dsb
datenschutzbeauftragter
kanton zürich

Merkblatt

Datenschutzfreundliche Apps

Dieses Merkblatt behandelt eine Auswahl kostenloser oder günstiger Apps für Android- und iOS-Systeme, die bei folgenden Themen Hilfe bieten:

1 Anonymes Surfen
2 Lokalisieren des Smartphones
3 Verhindern von unerwünschten App-Zugriffen
4 Blockieren von Anrufen
5 Sicheres Löschen
6 Datenschutzfreundliche Nutzung von Karten
7 Sichere Online-Speicherung
8 Zusätzlicher Zugriffschutz für Daten und Apps
9 Sicheres Speichern der Passwörter
10 Schutz vor Trojanern und Spyware
11 Sicheres Kommunizieren
12 Privatsphären-Einstellungen
13 Verschlüsselung von Dateien

1 Anonymes Surfen

Wer im Internet surft, hinterlässt seine IP-Adresse und andere Spuren. Mit entsprechenden Apps können diese Spuren teilweise verhindert oder unkenntlich gemacht werden.

- Firefox Klar: Android und iOS
- Onion Browser: iOS
- Orfox: Android
- Orweb: Android

2 Lokalisieren des Smartphones

Smartphones können verloren gehen oder gestohlen werden. Für solche Fälle gibt es diverse Apps mit Lokalisierungsdiensten.

- Android-Gerätemanager: Android, Lokalisierungsdienst von Google
- Find My iPhone: iOS, Lokalisierungsdienst von Apple

3 Verhindern von unerwünschten App-Zugriffen

Viele Apps greifen auf persönliche Daten zu. Einstellungen der Standardfunktionen verhindern dies.

3.1 iOS

Die Zugriffe über Einstellungen → Datenschutz festlegen (ab iOS 6).

3.2 Android

Die App-Berechtigungen können unter Android detailliert konfiguriert werden, in der Android-Version 7 beispielsweise unter: Einstellungen → Anwendungen → App-Berechtigungen

4 Blockieren von Anrufen

4.1 iOS

Nummern können direkt in der Telefon-App gesperrt werden: Anruflisten → Symbol «i» → Kontakt sperren

4.2 Android

In den meisten Android-Versionen können unerwünschte Nummern direkt in der Telefon-App gesperrt werden: Einstellungen → Anrufeinstellungen → Nummern sperren

5 Sicheres Löschen

Beim Löschen von Dateien wird oft nur die Referenz auf eine Datei entfernt und der eigentliche Inhalt bleibt bis zum nächsten Überschreiben erhalten. Die Daten lassen sich mit entsprechender Software wiederherstellen. Um Dateien unwiderruflich zu löschen, sind zusätzliche Massnahmen erforderlich.

5.1 iOS

- Gerät zurücksetzen: Einstellungen → Allgemein → zurücksetzen
- Den ganzen Speicher über iTunes mit Datenmüll (beispielsweise MP3-Dateien) füllen

5.2 Android

- File Shredder: Android, sicheres Löschen einzelner Dateien
- Gerät zurückzusetzen: Einstellungen → Sichern und zurücksetzen → Auf Werkszustand zurücksetzen
- Den ganzen Speicher mit Datenmüll (beispielsweise MP3-Dateien) füllen

6 Datenschutzfreundliche Nutzung von Karten

Der bekannteste Kartenanbieter Google Maps verknüpft die Nutzungsdaten mit weiteren Informationen und erstellt daraus ein umfassendes Persönlichkeitsprofil. Die folgenden Kartendienste bieten datenschutzfreundliche Alternativen:

- ForeverMap: Android und iOS, Offline-Karten von OpenStreetMap
- OsmAnd: Android und iOS, Offline-Karten von OpenStreetMap

7 Sichere Online-Speicherung

Bei vielen Online-Speicherdiensten sind die Daten für den Betreiber lesbar. Folgende Apps bieten eine clientseitige Verschlüsselung, die dies verhindert:

