Sicherheitsempfehlungen für Apple IOS 14

Zusammenfassung

Folgende Empfehlungen sollten beachtet werden.

Diese Anleitung richtet sich besonders an folgende Zielgruppen:

- **Studierende**
- **Zweit- und Gasthörende**
- **Lehrende**
- **Mitarbeitende**
- **Einrichtungen und Gremien (z.B. Fachschaftsräte)**
- **Arbeitsbereiche / Gruppen (z.B. Projekte)**
- **Sekretariate**
- **Gäste der Friedrich-Schiller-Universität**

Auf dieser Seite sind Informationen zu folgenden Themen zu finden:

- Aufladen nur per Ladegerät
- Apple ID
- Exchange Account
- Ortungsdienste
- Passwortschutz
- Siri konfigurieren
- Diagnose- & Nutzungsdaten
- VPN
- Anwendungen
- Updates
- Datensicherung
- Sicheres Löschen
- Vorgehen bei Verlust

Aufladen nur per Ladegerät

Das iOS-Gerät sollte, außer bei einer geplanten Datensicherung, über das mitgelieferte Netzteil geladen werden. Eine Verbindung über das USB-Kabel könnten ungewollt Daten mit iTunes synchronisiert oder Schadsoftware auf das iOS-Gerät übertragen.

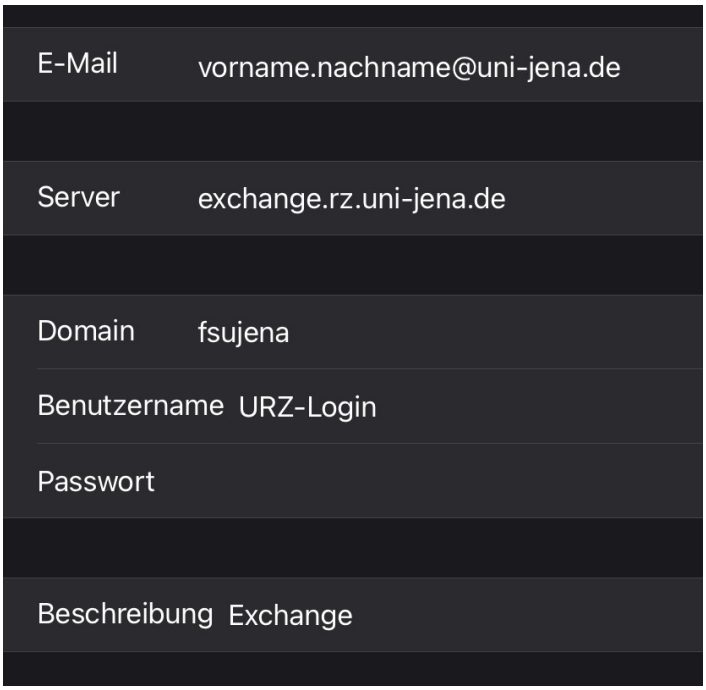
Apple ID

Die Apple ID ist für den Einkauf von Apps und zur Authentifizierung gegenüber verschiedensten Diensten von Apple notwendig. Für dienstliche iOS-Geräte ist die Nutzung einer Apple ID nicht erwünscht.

Exchange Account

Die Nutzung von persönlichen E-Mail-Accounts ist auf dienstlich genutzten iOS-Geräten nicht erlaubt. Ein Exchange-Konto an der Universität Jena vorausgesetzt, besteht die Möglichkeit, dieses über ActivSync einzubinden.

1. Einstellungen
2. Mail, Kontakte oder Kalender
3. Accounts
4. Account hinzufügen
5. Exchange
6. URZ E-Mail und Beschreibung eingeben
    a. E-Mail: vorname.nachname@uni-jena.de
    b. Beschreibung: (frei wählbar)
7. Manuell konfigurieren
    a. Passwort: „zum URZ-Login gehörendes Passwort“
    b. Server: exchange.rz.uni-jena.de
    c. Domain: FSUJENA
    d. Benutzername: „URZ-Login“
8. Auswählen welche Dienste synchronisiert werden sollen



Ortungsdienste

Unter Verwendung von GPS, Bluetooth, WLAN und Mobilfunk, ermitteln die Ortungsdienste den ungefähren Standort des iOS-Gerätes und sollten deaktiviert werden.

