# Merkliste: Schritt für Schritt sicher im Netz unterwegs – damit du nicht zum Opfer wirst!

## Für Android: Wenn du mehr willst als nur „Flugmodus“ und „Bildschirmsperre“ am Handy

*Hinweis: Jedes Handy tickt ein bisschen anders!*

*Je nach Hersteller (z. B. Samsung, Xiaomi, Google), Android-Version und Oberfläche (z. B. One UI, MIUI, Pixel UI) sehen Menüs und Funktionen unterschiedlich aus.*

*Manche Tricks findest du unter anderen Namen – oder gar nicht.*

*Probiere aus, was bei deinem Gerät möglich ist!*

*Nutze die Suchfunktion in den Einstellungen (oft oben rechts mit einer Lupe) – oder frag jemanden, der sich gut auskennt.*

*Wichtig: Nicht jede Funktion ist für jeden sinnvoll – wähle, was zu deinem Alltag passt.*

*App-Cloning für Zwei-Identitäten – ohne Spionage-Apps:*
*Viele Android-Geräte bieten die Möglichkeit, Apps zu „klonen“ (z. B. WhatsApp, Signal, Instagram). Diese Funktion versteckt sich oft unter Erweiterte Funktionen > Dual Apps / App-Twin / Klonen.*
*So kannst du private und berufliche Nutzung strikt trennen – ohne zusätzliche App-Berechtigungen freizugeben.*

*Unsichtbarer Modus - MAC-Adresse zufällig machen:*
*Viele WLAN-Netzwerke speichern deine Gerätekennung (MAC-Adresse). Gehe zu WLAN > Netzwerk > Erweiterte Einstellungen > MAC-Adresse, und stelle auf „Zufällig" statt „Geräte-MAC".*
*So kannst du dich z. B. in öffentlichen Netzwerken bewegen, ohne dauerhafte Spuren zu hinterlassen.*

*Zugriff bei Diebstahl sofort sperren – mit Android Gerätemanager:*
*Viele vergessen: Der „Mein Gerät finden"-Service von Google kann das Handy sperren, orten oder löschen. Stelle sicher, dass dieser aktiviert ist unter Google > Sicherheit > Mein Gerät finden.*
*Teste regelmäßig, ob der Zugriff auch klappt: android.com/find*

*Private DNS aktivieren (DNS over TLS):*
*In Netzwerk & Internet > Erweitert > Privates DNS kannst du z. B. dns.quad9.net oder dns.adguard.com eingeben.*
*Damit schützt du dich vor Tracking, Werbung und unseriösen Seiten – ohne Zusatz-App.*

*Google Play Protect ist nur der Anfang:*
*Aktiviere Play Protect, aber verlasse dich nicht allein darauf. Nutze zusätzlich lokale Scanner oder setze auf App-Analyse-Dienste wie Exodus Privacy (exodus-privacy.eu.org), um zu sehen, welche Tracker in deinen Apps versteckt sind.*
*Auch manche populären Apps enthalten bis zu 15 Tracker – ohne dass du es merkst.*

*App-Berechtigungen regelmäßig kontrollieren – und entziehen:*
*Viele Apps fordern unnötige Berechtigungen. Gehe zu Einstellungen > Sicherheit & Datenschutz > Berechtigungsmanager und überprüfe dort kritisch, was wirklich nötig ist.*
*Pro-Tipp: Apps mit Standortzugriff im Hintergrund entlarven oft Tracking-Versuche.*

*Android verschlüsseln & Bootloader gesperrt halten:*
*Moderne Androids sind standardmäßig verschlüsselt – überprüfe unter Sicherheit > Verschlüsselung & Anmeldedaten, ob die Verschlüsselung aktiv ist.*
*Wenn du ein Custom-ROM nutzt: Den Bootloader wieder sperren, sonst sind deine Daten trotz Passwort nicht sicher.*

*DNS-Filter nicht nur am Handy nutzen: Dienste wie Quad9 oder OpenDNS blockieren bekannte gefährliche Webseiten automatisch.*

*Auf KI-Plattformen achtsam sein: Gib keine vertraulichen Daten in ChatGPT oder andere KI-Tools ein.*

**Hinweis:**

Die genannten Beispiele dienen lediglich der Veranschaulichung und stellen keine Produktempfehlungen dar. Es gibt viele Alternativen auf dem Markt – wähle die, die am besten zu deinen Bedürfnissen passt!

Verlag:
eTransfusion
Michael Bätscher
Buchenweg 10
79664 Wehr
eTransfusion.de