

SMARTPHONES SICHER BENUTZEN DIE BASICS

1. SICHERHEITSFUNKTIONEN

- PIN der SIM-Karte und Bildschirmsperre des Smartphones aktivieren
- automatische Sperrzeit (Ruhemodus) des Bildschirms auf max. 5 Minuten setzen
- sensible Anwendungen (z. B. Onlinebanking, Online-Käufe per App) mit PIN oder Passwort schützen
- voreingestellte Sperrcodes durch eigene Kombinationen ersetzen
- schwierige Zahlenkombinationen wählen und logische Abfolgen oder Geburtstage vermeiden
- Gerät, wenn möglich, per Fingerabdruck oder Gesichtserkennung entsperren
- geringere Sicherheit bei Wischmustern



2. AUTOMATISCHE UPDATES

- Angriffe zielen oft auf Sicherheitslücken in der Software ab, die erst durch Updates der Hersteller geschlossen werden
- automatische Update-Funktion für das Betriebssystem und Apps aktivieren
- alternativ regelmäßige Kontrolle, ob Aktualisierungen verfügbar sind



3. APPS AUS SERIÖSEN QUELLEN

- Apps nur aus seriösen Quellen herunterladen und installieren (Appstore)
- nur Anwendungen herunterladen, die tatsächlich benötigt werden
- Quellen meiden, deren Seriosität zweifelhaft ist
- Deinstallieren von Apps, die nicht mehr genutzt werden
- Kritisch prüfen, ob umfassende Zugriffsrechte von Apps auf bspw. Standortdaten, das Adressbuch, etc. wirklich notwendig sind. Wenn möglich individuelle Einstellungen tätigen. Im Zweifelsfall die App besser nicht installieren.



4. NUTZUNG VON ÖFFENTL. HOTSPOTS

- Erhöhtes Risiko durch öffentliche Hotspots, bspw. WLAN im Café oder am Flughafen, die häufig kein Kennwort oder für alle Teilnehmer ein gemeinsames Kennwort nutzen
- Angreifer können Daten abgreifen
- Kommunikation zwischen Endgerät und dem Internetserver sollte verschlüsselt sein
- sichere Kommunikation wird über das https-Protokoll hergestellt, im Browser erkennbar durch das Schlosssymbol in der Adresszeile



5. GERÄT NICHT UNBEAUF SICHTIGT LASSEN

- Smartphones und Tablets niemals unbeobachtet lassen
- Verlorene oder gestohlene Geräte können mithilfe von Apps aus der Ferne gesperrt werden
- Smartphones oder mobilfunkfähige Tablets können anhand der IMEI-Nummer unter bestimmten Bedingungen über den Netzbetreiber geortet werden. Diese sollte im Vorfeld notiert werden.