Einstellungen Datenschutz Ortungsdienste deaktivieren

Passwortschutz

Das iOS-Gerät ist immer vor unberechtigten Zugriff durch mindestens eine 4-stellige PIN zu schützen.

1. Einstellungen
2. Face ID & Code bzw. Touch ID & Code
3. Code aktivieren
4. Code festlegen

Zusätzlich wird empfohlen die Funktion „Daten löschen“ zu aktivieren. (Nach 10 fehlgeschlagenen Anmeldeversuchen alle Daten auf diesem iPhone löschen.)

1. Einstellungen
2. Face ID & Code bzw. Touch ID & Code
3. Daten löschen aktivieren

Siri konfigurieren

Siri ist eine Spracherkennungssoftware innerhalb von iOS , die verschiedene Aktionen auslösen kann. Konvertiert wird die Spracheingabe nicht auf dem iOS-Gerät selbst, sondern auf weltweit verteilten Servern. Zudem kann Siri auch Aktionen bei gesperrtem iOS-Gerät durchführen, wenn diese Funktion nicht gesperrt ist. Siri sollte deshalb deaktiviert werden.

1. Einstellungen
2. Siri & Suchen
3. Auf Hey Siri achten und Für Siri Seitentaste drücken deaktivieren

Diagnose- & Nutzungsdaten

Bei aktivierter Funktion werden täglich Diagnose- und Nutzungsdaten, zur Verbesserung von Produkten und Diensten, an Apple gesendet, welche u.a. auch Ortsinformationen enthalten können. Diese Funktionen deaktivieren.

1. Einstellungen
2. Datenschutz

3. Analyse und Verbesserungen
4. iPhone- Analyse teilen, Siri & Diktat verbessern und iCloud-Analyse teilen deaktivieren

und

1. Einstellungen
2. Datenschutz
3. Apple-Werbung
4. Personalisierte Werbung deaktivieren

VPN

Außerhalb vom „eduroam“ sollte immer eine VPN Verbindung genutzt werden.

Anwendungen

Die Installation von Anwendungen unbekannter Quellen ist nicht empfehlenswert.

Updates

Das iOS-Gerät sollte wöchentlich auf Softwareaktualisierungen überprüft werden. Andernfalls können bekannt gewordene Sicherheitslücken ausgenutzt werden.

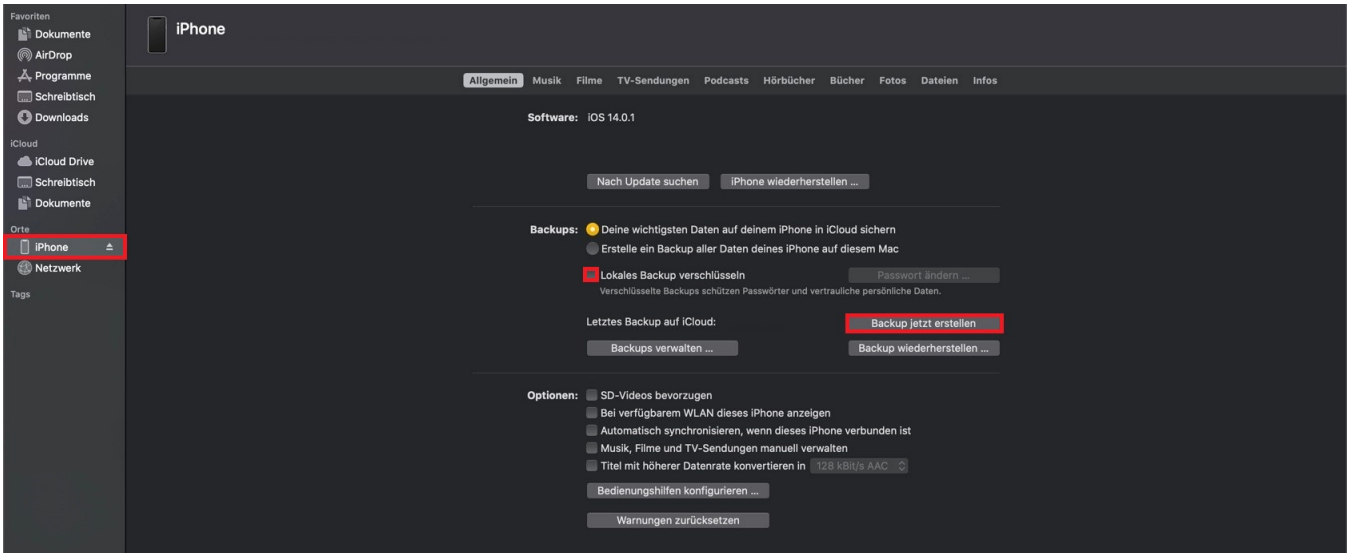
1. Einstellungen
2. Allgemein
3. Softwareaktualisierung

