupdates installiert haben. Weitere Informationen findest du unter [Apple-Software aktualisieren](#).

*Hinweis:* Das Vollenden von Geräteupdates kann Zeit und Batteriekapazität in Anspruch nehmen. Wenn du dich in einer dringlichen Situation oder in einer Notsituation befindest, solltest du mit dem nächsten Schritt fortfahren.

### Schritt 3. Geführte Lösungen verwenden

Die meisten technologiebasierten persönlichen Sicherheitsprobleme lassen sich auf Freigaben und Zugriff zurückführen. Verwende für geführte Hilfe bei diesen Problemen entweder:

- *Sicherheitsprüfung*: Der schnellste und einfachste Weg, deine Freigaben direkt auf deinem iPhone anzuzeigen und zu verwalten. Weitere Informationen dazu findest du unter [Sicherheitsprüfung](#) weiter unten in diesem Dokument.

Verwende dein iPhone mit iOS 16 oder neuer für den Zugriff: Wähle „Einstellungen“ > „Datenschutz & Sicherheit“ > „Sicherheitsprüfung“. (Möglicherweise musst du nach unten scrollen.)

- *Checklisten*: Weitere Informationen für iOS 15 (oder älter) oder für andere Apple-Geräte findest du weiter unten in diesem Dokument:
  - [Zugriffsbeschränkungen](#)
  - [Freigabe beenden](#)
  - [Standort verwalten](#)

### Schritt 4. Weitere Maßnahmen

Manche Dinge können nicht mit den geführten Lösungen überprüft oder geändert werden. Überprüfe diese wichtigen [zusätzlichen Schritte](#).

Dieses Dokument enthält zahlreiche Artikel zur persönlichen Sicherheit bei Geräten, Funktionen und Einstellungen. Wenn du lieber gezielte Hilfe für eine bestimmte Funktion oder ein Problem hättest, verwende:

- Das Suchfeld (oben links)
- Das Inhaltsverzeichnis dieses Dokuments (oben links)
- Hilfe bei bestimmten Situationen (unten)

## Dringliche Maßnahmen

⚠ **WICHTIG:** Bevor du Änderungen vornimmst oder Informationen löschst, solltest du dir über die [potenziellen Auswirkungen auf deine Sicherheit](#) und deinen Datenschutz bewusst sein.

### Schnelle Hilfe

- Schnell alle Freigaben mit dem [Notfall-Reset](#) stoppen (Option Eins)
- [Notruf tätigen oder Notfalltextnachricht auf dem iPhone oder der Apple Watch senden](#)
- [Anrufe und Nachrichten von bestimmten Personen blockieren](#)
- [Unbekannte Anmeldeversuche ablehnen](#)
- [Warnungen vor sensiblen Bildern und Videos erhalten](#)
- [Home-Zubehör sicher kontrollieren](#)
- [Touch ID-Fingerabdrücke verwalten](#)

### Nachweise sammeln

- [Verdächtige Aktivitäten aufzeichnen](#)
- [Nachweise zu einem anderen Apple Account erhalten](#)

### Gerät auf die Werkseinstellungen zurücksetzen

Wenn du alle Informationen und Einstellungen – einschließlich alle Apps, die ohne dein Wissen installiert wurden – löschen und deine Datenschutzeinstellungen zurücksetzen möchtest, sodass du deinen Standort nicht mehr mit Personen oder Apps teilst, findest du weitere Informationen unter [Gerät auf die Werkseinstellungen zurücksetzen](#).

### Blockierungsmodus

Wenn du befürchtest, dass du ein Opfer von hochentwickelten Cyberangriffen, wie z. B. von privaten Unternehmen, die staatlich geförderte Spionageprogramme entwickeln, geworden bist, findest du weitere Informationen unter [Gerät mit dem Blockierungsmodus stärken](#).

## Hilfe bei bestimmten Situationen

Es wird empfohlen, erst die Schritte 1-4 durchzugehen, aber du kannst auch die Bereiche unten verwenden, um schnell Artikel zu finden, die dir bei deiner Situation behilflich sein könnten.

### **Jemand weiß immer, wo ich gerade bin**

Dies kann an deinem Apple Account, einer Familienfreigabegruppe oder Standort- oder Inhaltsfreigaben liegen (wie z. B. geteilte Kalender oder Fotos, die auf sozialen Medien oder geteilten Kalender hochgeladen wurden).

Starte mit den oben genannten Schritten 1-4. Wenn du die Checklisten in Schritt 3 verwendest, beginne mit [Zugriff beschränken](#) und [Standort verwalten](#).

### **Ich kann mich nicht bei meinem Apple Account anmelden**

Um wieder auf deinen Apple Account zugreifen zu können, beachte die folgenden Apple Support-Artikel:

- [Wenn du vermutest, dass eine unbefugte Person Zugriff auf deinen Apple Account hat](#)
- [Dein Apple Account wurde gesperrt, ist nicht aktiv oder deaktiviert](#)
- [Wenn du dein Apple Account-Passwort vergessen hast](#)
- [So verwendest du die Accountwiederherstellung, wenn du dein Apple Account-Passwort nicht zurücksetzen kannst](#)

Nachdem du wieder Zugriff hast, erwäge die folgenden Optionen:

- [Primäre E-Mail-Adresse deines Apple Accounts ändern – Apple Support-Artikel](#)
- [Passwörter für dein Gerät, Apps und Websites schützen](#)
- [Apple Account- und Geräteaussperrungen vorbeugen](#)
- [Proaktive Wege, um dich vor zukünftigen Problemen zu schützen:Handbuch für die geplante SicherheitHandbuch für die geplante Sicherheit](#)

### **Jemand hat mich aus meinem Gerät ausgesperrt oder ich kann mein Gerät nicht entsperren**

Weitere Informationen, um wieder Zugriff zu erhalten, findest du im Apple Support-Artikel [Wenn du deinen iPhone-Code vergessen hast oder dein iPhone deaktiviert ist](#).

Nachdem du wieder Zugriff erlangt hast, erwäge die folgenden Ressourcen, um dein Gerät zukünftig zu schützen:

- [Checkliste 1:Zugriff von Geräten und Accounts begrenzenZugriff von Geräten und Accounts begrenzen](#)
- [Eindeutigen Geräte-Code oder Passwort festlegen](#)
- [Touch ID](#) verwenden, um deine Geräte zu schützen oder unbekannte Fingerabdrücke zu löschen
- [Gerät mit Face ID sichern](#) (iPhone oder iPad)
- [Wiederherstellungskontakt hinzufügen](#)
- Vorsichtsmaßnahmen mit dem [Handbuch für die geplante Sicherheit](#) ergreifen.

## **Ich will oder plane eine Beziehung zu verlassen, in der ich mich nicht sicher fühle**

Weitere Informationen zur Verbindung mit Organisationen, die Unterstützung für Opfer bei Belästigung, häuslicher Gewalt, Stalking oder anderen Problemen bieten, findest du auf der Webseite [Here to Help](https://learn.apple.services.apple/here-to-help) (https://learn.apple.services.apple/here-to-help).

1. Verwende die (oben genannten) geführten Lösungen, um deine Zugriffs- und Freigabeeinstellungen zu überprüfen und Änderungen vorzunehmen, wenn es für dich sicher ist, dies zu tun.
2. Überprüfe diese [dringlichen Maßnahmen](#), um mehr über Blockieren, Nachweissammlung und mehr zu erfahren.
3. Überprüfe diese [zusätzlichen Sicherheitsmaßnahmen](#), die unerwünschte Tracking-Mitteilungen, Accounts, die nicht von Apple stammen, Mobilfunkverträge und mehr beinhalten.

## **Ich brauche Schutz bei etwas anderem**

### **Zugriff auf deine Geräte**

Checkliste 1 überprüfen: [Begrenzen des Zugriffs von Geräten und Accounts](#).

Erwäge auch:

- [Eindeutigen Code oder Passwort festlegen](#)
- [Verhindern, dass du ausgesperrt wirst](#)
- [Blockierungsmodus verwenden](#)

Um weitere Artikel zum Schutz deiner Geräte und Accounts anzuzeigen, finde weitere Informationen im Inhaltsverzeichnis (oben links) unter „Begrenzen des Zugriffs von Geräten und Accounts – Artikel“.

### **Dein Standort**

Checkliste 2 überprüfen: [Standortinformationen verwalten](#).

Erwäge auch:

- [Browserverlauf in Safari und „Karten“ schützen](#)

### **Dein Inhalt**

Checkliste 3 überprüfen: [Inhalte verwalten](#)

Erwäge auch:

- [Sicher verwalten, wie Inhalte weitergeleitet werden \(E-Mail, SMS und Anrufe\)](#)
- [Warnungen vor sensiblen Bildern und Videos](#)
- [Fotofreigabeeinstellungen verwalten](#)
- [Standortmetadaten in der App „Fotos“ verwalten](#)

## Deine Apps und Browser

- [Passwortsicherheit](#)
- [Geteilte Passwörter und Passkeys](#)
- [Datenschutzfunktionen von Apps](#)
- [Apps überprüfen und löschen](#)
- [Einstellungen für Apps von Drittanbietern](#)
- [Datenschutz für den Surfverlauf in Safari](#)
- Nachrichten
  - [Sicherheitseinstellungen](#)
  - [Blockieren von Anrufen und Nachrichten von bestimmten Personen](#)
  - [Verwenden der Wegbegleitung](#)
- Fotos
  - [Fotofreigabeeinstellungen verwalten](#)
  - [Standortmetadaten verwalten](#)

## Deine Familie und dein Zuhause

- [Familienfreigabe](#)
- [Home-Zubehör](#)

## Welche Geräte hast du?

### iPhone, iPad und Mac

Fast alle Inhalte des Handbuchs zu persönliche Sicherheit können auf das iPhone, iPad und den Mac angewendet werden.

- Um andere Personen zu überprüfen, zu beschränken oder sie daran zu hindern, auf deine Geräte, deinen Account oder persönliche Informationen zuzugreifen, findest du weitere Informationen unter [Strategien für mehr Sicherheit](#) weiter oben in diesem Dokument.
- Weitere Informationen zum Vorausplanen, wenn du andere Personen davon abhalten möchtest, Zugriff zu erlangen, findest du im [Handbuch für die geplante Sicherheit](#).
- Weitere Informationen zu zusätzlichen Wegen, um das breite Inhaltsangebot in diesem Dokument zu verwenden, findest du in der [Übersicht](#).

Weitere Informationen zu anderen Themen zu diesen Geräten findest du im [iPhone – Benutzerhandbuch](#), [iPad – Benutzerhandbuch](#) oder im [Mac – Benutzerhandbuch](#).

## Apple Watch

Weitere Informationen zu persönlichen Sicherheitsinformationen, die für die Apple Watch relevant sind, findest du unter:

- [Teilen von Aktivitäten auf der Apple Watch verwalten](#)
- [„Wo ist?“ zur Verwaltung der Standortfreigabe verwenden](#)
- [Notfall-Nachricht verfassen](#)
- [Sicheres NameDrop \(proaktiv\)](#)
- [Wegbegleitung für „Nachrichten“ verwenden \(proaktiv\)](#)

Weitere Informationen zu anderen Themen findest du im [Apple Watch – Benutzerhandbuch](#).

## Home-Zubehörgeräte

Weitere Informationen zur App „Home“ findest du unter [Home-Zubehör sicher kontrollieren](#).

Weitere Informationen zu anderen Themen findest du im [Home – Benutzerhandbuch](#).

## AirTag

Weitere Informationen zu AirTags findest du unter [Unerwünschte Tracking-Objekte erkennen](#).

Für weitere Informationen, suche im [Apple Support](#) nach „AirTag“.

# Handbuch für die geplante Sicherheit

Diese Seite ist für Personen, die bei der Suche nach Schutz gegen potenziellen, technologiebasierten Missbrauch, Stalking und Belästigung Unterstützung benötigen. Wenn du gerade Erfahrungen mit einem ähnlichen Thema machst, findest du Informationen im [Handbuch für die derzeitige Sicherheit](#) weiter oben in diesem Dokument. Andere Arten von Hilfe für ein Apple-Produkt oder einen Apple-Dienst findest du unter [Weitere Support-Ressourcen](#) weiter unten in diesem Dokument.

## Strategien für mehr Sicherheit

Apple stellt zahlreiche Funktionen zur Verfügung, mit denen du deine persönliche Sicherheit und deinen Datenschutz stärken kannst. Dies sind einige Möglichkeiten zu Verwendung:

### Level 1: Minimaler Schutz

Als erste Abwehrlinie sollten alle Personen die folgenden Schritte vornehmen, um ihre Geräte und ihren Apple Account zu schützen.

- Aktualisiere die Apple-Software auf all deinen Apple-Geräten, um sicherzustellen, dass du die neuesten Sicherheits- und Datenschutzupdates hast. Weitere Informationen findest du unter „Apple-Software aktualisieren“. Weitere Informationen findest du unter [Apple-Software aktualisieren](#).
- Zugriff auf deine Geräte schützen:
  - [Eindeutigen Code oder Passwort festlegen](#)
  - [iPhone oder iPad mit Face ID schützen](#)
  - [Touch ID-Fingerabdrücke verwalten](#)
  - [Geteilte Passwörter und Passkeys verwalten](#)

Apple Account sichern:

- [Apple Account schützen](#)
- [Zwei-Faktor-Authentifizierung verwenden](#)
- [Wiederherstellungskontakt festlegen](#)

## Level 2: Besserer Schutz

Zusätzlich zu Level 1 kannst du deine Apps, den Schutz entsprechender Passwörter und die Verwaltung von mit ihnen geteilten Daten in Erwägung ziehen.

- [Passwörter für dein Gerät, Apps und Websites schützen](#).
- Spezifische Freigabeeinstellungen überprüfen:
  - Option „[Teilen & Zugriff' verwalten](#)“ (Option Zwei) der Sicherheitsprüfung auf iPhones mit iOS 16 (oder neuer) verwenden
  - [Checkliste 3: Inhalte verwalten](#) (auf anderen Geräten oder iOS 15 oder älter)
  - [Sicheres AirDrop](#).
  - [Sicheres NameDrop](#).
  - [Geteilte Tabgruppen in Safari verwalten](#)
  - [Einstellungen für „Mit dir geteilt“ verwalten](#)
- App-Datenschutz verwalten:
  - [Datenschutzfunktionen von Apps](#).
  - [Apps überprüfen und löschen](#)
  - [Einstellungen für Apps von Drittanbietern](#).
  - [„Safari“ und „Karten“: Browserverlauf in Safari und „Karten“ schützen](#)

### Level 3: Bester Schutz

Zusätzlich zu Level 1 und 2 kannst du mehr zu den persönlichen Sicherheitswerkzeugen von Apple erfahren und Sicherheit zur Gewohnheit machen, damit du den bestmöglichen Schutz erhältst.

- Sei vorbereitet
  - [Mitteilungen zu unerwünschtem Tracking aktivieren](#)
  - [Betrügerische Anfragen zum Teilen von Informationen erkennen](#)
  - [Unbekannte Anmeldeversuche ablehnen](#)
  - [Erfahren, wie du bestimmte Personen blockieren kannst](#)
  - [„Nachrichten“, AirDrop, „FaceTime“:Warnungen vor sensiblen Bildern und VideosWarnungen vor sensiblen Inhalten einrichten](#)
  - [In Erwägung ziehen, die Wegbegleitung für „Nachrichten“ zu verwenden, um anderen Personen automatisch mitzuteilen, dass du Zuhause angekommen bist](#)
  - [So kannst du einen Notruf oder eine Notrufnachricht absetzen](#) (iPhone oder Apple Watch; abhängig von Land oder Region)
- Sicherheit zur Gewohnheit machen
  - Nimm [zusätzliche Schritte](#) vor, um deine Accounts, die nicht von Apple stammen, Drittanbieter-Apps, Passwörter und soziale Medien sowie „Home“, Apple Wallet und die Familienfreigabe zu schützen.
  - Verwende die [Sicherheitsprüfung](#) auf iPhones mit iOS 16 (oder neuer) in regelmäßigen Abständen, um deine Freigaben zu verwalten.

#### Weitere Optionen

- [Touch ID-Fingerabdrücke verwalten](#)
- [Gerät mit dem Blockierungsmodus stärken](#)
- [Sicherheitseinstellungen in der App „Nachrichten“ verwalten](#)
- [Nachweise zu einem anderen Apple Account erhalten](#)

# Sicherheitsprüfung

## Sicherheitsprüfung auf einem iPhone mit iOS 16 oder neuer

Die Sicherheitsprüfung ist eine Funktion, die über die App „Einstellungen“ auf einem Gerät mit iOS 16 (oder neuer) aufgerufen werden kann. Mit ihr kannst du die Informationen, die du mit einzelnen Personen oder Apps teilst, schnell überprüfen, aktualisieren oder das Teilen beenden. Die Sicherheitsprüfung verfügt über zwei Optionen:

- Verwalte Optionen für die Freigabe und den Zugriff, um sie zu überprüfen und einzelne Änderungen vorzunehmen.
- Verwende den Notfall-Reset, um die Freigabe all deiner Informationen sofort zu beenden.

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

 **WICHTIG:** Bevor du Änderungen vornimmst oder Informationen löschst, solltest du dir über die [potenziellen Auswirkungen auf deine Sicherheit](#) und deinen Datenschutz bewusst sein.

### Anforderungen

- Ein iPhone mit iOS 16 oder neuer.
  - Um deine iOS-Version herauszufinden, wähle „Einstellungen“  > „Allgemein“ > „Info“.
  - Um ab iOS 15.8.3 oder älter zu aktualisieren: „Einstellungen“  > „Allgemein“ > „Softwareupdate“. Weitere Informationen zu zusätzlichen Optionen findest du unter [Apple-Software aktualisieren](#).
- Einen Apple Account, der die Zwei-Faktor-Authentifizierung verwendet.
- Du musst außerdem unter „Einstellungen“ > „[dein Name]“ auf deinem iPhone angemeldet sein.

*Hinweis:* Möglicherweise fallen dir Unterschiede bei der Sicherheitsprüfung auf, wenn auf deinem iPhone der Schutz für gestohlene Geräte aktiviert ist. Weitere Informationen über den Schutz für gestohlene Geräte findest du im Apple Support-Artikel [Schutz für gestohlene Geräte für das iPhone](#).

### Alternative: Checklisten

Wenn du ein anderes Gerät (iPad, Mac) verwendest oder du Probleme bei der Sicherheitsprüfung hast, kannst du die Freigabe und den Zugriff manuell mit den folgenden Checklisten anpassen:

- [Checkliste 1: Zugriff von Geräten und Accounts begrenzen](#)
- [Checkliste 2: Standortinformationen verwalten](#)
- [Checkliste 3: Inhalte verwalten](#)

## Übersicht

Mit der Sicherheitsprüfung auf dem iPhone kannst du das Teilen deiner Informationen schnell stoppen oder prüfen und aktualisieren, was mit einzelnen Personen und Apps geteilt wird. Du kannst:

- Prüfen, mit wem Informationen geteilt werden
- Geräte, die mit deinem Apple Account verbunden sind, prüfen und ändern
- Systemdatenschutzberechtigungen für Apps zurückzusetzen
- Deinen iPhone-Code ändern
- Dein Apple Account-Passwort ändern
- Weitere Änderungen vornehmen



## Sicherheitsüberlegungen bevor du beginnst

⚠ **WICHTIG:** Sorge für deine Sicherheit.

- Bevor du Änderungen vornimmst oder Informationen löschst, solltest du dir über die [potenziellen Auswirkungen auf deine Sicherheit](#) und deinen Datenschutz bewusst sein.
- Mit „Schnell verlassen“ kannst du deinen Datenschutz schnell schützen. Tippe auf „Schnell verlassen“, um die App „Einstellungen“ sofort zu schließen und zum Home-Bildschirm zurückzukehren (oben rechts auf allen Bildschirmen in der Sicherheitsprüfung). Änderungen, die du vor dem Verwenden von „Schnell verlassen“ vorgenommen hast, werden gesichert.
- 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. Einige Apps oder Dienste benachrichtigen dich darüber, dass du erneut Inhalte teilst.

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 Account-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/120340) (<https://support.apple.com/120340>).

*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?**

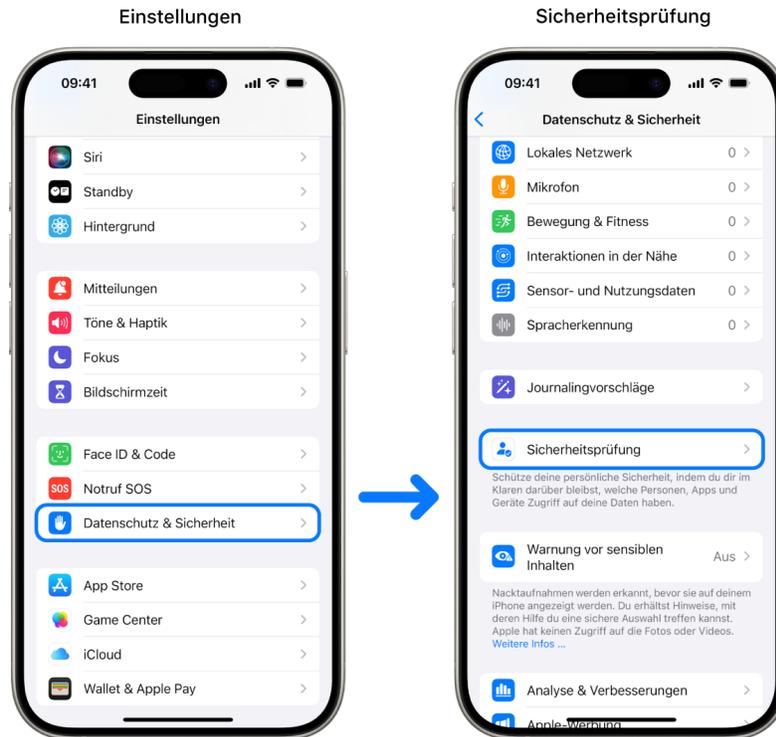
Die Sicherheitsprüfung ist nur auf iPhones mit iOS 16 oder neuer verfügbar. Für die Nutzung der Sicherheitsprüfung benötigst du einen Apple Account, der die Zwei-Faktor-Authentifizierung verwendet. Du musst außerdem unter „Einstellungen“ > „[dein Name]“ auf deinem iPhone angemeldet sein. (Um festzustellen,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

Um auf die Sicherheitsprüfung zuzugreifen, wähle „Einstellungen“  > „Datenschutz & Sicherheit“ > „Sicherheitsprüfung“. (Möglicherweise musst du nach unten scrollen.)

