DÉNIA PC DOC · ANLEITUNG

Werbetrojaner auf dem Handy entfernen

Samsung Galaxy zuerst — mit den Unterschieden für Xiaomi, Google und Huawei

> **Zuerst die Entwarnung:** Wenn plötzlich Werbung auf dem Sperrbildschirm erscheint oder sich beim Tippen ein Browserfenster öffnet, ist Ihr Handy in den allermeisten Fällen **nicht gehackt**. Es ist Werbung — von einer App, die sie mitbringt, oder von einer Webseite, der Sie einmal erlaubt haben, Ihnen Nachrichten zu schicken. Es wurden dabei in der Regel keine Passwörter gestohlen und kein Geld abgebucht. Sie brauchen kein neues Handy, keine „Reinigungssoftware“ und keine kostenpflichtige Hilfe, um das loszuwerden.

Was da wirklich passiert

„Werbetrojaner“ sagt man im Alltag, technisch heißt es meist **Adware**: ein Programm, das Werbung einblendet und damit Geld verdient — pro Klick, pro Anzeige. Ein echter Trojaner tarnt sich dagegen und will an Ihre Zugangsdaten oder Ihr Geld. Der Unterschied ist wichtig, weil er die Lage bestimmt: Adware ist lästig, ein Banking-Trojaner ist gefährlich. Weiter unten steht, woran Sie den Unterschied erkennen.

Was Adware typischerweise tut: Sie zeigt Anzeigen im Sperrbildschirm, öffnet beim Entsperren eine Webseite, legt Werbesymbole auf den Startbildschirm oder leitet Ihre Suche im Browser auf Vergleichsportale um. Was sie nicht tut: Ihr Gerät sperren, Ihre Fotos verschlüsseln oder von sich aus Geld abbuchen. Das sind Drohungen aus der Werbung selbst — nicht die Realität.

Wie es auf das Handy kommt

- **Kostenlose Apps mit Werbemodul.** Taschenlampe, QR-Scanner, „Handy-Reiniger“, Taschenrechner, einfache Spiele — der Klassiker. Die App funktioniert, aber sie finanziert sich über Werbung, die sie auch außerhalb der App zeigt.

- **Apps aus dem Netz statt aus dem Play Store.** Eine „Gratis-Version“ von WhatsApp, Netflix oder einem Spiel, per Link verschickt oder in einem Video verlinkt. Wer eine solche Datei installiert, hat keinen, der sie prüft.
- **Erlaubte Browser-Benachrichtigungen.** Kein Programm, nur eine einmal erteilte Erlaubnis. Sie haben irgendwann auf „Zulassen“ getippt, als eine Seite fragte. Das ist der häufigste Fall — und der am schnellsten behobene.
- **Hersteller-eigene „Empfehlungen“.** Manche Geräte zeigen von Haus aus Werbung in eigenen Apps an. Auch das ist keine Infektion, lässt sich aber meist abschalten.

Zuerst prüfen: ist es nur eine Benachrichtigung?

Nach meiner Erfahrung ist das der häufigste Fall — deshalb steht er hier vor dem großen Aufräumen. Wischen Sie die Werbung weg, aber nicht ganz: Tippen Sie auf das kleine Zahnrad oder „Info“ an der Benachrichtigung. Dort steht, wer sie geschickt hat.

- Steht dort **Chrome**, **Samsung Internet** oder **Firefox**: Dann ist es eine Webseite, keine App. So ist es erledigt: Chrome → drei Punkte oben rechts → Einstellungen → Website-Einstellungen → Benachrichtigungen → alle Einträge entfernen. Bei Samsung Internet: drei Punkte → Einstellungen → Websites und Downloads → Benachrichtigungen.
- Steht dort ein **App-Name**, den Sie nicht kennen: weiter mit dem Plan unten.

Der Plan in sechs Schritten — Samsung Galaxy

Die Wege unten stammen aus One UI 6 (Android 14); in One UI 5, 7 und 8 heißen die Punkte gleich oder ähnlich. Fehlt ein Menüpunkt bei Ihnen, tippen Sie ihn in der Suche der Einstellungen ein (Lupe oben rechts) — die Reihenfolge bleibt in jedem Fall dieselbe.

1. **Sicheren Modus starten.** Ausschalt-Taste lange drücken, dann „Ausschalten“ lange gedrückt halten und „Sicherer Modus“ bestätigen. Im sicheren Modus sind nur die vorinstallierten Apps aktiv. Ist die Werbung jetzt weg, wissen Sie: eine selbst installierte App ist die Ursache.

2. **Die App suchen.** Einstellungen → Apps. Tippen Sie oben auf „Ihre Apps“ und gehen Sie die Liste durch. Verdächtig sind Namen, die nach Funktion klingen, aber nichts erklären („System Service“, „Clean Master“, „Phone Booster“, „QR Scan Pro“), Einträge ohne echtes Symbol und Apps, an deren Installation Sie sich nicht erinnern.

3. **Deinstallieren.** App antippen → „Deinstallieren“. Bei Samsung-Apps, die sich nicht entfernen lassen: „Ausschalten“ wählen — das reicht meist auch.