Datensicherung

Es wird empfohlen das iOS-Gerät mit dem Programm iTunes auf ein Windows- oder OS X-System zu sicheren und die Sicherungskopie zu verschlüsseln. Die Datensicherung ist vor unberechtigten Zugriff zu schützen.

Mac OS:

1. iPhone mit Mac per USB Kabel verbinden
2. im Finder iPhone auswählen
3. auf beiden Geräten vertrauen wählen
4. Allgemein
5. Backups
6. Backup Art wählen: nur wichtige Daten oder alle Daten
7. Lokales Backup verschlüsseln und Passwort dafür festlegen
8. Backup jetzt erstellen wählen



Sicheres Löschen

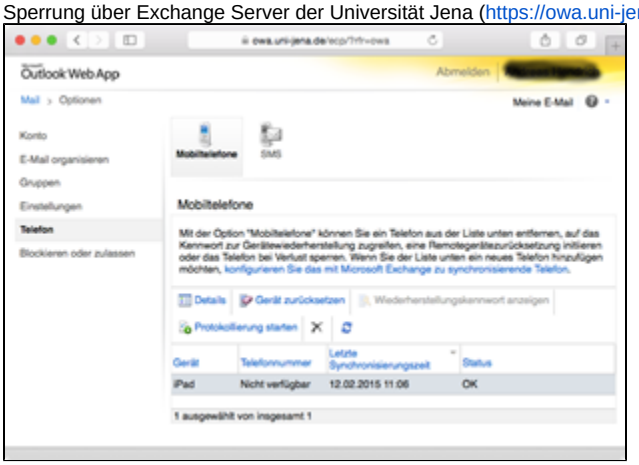
Bei Stilllegung und Nutzerwechsel sind alle Medien, Daten und Einstellungen unwiderruflich zu löschen.

Einstellungen Allgemein Zurücksetzen Alle Inhalte & Einstellungen löschen

Vorgehen bei Verlust

Wird ein iOS-Gerät gestohlen oder verloren, muss es aus der Ferne deaktiviert werden, um unbefugten Zugang zu verhindern. Wird der Exchange-Server der Universität Jena genutzt und besteht eine Netzverbindung zum iOS-Gerät, dann kann eine Sperrung oder eine vollständige Löschung über Exchange ActiveSync erfolgen.

- Sperrung über Exchange Server der Universität Jena (https://owa.uni-jena.de/owa)



- Bei Verlust eines iOS-Gerätes ist umgehend das IT-Servicezentrum zu informieren
- Ein Diebstahl ist zusätzlich und unverzüglich bei der nächsten Polizeidienstelle, für Jena Telefon +49 3641 810, anzuzeigen und das Aktenzeichen zu notieren