*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 [Checkliste 3: Inhalte verwalten](#) weiter unten.

## Schritt 1: Sicherheitsprüfung öffnen

Wähle auf deinem iPhone „Einstellungen“ > „Datenschutz & Sicherheit“ > „Sicherheitsprüfung“. (Möglicherweise musst du nach unten scrollen.)

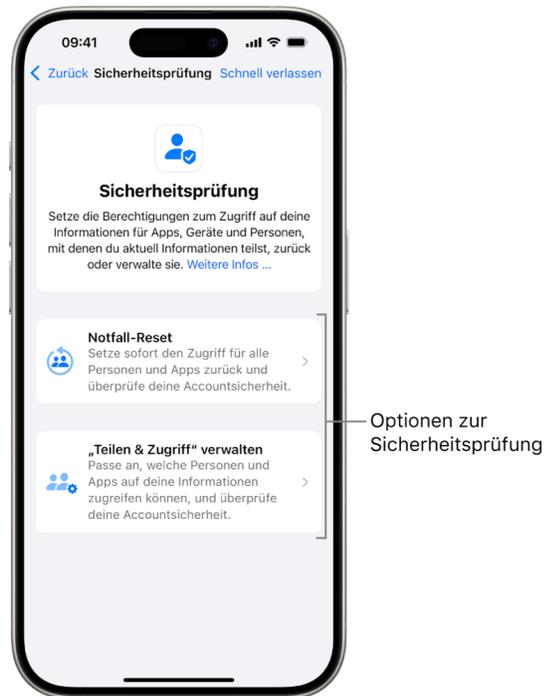


## Schritt 2: Eine Option wählen

Die Sicherheitsprüfung bietet zwei Möglichkeiten an, wie du die Freigabe, den Zugriff und die Accountsicherheit verwalten kannst:

- **Notfall-Reset:** Sofortiger und universaler Reset für sämtliche Freigaben mit allen Personen und Apps.
- **„Teilen & Zugriff“ verwalten:** Überprüfe die Freigabe und den Zugriff für einzelne Personen und Apps und passe sie an.

Weitere Informationen zu bestimmten Details darüber, was mit der Sicherheitsprüfung geändert werden kann, findest du im [FAQ zur Sicherheitsprüfung](#) weiter unten in diesem Dokument.



## Notfall-Reset (Option Eins)

Verwende den Notfall-Reset, um:

- Die Freigabe mit allen Personen und Apps schnell zu stoppen (genauer findest du im [FAQ zur Sicherheitsprüfung](#)).
- Deine Notfallkontakte zu aktualisieren.
- Geräte, die mit deinem Apple Account verbunden sind, zu überprüfen.
- Telefonnummern, die zum Bestätigen deiner Identität verwendet werden, zu überprüfen.
- Dein Apple Account-Passwort zu ändern und die Geräte- und Accountsicherheit zu überprüfen.



- Tippe auf „Notfall-Reset“ und befolge die Anleitung auf dem Bildschirm. Der Fortschritt wird gesichert, während du fortfährst.

*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/120340) (<https://support.apple.com/120340>).

## „Teilen & Zugriff“ verwalten (Option Zwei)

Die Option „Teilen & Zugriff“ verwalten“ hilft dir dabei, Informationen, die du mit Personen teilst und auf die Apps Zugriff haben zu überprüfen und zu verwalten. Außerdem kannst du deine Geräte und Apple Account-Sicherheit aktualisieren. Folge diesen 5 Schritten:

1. Tippe auf „Teilen & Zugriff“ verwalten“. (Deine Änderungen werden während des Vorgangs gesichert.)
2. Um die Freigabe von Informationen mit anderen Personen zu beenden, kannst du entweder:
  - *Auf „Personen“ tippen:* 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.
  - *Oder auf „Informationen“ tippen:* 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. Wenn bestimmte Apple-Apps gelöscht wurden, wie z. B. „Fitness“ oder „Notizen“, musst du sie möglicherweise erneut laden, um zu sehen, welche Informationen du geteilt hast.
3. Um die Freigabe von Informationen mit anderen Apps zu beenden, kannst du entweder:
  - *Auf „Apps“ tippen:* 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.
  - *Oder auf „Informationen“ tippen:* 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.



4. Tippe auf „Fortfahren“ und führe einen der folgenden Schritte aus:
  - Überprüfe und entferne Geräte, die mit deinem Apple Account verknüpft sind.
  - Überprüfe und aktualisiere Telefonnummern, die zum Bestätigen deiner Identität verwendet werden.
  - Aktualisiere dein Apple Account-Passwort.
  - Füge Notfallkontakte hinzu oder aktualisiere sie.
  - Aktualisiere deinen Gerätecode oder deine Face ID- oder Touch ID-Informationen.
  - Wenn deine Computer synchronisiert sind, kannst du sie prüfen und entfernen (nur iOS 17 oder neuer).
  - Wenn auf deinen Computern die iPhone-Synchronisierung eingerichtet ist, kannst du sie prüfen und entfernen (nur iOS 18 oder neuer).
  - Wenn du über iCloud+ verfügst und Privat-Relay noch nicht eingeschaltet hast, kannst du dies jetzt nachholen (nur iOS 17 oder neuer).
5. Tippe auf „Fertig“.



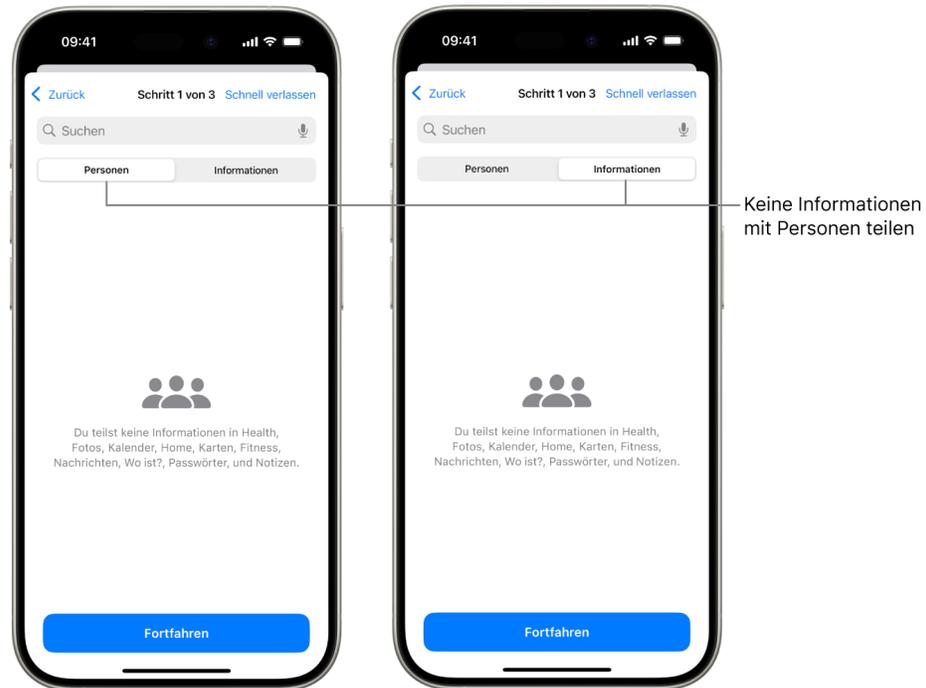
6. Wenn du fertig bist, fahre mit der nächsten Schritt fort, um zu überprüfen, ob du die Freigabe gestoppt hast.

▼ **WICHTIG:** Überprüfe [zusätzliche Schritte](#) weiter unten in diesem Dokument, um über Tipps zu Schutzmaßnahmen für deine privaten Informationen, die über die Sicherheitsprüfung hinausgehen, zu erfahren.

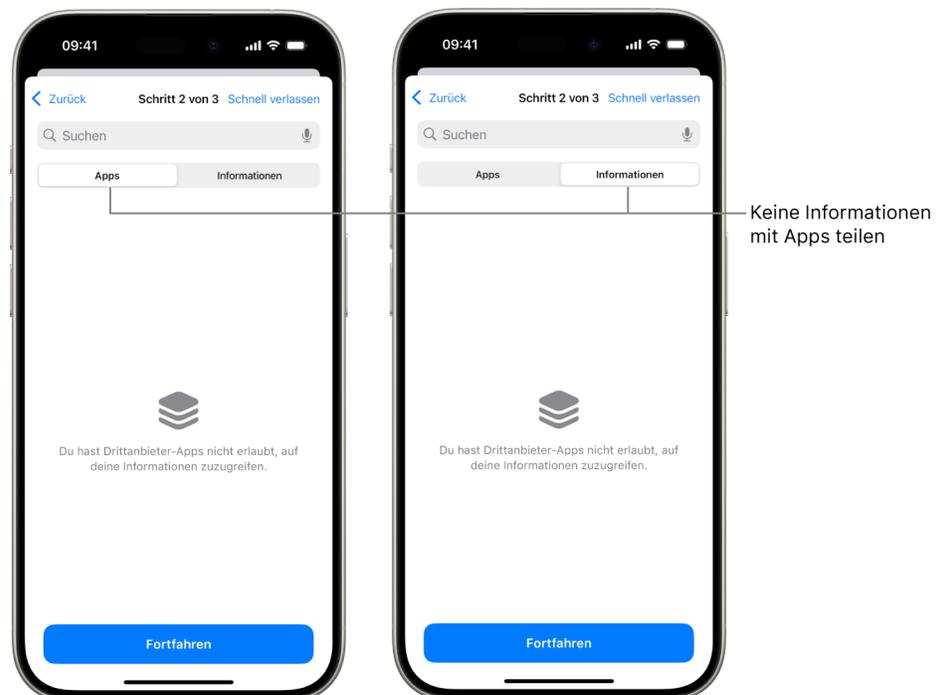
### Schritt 3: Änderungen bestätigen

Nachdem du die Sicherheitsprüfung verwendet hast, kannst du die an deinen Freigabeoptionen vorgenommenen Änderungen mit diesen 4 Schritten bestätigen.

1. Tippe auf die Taste „Zurück“ (oder schließe die Sicherheitsprüfung und starte sie erneut).
2. Bestätige, dass die beabsichtigten Änderungen in Bezug auf die Informationen, die du mit anderen Personen teilst, vorgenommen wurden.

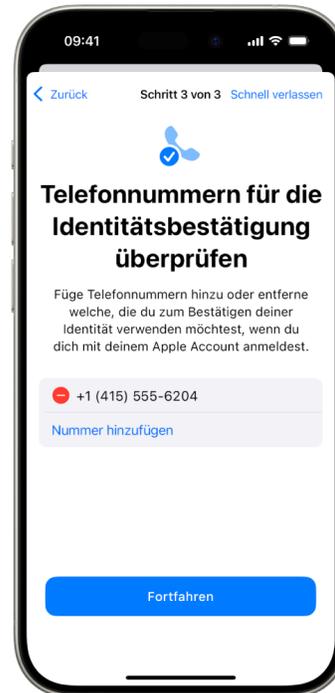


3. Bestätige, dass die beabsichtigten Änderungen in Bezug auf die Informationen, die du mit anderen Apps teilst, vorgenommen wurden.



4. Bestätige sämtliche Änderungen, die du an deinem Account vorgenommen hast:

- Geräte, die mit deinem Apple Account verknüpft sind.
- Telefonnummern, die zum Bestätigen deiner Identität verwendet werden.



- Notfallkontakte, die du hinzugefügt oder geändert hast.



- Synchronisierte Computer, die du entfernt hast.



## Über die Sicherheitsprüfung hinaus

Die Sicherheitsprüfung kann in manchen Fällen keine Änderungen an geteilten Informationen vornehmen, unter anderem:

- Accounts und Passwörter, die nicht von Apple stammen.
- Freigabe in sozialen Medien.
- Geräte, auf denen du mit einem anderen Apple Account angemeldet bist.
- Ein iPad oder Mac, auf dem die Einstellungen für das Teilen von Informationen für andere Apps aktiviert ist.

## FAQ zur Sicherheitsprüfung

### Welche Apple-Apps und -Funktionen kann ich mit der Sicherheitsprüfung überprüfen und verwalten?

Du kannst die Sicherheitsprüfung verwenden, um die Informationen, die du mit anderen Personen aus den folgenden Apple-Apps teilst, überprüfen oder die Freigabe beenden:

App	Informationen, die verwaltet werden soll
	Aktivität
	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?“
	Wegbegleitung

## Welche Zugriffe von Drittanbieter-Apps kann ich mit der Sicherheitsprüfung überprüfen und verwalten?

Du kannst die Sicherheitsprüfung verwenden, um den Zugriff von Drittanbieter-Apps auf die folgenden Arten von Informationen zu deaktivieren.

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

## Welche Änderungen kann ich mit der Sicherheitsprüfung an meinem Apple Account vornehmen?

Die Sicherheitsprüfung kann verwendet werden, um Informationen im Zusammenhang mit deinem Apple Account zu ändern. Zum Beispiel:

- Prüfe und entferne Geräten, die bei deinem Account angemeldet sind.
- Prüfe und aktualisiere vertrauenswürdige Telefonnummern.
- Ändere dein Apple Account-Passwort.
- Aktualisiere deine Notfallkontakte.
- Aktualisiere deinen Gerätecode und deine Face ID- oder Touch ID-Informationen.

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/120340) (<https://support.apple.com/120340>).

## Warum gibt es die Taste „Schnell verlassen“?

Personen in Missbrauchssituationen müssen möglicherweise schnell ihre Verwendung der Sicherheitsprüfung verbergen. Mit der Taste „Schnell verlassen“ ist das möglich.

## Weitere Sicherheitsschritte

Die meisten persönlichen Sicherheitsprobleme lassen sich auf Freigaben und Zugriff zurückführen. Verwende für eine geführte Hilfe beim Verwalten dieser Problemen entweder:

- *Sicherheitsprüfung*: Öffne auf deinem iPhone mit iOS 16 (oder neuer) „Einstellungen“  > „Datenschutz & Sicherheit“ > „Sicherheitsprüfung“ oder gehe zu „[Sicherheitsprüfung](#)“.
- *Checklisten*: Beachte die folgenden Checklisten für frühere iOS-Versionen oder andere Geräte: [Zugriffsbeschränkungen](#), [Teilen stoppen](#) oder [Standort verwalten](#).

Manche Dinge können nicht mit der Sicherheitsprüfung oder Checklisten überprüft oder geändert werden. Um die Freigabe noch weiter zu beschränken, ziehe die folgenden zusätzlichen Schritte in Erwägung.

 **WICHTIG:** Bevor du Änderungen vornimmst oder Informationen löschst, solltest du dir über die [potenziellen Auswirkungen auf deine Sicherheit](#) und deinen Datenschutz bewusst sein.

## Schritte, die nicht von Apple ausgehen

### Apps, die nicht von Apple stammen

Auf deinem Gerät installierte Apps können Informationen zu deinem ungefähren Standort erfassen. Unter Berücksichtigung der [potenziellen Auswirkungen auf deine Sicherheit und deinen Datenschutz](#), möchtest du möglicherweise installierte Apps überprüfen und diejenigen löschen, die du nicht verwendest oder nicht kennst. Weitere Informationen findest du unter [Apps überprüfen und löschen](#) und [Einstellungen für Apps von Drittanbietern](#).

### Accounts und Passwörter, die nicht von Apple stammen

Schütze sensible persönliche Informationen in Apps für Online-Banking, Einkäufe, E-Mail, soziale Medien, Bildung:

- Ändere deine Account-Passwörter.
- Überprüfe deine Einstellungen zu Sicherheit und Datenschutz.
- Überprüfe Kommunikations-Accounts (E-Mail, Telefon, Nachrichten), um sicherzustellen, dass nichts ohne deine Erlaubnis weitergeleitet wird.

### Soziale Medien, Einkäufe und andere Accounts

Gepostete Fotos und andere persönliche Informationen auf sozialen Medien, Apps für Einkäufe oder anderen Websites können Details über deinen Standort und deine Privatsphäre preisgeben. Stelle Folgendes sicher:

- Überprüfe die Einstellungen für Datenschutz und Sicherheit in deinen Accounts für soziale Medien und Einkäufe sowie anderen web-basierten Accounts.
- Überprüfe deine Listen mit Verknüpfungen und Follower:innen.
- Denke genau darüber nach, was du postest, um dein benötigtes Sicherheitslevel zu erhalten.
- Standortmetadaten in der App „Fotos“ verwalten

Weitere Informationen findest du unter [Standortmetadaten in der App „Fotos“ verwalten](#) weiter unten in diesem Dokument.

### Andere Geräte, die du verwendest oder besitzt

Prüfe die Freigabe- und Zugriffseinstellungen für alle anderen Geräte, die du zum Schutz deiner Informationen verwendest. Weitere Informationen dazu findest du in der Checkliste [Zugriff von Geräten und Accounts begrenzen](#). 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.

## 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. Unter Berücksichtigung der [potenziellen Auswirkungen auf deine Sicherheit und deinen Datenschutz](#) möchtest du möglicherweise die Passwörter, PIN-Codes oder andere Sicherheitsfunktionen, die mit deinem Mobilfunkplan verknüpft sind, aktualisieren.

## Mit Apple verbundene Schritte

### Unerwünschtes Tracking

Du könntest Mitteilungen über unerwünschtes Tracking aktivieren (wie für AirTags oder anderes „Wo ist?“-Netzwerkzubehör). Um die Hinweise zu aktivieren, wenn sich eines dieser Geräte mit dir bewegt, aktiviere:

- Bluetooth
- Ortungsdienste
- Tracking-Mitteilungen (öffne die App „Wo ist?“, tippe auf „Ich“, scrolle zu „Tracking-Mitteilungen anpassen“ und aktiviere dann „Mitteilungen erlauben“)

Weitere Informationen findest du unter [Unerwünschte Tracking-Objekte erkennen](#) weiter unten in diesem Dokument.

### 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 [Home-Zubehör sicher kontrollieren](#) weiter unten in diesem Dokument.

### Apple Wallet

Wenn du Geldkarten oder Zugriffsschlüssel mit einer anderen Person über Apple Wallet teilst, kann diese Person unter Umständen deinen Transaktions- oder Türschlossverlauf sehen.

Einzelheiten von finanziellen Transaktionen können auch über geteilte Bankkonten oder Kreditkarten gesehen werden. Wenn eine andere Person online auf deine Finanz-Accounts hat, kann sie diese ebenfalls einsehen. Öffne Apple Wallet, um deine letzten Transaktionen und Protokolle anzuzeigen. Unter Berücksichtigung der [potenziellen Auswirkungen auf deine Sicherheit und deinen Datenschutz](#) möchtest du möglicherweise die Passwörter, die mit deinen Bank- und Kreditkarten verknüpft sind, 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“. Obwohl du den Account eines Kindes nicht aus einer Familienfreigabegruppe entfernen kannst, kannst du den Account in eine andere Familienfreigabegruppe bewegen oder einfach deren Apple Account löschen.

Weitere Informationen findest du unter [Familienfreigabegruppe verlassen oder Mitglied daraus entfernen](#) weiter unten.

*Hinweis:* Überprüfe, ob du Teil einer Familienfreigabegruppe bist. Wähle dazu „Einstellungen“  > [dein Name] und dann den Bereich „Familienfreigabe“. Wenn du den Namen der Familienmitglieder sehen kannst, bist du in einer Familienfreigabegruppe.

# Checklisten für Geräte mit iOS 15 oder älter

## Checkliste 1: Zugriff von Geräten und Accounts begrenzen

Das Schützen des Zugriffs auf deine Geräte und deinen Apple Account ist unerlässlich für deine technologiebezogene persönliche Sicherheit. Diese Checkliste bietet entsprechende Pfade, die du überprüfen und aktualisieren kannst, um die Freigabe deiner Geräte auf die Personen zu beschränken, denen du Zugriff gewähren möchtest.

▼ **WICHTIG:** Wenn du ein iPhone mit iOS 16 (oder neuer) hast, kannst du die Funktion „[Sicherheitsprüfung](#)“ verwenden.

▼ **WICHTIG:** Wenn du ein iPhone mit iOS 16 (oder neuer) hast, kannst du die Funktion „[Sicherheitsprüfung](#)“ verwenden, die weiter oben in diesem Dokument vorgestellt wird.



## Zugriff auf deine Geräte begrenzen

1. Ändere den Code auf deinem iPhone oder iPad und ändere das Anmeldepasswort auf deinem Mac. Weitere Informationen dazu findest du unter [Eindeutigen Geräte-Code oder Passwort festlegen](#) weiter unten in diesem Dokument.
2. Wenn du die Geräte überprüfen möchtest, die bei deinem Apple Account angemeldet sind, wähle „Einstellungen“  > [*dein Name*] > „Geräte“. Wenn du ein Gerät entfernen möchtest, das du nicht kennst, tippe auf den Gerätenamen und wähle „Aus dem Account entfernen“. Weitere Informationen findest du unter [Apple Account schützen](#) weiter unten.
3. Überprüfe deine Geräte auf unerwartete [Face ID](#)-Erscheinungsbilder oder [Touch ID-Fingerabdruck](#)-Daten. Du findest weitere Informationen zu Face ID und Touch ID weiter unten in diesem Dokument.
4. Überprüfe die persönlichen und Sicherheitsinformationen deines Apple Accounts, indem du dich auf der [Apple Account-Website](#) anmeldest. Weitere Informationen findest du unter [Apple Account schützen](#) weiter unten.
5. Wenn du die [Zwei-Faktor-Authentifizierung](#) verwendest, überprüfe die vertrauenswürdigen Geräten auf Geräten, die du nicht kennst. Weitere Informationen findest du weiter unten unter „Zwei-Faktor-Authentifizierung“.
6. Überprüfe die Apps, die auf deinem Gerät installiert sind, auf Apps, die du nicht kennst oder die du deiner Erinnerung nach nicht installiert hast. Weitere Informationen dazu findest du unter [Apps überprüfen und löschen](#) weiter unten in diesem Dokument.
7. Überprüfe, ob die iPhone-Synchronisierung eingerichtet ist, und entziehe ihr, falls nötig, den Zugriff. Weitere Informationen dazu findest du unter [iPhone-Synchronisierung auf deinem iPhone oder Mac verwalten](#) weiter unten in diesem Dokument.
8. Suche nach einem potenziell unbekanntem MDM-Konfigurationsprofil (Mobile Geräteverwaltung). MDM-Profile werden üblicherweise von Arbeitgebern, Schulen oder anderen offiziellen Organisationen installiert. Weitere Informationen dazu findest du unter [Konfigurationsprofile überprüfen und löschen](#) weiter unten in diesem Dokument.
9. Überprüfe und verwalte, was du teilst mit der [Checkliste 3: Inhalte verwalten](#) weiter unten in diesem Dokument.

