Checkliste:
Sicherer Umgang mit mobilen Endgeräten und Apps

DigiBitS-Code: 42105

Auf einen Blick:

Themen: IT-Sicherheit, Apps, mobile Geräte, technische Schutzvorkehrungen

Vorkenntnisse: keine

Medienkompetenzen: Anwenden, Schützen

Fachbereich: Medienbildung – allgemeine Infos

1) Allgemeine Schutzmaßnahmen für mobile Endgeräte anwenden

- [ ] PIN-Abfrage für die SIM-Karte nutzen.
- [ ] Bildschirmsperre mit sicherem Code/Passwort einrichten.

  Achtung: Eine Mustersperre ist nicht sicher, da man anhand der Spuren auf dem Display den Code nachvollziehen kann.

  Hinweis: Durch die Aktivierung einer Bildschirmsperre werden in modernen Geräten die Daten automatisch verschlüsselt. Bei Android darauf achten, dass auch die SD-Karte verschlüsselt wird.
- [ ] Das Betriebssystem auf dem aktuellen Stand halten.
- [ ] Funktionen zur Standortbestimmung (GPS oder internetbasiert) nur bei Bedarf aktivieren – bzw. gezielt für Apps freigeben (siehe dazu Punkt 4) – und anschließend wieder ausschalten.
- [ ] Datenverbindungen (WLAN, Bluetooth) nur bei Bedarf aktivieren und anschließend wieder abschalten.

2) Virenschutz-App installieren

- [ ] Android-Smartphones/ -Tablets durch Antiviren-Apps schützen.

  Hinweis: Für iOS-Geräte gibt es keinen Virenscanner.

  Achtung: Eine Virenscanner-App schützt nicht vor ungewollten Zugriffsberechtigungen – siehe dazu Punkt 4.

Kostenlose Virenscanner im Test:
www.av-test.org/de/antivirus/mobilgeraete

Bestenliste Virenschutz-Apps
www.chip.de/bestenlisten/Bestenliste-Antivirenprogramme-Android-2017--index/index/id/1425

3) Die Downloadquelle sorgsam auswählen

- [ ] Vorsicht bei Drittanbieter-Stores für Apps!
  Nur aus seriösen Quellen Apps herunterladen, wie zum Beispiel aus den offiziellen Stores der Smartphone-Hersteller (im Google Play Store, dem Apple App Store oder im Windows Phone Store). Diese Quellen führen Sicherheitsprüfungen durch, bevor bestimmte Apps zum Download zur Verfügung gestellt werden.

4) Die Zugriffsrechte vor der Installation überprüfen

- [ ] Zugriffsrechte prüfen, ggfs. anpassen
  (in iOS und Android ab Version 6.0) oder die Installation/ Nutzung unterbinden.
- [ ] Prüfen, ob die Berechtigungen mit den Funktionen der App zusammenpassen.

  Hinweis: Bestenlisten sagen nichts über den Datenschutz aus, auch der beliebteste Download kann ein ungewollter Datensammler sein.

Mehr zum Thema Berechtigungen unter
www.handysektor.de/berechtigungen

5) AGB lesen

- [ ] Die Allgemeinen Geschäftsbedingungen (kurz: AGB) können viele, auch böse, Überraschungen bereithalten. Daher: Genau lesen!
- [ ] Besonderes Augenmerk auf Regelungen über die Datenverwendung, den Zahlungsverkehr sowie Altersbeschränkungen legen.
- [ ] Bei Unsicherheiten in Hinblick auf die Inhalte: Am besten die App nicht installieren und einen Experten fragen.

Hinweise zu AGBS unter *www.handysektor.de/agbs*

Checkliste:
Sicherer Umgang mit mobilen Endgeräten und Apps

DigiBitS-Code: 42105

6) Andere Meinungen einholen

- [ ] Kommentare von anderen können dabei helfen, schwarze Schafe zu entdecken:
Hinweise zu Sicherheits- und Datenschutzmängeln der App prüfen.

7) Updates kontrollieren

- [ ] Neue Updates prüfen (sinnvoll oder unnötig?) und zeitnah installieren, da oft Sicherheitslücken geschlossen werden.
- [ ] Nach Aktualisierung: (Privatsphäre-)Einstellungen prüfen! Manchmal werden manuelle Einstellungen zurückgesetzt.
- [ ] Nicht mehr länger genutzte Apps deinstallieren.

8) Vorsicht bei In-App-Käufen

- [ ] Aufpassen: Nicht jede App, die beim Download kostenlos ist, bleibt das auch für immer. Vorab prüfen, ob nach einer gewissen Laufzeit Kosten anfallen oder ob die App ohne In-App Käufe nicht in vollem Umfang nutzbar ist.

Hinweise zu In-App-Käufen und wie man sie vermeiden kann:
www.handysektor.de/agbs

9) Apps zurückgeben – das geht

- [ ] Bei Unzufriedenheit oder versehentlichem Kauf: Rückgabe im Store veranlassen!
Mehr dazu:
www.handysektor.de/apps-upps/detailansicht/article/geld-zurueck-bei-apps-wie-funktioniert-die-rueckgabe.html

10) Diebstahlschutz aktivieren

- [ ] Die persönliche Identifikationsnummer des Smartphones IMEI (wird sichtbar durch Tastenkombination *#06#) notieren! Diese hilft beim Wiederfinden eines gestohlenen Geräts.
- [ ] Externe Sperr- und Löschmöglichkeiten, ggfs. Ortungsmöglichkeit einrichten: Für iOS via icloud.com, für Android via google.com/android/find
- [ ] Backups einrichten, um wichtige Daten gesichert zu haben.

Weitere Informationen zu Schutzmaßnahmen für mobile Geräte: *www.handysektor.de* **oder** *DigiBitS-Webcode 42246*

www.klicksafe.de/smartphones **oder** *DigiBitS-Webcode 42248*

Die Checkliste *"Sicherer Umgang mit mobilen Endgeräten und Apps"* wurde in Kooperation mit Handysektor erstellt.