4. **Wenn „Deinstallieren“ grau ist:** Die App hat sich als Geräteadministrator eingerichtet. Einstellungen → Sicherheit und Datenschutz → Weitere Sicherheitseinstellungen → Geräteadministrator-Apps → Häkchen bei der App entfernen → zurück zu Einstellungen → Apps → jetzt deinstallieren.
5. **Zwei Rechte prüfen, die Adware gern nutzt:** Einstellungen → Apps → Spezieller Zugriff → „Über anderen Apps anzeigen“ und „Bedienungshilfen“. Steht dort eine App, die Sie nicht kennen, ausschalten und deinstallieren.
6. **Gegenprüfen lassen.** Play Store öffnen → Profilbild oben rechts → Play Protect → „Scannen“. Danach Einstellungen → Benachrichtigungen → App-Benachrichtigungen: bei allen Apps, die keine Nachrichten schicken sollen, den Schalter aus.

> **Wenn danach noch Werbung kommt:** Einstellungen → Allgemeine Verwaltung → Zurücksetzen → „App-Einstellungen zurücksetzen“. Das löscht keine Fotos und keine Nachrichten, setzt aber Berechtigungen und Standard-Apps zurück. Erst wenn auch das nicht hilft, ist der Weg über „Auf Werkseinstellungen zurücksetzen“ richtig — vorher sichern, und wenn Sie unsicher sind, lieber gemeinsam mit mir.

Andere Hersteller: Xiaomi, Google, Huawei

Der Ablauf ist überall derselbe, nur die Wege heißen anders. Nach Marktanteilen in Deutschland (Samsung rund 40 %, Xiaomi rund 21 %, Google rund 1,6 %, Huawei rund 1,5 %) lohnt ein eigener Blick vor allem auf **Xiaomi**.

- **Xiaomi (HyperOS / MIUI):** Einstellungen → Apps → Apps verwalten. Die „Sicherheit“-App hat einen eigenen Virenscan; Play Protect ist vorhanden. Die Werbung, die Xiaomi selbst in eigenen Apps zeigt, schalten Sie in den Einstellungen der jeweiligen App ab („Mitteilungen“ / „Empfehlungen“) — das ist keine Infektion.
- **Google Pixel:** Einstellungen → Apps → Alle Apps; Play Protect wie oben. Sonst identisch.
- **Huawei (EMUI / HarmonyOS):** Kein Play Store und kein Play Protect — Apps kommen aus der AppGallery, der Scan läuft über die „Optimizer“-App. Die Geräteadministratoren finden Sie unter Einstellungen → Sicherheit → Weitere Sicherheitseinstellungen. Die Menünamen weichen am stärksten ab, die Schritte sind die gleichen.

Wann es ernst ist — und was dann zu tun ist

Diese Anzeichen gehören **nicht** zu Adware. Wenn eines davon zutrifft, hören Sie mit dem Ausprobieren auf und handeln sofort:

- Es fehlt Geld auf dem Konto oder der Kreditkarte, oder es kommen Abbuchungen, die Sie nicht kennen.
- Sie bekommen SMS mit Bestätigungscodes, die Sie nicht angefordert haben.
- Die Bank-App meldet eine Anmeldung von einem anderen Gerät.
- Eine App lässt sich trotz Geräteadministrator nicht entfernen, oder das Handy reagiert nicht mehr auf Ihre Eingaben.

Dann gilt: WLAN und mobile Daten ausschalten, alles Weitere von einem anderen Gerät aus tun (Passwörter ändern, Bank anrufen, Karte sperren), danach das Handy auf Werkseinstellungen zurücksetzen und Anzeige erstatten. Und ganz wichtig: **keine** „Reinigungssoftware“ kaufen, die Ihnen in der Werbung angeboten wird — die ist Teil des Geschäfts.

Vorbeugen

- Apps nur aus dem Play Store (bzw. der AppGallery) installieren — nicht aus Links, Videos oder „Gratis“-Seiten.
- Bei der Frage „Benachrichtigungen zulassen?“ im Browser grundsätzlich auf „Blockieren“ tippen.
- Einmal im Monat: Einstellungen → Apps durchsehen. Was Sie nicht nutzen, deinstallieren.
- Play Protect eingeschaltet lassen.
- Kein Handy „beschleunigen“ wollen: Reinigungs- und Booster-Apps sind selbst oft die Ursache.

ZUM AUSSCHNEIDEN — CHECKLISTE FÜR DEN ERNSTFALL

Werbung auf dem Handy? Der Reihe nach abhaken.

- ☐ Ruhe bewahren — das Handy ist meist nicht gehackt.
- ☐ Benachrichtigung antippen: Browser oder App?
- ☐ Browser-Benachrichtigungen löschen.
- ☐ Sicheren Modus starten, Werbung beobachten.
- ☐ Unbekannte App deinstallieren.
- ☐ Geräteadministrator-Rechte entziehen, dann löschen.
- ☐ Play Protect scannen lassen.
- ☐ Bei Geldabgang: Bank anrufen, Karte sperren.
- ☐ Unsicher? Anrufen: +34 649 25 07 32

deniapcdoc.com · Anleitung „Werbetrojaner entfernen“

Diese Anleitung steht unter der Lizenz CC BY 4.0 — Weitergabe unverändert erlaubt, Quelle: deniapcdoc.com. Stand: 2026-11-08. Fragen: pcdoc@f1-admin.com · +34 649 25 07 32