## Checkliste 2: Standortinformationen verwalten

Wenn du ein iPhone mit iOS 15 (oder älter) verwendest, verwende diese Checkliste, um zu begrenzen, wer deinen Standort sehen kann oder die Standortfreigabe ganz zu beenden. Wenn du ein iPhone mit iOS 16 (oder neuer) hast, findest du weitere Informationen unter [Sicherheitsprüfung](#).



1. Wenn du nicht die neueste Version von iOS, iPadOS oder macOS hast und befürchtest, dass jemand physischen Zugriff auf dein Gerät hatte, kannst du das Gerät auf die Werkseinstellungen zurücksetzen. 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 beim Zurücksetzen auf Werkseinstellungen die neueste Version des jeweiligen Betriebssystems installiert. Weitere Informationen zum Zurücksetzen auf die Werkseinstellungen findest du unter [Gerät auf die Werkseinstellungen zurücksetzen](#).
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 Standortfreigabe. Daraufhin können alle Apps auf deinem Gerät, sogar 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 . 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 deinen Apple Account haben, wähle „Wo ist?“, tippe auf „Geräte“ und überprüfe die Liste. Wenn sich darin ein unbekanntes Gerät befindet, das du entfernen 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.

## Checkliste 3: Inhalte verwalten

Wenn du ein iPhone mit iOS 15 (oder älter) verwendest, verwende diese Checkliste, um zu erfahren, wie du die Freigabe für Personen beendest, mit denen du bereits Inhalte geteilt hast. Wenn du ein iPhone mit iOS 16 (oder neuer) hast, findest du weitere Informationen unter [Sicherheitsprüfung auf einem iPhone mit iOS 16 oder neuer](#) weiter oben in diesem Dokument.



1. Überprüfe, ob du Teil einer Familienfreigabegruppe bist. Wähle dazu „Einstellungen“  > [dein Name] und suche nach dem Tab „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 , 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 auf „Kalender löschen“ am unteren Bildschirmrand tippen.
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 [Fotofreigabeeinstellungen verwalten](#).

# Zugriff von Geräten und Accounts begrenzen

## Apple Account-Zugriff

### Apple Account schützen

Dein Apple Account 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 deinen Apple Account haben, können sie Informationen sehen, die geräteübergreifend synchronisiert werden, wie z. B. „Nachrichten“ und dein Standort. Erfahre hier, wie du deinen Apple Account auf dem iPhone, iPad und Mac schützen kannst.



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

### Apple Account sichern

1. Teile deinen Apple Account nicht mit anderen Personen – auch nicht mit Familienmitgliedern, Partner:innen und engen Freund:innen. Wenn du deinen Apple Account teilst, gibst du einer anderen Person Zugriff auf alle deine persönlichen Daten und Inhalte. Wenn eine andere Person deinen Apple Account 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 deinen Apple Account. 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 BestätigungsCodes per SMS oder einen automatisierten Anruf erhalten kannst.

3. Achte auf Mitteilungen zu deinem Apple Account. Apple benachrichtigt dich per E-Mail, SMS 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 besonders wichtig, dass deine Kontaktinformationen auf dem neuesten Stand sind.

Weitere Informationen findest du unter [Unbekannte Anmeldeversuche ablehnen](#) 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.

## Apple Account-Sicherheitsinformationen überprüfen und aktualisieren

So stellst du sicher, dass die persönlichen Informationen, die mit deinem Apple Account verknüpft sind, auch von dir stammen:

1. Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad:* Wähle „Einstellungen“  > [dein Name].
  - *Auf dem Mac:* Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke oben in der Seitenleiste auf deinen Namen.
  - *In einem Webbrowser auf deinem Mac oder Windows-PC:* Gehe zur [Apple Account-Website](https://account.apple.com) (<https://account.apple.com>).
2. Aktualisiere im Bereich „Anmeldung & Sicherheit“ 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 siehst, 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 [Zwei-Faktor-Authentifizierung verwenden](#) weiter unten in diesem Dokument.

## Deinen Account sichern und unbekannte Geräte entfernen

Wenn Geräte mit deinem Apple Account 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 Bestätigungs\_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 die nachfolgenden 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] > „Anmeldung & Sicherheit“ > „Passwort ändern“. Wähle ein sicheres Passwort (mindestens acht Zeichen mit Groß- und Kleinbuchstaben sowie mindestens eine Zahl).
- *Auf dem Mac:* Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke oben in der Seitenleiste auf deinen Namen. Klicke auf „Anmeldung & Sicherheit“ und dann auf „Passwort ändern“.

2. Wenn du für mehr Sicherheit die E-Mail-Adresse ändern möchtest, die mit deinem Apple Account verknüpft ist, öffne Safari  und melde dich auf der [Apple Account-Website](https://appleid.apple.com) (<https://appleid.apple.com>) an. Wähle „Account“ und wähle unter deinem aktuellen Apple- Account „Apple Account 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 dem Mac:* Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke oben in der Seitenleiste auf deinen Namen. Scrolle in der Geräteliste nach unten, tippe auf das Gerät, das du entfernen möchtest, und tippe auf „Aus dem Account entfernen“.

## Sicherer Web-Zugriff auf deine iCloud-Daten

iCloud hilft dir dabei, deine wichtigsten Informationen, wie Fotos, Dateien und Backups, sicher aufzubewahren, auf dem neuesten Stand zu halten und auf all deinen Geräten zur Verfügung zu stellen. iCloud.com bietet Zugriff auf deine iCloud-Daten über einen beliebigen Webbrowser.

Wenn du sicherstellen möchtest, dass niemand anderes bei deinem Apple Account oder auf iCloud angemeldet ist, kannst du dich sofort von allen Browsern abmelden. Führe die folgenden Schritte aus:

- Gehe zu [icloud.com/settings](https://icloud.com/settings), klicke auf „Von allen Browsern abmelden“ und klicke dann auf „Abmelden“.

Für zusätzliche Sicherheitsstufen und zum Erhalten von mehr Kontrolle über deine persönlichen Daten kannst du auch auswählen, ob der Web-Zugriff auf deine iCloud-Daten deaktiviert werden soll, damit deine Daten nur auf deinen vertrauenswürdigen Geräten verfügbar sind. Führe einen der folgenden Schritte aus:

- *Auf iPhone oder iPad:* Öffne die App „Einstellungen“, tippe auf deinen Namen, tippe auf „iCloud“ und deaktiviere dann „Über das Internet auf iCloud-Daten zugreifen“.
- *Auf dem Mac:* Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf deinen Namen, klicke auf „iCloud“ und deaktiviere dann „Über das Internet auf iCloud-Daten zugreifen“.

Weitere Informationen findest du im Apple Support-Artikel [Web-Zugriff auf deine iCloud-Daten verwalten](#).

## Zwei-Faktor-Authentifizierung verwenden

Die Zwei-Faktor-Authentifizierung stellt eine zusätzliche Sicherheitsstufe für deinen Apple Account 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] > „Anmeldung & Sicherheit“.
2. Tippe auf „Zwei-Faktor-Authentifizierung aktivieren“ und dann auf „Fortfahren“.
3. Gib eine vertrauenswürdige Telefonnummer ein. Über diese Nummer erhältst du die Bestätigungscode 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?“.

Du wirst auf deinem iPhone erst wieder nach einem Verifizierungscode gefragt, wenn du einen der folgenden Schritte ausführst:

- Vollständiges Abmelden
- iPhone löschen
- Über die Apple Account-Webseite bei deinem Apple Account anmelden
- Erzwungenes Ändern deines Apple Account-Passworts aus Sicherheitsgründen

Nachdem du die Zwei-Faktor-Authentifizierung aktiviert hast, kannst du sie zwei Wochen lang wieder deaktivieren. Nach diesem Zeitraum kannst du die Zwei-Faktor-Authentifizierung 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.

## Zwei-Faktor-Authentifizierung auf dem Mac einrichten

1. Wähle Menü „Apple“  > „Systemeinstellungen“, klicke oben in der Seitenleiste auf deinen Namen und klicke dann auf „Anmeldung & 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 deinem Apple Account ab, löschst deinen Mac oder musst aus Sicherheitsgründen dein Passwort ändern.

## Sicherheitsschlüssel für den Apple Account

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 bei deinem Apple Account über die Zwei-Faktor-Authentifizierung anmeldest. Der Sicherheitsschlüssel für den Apple Account 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, stärken Sicherheitsschlüssel den Zwei-Faktor-Authentifizierungsprozess und verhindern, 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 den Apple Account](https://support.apple.com/102637) (<https://support.apple.com/102637>).

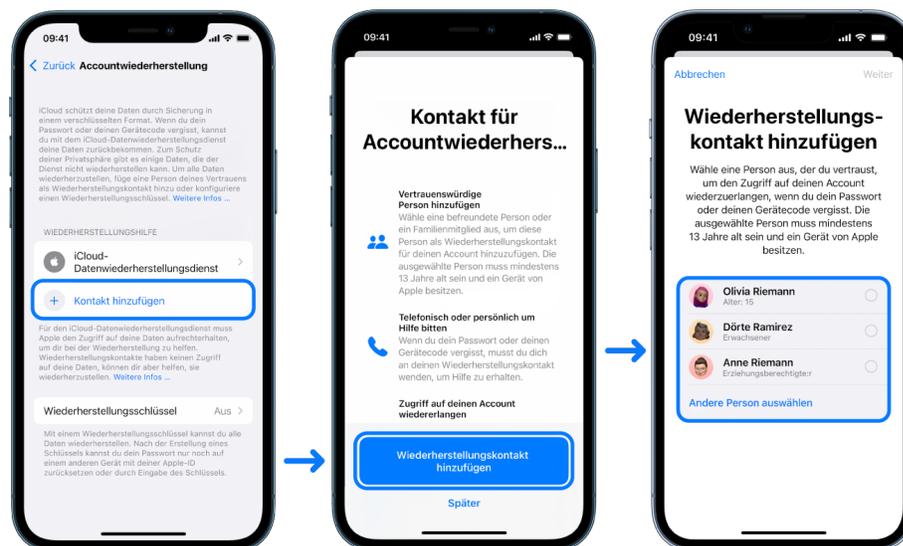
## Apple Account- und Geräteaussperrungen vorbeugen

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 wieder Zugriff auf deine Daten erhältst, 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 [Einem Nachlasskontakt für deinen Apple Account 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 ihren Apple Account aktiviert und einen Code auf ihrem Gerät eingerichtet haben.



## Wiederherstellungskontakt einrichten

Wenn du befürchtest, dass jemand auf deinen Account zugreifen 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 wieder Zugriff erhältst.

1. Führe einen der folgenden Schritte aus:
  - *Auf iPhone oder iPad:* Wähle „Einstellungen“  > [dein Name] und tippe auf „Anmeldung & Sicherheit“.
  - *Auf dem Mac:* Wähle Menü „Apple“  > „Systemeinstellungen“, klicke oben in der Seitenleiste auf deinen Namen und klicke dann auf „Anmeldung & 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 deine Anfrage bestätigt hat, wirst du in einer Nachricht darüber informiert, dass die Person 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 „Anmeldung & Sicherheit“.
  - *Auf dem Mac:* Wähle Menü „Apple“  > „Systemeinstellungen“, klicke oben in der Seitenleiste auf deinen Namen und klicke dann auf „Anmeldung & Sicherheit“.
2. Unter „Wiederherstellungshilfe“ wird eine Liste deiner Wiederherstellungskontakte angezeigt.
3. Wähle den Wiederherstellungskontakt aus, den du entfernen möchtest, und entferne dann den Kontakt.

# Gerätezugriff

## Touch ID-Fingerabdrücke verwalten

Du kannst Touch ID verwenden, um dein iPhone, iPad oder deinen Mac 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, iPad oder Mac einrichten.

⚠ **WICHTIG:** Bevor du Änderungen vornimmst oder Informationen löschst, solltest du dir über die [potenziellen Auswirkungen auf deine Sicherheit](#) und deinen Datenschutz bewusst sein.



## Geräte mit Touch ID schützen

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

### Touch ID auf dem iPhone oder iPad einrichten

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.

*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) (<https://support.apple.com/101612>).

## Touch ID auf dem Mac oder Magic Keyboard einrichten

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

1. Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke dann in der Seitenleiste auf „Touch ID & Passwort“ .
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.

## Unbekannte Fingerabdrücke vom iPhone oder iPad löschen

Wenn es mehrere Touch ID-Fingerabdrücke auf deinem iPhone oder iPad gibt, kannst du diese löschen, um den Zugriff auf dein Gerät zu sichern.

1. Wähle „Einstellungen“  > „Touch ID & Code“.
2. Wenn mehr als ein Fingerabdruck verfügbar ist und diese nicht benannt sind, lege einen Finger auf die Home-Taste, um seinen Abdruck zu bestimmen. Erwäge die Benennung deiner Fingerabdrücke, damit du sie später identifizieren kannst.
3. Tippe falls nötig auf den Fingerabdruck und tippe dann auf „Fingerabdruck löschen“.

*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](#).

## Unbekannte Touch ID-Fingerabdrücke vom Mac oder Magic Keyboard löschen

Wenn es mehrere Touch ID-Fingerabdrücke auf deinem Mac oder Magic Keyboard gibt, kannst du diese löschen, um den Zugriff auf dein Gerät zu sichern.

1. Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke dann in der Seitenleiste auf „Touch ID & Passwort“ .
2. Führe beliebige der folgenden Schritte aus:
  - *Einen Fingerabdruck löschen:* Klicke auf einen Fingerabdruck, gib dein Passwort ein, klicke auf „OK“ und dann auf „Löschen“.
  - *Einen Fingerabdruck hinzufügen:* Klicke auf „Fingerabdruck hinzufügen“, um einen neuen Fingerabdruck hinzuzufügen, und wähle, welche Optionen du mit Touch ID verwenden möchtest.

## iPhone oder iPad mit Face ID schützen

Face ID lässt sich von allen nutzen, die ihr iPhone oder iPad mit einer zusätzlichen Sicherheitsstufe sichern möchten. Sie 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>).



## iPhone oder iPad mit Face ID schützen

- 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 bei 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 „[Einstellungen für Face ID und Aufmerksamkeit auf dem iPhone ändern](https://support.apple.com/guide/iphone/iph646624222)“ (<https://support.apple.com/guide/iphone/iph646624222>) im iPhone – Benutzerhandbuch oder unter „[Einstellungen für Face ID und Aufmerksamkeit auf dem iPad ändern](https://support.apple.com/guide/ipad/ipad058b4a31)“ im iPad – Benutzerhandbuch (<https://support.apple.com/guide/ipad/ipad058b4a31>).

## Face ID zum Löschen anderer Erscheinungsbilder zurücksetzen

Wenn ein alternatives Face ID-Erscheinungsbild eingerichtet ist, das 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.

## Unbekannte Anmeldeversuche ablehnen

Wenn die Zwei-Faktor-Authentifizierung aktiviert ist und auf einem neuen Gerät ein Anmeldeversuch vorgenommen wird, erhältst du eine Mitteilung auf deinen anderen vertrauenswürdigen Geräten. Diese Mitteilung enthält eine Karte mit dem Standort des neuen Geräts. Diese Mitteilung kann auf jedem vertrauenswürdigen iPhone, iPad oder Mac angezeigt werden.

Der ungefähre Standort des Anmeldeversuchs basiert auf der IP-Adresse oder des Netzwerks, die/das vom Gerät aktuell genutzt wird. Es ist nicht der exakte Standort des Geräts.

Wenn du eine Mitteilung darüber erhältst, dass dein Apple Account für die Anmeldung auf einem neuen Gerät verwendet wird, die nicht von dir ausgeht, tippe auf „Nicht erlauben“, um den Anmeldeversuch zu blockieren.

 **WICHTIG:** Außerdem solltest du ein Bildschirmfoto von der Mitteilung machen, bevor du sie schließt. Weitere Informationen findest du unter [„Verdächtige Aktivitäten aufzeichnen“](#) weiter unten in diesem Dokument.

Wenn du glaubst, dass dein Apple Account kompromittiert sein könnte, beachte die Hinweise unter [Apple Account schützen](#) (weiter unten in diesem Dokument) und entferne unbekannte Geräte.

## Apple-Software aktualisieren

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 deinen Apple Account 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/100100) (<https://support.apple.com/100100>).

### iPhone und iPad automatisch aktualisieren

Wenn du die automatischen Updates nicht bereits bei der Ersteinrichtung deines Geräts aktiviert hast, kannst du das nun tun.

1. Wähle „Einstellungen“  > „Allgemein“ > „Softwareupdate“ > „Automatische Updates“.
2. Aktiviere die folgenden drei Optionen: „[iOS oder iPadOS]-Updates automatisch installieren“, „Sicherheitsmaßnahmen und Systemdateien“ und „[iOS oder iPadOS]-Updates automatisch laden“.

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.

Um automatische Updates zu deaktivieren, wähle „Einstellungen“ > „Allgemein“ > „Softwareupdate“ > „Automatische Updates“ und deaktiviere dann „[iOS oder iPadOS]-Updates automatisch installieren“ und „Sicherheitsmaßnahmen und Systemdateien“.

## iPhone oder 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 oder 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
  - Ein Windows-Gerät 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) installiert sein. Wenn du eine ältere Version von macOS hast, [verwende iTunes](#), um das Gerät zu aktualisieren. Weitere Informationen findest du unter „Software auf iOS-Geräten in iTunes auf dem Mac aktualisieren“ (<https://support.apple.com/guide/itunes/itns3235/12.9/mac/10.14>).
  - *In der App „iTunes“ auf deinem Windows-Gerät:* 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. Wähle Menü „Apple“  > „Systemeinstellungen“, klicke in der Seitenleiste auf „Allgemein“  und klicke dann 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.

- Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Allgemein“  und dann 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.

## Konfigurationsprofile überprüfen und löschen

Möglicherweise nutzen Organisationen (wie Bildungseinrichtungen und Unternehmen) Gerätekonfigurationsprofile, Werkzeuge für 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.

Ein Konfigurationsprofil kann eine Reihe von Einstellungen für einen Benutzeraccount sowie andere Gerätefunktionalitäten verwalten. Konfigurationsprofile können für das iPhone, iPad, den Mac, das Apple TV und die Apple Watch 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:** Bevor du Änderungen vornimmst oder Informationen löschst, solltest du dir über die [potenziellen Auswirkungen auf deine Sicherheit](#) und deinen Datenschutz bewusst sein.

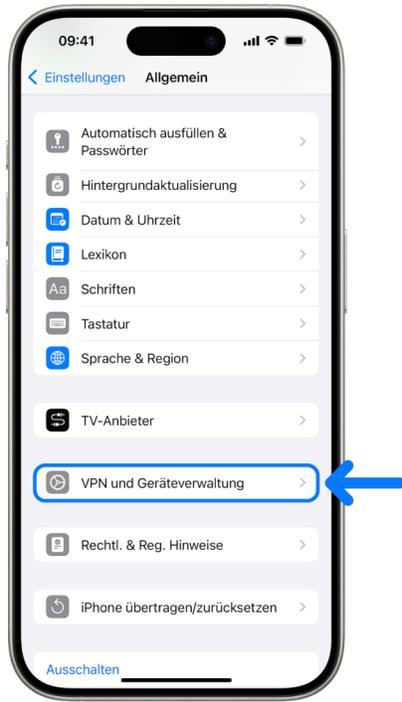


### Konfigurationsprofile überprüfen

**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

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.



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.
3. Starte dein Gerät neu.

## Unbekannte Konfigurationsprofile auf deinem Mac löschen

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.

1. Führe einen der folgenden Schritte aus:
  - Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke in der Seitenleiste auf „Allgemein“  und klicke dann auf „Geräteverwaltung“.
  - Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke dann 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 .
3. Starte deinen Mac neu.

## iPhone-Synchronisierung auf deinem iPhone oder Mac verwalten

Die iPhone-Synchronisierung erlaubt den Zugriff auf und die Steuerung des iPhone direkt vom Mac aus und schickt außerdem iPhone-Mitteilungen direkt an den Mac.

Die iPhone-Synchronisierung funktioniert nur, wenn sich dein iPhone in der Nähe befindet und gesperrt ist. Sobald du dein iPhone direkt verwendest, wird die iPhone-Synchronisierung automatisch beendet.

Du kannst den Zugriff auf die iPhone-Synchronisierung von einem der Geräte aus widerrufen, auch wenn du eine Mitteilung erhältst, dass die iPhone-Synchronisierung aktiv ist. Das Widerrufen des Zugriffs setzt die iPhone-Synchronisierung zurück. Du musst also den Konfigurationsprozess noch einmal durchlaufen, wenn du die iPhone-Synchronisierung wieder verwenden willst.

⚠️ **WICHTIG:** Bevor du Änderungen vornimmst oder Informationen löschst, solltest du dir über die [potenziellen Auswirkungen auf deine Sicherheit](#) bewusst sein.