- SecureSafe: Android und iOS
- TeamDrive: Android und iOS
- Tresoit: Android und iOS, kostenpflichtig

- Weiterführende Informationen im Merkblatt Online-Speicherdienste

8 Zusätzlicher Zugriffschutz auf Daten und Apps

Mit der folgenden App kann der Zugriff auf Apps und Daten zusätzlich geschützt werden, beispielsweise mit einem Passwort:

- App Lock: Android

9 Sicheres Speichern der Passwörter

Passwörter sollten nicht aufgeschrieben und für jeden Dienst sollte ein anderes Passwort gewählt werden. Diverse Softwarelösungen bieten Unterstützung an, um die Passwörter sicher abzuspeichern und automatisiert einzugeben. Wir empfehlen, Passwörter für sensitive Bereiche nicht in diesen Tools zu speichern.

- KeePassDroid: Android
- LastPass: Android und iOS, Passwort-Synchronisation
- MiniKeePass: iOS
- SecureSafe: Android und iOS

- Weiterführende Informationen im Merkblatt Passwortmanager

10 Schutz vor Trojanern und Spyware

Virenschutz- oder Personal-Firewall-Apps erhöhen die Sicherheit des Geräts.

10.1 Virenschutz / Sicherheitslösungen

- Avast Mobile Security: Android, umfassende Sicherheitslösung
- AVG Anti Virus: Android, Viren-, Daten- und Diebstahlschutz
- ESET Mobile Security: Android, kostenpflichtig
- Sophos Security & Antivirus: Android, Viren- und Diebstahlschutz
- TrustGo: Android

10.2 Personal Firewall

- NetGuard: Android

11 Sicheres Kommunizieren

Die unverschlüsselte Kommunikation, beispielweise per E-Mail oder SMS, kann abgefangen und mitgelesen werden. Diverse Apps ermöglichen verschlüsselte und sichere Kommunikation.

- Acrobits Softphone: Android und iOS, verschlüsseltes Telefonieren, kostenpflichtig
- ChatSecure: iOS, verschlüsseltes Chatten per XMPP mit OTR
- CipherMail Email Encryption: Android, verschlüsseltes E-Mailen
- CSipSimple: Android, verschlüsseltes Telefonieren
- K9-Mail (mit OpenKeychain: Easy PGP): Android, verschlüsseltes E-Mailen
- PixelKnot: Android, Nachrichten in öffentlichen Bildern verstecken
- Signal: Android und iOS, verschlüsseltes Chatten und Telefonieren
- Threema: Android und iOS, verschlüsseltes Chatten, kostenpflichtig
- Wire: Android und iOS, verschlüsseltes Chatten und Telefonieren
- Xabber: Android, verschlüsseltes Chatten per XMPP mit OTR

- Weiterführende Informationen im Merkblatt Kommunikationssoftware

12 Privatsphären-Einstellungen

Systeme datenschutzfreundlich zu konfigurieren, ist oft sehr aufwendig. Die folgende App bietet Hilfestellung:

- aSpotCat: Android, App-Rechte auflisten

13 Verschlüsselung von Dateien

Jede Person mit Zugriff auf das Gerät kann unverschlüsselt gespeicherte Dateien lesen. Dies ist besonders bei Diebstahl, Verkauf oder Verlust des Geräts problematisch. Deshalb sollten entweder der komplette Speicher oder mindestens die sensitiven Dateien verschlüsselt werden. Die folgenden Apps helfen auch, um Dateien sicher in der Cloud zu speichern:

- Boxcryptor: Android und iOS, verschlüsselt Dateien in Online-Speichern wie Dropbox, Google Drive, Microsoft Onedrive etc.
- Encryption Manager: Android, kostenpflichtig

dsb

datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
Fax 043 259 51 38

datenschutz@dsb.zh.ch
www.datenschutz.ch