

Checkliste: Sichere dein Handy!

Bildschirmsperre aktivieren

- Stelle sicher, dass dein Handy durch eine PIN, ein Passwort oder biometrische Daten (Fingerabdruck oder Gesichtserkennung) geschützt ist.

Zwei-Faktor-Authentifizierung (2FA) einrichten

- Aktiviere die 2FA für wichtige Konten wie E-Mail, soziale Netzwerke (z. B. Instagram, Snapchat, WhatsApp) und Cloud-Dienste (z. B. Google, iCloud).

Apps regelmäßig aktualisieren

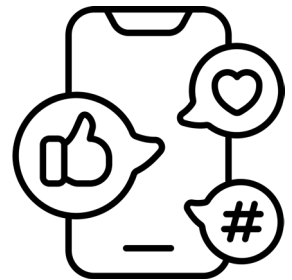
- Halte alle Apps und das Betriebssystem deines Handys auf dem neuesten Stand, um Sicherheitslücken zu schließen.

Berechtigungen prüfen

- Gehe in die Einstellungen und überprüfe, welche Apps Zugriff auf deine Kamera, deinen Standort, dein Mikrofon oder deine Kontakte haben. Entferne unnötige Berechtigungen.

Standortfreigabe kontrollieren

- Deaktiviere die Standortfreigabe, wenn du sie nicht brauchst. Nutze die Option „Nur während der Nutzung“ für Apps, die deinen Standort benötigen.



Öffentliches WLAN sicher nutzen

- Vermeide es, dich in öffentlichen WLANs einzuloggen, besonders ohne Passwortschutz. Nutze bei Bedarf ein VPN.

Datenschutz in sozialen Netzwerken

- Stelle dein Profil auf „privat“. Kontrolliere, wer dir folgen kann, wer deine Beiträge sieht und ob dein Standort bei Beiträgen geteilt wird.



Fremde Nachrichten ignorieren

- Öffne keine Links oder Anhänge von unbekannten Absendern in E-Mails, SMS oder sozialen Netzwerken. Das könnten Phishing-Versuche sein.

Backups aktivieren

- Stelle sicher, dass automatische Backups für wichtige Daten aktiviert sind (z. B. in Google Drive oder iCloud), damit du im Notfall deine Daten wiederherstellen kannst.



App-Downloads nur aus offiziellen Stores

- Installiere Apps nur aus dem Google Play Store (Android) oder dem App Store (iOS). Vermeide dubiose Drittanbieter-Apps.

Unbekannte Geräte und Netzwerke meiden

- Verwalte Bluetooth- und WLAN-Verbindungen. Stelle sicher, dass dein Gerät nur mit bekannten Netzwerken oder Geräten verbunden ist.

Werbung und Tracking blockieren

- Aktiviere die „Tracking verhindern“-Funktion (iOS) oder „Anzeigenpersonalisiertes Tracking deaktivieren“ (Android) in den Einstellungen.



Datenverbrauch prüfen

- Kontrolliere regelmäßig, ob Apps im Hintergrund ungewöhnlich viele Daten verbrauchen – das kann ein Hinweis auf Malware sein.

Alarmer für verdächtige Aktivitäten einrichten

- Aktiviere Benachrichtigungen für Anmeldungen auf neuen Geräten oder ungewöhnliche Aktivitäten in deinen Konten.