### iPhone-Synchronisierung anzeigen und Zugriff beim Erhalten einer Mitteilung widerrufen

Wenn die iPhone-Synchronisierung aktiv ist oder bis vor kurzem aktiv war, erhältst du eine Mitteilung auf deinem iPhone. Du kannst auf die Mitteilung tippen, um den Sitzungsverlauf anzuzeigen und den Zugriff eines bestimmten Mac zu widerrufen.

1. Tippe auf deinem iPhone auf die Mitteilung.

Eine Liste mit Mac-Computern, die für die iPhone-Synchronisierung konfiguriert sind, wird angezeigt. Informationen zu früheren Sitzungen, einschließlich der Informationen zum Start und zur Dauer der Sitzungen, ist ebenfalls sichtbar.

2. Tippe oben rechts auf „Bearbeiten“ und wähle dann den Mac aus, der entfernt werden soll.

## **iPhone-Synchronisierung anzeigen und Zugriff auf dem iPhone widerrufen**

 **Tip:** Du kannst auch die Sicherheitsprüfung verwenden, um Informationen anzuzeigen und Mac-Computer zu entfernen. Weitere Informationen findest du unter [Sicherheitsprüfung auf einem iPhone mit iOS 16 oder neuer](#).

1. Wähle auf deinem iPhone „Einstellungen“  > „Allgemein“.
2. Tippe auf „AirPlay & Integration“ und tippe dann auf „iPhone-Synchronisierung“.  
Eine Liste mit Mac-Computern, die für die iPhone-Synchronisierung konfiguriert sind, wird angezeigt. Informationen zu früheren Sitzungen, einschließlich der Informationen zum Start und zur Dauer der Sitzungen, ist ebenfalls sichtbar.
3. Tippe oben rechts auf „Bearbeiten“ und wähle dann einen Mac aus, der entfernt werden soll.

## **Zugriff auf die iPhone-Synchronisierung auf dem Mac widerrufen**

1. Öffne die App „iPhone-Synchronisierung“ auf deinem Mac.
2. Wähle oben in der Menüleiste „iPhone-Synchronisierung“ > „Einstellungen“.
3. Wähle „Zugriff auf ‚[Name deines iPhone]‘ widerrufen“.

## **Touch ID oder Code für die iPhone-Synchronisierung anfordern**

Mit dem Festlegen bestimmter Einstellungen für die iPhone-Synchronisierung können sich deine Geräte automatisch verbinden. Du kannst auswählen, ob stattdessen eine Authentifizierung angefordert werden soll, wie z. B. Touch ID oder dein Geräte-Code.

1. Öffne die App „iPhone-Synchronisierung“ auf deinem Mac.
2. Wähle oben in der Menüleiste „iPhone-Synchronisierung“ > „Einstellungen“.
3. Wähle „Jedes Mal fragen“.

## **App am Senden von Mitteilungen hindern**

Wenn die iPhone-Synchronisierung aktiv ist, werden iPhone-Mitteilungen direkt an den Mac gesendet. Du kannst diese Option für bestimmte Apps deaktivieren.

1. Wähle auf deinem iPhone „Einstellungen“  > „Mitteilungen“.
2. Wähle eine beliebige App aus und deaktiviere dann „Auf Mac anzeigen“.

## Gerät mit dem Blockierungsmodus stärken

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 Menü „Apple“  > „Systemeinstellungen“, klicke in der Seitenleiste auf „Datenschutz & Sicherheit“  und klicke dann auf „Blockierungsmodus“. Klicke auf „Aktivieren“ und gib dann, wenn du dazu aufgefordert wirst, dein Passwort ein und klicke auf „Aktivieren und neu starten“.

## Home-Zubehör sicher kontrollieren

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/home-app/accessories/) (https://www.apple.com/home-app/accessories/).

## Teilen deines Zuhauses mit einer anderen Person beenden

1. Wähle die 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. Wähle unter „Personen“ den/die Benutzer:in, den/die du aus deinem Zuhause entfernen möchtest und wähle dann „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. Wähle in der App „Home“  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 wähle dann „Zuhause verlassen“. Wähle „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. Wähle in der App „Home“  das Home-Symbol und wähle „Einstellungen des Zuhauses“.
2. Wähle unten im Dialog „Zuhause entfernen“ und dann „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.

# Passwörter, Passkeys und Codes

## Passwörter für dein Gerät, Apps und Websites schützen

Auf deinem iPhone oder iPad mit iOS 17, iPadOS 17 (oder älter) 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.

Auf deinem iPhone oder iPad mit iOS 18, iPadOS 18 oder neuer kannst du deine Passwörter in der App „Passwörter“ verwalten. Hier findest du all deine Passwörter, Passkeys und Bestätigungs-codes an einer Stelle. Du kannst sie auf all deinen Geräten blockieren, wenn du dich mit demselben Apple Account bei iCloud anmeldest und „Passwörter & Schlüsselbund“ in den iCloud-Einstellungen aktivierst. Und wenn du automatisches Ausfüllen für die Anmeldung bei Apps und Websites verwendest, werden deine Passwörter automatisch in „Passwörter“ angezeigt.



### Passwörter mit iOS 18, iPadOS 18 oder neuer verwalten

1. Öffne die App „Passwörter“  auf deinem iPhone.
2. Tippe auf „Alle“ und tippe dann auf den Account für das Passwort, das du verwalten möchtest.
3. Tippe auf „Bearbeiten“.
4. Ändere oder lösche das Passwort und tippe dann zur Bestätigung.

## Passwörter mit iOS 17, iPadOS 17 oder älter 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 mit iOS 17, iPadOS 17 oder älter 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.

## Einmalige Bestätigungs\_codes automatisch löschen

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

- Führe einen der folgenden Schritte aus:
  - Auf einem iPhone oder iPad mit iOS 18, iPadOS 18 oder neuer: Wähle „Einstellungen“  > „Allgemein“ > „Automatisch ausfüllen & Passwörter“. Tippe unter „Bestätigungs\_codes“ auf „Nach Nutzung löschen“ und aktiviere sie dann.
  - Auf einem iPhone oder iPad mit iOS 17, iPadOS 17 oder älter: Wähle „Einstellungen“  > „Passwort“, tippe auf „Passwortoptionen“ und aktiviere die Option „Automatisch löschen“.
  - Auf einem Mac mit macOS 15: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke in der Seitenleiste auf „Allgemein“  und klicke dann auf „Automatisch ausfüllen & Passwörter“. Aktiviere „Nach Nutzung löschen“ unter „Bestätigungs\_codes“.
  - Auf einem Mac mit macOS 14 oder macOS 13: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke in der Seitenleiste auf „Passwörter“ , klicke auf „Passwortoptionen“ und aktiviere die Option „Automatisch löschen“.

## Eindeutigen Geräte-Code oder Passwort festlegen

Wenn du verhindern möchtest, dass andere deine Geräte verwenden oder auf deine Informationen zugreifen, lege einen eindeutigen, nur dir bekannten Code oder ein Passwort fest. Wenn du ein Gerät teilst oder wenn andere Personen deinen Code oder dein Passwort kennen, können sie die Informationen auf deinem Gerät und dem damit verbundenen Apple Account anzeigen und Änderungen vornehmen. Wenn du denkst, dass eine andere Person deinen Gerätecode oder dein Passwort kennt, und du einen nur dir bekannten Code oder ein Passwort festlegen möchtest, kannst du den Code oder das Passwort je nach Gerät unter „Einstellungen“ oder „Systemeinstellungen“ zurücksetzen (siehe Anleitung unten).



### 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 Account-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.

## Code 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.
5. Tippe auf „Zugriff überprüfen“ (falls verfügbar), um die Einstellungen zu prüfen, mit denen dauerhafter Zugriff auf deinen Daten gewährt wird, auch nachdem du deinen Code geändert hast. Weitere Informationen findest du unter [Sicherheitsprüfung auf einem iPhone mit iOS 16 oder neuer](#) weiter oben.

 **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, gehe zu „Einstellungen“ > „Face ID & Code“ (oder „Touch ID & Code“) und tippe dann auf „Vorherigen Code ungültig machen“.

## Anmeldepasswort auf dem Mac ändern

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 Account-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 in der Seitenleiste auf „Benutzer:innen & Gruppen“  und klicke auf .
- Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke dann in der Seitenleiste auf „Benutzer:innen & Gruppen“ .

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  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“.

## Geräte automatisch sperren

Um den Schutz deiner Daten noch weiter zu erhöhen, kannst du dein Gerät so einrichten, dass es unter bestimmten Verhältnissen automatisch gesperrt wird.

- *iPhone, iPad:* Wähle „Einstellungen“ > „Anzeige & Helligkeit“ > „Automatische Sperre“ und lege eine Dauer fest.
- *Mac:* Wähle Menü „Apple“  > „Systemeinstellungen“, klicke in der Seitenleiste auf „Sperrbildschirm“  und lege dann eine Zeitdauer fest.

Weitere Informationen findest du unter [Systemeinstellung „Sperrbildschirm“ auf dem Mac anpassen](#) im Mac – Benutzerhandbuch. (<https://support.apple.com/guide/mac-help/mh11784>)

- *Apple Watch:* Öffne die App „Einstellungen“, tippe auf „Code“ und aktiviere oder deaktiviere „Handgelenkerkennung“.

Weitere Informationen findest du unter [Automatisches Sperren](#) im Apple Watch – Benutzerhandbuch. (<https://support.apple.com/guide/watch/apd0e1e73b6f#apd6771615db>)

## Geteilte Passwörter und Passkeys verwalten

In iOS 17, iPadOS 17 und macOS 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 „[Zuletzt gelöscht Passwort oder Passkey auf dem Mac wiederherstellen](https://support.apple.com/guide/passwords/mchlee73013a/mac)“ (<https://support.apple.com/guide/passwords/mchlee73013a/mac>) im Passwörter – Benutzerhandbuch für den Mac.

## Deine Rolle in einer Gruppe für geteilte Passwörter ermitteln

- Führe einen der folgenden Schritte aus:
  - *Auf einem iPhone oder iPad mit iOS 18 oder iPadOS 18 (oder neuer):* Öffne die App „Passwörter“, tippe auf den Namen der Gruppe und überprüfe dann, ob du Eigentümer:in oder Mitglied der Gruppe bist.
  - *Auf einem iPhone oder iPad mit iOS 17 oder iPadOS 17 (oder älter):* 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 einem Mac mit macOS 15 (oder neuer):* Öffne die App „Passwörter“, klicke in der Seitenleiste auf die geteilte Gruppe, klicke auf „Verwalten“ und prüfe dann, ob du *Eigentümer:in* oder *Mitglied* der Gruppe bist.
  - *Auf einem Mac mit macOS 14 (oder älter):* Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke dann in der Seitenleiste auf „Passwörter“ . Suche nach einer Gruppe für geteilte Passwörter , wähle die Gruppe aus, klicke auf „Verwalten“ und prüfe, ob du *Eigentümer:in* oder *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 einem iPhone oder iPad mit iOS 18 oder iPadOS 18 (oder neuer):* Öffne die App „Passwörter“, tippe auf den Namen der Gruppe und entferne dann ein Mitglied.
  - *Auf einem iPhone oder iPad mit iOS 17 oder iPadOS 17 (oder älter):* Wähle „Einstellungen“  > „Passwort“, suche nach einer Gruppe für geteilte Passwörter , wähle die Gruppe aus und entferne das Mitglied.
  - *Auf einem Mac mit macOS 15 (oder neuer):* Öffne die App „Passwörter“, klicke in der Seitenleiste auf die geteilte Gruppe, klicke auf „Verwalten“ und entferne dann ein Mitglied.
  - *Auf einem Mac mit macOS 14 (oder älter):* Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke dann in der Seitenleiste auf „Passwörter“ . Suche nach einer Gruppe für geteilte Passwörter , wähle die Gruppe aus, klicke auf „Verwalten“ und entferne dann ein 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 einem iPhone oder iPad mit iOS 18 oder iPadOS 18 (oder neuer):* Öffne die App „Passwörter“, tippe auf den Namen der Gruppe und entferne dann dich selbst.
  - *Auf einem iPhone oder iPad mit iOS 17 oder iPadOS 17 (oder älter):* Wähle „Einstellungen“  > „Passwort“, suche nach einer Gruppe für geteilte Passwörter , wähle die Gruppe aus und entferne dich aus der Gruppe.
  - *Auf einem Mac mit macOS 15 (oder neuer):* Öffne die App „Passwörter“, klicke in der Seitenleiste auf die geteilte Gruppe, klicke auf „Verwalten“ und entferne dann dich selbst daraus.
  - *Auf einem Mac mit macOS 14 (oder älter):* Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke dann in der Seitenleiste auf „Passwörter“ . Suche nach einer Gruppe für geteilte Passwörter , wähle die Gruppe aus, klicke auf „Verwalten“ und entferne dann dich selbst daraus.

## 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 [Zuletzt gelöscht Passwort oder Passkey auf dem Mac wiederherstellen](#) im Passwörter – Benutzerhandbuch für den Mac (<https://support.apple.com/guide/passwords/mchlee73013a/mac>).

- Führe einen der folgenden Schritte aus:
  - *Auf einem iPhone oder iPad mit iOS 18 oder iPadOS 18 (oder neuer):* Öffne die App „Passwörter“, tippe auf den Namen der Gruppe und tippe dann auf den Account mit dem Passwort oder dem Passkey, das bzw. der gelöscht werden soll. Tippe auf „Bearbeiten“, tippe auf „Löschen“ und tippe dann zur Bestätigung erneut auf „Passwort löschen“ oder „Passkey löschen“.
  - *Auf einem iPhone oder iPad mit iOS 17 oder iPadOS 17 (oder älter):* Wähle „Einstellungen“  > „Passwort“, suche nach einer Gruppe für geteilte Passwörter , wähle die Gruppe aus und tippe dann auf „Passwort löschen“ oder „Passkey löschen“.
  - *Auf einem Mac mit macOS 15 (oder neuer):* Öffne die App „Passwörter“, klicke in der Seitenleiste auf die geteilte Gruppe und klicke dann auf den Account mit dem Passwort oder dem Passkey, das bzw. der gelöscht werden soll. Klicke auf „Bearbeiten“, klicke auf „Passwort löschen“ oder „Passkey löschen“ und klicke dann (erneut) auf „Passwort löschen“ oder „Passkey löschen“.
  - *Auf einem Mac mit macOS 14 (oder älter):* Wähle Menü „Apple“  > „Systemeinstellungen“, klicke in der Seitenleiste auf „Passwörter“  und klicke auf  neben dem Account mit dem zu löschenden Passwort oder Passkey. Klicke auf „Passwort löschen“ oder „Passkey löschen“ und klicke dann (erneut) auf „Passwort löschen“ oder „Passkey löschen“.

# Standortinformationen verwalten

## Wegbegleitung für „Nachrichten“ verwenden

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 auswählen, 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 eine Zeitdauer 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 angestrebtes 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.

# AirTags und andere Objekte verwalten

## Unerwünschte Tracking-Objekte erkennen

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. Hiermit können sich Benutzer:innen (von iPhone, iPad und Android) benachrichtigen lassen, wenn sie getrackt werden.



Wenn du denkst, 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 Informationen zum Objekt anzufordern. Weitere Informationen findest du unter „Legal Process Guidelines“ für [innerhalb der USA](https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf) (https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf) und [außerhalb der USA](https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf) (https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-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.

## Unerwünschte Tracking-Mitteilungen

Verfügbarkeit der Software für unerwünschte Tracking-Mitteilungen:

- Mitteilungen bei unerwünschtem Tracking sind für AirTags und anderem Zubehör, das sich im „Wo ist?“-Netzwerk befindet, auf einem iPhone oder iPad mit iOS 14.5, iPadOS 14.5 oder neuer verfügbar.
- Mitteilungen bei unerwünschtem Tracking für unbekannte Bluetooth-Trackinggeräte, die mit der Industriespezifikation [DULT \(Detecting Unwanted Location Trackers\)](#) kompatibel sind, sind auf einem iPhone mit iOS 17.5 (oder neuer) verfügbar.
- Google stellt die [Erkennung von unerwünschtem Tracking](#) auf Geräten mit Android 6.0 (oder neuer) bereit. Geräte mit älteren Betriebssystemen können ihre Version aktualisieren oder [die App „Tracker-Erkennung“](#) verwenden.

## Unerwünschte Tracking-Mitteilungen aktivieren

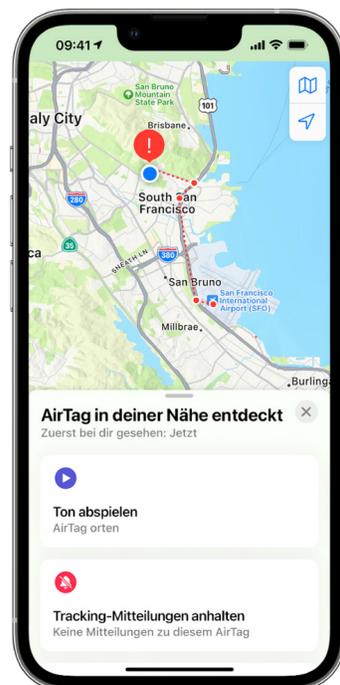
Um Mitteilungen zu unerwünschtem Tracking auf einem iPhone oder iPad mit iOS 14.5, iPadOS 14.5 oder neuer zu erhalten, stelle die folgenden Bedingungen sicher:

- Wähle „Einstellungen“ > „Datenschutz & Sicherheit“ > „Ortungsdienste“ und aktiviere „Ortungsdienste“.
- Wähle „Einstellungen“ > „Datenschutz & Sicherheit“ > „Ortungsdienste“ > „Systemdienste“ und aktiviere „Mein iPhone suchen“.
- Wähle „Einstellungen“ > „Bluetooth“ und aktiviere „Bluetooth“.
- Wähle „Einstellungen“ > „Mitteilungen“, scrolle nach unten zu „Tracking-Mitteilungen“ und aktiviere dann „Mitteilungen erlauben“.
- Deaktiviere den Flugmodus. Wenn sich dein Gerät im Flugmodus befindet, erhältst du keine Tracking-Mitteilungen.

## Wenn du eine Mitteilung zu unerwünschtem Tracking erhältst

Folge den folgenden Schritten, um das Objekt zu suchen:

1. Tippe auf die Mitteilung.
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 unbekanntem 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 durchsuche deine Besitztümer, 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 bereits eine Mitteilung zu unerwünschtem Tracking erhalten hast und die Informationen erneut überprüfen möchtest, 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“.

**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.



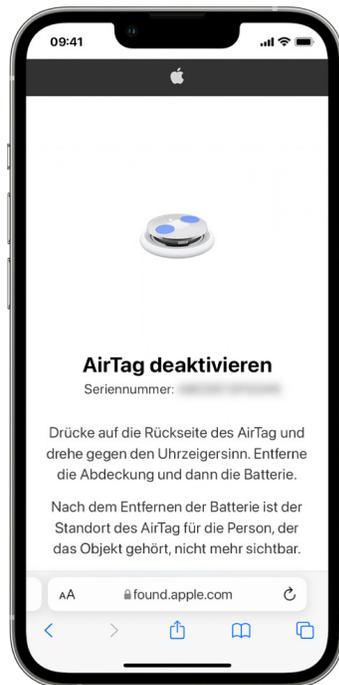
### Wenn du befürchtest, dass das Objekt verwendet wird, um dich zu tracken

▼ **WICHTIG:** Bevor du Änderungen vornimmst, solltest du dir über die [potenziellen Auswirkungen auf deine Sicherheit](#) und deinen Datenschutz bewusst sein. 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](#) (<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.

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 Informationen zum Objekt anzufordern. Du musst unter Umständen das AirTag, die AirPods, das Zubehör, das sich im „Wo ist?“-Netzwerk befindet, sowie die Seriennummer des Geräts bereitstellen.

Weitere Informationen findest du unter „Legal Process Guidelines“ für [innerhalb der USA](#) (<https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>) und [außerhalb der USA](#) (<https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf>).

Nach dem Deaktivieren des Objekts kann die Person, der das Objekt gehört, keine aktuellen Standortinformationen des Objekts mehr abrufen. Außerdem erhältst du keine Mitteilungen 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](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 seinem:seiner Eigentümer:in getrennt wird, 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 Nahfeldkommunikationstechnologie (Near Field Communication, kurz NFC), etwa einem iPhone oder Android-Smartphone, herausfinden, ob es als verloren markiert wurde, und dabei helfen, es der Person zurückzugeben, der das Objekt gehört.

⚠️**WICHTIG:** 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 möglicherweise das AirTag oder seine Seriennummer zur Verfügung stellen.

## Mit einem anderen Apple Account verbundene Geräte

Wenn du AirPods, ein AirTag oder „Wo ist?“-Netzwerkzubehör einrichtest und eine Nachricht siehst, dass das Gerät oder das Objekt mit einem anderen Apple Account gekoppelt ist, muss es zuerst von dem anderen Apple Account entfernt werden. Weitere Informationen zum Entfernen oder Entkoppeln deines Zubehörs oder Geräts oder zur Einrichtung mit einem anderen Apple Account findest du im Apple Support-Artikel [Wenn ein Gegenstand oder Gerät mit einem anderen Apple Account verbunden ist](https://support.apple.com/102620) (<https://support.apple.com/102620>).

## Teilen eines AirTag beenden

Besitzer:innen eines AirTag (oder eines Objekts eines Drittanbieters, das mit „Wo ist?“ kompatibel ist) können es mit bis zu fünf Personen gleichzeitig teilen. Wenn eine Person den AirTag teilt, wird eine Gruppe erstellt, die auch *Freigabegruppe* genannt wird. Mitglieder dieser Freigabegruppe können:

- Den Standort des AirTag in der App „Wo ist?“ auf ihrem Gerät sehen
- Mit der Funktion „Genaue Suche“ das AirTag orten
- Einen Ton zum Finden eines verloren gegangenen AirTag abspielen
- Sich benachrichtigen lassen, wenn eine neue Person der Freigabegruppe beitrifft
- Der Apple Account jedes Mitglieds der Freigabegruppe anzeigen (oder die Kontaktinformationen, wenn die entsprechende Person in ihren Kontakten gesichert ist)

*Hinweis:* Nur der:die Besitzer:in kann sehen, welche Mitglieder der Freigabegruppe das AirTag haben.

