Apps vorab prüfen und verstehen

Da Apps ein zentraler Bestandteil deines Android-Smartphones sind, solltest du

- Apps nur aus vertrauenswürdigen Quellen installieren (z. B. Google Play),
- vor Installation oder Update einer App die Datenschutzerklärung lesen und kritisch prüfen, welche Berechtigungen die App auf deinem Gerät einfordert,
- Rezensionen (Bewertungen) zu der App im Google Play Store sorgfältig lesen und bei Unklarheiten beim Hersteller nachfragen und
- dich bei konkreten Hinweisen auf Schadsoftware oder „Datenklau“ durch eine App an die zuständige Datenschutzaufsichtsbehörde wenden.

Richtig handeln bei Verlust & Diebstahl

Behalte bei Verlust oder Diebstahl einen kühlen Kopf und leite die notwendigen Schritte ein:

- Lass deine SIM-Karte unverzüglich bei deinem Mobilfunkanbieter sperren und melde Diebstahl bei der örtlichen Polizeidienststelle.
- Nutze den „Android-Gerätemanager“, um dein Smartphone zu orten oder zurückzusetzen. Hierfür musst du die Software vorher auf deinem PC installieren und auf deinem Smartphone unter Sicherheit > Geräteadministratoren den Punkt Android Gerätemanager aktivieren.
- Beim Verkauf deines Smartphones solltest du darauf achten, dass du deine persönlichen Daten entfernst. Nutze hierzu z. B. Sichern & Zurücksetzen in den Einstellungen und wähle Auf Werkszustand zurück.

Smartphone-Tipps kompakt:

1. Nicht unbeaufsichtigt liegen lassen
2. PIN und Passwort verwenden
3. Automatische Zugriffssperre einstellen
4. Kontrolle über den Standort behalten
5. Sicherheitstechniken nicht aushebeln
6. Vorkehrungen für Backups treffen
7. Apps vorab prüfen und verstehen
8. Richtig handeln bei Verlust & Diebstahl

Diesen Flyer und weitere Informationen findest du auf **www.lda.bayern.de/smartphone**

Herausgeber:
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27, 91522 Ansbach

Tel.: 0981 / 53 - 1300
Fax: 0981 / 53 - 5300
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Stand: August 2014

BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT

Gib 8 auf dein Smartphone

Datenschutztipps für Android

Nicht unbeaufsichtigt liegen lassen

Lass dein Android-Smartphone nicht aus den Augen, denn Unbefugte können heimlich

- Einblick in deine persönlichen E-Mails, SMS oder Notizen erhalten und so vertrauliche Informationen lesen und gegen dich nutzen,
- Spionage-Apps auf deinem Smartphone installieren und dich dadurch überwachen,
- kostenpflichtige Apps installieren oder teure SMS-Dienste missbräuchlich nutzen,
- auf dem Smartphone gespeicherte Accountdaten nutzen und so auf deine Kosten online shoppen,
- in deinem Namen gefälschte Nachrichten an Freunde und Bekannte versenden oder
- dein Android-Smartphone stehlen.

PIN und Passwort verwenden

Unter Einstellungen > Sicherheit kannst du sowohl die Display-Sperre als auch die SIM-Sperre einrichten. Dadurch erreichst du einen wichtigen Basisschutz für dein Smartphone.

- Verwende die SIM-Sperre, um deine SIM-Karte vor Missbrauch bei Verlust und Diebstahl zu schützen.
- Nutze zusätzlich ein sicheres Passwort für die Display-Sperre, um auch die Daten auf deinem Smartphone vor Fremden zu schützen.

Beispiele:	1234	● unsicher
	A_790	● gut
	iyL@v3u	● sehr gut

Je länger und komplexer das Passwort ist, desto besser ist dein Smartphone auch bei Verlust vor unbefugtem Zugriff geschützt. Du musst dir das Passwort jedoch auch merken können.

Automatische Zugriffssperre einstellen

In Einstellungen und Sicherheit kannst du unter Automatisch sperren die Zeit bestimmen, nach der die Zugriffssperre für dein Smartphone automatisch aktiviert wird:

- Je kürzer die Zeit eingestellt wird, desto unwahrscheinlicher ist es, dass ein Fremder dein Smartphone ungesperrt im Ruhezustand vorfindet.
- Wenn es dein Android-Gerät ermöglicht, kannst du unter Sicherheit > Info zum Eigentümer Kontaktinformationen zu deiner Person angeben, die bei Verlust des Gerätes auf dem Sperrbildschirm angezeigt werden und den Finder informieren. So bekommst du dein Gerät vielleicht wieder.

Kontrolle über den Standort behalten

Damit du dauerhaft Kontrolle darüber hast, ob auf deine Standortdaten zugegriffen werden darf, kannst du unter Einstellungen > Nutzer > Standortzugriff (bzw. Standortdienste)

- festlegen, ob du Apps den Zugriff auf deinen Aufenthaltsort grundsätzlich erlaubst und
- bestimmen, welche Quellen (GPS, WLAN, Mobilfunknetze) verwendet werden dürfen, um deinen Standort zu ermitteln.
- Tipp: Schalte Standortdienste aus, wenn du sie nicht benötigst und aktiviere sie dann gezielt bei Bedarf - so hast du die beste Kontrolle darüber und sparst gleichzeitig Akkuleistung.

Sicherheitstechniken nicht aushebeln

Um die Sicherheit deines Android-Smartphones nicht zu gefährden, solltest du

- keinen Rooting-Versuch unternehmen, um dir eventuell mehr Rechte auf deinem Smartphone zu verschaffen, da dies bösartigen Apps umfassende Möglichkeiten verschafft, dein Gerät zu manipulieren und Missbrauch zu betreiben,
- Entwickleroptionen des Geräts (z. B. USB-Debugging) nicht aktivieren und in der täglichen Nutzung darauf verzichten und
- regelmäßig Softwareupdates für dein Android-System und deine Apps über Google Play installieren.

Vorkehrungen für Backups treffen

Um dich vor unerwünschtem Datenverlust zu schützen, kannst du

- mit speziellen Apps eine Komplett-Sicherung deines Smartphones durchführen,
- manche Daten, wie z. B. Bilder deiner SD-Karte im Gerät, lokal auf deinem PC sichern, wenn du dich regelmäßig mit deinem PC verbindest oder
- auf deinem Smartphone unter Einstellungen > Konten > Google die Synchronisierung von Google nutzen, um festzulegen, ob und welche deiner persönlichen Daten mit deinem Google-Konto synchronisiert werden sollen.