Da alle Mitglieder einer Freigabegruppe den Standort des AirTag sehen können, werden unerwünschte Tracking-Mitteilungen für das AirTag für alle Gruppenmitglieder unterdrückt. Wenn eine Person die Freigabegruppe verlässt oder der:die Besitzer:in sie aus der Gruppe entfernt, kann sie den Standort des AirTag nicht mehr sehen und die Mitteilungen bei unerwünschtem Tracking werden wieder gesendet.

Weitere Informationen findest du unter [AirTag oder anderes Objekt in der App „Wo ist?“ teilen](https://support.apple.com/guide/iphone/iph419cc5f28/ios) im iPhone – Benutzerhandbuch. (<https://support.apple.com/guide/iphone/iph419cc5f28/ios>)



### Teilen eines AirTag in „Wo ist?“ auf dem iPhone oder iPad beenden

1. Öffne die App „Wo ist?“  auf deinem iPhone oder iPad.
2. Tippe auf „Objekte“ und tippe dann auf den Objektnamen.
3. Führe einen der folgenden Schritte aus:

- *Dich selbst entfernen*: Tippe auf „Entfernen“ und tippe dann zur Bestätigung erneut auf „Entfernen“.

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

- *Andere Person entfernen (wenn du Eigentümer:in bist)*: Tippe auf den Namen der Person, tippe auf „Entfernen“ und tippe dann auf „Freigabe stoppen“.

### Teilen eines AirTag in „Wo ist?“ auf dem Mac beenden

1. Öffne die App „Wo ist?“  auf deinem Mac.
2. Klicke auf „Objekte“, wähle das Objekt aus, dessen Freigabe du beenden möchtest, und klicke dann auf der Karte auf .
3. Führe einen der folgenden Schritte aus:

- *Dich selbst entfernen*: Klicke auf „Entfernen“ und klicke dann zur Bestätigung erneut auf „Entfernen“.

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

- *Andere Person entfernen (wenn du Eigentümer:in bist)*: Klicke auf den Namen der Person, klicke auf „Entfernen“ und klicke dann auf „Freigabe stoppen“.

### Teilen eines AirTag mit der Sicherheitsprüfung auf dem iPhone beenden

Du kannst dich selbst mithilfe der Sicherheitsprüfung aus einer Freigabegruppe entfernen. Als Eigentümer:in kannst du auch andere Personen entfernen.

1. Wähle „Einstellungen“  > „Datenschutz & Sicherheit“ > „Sicherheitsprüfung“.
2. Tippe auf „Teilen & Zugriff‘ verwalten“ und tippe dann auf „Fortfahren“.
3. Tippe auf „Informationen“, tippe auf „Objekte“ und dann auf „Teilen stoppen“.

*Hinweis*: Das Suchen nach Objekten und Teilen des Objektstandorts ist nicht in allen Ländern oder Regionen verfügbar.

## Teilen des Standorts eines verloren gegangenen AirTag beenden

In „Wo ist?“ können Eigentümer:innen eines AirTag (oder eines Objekts eines Drittanbieters, das mit „Wo ist?“ kompatibel ist) dessen Standort über eine zeitlich begrenzte Webseite teilen. Sie können zum Beispiel die Webseite mit einer Fluggesellschaft teilen, um ihr bei der Suche nach verlorenen Gepäckstücken zu helfen.

Wenn eine Person den Link öffnet, müssen sie sich mit ihrem Apple Account oder ihrer Partner-E-Mail-Adresse (für Unternehmen, die mit Apple zusammenarbeiten, um diesen Dienst zur Verfügung zu stellen, z. B. Fluggesellschaften) anmelden. Die Webseite enthält:

- Den Standort des AirTag auf einer Karte, sofern verfügbar
- Die registrierte Telefonnummer des:der Eigentümer:in
- Die Seriennummer des AirTag

Weitere Informationen findest du unter [Standort eines verloren gegangenen Objekts in der App „Wo ist?“ teilen](https://support.apple.com/guide/iphone/iph3bedf2cc5/ios) im iPhone – Benutzerhandbuch. (<https://support.apple.com/guide/iphone/iph3bedf2cc5/ios>)



## Standortaktualisierungen auf dem iPhone oder iPad beenden

Die Freigabe wird beendet, wenn das AirTag wieder bei dir ist, nach sieben Tagen oder du sie manuell in der App „Wo ist?“ beendest, je nachdem, welches Ereignis zuerst eintritt.

In der App „Wo ist?“ manuell beenden:

1. Öffne die App „Wo ist?“  auf deinem iPhone oder iPad.
2. Tippe auf „Objekte“, tippe auf das Objekt mit der geteilten Webseite und tippe dann auf „Objektstandort teilen“.
3. Tippe auf „Objektstandort nicht mehr teilen“.

### Standortaktualisierungen auf dem Mac beenden

Die Freigabe wird beendet, wenn das AirTag wieder bei dir ist, nach sieben Tagen oder du sie manuell in der App „Wo ist?“ beendest, je nachdem, welches Ereignis zuerst eintritt.

In der App „Wo ist?“ manuell beenden:

1. Öffne die App „Wo ist?“  auf deinem Mac.
2. Klicke auf „Objekte“, wähle das Objekt mit der geteilten Webseite aus und klicke dann auf der Karte auf .
3. Klicke auf „Objektstandort teilen“ unter „Verlorenes [Objekt]“.
4. Klicke auf „Objektstandort nicht mehr teilen“.

*Hinweis:* Das Suchen nach Objekten und Teilen des Objektstandorts ist nicht in allen Ländern oder Regionen verfügbar.

## „Wo ist?“ und die Standortfreigabe

Mit der App „Wo ist?“ auf dem iPhone, iPad, Mac und der Apple Watch kannst du deine Geräte im Blick behalten. Außerdem können du und anderen Personen eure Standorte miteinander 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 [Familienfreigabegruppe verlassen oder Mitglied daraus entfernen](#) weiter unten.

### **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
 App „Wo ist?“	In der App „Wo ist?“ können andere Personen den Tab „Personen“ öffnen und auf deinen Namen tippen, um deinen Standort zu sehen.
 App „Wo ist?“	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 ihrem Standort entfernt bist. Wenn eine andere Person dich mit der Funktion „Genaue Suche“ sucht, erhältst du eine Mitteilung darüber, dass diese Person dich sucht.  Weitere Informationen findest du unter <a href="https://support.apple.com/de-de/guide/iphone/iph3effd0ed6">Funktion „Genaue Suche“ auf dem iPhone verwenden, 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> )
 App „Wo ist?“	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 ihr euren Standort miteinander teilt. Weitere Informationen findest du unter <a href="#">Familienfreigabegruppe verlassen oder ein Mitglied daraus entfernen</a> weiter unten.

App	Beschreibung
 App „Nachrichten“	Wenn andere Personen in der App „Nachrichten“, mit denen du bereits deinen Standort geteilt hast, auf dein Kontaktsymbol tippen, wird ihnen die Detailansicht mit deinem aktuellen über „Wo ist?“ geteilten Standort angezeigt.
 App „Nachrichten“	In der App „Nachrichten“ in iOS 17 und iPadOS 17 (oder neuer) können andere Personen auch deinen ungefähren Standort oben im Konversationsverlauf sehen.
 App „Karten“	Wenn andere Personen, mit denen du bereits deinen Standort geteilt hast, deinen Namen in der App „Karten“ suchen, sehen sie deinen aktuellen über „Wo ist?“ geteilten Standort auf der Karte.

### Mitteilungen zu Standortänderungen

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.

- Um alle Mitteilungen über dich anzuzeigen, 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 .
- 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.
- Siehst du eine Mitteilung, die du löschen möchtest, wähle zunächst einen Namen und dann eine Mitteilung aus.
- Lösche die Mitteilung und bestätige, dass du sie löschen willst.

## Standortfreigabe in „Wo ist?“ auf dem iPhone oder iPad beenden

Wenn du das Teilen deines Standorts durch beliebige der folgenden Methoden beendest, wird dein Standort nicht mehr in den Apps „Wo ist?“, „Karten“, „Kontakte“ und „Nachrichten“ auf Geräten anderer Personen angezeigt.

▼ **WICHTIG:** Wenn du deinen Standort nicht mehr teilst, können andere Personen, mit denen du deinen Standort bereits geteilt hast, möglicherweise darüber informiert werden. Bei älteren Betriebssystemen erhalten sie möglicherweise eine Mitteilung in „Nachrichten“, dass du die Freigabe beendet hast.

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“.

*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.

## Standortfreigabe in der App „Nachrichten“ auf dem iPhone oder 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.

## Standortfreigabe in der App „Kontakte“ auf dem iPhone oder 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

„Mein iPhone suchen“ (in „Einstellungen“  > „Wo ist?“) hilft dir, wenn du dein Handy verloren hast oder es gestohlen wurde.

Wenn „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.

**VORSICHT:** 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 dem Mac:* Wähle Menü „Apple“  > „Systemeinstellungen“, klicke oben in der Seitenleiste auf deinen Namen und klicke dann auf „iCloud“. Klicke auf „Weitere Apps anzeigen“ und klicke dann auf „Meinen Mac suchen“.

# Einstellungen für Ortungsdienste verwalten

Die Ortungsdienste ermöglichen dir, die Apps (wie „Karten“, „Kamera“, „Wetter“ und andere) und Websites auszuwählen, mit denen du deinen Standort teilen möchtest. Wenn die Ortungsdienste aktiviert sind, können sie Informationen von verschiedenen Netzwerken verwenden, um deinen ungefähren oder genauen Standort zu bestimmen. Die Ortungsdienste findest du auf dem iPhone, iPad, Mac und der Apple Watch.



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 aktivieren oder deaktivieren

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

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

## **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 für einzelne Apps prüfen und ändern sowie angeben, wie oft sie deinen Standort nutzen können. Es folgen Anleitungen für iPhone oder iPad.

1. Wähle „Einstellungen“  > „Datenschutz & Sicherheit“ > „Ortungsdienste“ und prüfe oder ändere die Zugriffseinstellungen für eine 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 in der Seitenleiste auf „Datenschutz & Sicherheit“  und klicke dann auf „Ortungsdienste“. Deaktiviere „Ortungsdienste“, gib dein Passwort ein und klicke auf „Entsperren“.
- Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke in der Seitenleiste auf „Sicherheit & Datenschutz“ , klicke auf „Ortungsdienste“ und klicke dann auf „Ortungsdienste aktivieren“. Eventuell musst du die Systemeinstellungen entsperren, bevor du Änderungen vornehmen kannst. Klicke dazu auf  unten links und gib dein Passwort ein.

2. Aktiviere das Markierungsfeld neben einer App, um ihr die Verwendung der Ortungsdienste zu erlauben. Hebe die Auswahl des Markierungsfelds auf, um die Ortungsdienste für die App zu deaktivieren.

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.

3. Scrolle zu „Systemdienste“ am Ende der Liste und klicke auf die Taste „Details“, um die Systemdienste anzuzeigen, die deinen Standort 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 . Um alle Standorte zu entfernen, klicke auf  und klicke auf „Verlauf löschen“.

## Automatische Freigabe der erwarteten Ankunftszeit in „Karten“ verwalten

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.



### Freigabe der erwarteten Ankunftszeit auf dem iPhone oder iPad verwalten

1. Tippe in der App „Karten“  auf deinem iPhone oder iPad (Wi-Fi + Cellular-Modelle) auf dein Profilsymbol rechts neben dem Suchfeld.
2. Wähle „Favoriten“, um ein Fenster zu öffnen, das alle Orte enthält, die du als Favorit angegeben hast.
3. Tippe auf  neben der favorisierten Sehenswürdigkeit.
4. Scrolle nach unten zum Abschnitt „Ankunftszeit teilen“, um die Namen der Personen zu überprüfen, mit denen du deine Ankunftszeit automatisch teilst.
5. Um eine Person zu entfernen, tippe auf „Ankunftszeit nicht mehr teilen“ neben dem Namen der betreffenden Person.
6. Um eine Person hinzuzufügen, tippe auf „Person hinzufügen“. Wähle dann die Person aus der App „Kontakte“ aus, 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 „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.

## Standortmetadaten in der App „Fotos“ verwalten

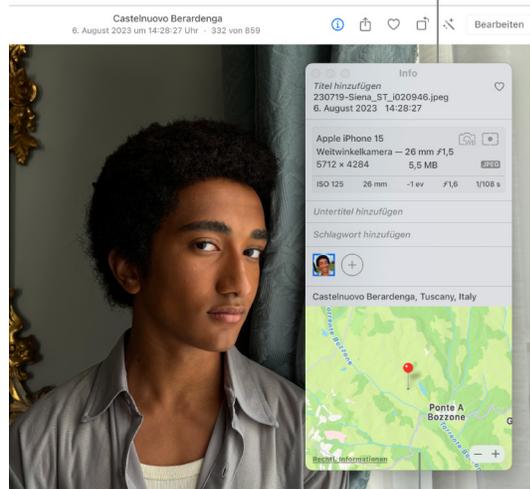
Wenn die Ortungsdienste für die App „Kamera“ aktiviert sind, werden Informationen (bekannt als Metadaten) aus dem Mobilfunknetz, aus dem WLAN, aus GPS-Netzwerken und aus Bluetooth verwendet, um den Standort für Fotos und Videos zu bestimmen. Diese Koordinaten werden in jedes Foto und Video eingebettet, sodass du später in der App „Fotos“ auf der Basis des Orts, an dem die Fotos und Videos aufgenommen wurden, nach diesen suchen oder ortsbasierte 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

Fenster „Info“ verwenden, um die Informationen eines Bildes anzuzeigen und zu bearbeiten



Wenn ein Foto GPS-Informationen enthält, wird der Standort des Fotos im Fenster „Info“ angezeigt

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  und prüfe dann die Standortinformationen.

## 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  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 die 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  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.

# Inhalte verwalten

## Allgemein

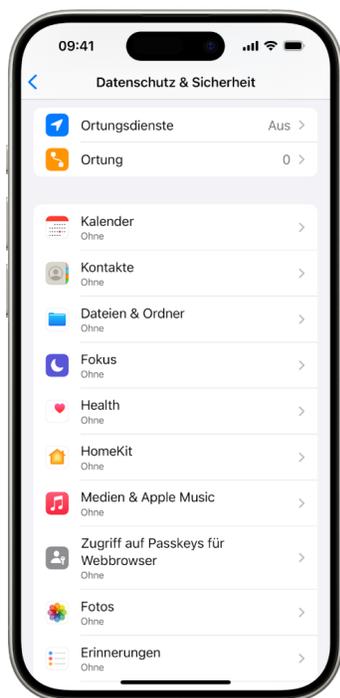
### Datenschutzfunktionen von Apps in Apple-Produkten

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 dem Mac: Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke dann in der Seitenleiste auf „Datenschutz & Sicherheit“ .
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 & Sicherheit“ .
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.

## Apps überprüfen und löschen

Wenn du befürchtest, dass eine Person ohne deine Erlaubnis eine App auf deinem Gerät installiert haben könnte, kannst du eine Liste von Apps überprüfen, um sicherzustellen, dass keine unerwünschten Inhalte existieren (Anleitung beginnt im nächsten Bereich weiter unten).

Wenn du dir nicht sicher bist, was der Zweck einer Apps ist, kannst du im App Store nachsehen.

Du kannst die Art von Daten, auf die jede App Zugriff hat (z. B. Standort, Fotos etc.), über die Funktion „[Sicherheitsprüfung](#)“ (iOS 16 oder neuer) überprüfen und ändern.

Möglicherweise möchtest du auch die [Einstellungen für Apps von Drittanbietern](#), die nur in der jeweiligen App verfügbar sind und nicht von Apple verwaltet werden können, überprüfen.

⚠️ **WICHTIG:** Bevor du Änderungen vornimmst oder Informationen löschst, solltest du dir über die [potenziellen Auswirkungen auf deine Sicherheit](#) und deinen Datenschutz bewusst sein.



## Eine App aus der App-Mediathek auf dem iPhone oder iPad löschen



1. Gehe zum Home-Bildschirm und streiche nach links, vorbei an allen deinen Home-Bildschirmseiten, um die App-Mediathek zu erreichen.
2. Tippe in das Suchfeld. Eine alphabetische Liste mit allen Apps auf dem Gerät wird angezeigt.
3. Wenn du eine App siehst, die du entfernen möchtest, lege den Finger auf das App-Symbol, bis das Menü angezeigt wird.
4. Tippe zum Löschen auf „App löschen“.

Weitere Informationen findest du unter [Apps auf dem iPhone entfernen oder löschen](#) im iPhone – Benutzerhandbuch.

(<https://support.apple.com/guide/iphone/iph248b543ca>)

### App vom Home-Bildschirm löschen

1. Lege den Finger auf die App auf dem Home-Bildschirm.
2. Tippe auf „App entfernen“ und dann auf „App löschen“, um sie zu löschen.

Weitere Informationen findest du unter [Apps auf dem iPhone entfernen oder löschen](#) im iPhone – Benutzerhandbuch.

(<https://support.apple.com/guide/iphone/iph248b543ca>)

## App vom Mac löschen

Du kannst Apps löschen, die aus dem Internet oder von einem externen Datenträger (z. B. ein USB-Gerät) 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] Deinstallationsprogramm“ 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:* 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.

## Apps auf dem iPhone sperren oder ausblenden

Wenn du jemandem etwas auf deinem iPhone zeigen möchtest, du aber beruhigt sein willst, dass diese Person keinen Zugriff auf bestimmte Apps erhält, kannst du die Apps sperren oder ausblenden.

- *App sperren:* Face ID, Touch ID oder dein Code ist zum Öffnen der App erforderlich. Informationen in einer gesperrten App werden an einigen Orten auf deinem iPhone angezeigt, z. B. in Mitteilungsvorschauen, Siri-Vorschlägen oder deinem Anrufverlauf.
- *App ausblenden:* Die App ist wie oben beschrieben gesperrt und wird außerdem nicht auf deinem Home-Bildschirm angezeigt und in den Ordner „Ausgeblendet“ unten in der App-Mediathek bewegt. Die App ist an anderen Orten noch immer auf deinem iPhone sichtbar.

**⚠️ WICHTIG:** Wenn du eine App auf deinem Gerät sperrst oder ausblendest, ist sie nur auf diesem Gerät gesperrt oder ausgeblendet. Der gesperrte oder ausgeblendete Status einer App wird nicht mit iCloud synchronisiert.

*Hinweis:* Kinder unter 13 Jahren in einer Familienfreigabegruppe können Apps nicht sperren oder ausblenden. Personen von 13 bis 17 Jahren in einer Familienfreigabegruppe können eine App sperren oder ausblenden, aber ein Elternteil oder eine erziehungsberechtigte Person kann sehen, dass die App geladen wurde und wie lange sie verwendet wurde, sowie mithilfe von „Bildschirmzeit“ den Zugriff darauf beschränken. (Das Alter kann je nach Land oder Region variieren.)



### **App sperren**

*Hinweis:* Einige auf dem iPhone integrierte Apps können nicht gesperrt werden, einschließlich „Rechner“, „Kamera“, „Uhr“, „Kontakte“, „Wo ist?“, „Karten“, „Kurzbefehle“ und „Einstellungen“.

1. Gehe zum Home-Bildschirm auf deinem iPhone und suche nach der App, die gesperrt werden soll.
2. Lege den Finger auf das App-Symbol, bis das Menü „Schnellaktionen“ geöffnet wird.
3. Tippe auf „Face ID anfordern“ (oder auf „Touch ID anfordern“ oder „Code anfordern“).
4. Tippe erneut auf „Face ID anfordern“ (oder auf „Touch ID anfordern“ oder „Code anfordern“) und authentifiziere dich mit Face ID (oder Touch ID oder einem Code).

## App ausblenden

*Hinweis:* Apps, die automatisch in iOS 18 (oder neuer) installiert sind, können nicht ausgeblendet werden. Nur separat geladene Apps können ausgeblendet werden.

1. Gehe zum Home-Bildschirm auf deinem iPhone und suche nach der App, die ausgeblendet werden soll.
2. Lege den Finger auf das App-Symbol, bis das Menü „Schnellaktionen“ geöffnet wird.
3. Tippe auf „Face ID anfordern“ (oder auf „Touch ID anfordern“ oder „Code anfordern“).
4. Tippe erneut auf „Ausblenden und Face ID anfordern“ (oder auf „Ausblenden und Touch ID anfordern“ oder „Ausblenden und Code anfordern“), authentifiziere dich mit Face ID (oder Touch ID oder einem Code) und tippe dann auf „App ausblenden“.

## Wo sind ausgeblendete Apps sichtbar?

Um deine ausgeblendeten Apps zu verwenden, gehe zum Home-Bildschirm, streiche nach links, an all deinen Home-Bildschirmseiten vorbei, um zur App-Mediathek zu gelangen, tippe auf den Ordner „Ausgeblendet“ und authentifiziere dich dann mit Face ID, Touch ID oder einem Code.

Es gibt einige andere Orte, an denen die Namen von ausgeblendeten Apps angezeigt werden können:

- „Einstellungen“  > „Apps“ > „Ausgeblendete Apps“ (Authentifizierung mit Face ID, Touch ID oder einem Code ist erforderlich)
- „Einstellungen“  > „Bildschirmzeit“
- „Einstellungen“  > „Batterie“ > „Batteriezustand & Ladevorgang“
- Kaufverlauf des App Store. Weitere Informationen findest du im Apple Support-Artikel [Einkäufe im App Store ausblenden](https://support.apple.com/108091) (https://support.apple.com/108091).

## Apps wieder einblenden

Du kannst das Ausblenden einer App beenden, damit sie wieder auf dem Home-Bildschirm angezeigt wird.

1. Gehe zum Home-Bildschirm auf deinem iPhone.
2. Streiche nach links, vorbei an allen deinen Home-Bildschirmseiten, um zur App-Mediathek zu gelangen.
3. Tippe unten in der App-Mediathek auf den Ordner „Ausgeblendet“ und authentifiziere dich mit Face ID (oder Touch ID oder einem Code).
4. Um die App aus dem Ordner „Ausgeblendet“ hinauszubewegen, lege den Finger auf die App, tippe auf „Face ID nicht anfordern“ (oder „Touch ID nicht anfordern“ oder „Code nicht anfordern“) und authentifiziere dich dann mit Face ID (oder Touch ID oder einem Code).  
Die App wird auf deinem Home-Bildschirm und oben in der App-Mediathek angezeigt.

# Einstellungen für Apps von Drittanbietern

## Einführung in Apps von Drittanbietern

Im Apple-Ökosystem sind zwei Arten von Apps verfügbar:

- *Erstanbieter-Apps*: Entwickelt von Apple, wie z. B. „Nachrichten“, „Kalender“, „Safari“ oder „FaceTime“.
- *Drittanbieter-Apps*: Entwickelt von Unternehmen und Organisationen, die nicht Apple sind, wie z. B. Instagram, YouTube, Threads oder Google.

Drittanbieter-Apps sind im App Store oder alternativen App-Stores verfügbar. Ihre Accounteinstellungen und Steuerelemente können sich von Apps, die von Apple entwickelt wurden, unterscheiden und auf manche dieser Steuerelemente kann möglicherweise nur innerhalb der App oder durch die Website der Entwickler der Drittanbieter-App zugegriffen werden. Diese Unterscheidung ist sehr wichtig, da Drittanbieter-Apps für gewöhnlich zusätzliche Schritte für die Freigabe- und Datenschutzeinstellungen erfordern.

## Apple-Einstellungen für Drittanbieter-Apps

Einige Einstellungen für Drittanbieter-Apps können über die App „Einstellungen“ verwaltet werden. Diese Einstellungen beinhalten, auf welche Funktionen des Apple-Geräts die App zugreifen und diese nutzen kann. Manche Beispiele beinhalten Zugriff auf Standort, Kontakte, Fotos oder die Möglichkeit Mitteilungen zu senden.

Um diese Einstellungen zu verwalten, öffne „Einstellungen“ , scrolle nach unten und tippe auf die gewünschte App.

## Nur In-App-verfügbare Drittanbiitereinstellungen

Manche Einstellungen für Apps von Drittanbietern können nicht über Apple verwaltet werden und können nur direkt in der App verwaltet werden. Um zu verwalten, wie Drittanbieter-Apps Informationen mit Dritten teilen, öffne die App und navigiere zu den Accounteinstellungen. Diese Einstellungen werden vielleicht unter einem anderen Namen aufgeführt, z. B. „Optionen“ und einige Einstellungen können in anderen Bereichen der Accounteinstellungen aufgeführt sein. Wichtige Bereiche, die du überprüfen solltest, sind Sicherheit, Datenschutz, das Teilen von Daten und Einstellungen zur Sichtbarkeit. Bei einigen Apps kann es notwendig sein in dazugehörigen Support-Artikeln oder FAQs zu suchen, um alle verfügbaren Einstellungen zu finden, die geändert werden können.

*Hinweis:* In manchen Fällen können bestimmte Einstellungen (z. B. Löschen des Accounts oder Anfrage für eine Kopie deiner Daten) nur über die Website der Entwickler der Drittanbieter-App verwaltet werden. Wenn du die Account-Einstellungen ändern möchtest, musst du dich auf der Website der Drittanbieter-App anmelden und die Einstellungen dort aktualisieren.

## Blockieren, Stummschalten und Entfreunden

Das Verwalten von Beziehungen innerhalb des Apple-Ökosystems wird nicht auf Einzelpersonen und Kommunikationen in einer Drittanbieter-App ausgedehnt. Beispielsweise resultiert das Blockieren einer Person in „Nachrichten“, „Telefon“ oder „FaceTime“ nicht darin, dass die Person auch in „Instagram“ blockiert wird. Diese Beziehungen müssen innerhalb der Drittanbieter-App selbst verwaltet werden. Überprüfe die Support-Seite der Drittanbieter-App für weitere Informationen, wie eine Person vorübergehend oder dauerhaft blockiert, stummgeschaltet oder entfreundet werden kann.

## Weiterleitungseinstellungen überprüfen

Du kannst überprüfen und verwalten, wie und an wen Inhalte weitergeleitet werden.

⚠ **WICHTIG:** Bevor du Änderungen vornimmst oder Informationen löschst, solltest du dir über die [potenziellen Auswirkungen auf deine Sicherheit](#) und deinen Datenschutz bewusst sein.



### iCloud Mail-Weiterleitung verwalten

Du kannst sehen, ob E-Mails in iCloud 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 Account-Benutzernamen und deinem Passwort an. Gib (falls erforderlich) den Code für die Zwei-Faktor-Authentifizierung ein.
2. Klicke auf „Mail“ und dann auf  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 verwendet, wird deine Nachricht als SMS versendet. Du kannst das iPhone so einrichten, dass beim Senden oder Empfangen einer SMS diese auf anderen Geräten, auf denen du mit deinem Apple Account angemeldet bist, erscheint. Diese Geräte können ebenfalls neue SMS versenden. Wenn du befürchtest, dass deine Nachrichten an andere Geräte weitergeleitet werden, kannst du die Geräteliste überprüfen und das Weiterleiten von SMS deaktivieren.

1. Wähle auf deinem iPhone „Einstellungen“  > „Apps“ > „Nachrichten“.
2. Tippe auf „SMS-Weiterleitung“, um zu sehen, welche Geräte SMS-Nachrichten an dein Gerät senden bzw. von diesem empfangen können.
3. Deaktiviere sämtliche Geräte, von denen du keine SMS erhalten möchtest und denen du auch keine senden möchtest.

## Anrufweiterleitung und Anrufe auf Geräten, die kein iPhone sind, 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“  > „Apps“ > „Telefon“ > „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.

## Fotos und Videos auf Apple-Geräten ausblenden

In „Fotos“ auf dem iPhone, iPad oder Mac kannst du Fotos ausblenden, die nicht angezeigt werden sollen. Die ausgeblendeten Fotos bleiben in deiner Mediathek und du kannst sie später, wenn du möchtest, wieder einblenden.



### Fotos auf dem iPhone oder iPad vorübergehend ausblenden

1. Öffne die App „Fotos“ 📷 auf deinem iPhone oder iPad.
2. Lege den Finger auf das Foto, das ausgeblendet werden soll.
3. Tippe auf „Ausblenden“ und bestätige dann, dass das Foto ausgeblendet werden soll.  
Das ausgewählte Foto verschwindet aus der Ansicht, wird jedoch nicht gelöscht.

### Fotos auf dem Mac vorübergehend ausblenden

1. Öffne die App „Fotos“ 📷 auf deinem Mac.
2. Klicke in der Seitenleiste auf „Mediathek“ und wähle dann die Fotos aus, die ausgeblendet werden sollen.
3. Wähle „Bild“ > „[Nummer] Fotos ausblenden“ und klicke dann auf „Ausblenden“.  
Die ausgewählten Fotos verschwinden aus der Ansicht, werden jedoch nicht gelöscht.

### Ausgeblendete Fotos auf dem iPhone oder iPad anzeigen

1. Öffne die App „Fotos“ 📷 auf deinem iPhone oder iPad.
2. Scrolle nach unten und tippe auf „Ausgeblendet“ (unter „Sonstige“).  
💡 **Tipps:** Auf dem iPad musst du möglicherweise erst auf das Seitenleistensymbol oben links tippen, um deine Alben anzuzeigen.
3. Tippe auf „Album anzeigen“ und verwende dann Face ID oder Touch ID, um das ausgeblendete Album zu entsperren.
4. Lege den Finger auf das Foto oder Video, das wieder eingeblendet werden soll, und tippe dann auf „Einblenden“.

## Ausgeblendete Fotos auf dem Mac anzeigen

1. Öffne die App „Fotos“  auf deinem Mac.
2. Klicke in der Seitenleiste auf „Mediathek“ und wähle dann „Darstellung“ > „Fotoalbum ‚Ausgeblendet‘ einblenden“.  

Das Album „Ausgeblendet“ wird in der Seitenleiste unter „Sonstige“ angezeigt. Wenn das Album „Ausgeblendet“ gesperrt ist, verwende Touch ID oder gib dein Passwort ein, um es zu entsperren. Um das Album „Ausgeblendet“ auszublenden, wähle „Darstellung“ > „Fotoalbum ‚Ausgeblendet‘ ausblenden“.
3. Wähle die Fotos aus, die angezeigt werden sollen und wähle dann „Bild“ > „[number] Fotos einblenden“.

## Sammlung „Ausgeblendet“ auf dem iPhone oder iPad ein- oder ausblenden

Standardmäßig ist das Album „Ausgeblendet“ in der Sammlung „Sonstige“ sichtbar. Du kannst es jederzeit verbergen.

1. Wähle auf deinem iPhone oder iPad „Einstellungen“ > „Apps“ > „Fotos“.
2. Scrolle nach unten und führe beliebige der folgenden Schritte aus:
  - *Fotoalbum „Ausgeblendet“ in „Sonstige“ einblenden:* Aktiviere „Album ‚Ausgeblendet‘ einblenden“.
  - *Fotoalbum „Ausgeblendet“ ausblenden:* Deaktiviere „Album ‚Ausgeblendet‘ einblenden“.

Für das Entsperren des Albums „Ausgeblendet“ ist Face ID, Touch ID oder ein Code erforderlich. Diese Einstellung kannst du in den Einstellungen „Fotos“ ändern.

## Sammlung „Ausgeblendet“ auf dem Mac ein- oder ausblenden

Standardmäßig ist das Album „Ausgeblendet“ gesperrt und nicht in der Ansicht sichtbar. Du kannst auswählen, dass es in der Sammlung „Sonstige“ sichtbar gemacht wird, oder es jederzeit verbergen.

1. Öffne die App „Fotos“  auf deinem Mac.
2. Klicke in der Seitenleiste auf „Mediathek“ und führe beliebige der folgenden Schritte aus:
  - *Fotoalbum „Ausgeblendet“ in „Sonstige“ einblenden:* Wähle „Darstellung“ > „Fotoalbum ‚Ausgeblendet‘ einblenden“.
  - *Fotoalbum „Ausgeblendet“ ausblenden:* Wähle „Darstellung“ > „Fotoalbum ‚Ausgeblendet‘ ausblenden“.

Für das Entsperren des Albums „Ausgeblendet“ ist ein Passwort oder Touch ID erforderlich. Diese Einstellung kannst du in den Einstellungen „Fotos“ ändern.

## Warnungen vor sensiblen Bildern und Videos

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.



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

1. Führe einen der folgenden Schritte aus:

- *Auf iPhone oder iPad:* Wähle „Einstellungen“  > „Datenschutz & Sicherheit“  und tippe auf „Warnung vor sensiblen Inhalten“.
- *Auf dem Mac:* Wähle Menü „Apple“  > „Systemeinstellungen“, klicke in der Seitenleiste auf „Datenschutz & Sicherheit“  und dann auf „Warnung vor sensiblen Inhalten“.



2. Aktiviere „Warnung vor sensiblen Inhalten“.

Wenn „Warnung vor sensiblen Inhalten“ feststellt, dass du ein Foto oder Video erhalten hast, das womöglich Nacktheit enthält, wird das Foto weichgezeichnet, eine Warnung angezeigt, dass es sich um sensible Inhalte handeln könnte, und Möglichkeiten zur Hilfebeschaffung angezeigt.

## Nachweise zu einem anderen Apple Account erhalten

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>)

## Verdächtige Aktivitäten aufzeichnen

Wenn du belästigt worden bist und dir Sorgen über verdächtige Aktivitäten auf deinem Account oder Gerät machst, kannst du eine Bildschirmaufnahme der betroffenen Inhalte machen. Eine Bildschirmaufnahme bezeichnet ein Bild von dem, was auf dem Bildschirm deines Geräts angezeigt wird. Eine Bildschirmaufnahme kann auch ein Video von dem, was auf dem Bildschirm deines Geräts angezeigt wird, sein. Sie enthält sämtliches Audio, was zum Zeitpunkt der Aufnahme auf deinem Gerät wiedergegeben wird. Du kannst diese als Bild- oder Videodateien auf deinem iPhone, iPad oder Mac sichern.

Wenn du von Apple Informationen über das Konto einer anderen Person im Zusammenhang mit einem Stalking- oder Belästigungsfall anfordern möchtest, findest du weitere Informationen unter [Nachweise zu einem anderen Apple Account erhalten](#) weiter unten.



## 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-Command-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  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.

## Gerät auf die Werkseinstellungen zurücksetzen

Wenn du befürchtest, dass eine andere Person physischen Zugriff auf dein Gerät hatte, die eingebauten Sicherheitsfunktionen des Geräts manipuliert hat und bösartige Software, wie z. B. Stalkerware, installiert haben könnte, kannst du das Gerät auf seine Werkseinstellungen zurücksetzen. So kannst du sicherstellen, dass du die einzige Person bist, die auf dein Gerät zugreifen kann.

### **WICHTIG:**

- Das Zurücksetzen auf Werkseinstellungen löscht alle Inhalte und Einstellungen. Bevor du das Gerät auf die Werkseinstellungen zurücksetzt, solltest du die Sicherheitsprüfung der Option „[Teilen & Zugriff verwalten](#)“ (Option Zwei) ausführen. Die Probleme, um die du dir Sorgen machst, können auch mit Freigabeoptionen oder App-Zugriffen zusammenhängen, von denen du nicht wusstest, dass sie aktiv sind.
- Wenn du alle Inhalte und Einstellungen löschst, weil du befürchtest, dass dein Gerät manipuliert wurde und bösartige Software installiert wurde, solltest du kein Backup wiederherstellen. Die Wiederherstellung eines Backups kann dazu führen, dass die bösartige Software, die du entfernen möchtest, erneut installiert wird.

Das Zurücksetzen auf Werkseinstellungen:

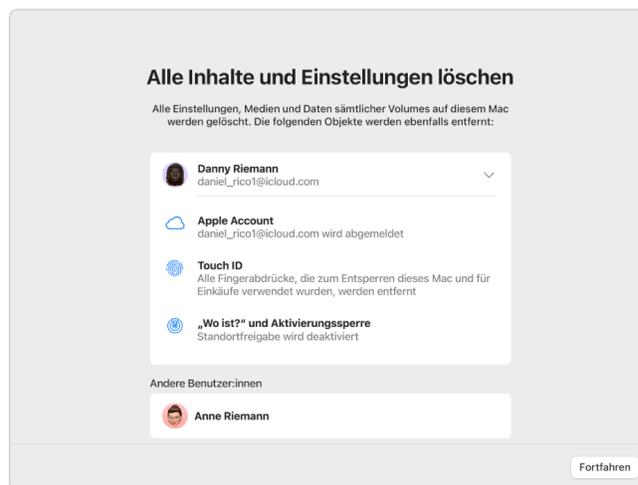
- Löscht alle Daten, die auf dem Gerät gespeichert sind, einschließlich den Daten für Face ID und Touch ID, den Code und Passwörtern, Nachrichten, E-Mails, Fotos, Dateien, Medien und mehr.
- Entfernt alle Apps, einschließlich Apps, die ohne dein Wissen installiert wurden.
- Setzt deine Datenschutzeinstellungen zurück, sodass dein Standort nicht mehr mit Personen oder Apps geteilt wird.
- Installiert die neueste Version des jeweiligen Betriebssystems (ganz egal, welche Version zuvor installiert war).



Anforderungen:

- Internetzugriff
- Gerätecode oder Passwort
- Apple Account-Passwort
- Zeit

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/102639)“ (<https://support.apple.com/102639>).



## Für iPhone und iPad

- Apple Support-Artikel [iPhone, iPad oder iPod mit einem Computer auf die Werkseinstellungen zurücksetzen](https://support.apple.com/108931) (<https://support.apple.com/108931>)

## Alle Inhalte und Einstellungen auf dem Mac löschen

- Lösche deinen Mac (macOS 12.0.1 oder neuer). Entferne deine Inhalte, Einstellungen und alle installierten Apps ohne macOS erneut zu installieren, damit zu ihn auf die Werkseinstellungen zurücksetzen kannst.
  - [Mac löschen](https://support.apple.com/guide/mac-help/mchl7676b710), um deine Inhalte (Apps, Daten) und Einstellungen (z. B. bevor du ihn verkaufst, eintauschst oder verschenkst) zu löschen (<https://support.apple.com/guide/mac-help/mchl7676b710>).
  - [macOS löschen und neuinstallieren](https://support.apple.com/guide/mac-help/mh27903) für einen Mac mit Apple Chips oder einem Intel-basierten Mac. (<https://support.apple.com/guide/mac-help/mh27903>)
- Apple Support-Artikel [Einen Mac mit Apple-Chip mithilfe des Festplattendienstprogramms löschen](https://support.apple.com/102506) (<https://support.apple.com/102506>)
- Apple Support-Artikel [Einen Intel-basierten Mac mithilfe des Festplattendienstprogramms löschen](https://support.apple.com/102639) (<https://support.apple.com/102639>)

# Bestimmte Apps und Funktionen

## Notruf tätigen oder Notfalltextnachricht auf dem iPhone oder der Apple Watch senden

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 „[Notfallpass einrichten und anzeigen](#)“ im iPhone – Benutzerhandbuch (<https://support.apple.com/guide/iphone/iph08022b192/>).

*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 [„Notfallpass einrichten und anzeigen“](https://support.apple.com/guide/iphone/iph08022b192) 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.

Notfallkontakte hinzufügen oder löschen:

1. Öffne die App „Health“  und tippe auf dein Profilbild.
2. Tippe auf „Notfallpass“.
3. Scrolle zu „Notfallkontakte“ und tippe dann auf „Bearbeiten“.
4. Füge einen Kontakt hinzu oder lösche ihn.
  - *Kontakt hinzufügen:* Tippe auf , um einen Notfallkontakt hinzuzufügen. (Der Rettungsdienst kann nicht als Notfallkontakt festgelegt werden.)
  - *Kontakt löschen:* Tippe auf  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 .

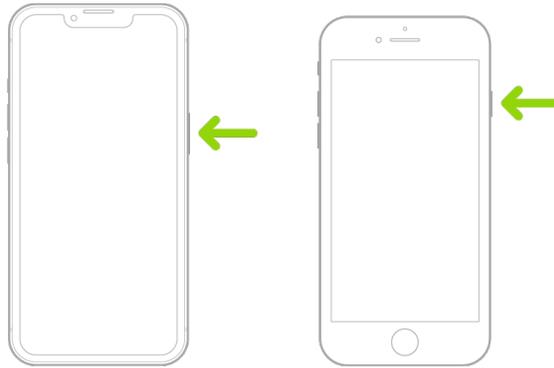
## „Notruf SOS“ auf dem iPhone verwenden (alle Länder und Regionen außer Indien)

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.

- 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 .

**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 , 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 , 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 verwenden](https://support.apple.com/101573) (https://support.apple.com/101573).

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

Weitere Informationen findest du unter [Wichtige Informationen über Notrufe auf dem iPhone](#) im iPhone – Benutzerhandbuch.

## Live-Videos oder vorhandene Fotos mit dem Rettungsdienst teilen (nicht in allen Ländern oder Regionen verfügbar)

Wenn dich der Rettungsdienst dazu auffordert, kannst du mit „Live-Video bei Notruf SOS“ Live-Video streamen oder vorhandene Fotos und Videos hochladen.

*Hinweis:* Der Rettungsdienst kann eine Kopie des gestreamten Live-Videos aufbewahren und von dir geteilte Videos oder Fotos behalten.

Wenn du während eines Notrufs eine Anfrage erhältst, Videos oder Fotos zu teilen, führe beliebige der folgenden Schritte aus:

- *Live-Video teilen:* Tippe auf „Teilen“, wenn du dazu aufgefordert wirst, um das Streamen eines Live-Videos mit dem Rettungsdienst zu beginnen. Du kannst die Freigabe jederzeit anhalten oder erneut starten, indem du auf die Kamerateaste tippst. Du kannst die Freigabe jederzeit beenden, indem du auf  tippst, und dann auf „Kamera nicht mehr teilen“ oder „Anruf beenden“ tippst.

*Hinweis:* Das Live-Video wird auf deinem Gerät nicht gesichert, aber kann vom Rettungsdienst gespeichert werden.

- *Vorhandene Fotos oder Videos teilen:* Tippe auf „Auswählen“, wenn du dazu aufgefordert wirst, und wähle dann die Fotos oder Videos aus, die du dem Rettungsdienst senden möchtest.
- *Ablehnen:* Tippe auf „Später“, wenn du dazu aufgefordert wirst, wenn du keine Videos oder Fotos mit dem Rettungsdienst teilen möchtest.

*Hinweis:* „Live-Video bei Notruf SOS“ ist auf dem iPhone 14 (oder neuer) verfügbar, abhängig von Geräteeinschränkungen, und möglicherweise nicht in allen Situationen verfügbar.

## Bildschirmfreigabe und Bildschirmsteuerung in FaceTime verwalten

Während eines FaceTime-Video- oder Audioanrufs mit einer anderen Person, kannst du deinen Bildschirm mit der Person teilen. Die Person kann auch fragen, ob sie deinen Bildschirm sehen darf. Nachdem du deinen Bildschirm geteilt hast, kann die Person fragen, ob sie deinen Bildschirm aus der Ferne steuern darf (oder du kannst es ihr erlauben).



### Wie kann ich erkennen, ob die Bildschirmfreigabe oder Bildschirmsteuerung aktiviert ist?

- **Bildschirmfreigabe:** Auf einem iPhone oder iPad wird  oben auf dem Bildschirm angezeigt. Du kannst auch auf den Bildschirm tippen, um die FaceTime-Steuerungen anzuzeigen, und dann überprüfen, ob „Zeigt meinen Bildschirm an“ unter dem Namen oder den Kontaktinformationen einer Person angezeigt wird.

Auf einem Mac wird  in der Menüleiste angezeigt.

- **Bildschirmsteuerung:** Auf einem iPhone oder iPad wird „Remotesteuerung aktiv“ unten auf dem Bildschirm angezeigt.

Auf einem Mac wird  in der Menüleiste angezeigt.

### Welche Zugriffsrechte hat die andere Person während der Bildschirmfreigabe?

Die Person, mit der du deinen Bildschirm teilst, kann:

- Die meisten Inhalte auf deinem Bildschirm sehen.
- Auf deinem Bildschirm tippen, zeichnen oder schreiben (der Kreis, die Zeichnung oder das Geschriebene verschwindet nach wenigen Sekunden).
- Remotesteuerung für dein Gerät anfordern (du kannst akzeptieren oder ablehnen).

Die Person, mit der du deinen Bildschirm teilst, *kann nicht*:

- Deine erhaltenen Mitteilungen anzeigen.
- Den Ziffernblock sehen, wenn du deinen Code eingibst. (Standardmäßig werden Codes und Passwörter als Punkte angezeigt.)
- Inhalte ansehen, für die ein Abonnement, ein kostenloses Probeabo oder ein Kauf bzw. eine Leihe für die Wiedergabe erforderlich ist.

## Welche Zugriffsrechte hat die andere Person während der Bildschirmsteuerung?

Die Person, die deinen Bildschirm aus der Ferne steuert, kann:

- Apps, Fenster oder Dateien öffnen und schließen.
- Einstellungen ändern.
- Objekte löschen.
- Nachrichten senden.
- Dein Gerät ausschalten oder deinen Mac neu starten (hierdurch wird der FaceTime-Anruf und die Bildschirmsteuerung beendet).

Die Person, die deinen Bildschirm aus der Ferne steuert, *kann nicht*:

- Einstellungen für deinen Apple Account oder Face ID ändern.
- Apple Pay verwenden. (Möglicherweise kann die Person Zahlungen mit Apps von Drittanbietern tätigen. Weitere Informationen findest du unter [Einführung in Apps von Drittanbietern](#).)
- Dein Gerät löschen.

Während einer Bildschirmsteuerungssitzung ist Face ID deaktiviert. Du kannst immer noch auf deinem Gerät navigieren, während dein Bildschirm aus der Ferne gesteuert wird. Deine Aktionen haben Priorität vor Remote-Aktionen.

### Bildschirmfreigabe beenden

- *iPhone oder iPad*: Tippe auf .
- *Mac*: Klicke auf  in der Menüleiste und klicke dann auf „Teilen stoppen“.

Durch das Beenden eines FaceTime-Anrufs wird auch die Bildschirmfreigabe beendet.

### Anfrage für Remotesteuerung ablehnen

Wenn du eine Anfrage für eine Remotesteuerung erhältst, die du ablehnen möchtest, tippe oder klicke auf „Nicht erlauben“. Die Bildschirmfreigabe wird fortgesetzt. Die andere Person erhält keine Mitteilung, dass du abgelehnt hast.

### Bildschirmsteuerung beenden

- *iPhone oder iPad*: Tippe unten auf dem Fenster der Bildschirmfreigabe auf „Stoppen“.
- *Mac*: Klicke auf  in der Menüleiste und klicke dann auf „Steuerung erlauben“. (Die Taste ist ausgegraut.)

Durch das Beenden eines FaceTime-Anrufs wird auch die Bildschirmsteuerung beendet.

## Teilen von Aktivitäten auf 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.



### Apple Watch zum Stoppen des Teilens verwenden

Im Tab „Teilen“ der Fitness-App kannst du deine Fortschritte verbergen oder die Freigabe für eine bestimmte Person vollständig beenden.

So stoppst du das Teilen der Aktivitätsringe mit einer Person auf deiner Apple Watch.

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:

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

## Sicherheitsprüfung zum Stoppen des Teilens von Informationen verwenden

Du kannst das Teilen der Aktivitätsringe mit einer Person mithilfe deines iPhone stoppen.



1. Öffne die App „Fitness“  auf deinem iPhone und tippe dann auf „Teilen“.
2. Tippe auf eine Person, mit der du teilst.
3. Tippe oben rechts auf die Taste „Teilen“.
4. Tippe entweder auf „Freund:in entfernen“ oder „Aktivität ausblenden“.

Weitere Informationen findest du unter:

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

# Sicheres AirDrop

## Was ist AirDrop?

Mit AirDrop  kannst du Bilder, Dokumente und andere Dateien unkompliziert auf verschiedenen Apple-Geräten in der Nähe teilen. Du kannst mit deinem Gerät Inhalte mit allen Personen in deiner Nähe teilen, das Teilen auf deine Kontakte beschränken oder mit niemandem teilen.

*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.



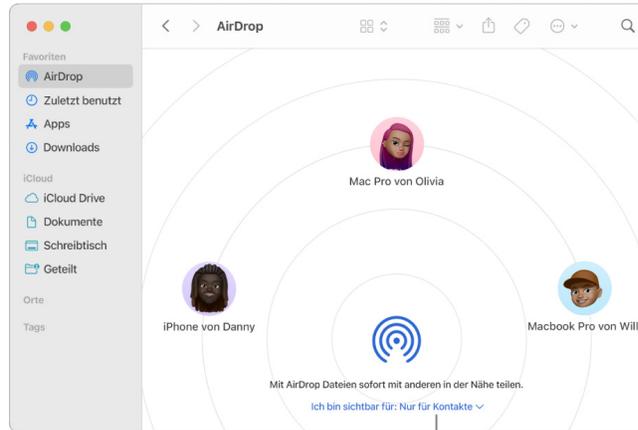
## iPhone oder iPad

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

## Auf einem Mac mit Finder



Steuern, wer dir Objekte schicken kann

1. Klicke im Dock auf das Finder-Symbol , 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.

Weitere Informationen findest du unter:

- [AirDrop zum Senden von Objekten an Apple-Geräte in der Nähe verwenden](#) im Mac – Benutzerhandbuch

(<https://support.apple.com/guide/mac-help/mh35868>)

## Auf einem Mac mit Kontrollzentrum



1. Klicke auf einem Mac auf  in der Menüleiste und klicke dann auf . Wenn es blau ist, ist es aktiviert.
2. Klicke auf  neben AirDrop und wähle deine bevorzugte Option aus.

Weitere Informationen findest du unter:

- [AirDrop zum Senden von Objekten an Apple-Geräte in der Nähe verwenden](#) im Mac – Benutzerhandbuch

(<https://support.apple.com/guide/mac-help/mh35868>)

## Kalenderfreigabeeinstellungen auf Apple-Geräten verwalten

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.

▼ **WICHTIG:** Wenn du einen Kalender löschst oder das Teilen eines Kalenders beendest, erhalten alle Teilnehmer:innen möglicherweise eine Mitteilung zu den Änderungen.



### Kalenderfreigabeeinstellungen auf dem iPhone oder iPad verwalten

1. Tippe auf „Kalender“  auf deinem iPhone oder iPad. Tippe dann auf  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“.

### Kalender auf dem Mac löschen

Manche Kalender können nicht gelöscht werden.

- Du kannst delegierte Kalender nicht löschen, aber du kannst sie im Hauptfenster von „Kalender“ ausblenden. Weitere Informationen findest du unter [Veröffentlichung eines Kalenders auf dem Mac stoppen](#).
- Wenn du einen Kalender für einen bestimmten Kalenderaccount nicht löschen kannst, kannst du den Kalender möglicherweise auf der Website des Accountanbieters löschen. Um beispielsweise einen Google-Kalender zu löschen, besuche [google.com](https://www.google.com/calendar).
- Wenn ein Kalenderaccount nur über einen Kalender verfügt (abgesehen von den geteilten Kalendern anderer Personen), kannst du diesen letzten Kalender nicht löschen.

1. Öffne die App „Kalender“  auf deinem Mac und klicke dann auf den Kalendernamen in der Kalenderliste.

Wenn die Kalenderliste links nicht angezeigt wird, wähle „Darstellung“ > „Kalenderliste einblenden“.

2. Wähle „Bearbeiten“ > „Löschen“.

Weitere Informationen findest du unter:

- [„Kalender auf dem Mac hinzufügen oder löschen“](#) im Kalender – Benutzerhandbuch (<https://support.apple.com/guide/calendar/icl1005>)

## Abonnement eines Kalenders auf dem Mac kündigen

Wenn du das Abonnement für den Kalender einer anderen Person beenden möchtest, kannst du das Abonnement kündigen.

- Öffne die App „Kalender“  auf deinem Mac, klicke bei gedrückter Control-Taste auf den Kalender in der Kalenderliste und klicke dann auf „Abo beenden“.

Wenn die Kalenderliste links nicht angezeigt wird, wähle „Darstellung“ > „Kalenderliste einblenden“.

*Hinweis:* Wenn du ein Kalenderabonnement kündigst, kannst du den Kalender auch als Spam melden. Das Melden von Spam hilft „Kalender“ dabei, Spam-Abonnements besser zu erkennen.

Weitere Informationen findest du unter:

- [„Kalender auf dem Mac abonnieren“](#) im Kalender – Benutzerhandbuch (<https://support.apple.com/guide/calendar/icl1022>)

## Veröffentlichung eines Kalenders auf dem Mac stoppen

Wenn deine Kalenderliste über den Bereich „Auf meinem Mac“ verfügt, kannst du einen Kalender in diesem Bereich auf einem WebDAV-Server, auf den du Zugriff hast, veröffentlichen. Andere Länder können deinen veröffentlichten Kalender abonnieren oder ihn in einem Webbrowser anzeigen. Du kannst die Veröffentlichung eines Kalenders jederzeit stoppen, ohne ihn von deinem Mac zu löschen.

*Hinweis:* Unveröffentlichte Kalender können nicht von deinem Mac gelöscht werden.

1. Öffne die App „Kalender“  auf deinem Mac und klicke auf den Namen oder der Gruppe des Kalenders in der Kalenderliste.

Wenn die Kalenderliste links nicht angezeigt wird, wähle „Darstellung“ > „Kalenderliste einblenden“. Ein veröffentlichter Kalender hat  neben seinem Namen.

2. Wähle „Bearbeiten“ > „Veröffentlichen stoppen“.

Nachdem du die Veröffentlichung eines Kalenders gestoppt hast, können neue Benutzer:innen ihn nicht mehr abonnieren. Benutzer:innen, die ihn bereits abonniert haben, können nur die zuletzt veröffentlichte Kopie sehen, bis sie ihn selbst löschen.

Weitere Informationen findest du unter:

- [„Kalender veröffentlichen oder Veröffentlichung auf dem Mac widerrufen“](#) im Kalender – Benutzerhandbuch (<https://support.apple.com/guide/calendar/icl1017>)

## Teilen eines iCloud-Kalenders auf dem Mac beenden

Wenn du [auf deinem Mac iCloud eingerichtet hast](#), kannst du „Kalender“ verwenden, um deine geteilten iCloud-Kalender zu verwalten. Wenn du einen iCloud-Kalender teilst oder dem geteilte iCloud-Kalender einer anderen Person beitredest, erhältst du möglicherweise eine E-Mail, wenn der geteilte Kalender aktualisiert wird. Du kannst einstellen, dass du diese E-Mails nicht mehr erhalten möchtest, indem du eine Einstellung in den Einstellungen „Kalender“ auf iCloud.com änderst.

Wenn du eine Einladung für einen auf iCloud geteilten Kalender erhältst, kannst du die Einladung auf deinem iPhone, iPad oder Mac annehmen, auf dem du mit demselben Apple Account angemeldet bist oder unter „Kalender“ in iCloud oder unter iCloud.com.

1. Öffne die App „Kalender“  auf deinem Mac.

Wenn die Kalenderliste links nicht angezeigt wird, wähle „Darstellung“ > „Kalenderliste einblenden“.

2. Führe beliebige der folgenden Schritte aus:

- *Teilen deines Kalenders mit bestimmten Personen beenden:* Positioniere den Zeiger über den Kalendernamen in der Kalenderliste und klicke dann auf . Klicke auf den Namen einer Person und drücke dann die Rückschritttaste.
- *Teilen des Kalenders mit allen Personen beenden:* Klicke mit gedrückter Control-Taste auf den Kalender in der Kalenderliste und wähle dann „Nicht mehr teilen“.
- *Abonnement für den Kalender einer anderen Person beenden:* Klicke mit gedrückter Control-Taste auf den Kalender in der Kalenderliste und wähle dann „Abo beenden“.

Wenn du ein Kalenderabonnement kündigst, kannst du den Kalender auch als Spam melden. Das Melden von Spam hilft „Kalender“ dabei, Spam-Abonnements besser zu erkennen.

Weitere Informationen findest du unter:

- [„Benachrichtigungen zu Kalendern auf iCloud.com erhalten“](#) im Kalender – Benutzerhandbuch

(<https://support.apple.com/guide/icloud/mm8074582205>)

## Familienfreigabegruppe verlassen oder ein Mitglied daraus entfernen

Die Familienfreigabe kann von bis zu fünf Familienmitgliedern genutzt werden, um Abonnements, Käufe, Fotos, Fotoalben, einen Kalender und mehr zu teilen, ohne die Apple Accounts der anderen Familienmitgliedern zu teilen. Wenn du einen iCloud-Speicherplan 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.

Überprüfe, ob du Teil einer Familienfreigabegruppe bist. Wähle dazu „Einstellungen“  > [dein Name] > „Familie“. Wenn „Familienfreigabe einrichten“ angezeigt wird, verwendest du die Familienfreigabe nicht mit diesem Apple Account. Wenn du das Symbol „Familienfreigabe“ siehst, kannst du auf es tippen, um deine Familienmitglieder und ihre Rollen zu sehen.



### Wer kann eine Familienfreigabegruppe verlassen?

Die Fähigkeit eine Familienfreigabegruppe zu ändern oder zu verlassen variiert.

- Organisator:innen können eine Familienfreigabegruppe verlassen, indem sie die Familienfreigabe deaktivieren. Wenn die Familienfreigabe deaktiviert wird, werden alle Familienmitglieder gleichzeitig aus der Familiengruppe entfernt. Wenn Kinder unter 13 Jahren Teile der Familiengruppe sind, muss der:die Organisator:in sie zu einer anderen Familienfreigabegruppe bewegen. Familienmitglieder haben keinen Zugriff mehr auf Abonnements, Käufe und andere Dienste, die durch die Familienfreigabe aktiviert werden.
- Alle Familienmitglieder, die älter als 13 Jahre sind, können sich selbst jederzeit aus einer Familiengruppe entfernen. Wähle einfach deinen Namen aus und wähle dann „Familie verlassen“. Du kannst dich auch bei der Apple Account-Website anmelden und „Account entfernen“ im Bereich „Familienfreigabe“ auswählen.
- Aus Sicherheitsgründen können Kinder (unter 13 Jahre) nicht aus einer Familie entfernt werden und die Freigabe von Informationen wie der Bildschirmzeit kann nicht ohne Eingabe des Bildschirmzeit-Codes beendet werden. Organisator:innen können auf geteilte Inhalte auf deinem Gerät zugreifen – darunter geteilte Fotoalben und geteilte Kalender – und deine Bildschirmzeit-Aktivitäten einsehen.

## 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.



Wenn du deinen Familienfreigabestatus ändern möchtest, ist es empfehlenswert, die Funktionen der verschiedenen Rollen in einer Familienfreigabegruppe zu kennen.

- *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, wenn in der Gruppe auch Kinder oder Teens Mitglied sind.
- *Kind oder Teen:* Ein Mitglied einer Familienfreigabegruppe, das unter 18 Jahre alt ist. Organisator:innen, Eltern oder Erziehungsberechtigte können einen Apple Account für Kinder erstellen, die zu jung sind, um diesen 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, die einen Apple Account haben, zur Familie hinzufügen und alle Personen ab 13 Jahren aus der Familiengruppe entfernen.

## Was passiert, wenn du eine Familienfreigabegruppe verlässt

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 Gerätestandorte von ehemaligen Familienmitgliedern werden nicht mehr in der App „Wo ist?“ auf iCloud.com oder auf deinen Mac, iPhone oder iPad angezeigt.
- Die Objekte ehemaliger Familienmitglieder werden nicht mehr im Bereich „Käufe“ im iTunes Store, App Store und in Apple Books angezeigt.
- Früher geladene Musiktitel, Filme, TV-Sendungen, Bücher und Apps können nicht mehr genutzt werden, wenn sie ursprünglich von einer anderen Person gekauft wurden. Ehemalige Familienmitglieder können diese aus deiner Sammlung geladenen Inhalte nicht mehr nutzen.
- In-App-Käufe sind nicht mehr verfügbar, 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.

## Familienfreigabegruppe auf dem iPhone oder iPad mit iOS 18 oder iPadOS 18 (oder neuer) verlassen

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

1. Wähle „Einstellungen“  > „Familie“ (unter deinem Namen).
2. Tippe auf deinen Namen und tippe dann auf „Nutzung der Familienfreigabe beenden“.

## Familienfreigabegruppe auf dem iPhone oder iPad mit iOS 17 oder iPadOS 17 (oder älter) verlassen

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

1. Wähle „Einstellungen“  > „[dein Name]“ > „Familienfreigabe“.
2. Tippe auf deinen Namen und tippe dann 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“  > „Systemeinstellungen“ und klicke dann in der Seitenleiste auf „Familie“ (unter deinem Namen).
  - Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Familienfreigabe“  und klicke dann auf „Familienfreigabe“.
2. Klicke in der Liste der Familienmitglieder auf deinen Namen oder 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 mit iOS 18 oder iPadOS 18 (oder neuer) deaktivieren**

Wenn du der:die Familienorganisator:in bist:

1. Wähle „Einstellungen“  > „Familie“ (unter deinem Namen).
2. Tippe auf deinen Namen und tippe dann auf „Nutzung der Familienfreigabe beenden“.

## **Familienfreigabe auf dem iPhone oder iPad mit iOS 17 oder iPadOS 17 (oder älter) deaktivieren**

Wenn du der:die Familienorganisator:in bist:

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

## **Familienfreigabe auf dem Mac deaktivieren**

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“  > „Systemeinstellungen“ und klicke dann in der Seitenleiste auf „Familie“ (unter deinem Namen).
  - Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Familienfreigabe“  und klicke dann auf „Familienfreigabe“.
2. Klicke auf  neben deinem Namen und klicke auf „Familienfreigabe beenden“.

## **Mitglieder aus einer Familienfreigabegruppe auf dem iPhone oder iPad mit iOS 18 oder iPadOS 18 (oder neuer) entfernen**

Wenn du der:die Familienorganisator:in bist:

1. Wähle „Einstellungen“  > „Familie“ (unter deinem Namen).
2. Tippe auf „[Name des Mitglieds]“, tippe auf „[Name des Mitglieds] aus Familie entfernen“ und dann erneut auf „[Name des Mitglieds] aus Familie entfernen“.

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

## **Mitglieder aus einer Familienfreigabegruppe auf dem iPhone oder iPad mit iOS 17 oder iPadOS 17 (oder älter) 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 Familienfreigabegruppe entfernen.

## Mitglieder auf dem Mac aus einer Familienfreigabegruppe entfernen

Wenn du der:die Familienorganisator:in bist:

### 1. Familienfreigabegruppe öffnen:

- Auf einem Mac mit macOS 13 oder neuer: Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke dann in der Seitenleiste auf „Familie“ (unter deinem Namen).
- Auf einem Mac mit macOS 12 oder älter: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke auf „Familienfreigabe“  und klicke dann auf „Familienfreigabe“.

### 2. Mitglied auswählen und entfernen:

- Auf einem Mac mit macOS 13 oder neuer: Wähle das Mitglied in der Liste aus, klicke auf „[Name des Mitglieds] aus Familienfreigabegruppe entfernen“ und dann erneut auf „[Name des Mitglieds] entfernen“.
- Auf einem Mac mit macOS 12 oder älter: Wähle das Mitglied aus der Liste aus, klicke auf — und bestätige dann durch Klicken, dass das Mitglied entfernt werden soll.

## Daten in iCloud sicher speichern

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, Fotos, Kalender, Standorte und mehr mit Freund:innen und Familienmitgliedern zu teilen. Mit deinem Apple Account 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 dem Mac*: Wähle Menü „Apple“  > „Systemeinstellungen“, klicke oben in der Seitenleiste auf deinen Namen und klicke 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 dann auf „Abmelden“.
- *Auf dem Mac*: Wähle Menü „Apple“  > „Systemeinstellungen“ und klicke oben in der Seitenleiste auf deinen Namen, scrolle nach unten und tippe dann auf „Abmelden“.

## 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.

Führe einen der folgenden Schritte aus:

- *Auf iPhone oder iPad:* Wähle „Einstellungen“  > „Nachrichten“ und aktiviere oder deaktiviere dann iMessage.
- *Auf dem Mac:* 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“.

### Nachrichten in iCloud auf dem iPhone oder iPad deaktivieren

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

1. 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 [Gerät] 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. Öffne die App „Nachrichten“  auf deinem Mac, wähle „Nachrichten“ > „Einstellungen“ und klicke dann auf „iMessage“.
2. Klicke auf „Einstellungen“ und hebe dann die Auswahl von „Nachrichten in iCloud aktivieren“ auf.
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](https://support.apple.com/guide/icloud/mm0de0d4528d)“ 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 dem Mac:* 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 wähle dann „Lesebestätigungen senden“ aus oder hebe die Auswahl auf.
- *Auf einem Mac mit macOS 12 oder älter:* Öffne „Nachrichten“ , wähle „Nachrichten“ > „Einstellungen“, klicke auf den Tab „iMessage“ und wähle dann „Lesebestätigungen senden“ aus oder hebe die Auswahl auf.

## 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 dem Mac:* Öffne „Nachrichten“ , klicke bei gedrückter Control-Taste 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 dem Mac:* Öffne „Nachrichten“ , klicke bei gedrückter Control-Taste 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.

## Betrügerische Anfragen zum Teilen von Informationen erkennen

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 deinen Apple Account, dein Passwort oder einen Verifizierungscode für die Zwei-Faktor-Authentifizierung preiszugeben.

Tipps dazu, wie du verhindern kannst, dass deine Accounts oder persönlichen Informationen kompromittiert werden, findest du im Apple Support-Artikel „[Social-Engineering-Schemata wie Phishing-Nachrichten, gefälschte Support-Anrufe 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.

## Anrufe und Nachrichten von bestimmten Personen blockieren

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 demselben Apple Account 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 ⓘ 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 ⓘ 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 Control-Taste 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 ⓘ, scrolle nach unten und tippe auf „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 „Konversation“ aus und klicke dann auf „Blockieren“.
- *In der App „Mail“ auf iPhone oder iPad:* Wähle in der App „Mail“ 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:* Wähle in der App „Mail“ eine E-Mail von einer Person aus, die du blockieren möchtest, klicke auf den Pfeil neben ihrem Namen oben in der E-Mail und wähle „Diesen 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 unter „Anrufe“ auf „Blockierte Kontakte“.
- *In der App „FaceTime“ auf dem Mac:* Öffne die App „FaceTime“, wähle „FaceTime“ > „Einstellungen“ in der Menüleiste 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“.

## Anruf auf dem iPhone aufnehmen und transkribieren

In einigen Ländern und Regionen kannst du einen Audio-Telefonanruf aufnehmen. Wenn eine Person eine Aufnahme startet, erhalten beide Teilnehmer:innen einen Audiohinweis, dass der Anruf aufgenommen wird. Der Audiohinweis wird während des Anrufs regelmäßig erneut abgespielt. Du kannst eine Person nicht daran hindern, einen Anruf aufzunehmen, aber du kannst die Aufnahme stoppen, indem du den Anruf beendest.

Die Anrufaufnahme ist nur in [bestimmten Regionen und Sprachen](#) verfügbar. Für die Person, die den Anruf tätigt, muss die Funktion jedoch verfügbar sein

⚠️ **WICHTIG:** Es kann Apps von Drittanbietern geben (Apps die nicht von Apple erstellt wurden), die einer Person erlauben, deinen Telefonanruf aufzunehmen, und dich möglicherweise nicht darauf hinweisen.



### Anruf aufnehmen

Bevor du beginnst, musst du sicherstellen, dass die andere am Telefonat teilnehmende Person damit einverstanden ist, aufgezeichnet zu werden.

1. Öffne die App „Telefon“  auf deinem iPhone.
2. Tätige einen Anruf.
3. Tippe während des Anrufs auf .

Beide Anrufteilnehmer:innen erhalten einen Audiohinweis, dass der Anruf aufgenommen wird.

4. Wenn du die Aufnahme beenden möchtest, tippe auf  oder leg einfach auf.

Anrufaufnahmen werden automatisch im Ordner „Anrufaufnahmen“ in der App „Notizen“ gesichert.

## Auf eine Anrufaufnahme oder ein Transkript zugreifen

Von dir initiierte Anrufaufnahmen werden automatisch im Ordner „Anrufaufnahmen“ in der App „Notizen“ gesichert. In [ausgewählten Regionen und Sprachen](#) kannst du auch ein Transkript eines aufgenommenen Anrufs anzeigen. Das Transkript ist möglicherweise nicht sofort verfügbar. Dann wird eine Nachricht angezeigt, dass die Transkription noch verarbeitet wird.

*Hinweis:* Überprüfe die Richtigkeit eines Transkripts, bevor du dich darauf verlässt. Möglicherweise ist es keine exakte Repräsentation der Konversation.

1. Öffne die App „Notizen“  auf deinem iPhone.
2. Wähle eine Notiz im Ordner „Anrufaufnahmen“ aus und führe dann einen der folgenden Schritte aus:
  - *Aufnahme wiedergeben:* Tippe auf .
  - *Transkript anzeigen:* Tippe auf „Transkript“.
  - *Audioaufnahme und Transkript sichern oder löschen:* Tippe auf  und wähle dann eine Option aus.

## Anrufaufnahme stoppen

Wenn du nicht möchtest, dass ein Anruf aufgenommen wird, führe einen der folgenden Schritte aus:

- Die Person, die die Aufnahme initiiert hat, kann sie durch Tippen auf  beenden. Eine Nachricht wird abgespielt, die darauf hinweist, dass die Anrufaufnahme beendet wurde.
- Beide Anrufteilnehmer:innen können den Anruf durch Tippen auf  beenden.

*Hinweis:* Alles, was bis dahin aufgenommen wurde, wird automatisch in der App „Notizen“ der Person, die die Aufnahme begonnen hat, gesichert.

## „Anrufaufnahme“ auf dem iPhone deaktivieren

Die Anrufaufnahme ist standardmäßig verfügbar, aber du kannst sie als Option entfernen. Hierdurch kannst du keine Anrufe aufnehmen, aber andere Personen werden nicht daran gehindert, einen Anruf mit dir aufzunehmen.

1. Wähle „Einstellungen“  > „Apps“ > „Telefon“.
2. Tippe auf „Anrufaufnahme“ und deaktiviere dann „Anrufaufnahme“.

Veröffentlicht: 31. März 2025

# Sicheres NameDrop

## Was ist NameDrop?

NameDrop (Teil von AirDrop) erlaubt Benutzer:innen vom iPhone und der Apple Watch ihre Kontaktinformationen zu teilen, indem sie einfach ihre Geräte aneinanderhalten. Du kannst die bestimmten Kontaktinformationen, die du teilen möchtest und welche Informationen du nicht teilen möchtest, auswählen.

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

*Hinweis:* Für NameDrop ist iOS 17.1 oder watchOS 10.1 (oder neuer) auf beiden Geräten erforderlich. NameDrop wird auf der Apple Watch SE (2. Generation), Apple Watch Series 7 (und neuer) und auf Apple Watch Ultra-Modellen unterstützt.



## 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). 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.

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 über NameDrop teilen möchtest.

Weitere Informationen findest du unter:

- [Kontakt Daten und Foto auf dem iPhone hinzufügen oder bearbeiten](https://support.apple.com/guide/iphone/iph18b749db1) im iPhone – Benutzerhandbuch  
(<https://support.apple.com/guide/iphone/iph18b749db1>)
- [Kontakt Daten und Foto auf dem iPad hinzufügen oder bearbeiten](https://support.apple.com/guide/ipad/ipadfcfa2d42) im iPad – Benutzerhandbuch  
(<https://support.apple.com/guide/ipad/ipadfcfa2d42>)

## Kontaktinformationen teilen

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.

Weitere Informationen findest du unter:

- [NameDrop auf dem iPhone zum Teilen deiner Kontaktinformationen verwenden](https://support.apple.com/guide/iphone/iph1b6c664b7) im Apple Watch – Benutzerhandbuch  
(<https://support.apple.com/guide/iphone/iph1b6c664b7>)
- [NameDrop auf der Apple Watch zum Teilen deiner Kontaktinformationen verwenden](https://support.apple.com/guide/watch/apd46c6e11cf) im Apple Watch – Benutzerhandbuch  
(<https://support.apple.com/guide/watch/apd46c6e11cf>)

## NameDrop deaktivieren

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

## Fotofreigabeeinstellungen auf Apple-Geräten verwalten

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 auch die Freigabeeinstellungen jederzeit ändern. Wenn du die Freigabe für ein Foto oder Album für eine Person beendest, wird ihr Zugriff auf das geteilte Album und seine Inhalte 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.



Weitere Informationen dazu, mit wem du Inhalte von deinem Mac teilst und die Freigabe verwaltest, findest du unter [Sicher steuern, mit wem Inhalte vom Mac geteilt werden](#) weiter unten.

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



1. Wähle ein geteiltes Album auf deinem iPhone oder iPad aus und tippe dann auf „Personen einladen“.
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“.
  - *Dich selbst aus deinem geteilten Album entfernen:* Führe einen der folgenden Schritte aus:
    - Tippe oben rechts auf die Ellipse und dann auf „Abo beenden“.
    - Tippe oben rechts auf das iCloud-Accountsymbol und dann auf „Abo beenden“.
  - *Mitteilungen deaktivieren:* Streichen, um Mitteilungen zu deaktivieren.

Weitere Informationen findest du unter:

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

## Einstellungen für die geteilte iCloud-Fotomediathek auf dem iPhone oder iPad verwalten

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.

Teilnehmer können eine geteilte Mediathek jederzeit verlassen.

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“.

- Wähle „Einstellungen“  > „Fotos“ > „Geteilte Mediathek“ und führe beliebige der folgenden Schritte aus:

- *Teilnehmer:innen aus einer geteilten Mediathek entfernen:* Tippe auf „Teilnehmer:innen löschen“.
- *Geteilte Mediathek verlassen:* 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.

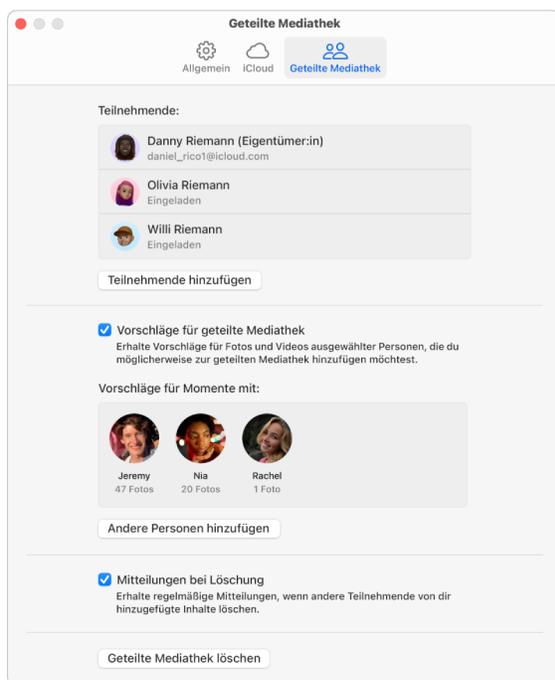
- *Geteilte Mediathek löschen (du musst ihre Organisator:in sein):* Tippe auf „Geteilte Mediathek löschen“.

Alle Teilnehmer werden benachrichtigt, dass die geteilte Mediathek gelöscht wurde.

Weitere Informationen findest du unter:

- [„Geteilte iCloud-Fotomediathek in der App „Fotos“ auf dem iPhone einrichten oder dazu beitreten“](#) im iPhone – Benutzerhandbuch  
(<https://support.apple.com/guide/iphone/iph28ac9ea81>)
- [„Geteilte iCloud-Fotomediathek in der App „Fotos“ auf dem iPad einrichten oder dazu beitreten“](#) im iPad – Benutzerhandbuch  
(<https://support.apple.com/guide/ipad/ipad94c5ed43>)

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



1. Öffne die App „Fotos“ 📷 auf deinem Mac. Klicke dann auf ein geteiltes Album unter „Geteilte Alben“ in der Seitenleiste.
2. Klicke auf 👤 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?](https://support.apple.com/guide/photos/pht7a4c765b) im Fotos-Benutzerhandbuch (https://support.apple.com/guide/photos/pht7a4c765b)
- [In einem geteilten Album Personen hinzufügen und entfernen](https://support.apple.com/guide/photos/phtdfcac5c5/) im „Fotos“ – Benutzerhandbuch (https://support.apple.com/guide/photos/phtdfcac5c5/)

## Teilnehmer:innen aus einer geteilten iCloud-Fotomediathek auf dem Mac entfernen

*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.

Ist eine Person seit weniger als 7 Tagen Teilnehmer:in an der geteilten Mediathek, kann sie nur die Objekte abrufen, die sie selbst beigetragen hat.

1. Wähle in der App „Fotos“  auf deinem Mac „Fotos“ > „Einstellungen“ und klicke auf „Geteilte Mediathek“.
2. Klicke auf  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>)

## Geteilte iCloud-Fotomediathek in der App „Fotos“ auf dem Mac verlassen oder löschen

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>)

## Geteilte Tabgruppen in Safari verwalten

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



### Geteilte Tabgruppen in Safari auf dem iPhone oder iPad verwalten

Wenn die Taste „Zusammenarbeiten“ nicht angezeigt wird, hast du keine geteilten Tabgruppen.

1. Tippe auf „Safari“  und dann rechts oben auf .
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 weiteren 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>)

## Geteilte Tabgruppen in Safari auf dem Mac verwalten

Wenn die Taste „Zusammenarbeiten“ nicht angezeigt wird, hast du keine geteilten Tabgruppen.

1. Klicke in der App „Safari“  auf deinem Mac auf  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 weiteren 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>)

## Browserverlauf in Safari und „Karten“ schützen

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 14 (oder neuer) 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 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.



### Browserverlauf löschen

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

## Letzte 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 favorisierten Ort, der gelöscht werden soll, von rechts nach links oder tippe auf „Bearbeiten“ und dann auf , 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 Control-Taste 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“  und tippe dann auf .
2. Tippe auf  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  und tippe auf , 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  und streiche auf den Tabs, die du schließen möchtest, nach links.

## Privates Fenster auf dem iPad öffnen

- Tippe in der App „Safari“ auf  und dann auf „Privat“.

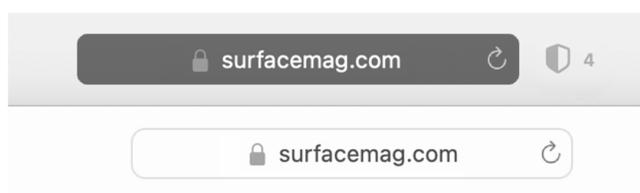
Wenn der Modus „Privates Surfen“ aktiviert ist, hat das Suchfeld keinen schwarzen, sondern einen weißen Hintergrund. Die Webseiten, die du besuchst, werden nicht im Verlauf auf dem iPad oder in der Tabliste auf anderen Geräten angezeigt. Du kannst mehrere private Tabs in der privaten Tabgruppe öffnen.

Wenn du die Webseiten ausblenden und den Modus „Privates Surfen“ beenden möchtest, tippe auf  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

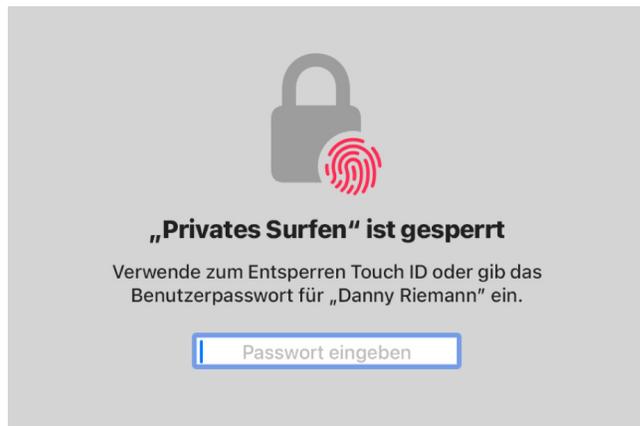
1. Wähle in der App „Safari“  „Ablage“ > „Neues privates Fenster“ oder wechsle zu einem Safari-Fenster, das bereits den Modus „Privates Surfen“ verwendet.

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



2. Du kannst so surfen wie gewohnt.

*Hinweis:* Wenn dein Gerät gesperrt oder im Ruhemodus ist oder wenn du Safari nicht aktiv verwendest, wird dein privates Fenster in Safari gesperrt. Wenn du dein Gerät entsperrst oder aus dem Ruhemodus holst oder wenn du Safari erneut verwendest, entsperre einfach dein privates Fenster mit Face ID, Touch ID oder deinem Gerätecode oder Passwort.



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

## Einstellungen für „Mit dir geteilt“ auf Apple-Geräten 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.



### Auf dem iPhone oder iPad nach Personen verwalten

Wenn du nicht möchtest, dass in der App „Nachrichten“ geteilte Inhalte in anderen 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:

- „[Inhalte in der App „Nachrichten“ teilen](https://support.apple.com/guide/iphone/iphb66cfeaad)“ im iPhone – Benutzerhandbuch (<https://support.apple.com/guide/iphone/iphb66cfeaad>)
- „[Inhalte in der App „Nachrichten“ teilen](https://support.apple.com/guide/ipad/ipad5bf3d77b)“ im iPad – Benutzerhandbuch (<https://support.apple.com/guide/ipad/ipad5bf3d77b>)

## Auf dem Mac nach Personen verwalten

Wenn du nicht möchtest, dass in der App „Nachrichten“ geteilte Inhalte in anderen Apps angezeigt werden, kannst du diese Funktion für einzelne Personen deaktivieren.

1. Öffne die App „Nachrichten“  auf dem Mac und wähle die Konversation aus.
2. Klicke auf ⓘ in oben rechts in der Konversation und hebe die Auswahl von „In ‚Mit dir geteilt‘ anzeigen“ auf, um geteilte 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:

- [Geteilte Inhalte in der App „Nachrichten“ auf dem Mac verfolgen](#) im Mac – Benutzerhandbuch

(<https://support.apple.com/guide/messages/ichtdc9ebc32>)

## Auf dem iPhone oder iPad nach App 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.

## Auf dem Mac nach App 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.

1. Öffne die App „Nachrichten“  auf deinem Mac.
2. Wähle „Nachrichten“ > „Einstellungen“.
3. Wähle „Mit dir geteilt“ und führe einen der folgenden Schritte aus:
  - *Alle Apps deaktivieren:* Klicke auf „Deaktivieren“.
  - *Ausgewählte Apps deaktivieren:* Hebe die Auswahl der Markierungsfelder neben den entsprechenden Apps auf.

Weitere Informationen findest du unter:

- [Geteilte Inhalte in der App „Nachrichten“ auf dem Mac verfolgen](#) im Mac – Benutzerhandbuch

(<https://support.apple.com/guide/messages/ichtdc9ebc32>)

# Zusätzliche Informationen

## Sicherheitshinweise

Bevor du Änderungen vornimmst oder Informationen löschst, bedenke Folgendes:

- Möglicherweise willst du verdächtige Aktivitäten aufzeichnen. Weitere Informationen findest du auch unter [Nachweise zu einem anderen Apple Account erhalten](#).
- Wenn du Änderungen an der Freigabe oder Zugriffen vornimmst, können diese von anderen Personen nachverfolgt werden. Suche im Handbuch nach diesem Symbol, um Informationen zur Sicherheit zu erhalten, die du möglicherweise beachten möchtest, bevor du aktiv wirst: .
- Wenn du eine Freigabebeziehung veränderst, kannst du den Zugriff auf Werkzeuge und Informationen verlieren, die wichtig für dich sein könnten.
- Apps, die von anderen Unternehmen entwickelt wurden (wie z. B. YouTube oder Instagram) verfügen über eigene Einstellungen, die Apple nicht steuern kann. Sieh dir die Anleitung jeder einzelnen App an, um zu überprüfen und zu verwalten, ob diese Apps Mitteilungen senden, wenn die Einstellungen verändert werden. Weitere Informationen findest du unter [Einstellungen für Apps von Drittanbietern](#).

## Weitere Ressourcen für die Technologiesicherheit

Wenn du weitere Informationen oder Unterstützung für die Technologiesicherheit benötigst, kannst du die folgenden Websites besuchen.

### USA

- [The Safety Net Project](#) at the National Network to End Domestic Violence
- [National Center for Victims of Crime](#)

### Vereinigtes Königreich

- [Refuge UK](#)

### Australien

- [WESNET Safety Net Australia](#)

## Weitere Support-Ressourcen

Bei anderen Bedenken, die Apple betreffen, beachte die folgenden Ressourcen.

### Apple Support

Allgemeine Assistenz bei Problemen mit Apple mithilfe von Selbsthilferessourcen oder durch die Verbindung mit Expert:innen. Apple Support verfügt mit deiner expliziten Erlaubnis über einen stark begrenzten Zugriff auf deine Informationen und hat keinen Zugriff auf deine Daten und/oder Passwörter.

- [Apple Support](https://support.apple.com) (https://support.apple.com)
- US – 1-800-275-2273; In Kanada – 1-800-263-3394

### Sicherheit der Apple-Plattformen

Für Informationen über Hardware und Systemsicherheit, Verschlüsselungs- und Datenschutz sowie Sicherheit bei Diensten – einschließlich Apple Account, iCloud, „Mit Apple anmelden“, Apple Pay, „Nachrichten“, FaceTime und „Wo ist?“ – findest du unter [Sicherheit der Apple-Plattformen](#).

### Apple Datenschutz

Entdecke die Website zum [Apple Datenschutz](#) mit weiteren Funktionen, die deine Daten und Einstellungen schützen und die du selbst steuern kannst, überprüfe Informationen zu Apps sowie Transparenzberichte für Regierungsanfragen und mache dich mit den Apple Datenschutzrichtlinien vertraut.

### Deine Daten und Datenschutz

Melde dich im [Web-Portal für Daten und Datenschutz](#) mit deinem Apple Account an, um mehr darüber zu erfahren, was Apple sammelt, eine Kopie deiner Daten zu erhalten oder zu übertragen und deine Daten zu korrigieren, zu deaktivieren oder zu löschen.

### Apple Support Community

Suche in der [Apple Support Community](#) nach Antworten und stelle Fragen an andere Kund:innen von Apple (global).

# Urheberrechte und Marken

Copyright © 2025 Apple Inc. Alle Rechte vorbehalten.

Die Verwendung des über die Tastatur erzeugten Apple-Logos (Option-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 Wallet, Apple Watch, Apple Watch SE, Apple Watch Series, Apple Watch Ultra, Digital Crown, Face ID, FaceTime, FileVault, Finder, Find My, HomeKit, HomePod, HomePod mini, iMessage, iPad, iPadOS, iPad Pro, iPhone, iTunes, Launchpad, Lightning, Mac, MacBook, MacBook Air, MacBook Pro, macOS, Magic Keyboard, Magic Mouse, Magic Trackpad, NameDrop, OS X, Safari, Siri und Touch ID sind Marken der Apple Inc., die in den USA und weiteren Ländern und Regionen eingetragen sind.

App Store, iCloud, iCloud+, iCloud Keychain 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 Namen und Logos von Produkten und Herstellern 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.

D028-00805