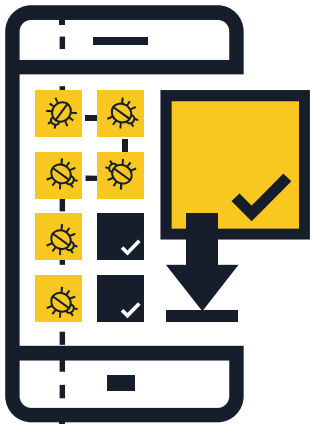
MOBILE MALWARE

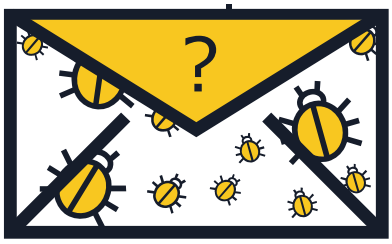
TIPPS & RATSCHLÄGE ZUM SCHUTZ IHRER GERÄTE

1 Installieren Sie Apps nur aus vertrauenswürdigen Quellen



- **Kaufen Sie bei seriösen App Stores** — Informieren Sie sich über die App und deren Herausgeber, bevor Sie die App herunterladen. Seien Sie aufmerksam bei Links in E-Mails und Textnachrichten, die Sie dazu verleiten wollen, Apps einer Drittpartei oder bei einer unbekannten Quelle herunterzuladen.
- **Lesen Sie Rezensionen und Bewertungen anderer Benutzer,** falls vorhanden.
- **Lesen Sie die Zugriffsrechte der App** — Kontrollieren Sie, auf welche Daten die App zugreifen kann und ob sie Ihre Informationen mit externen Parteien teilen könnte. Falls Sie misstrauisch sind oder Ihnen die Bedingungen unbehaglich sind, laden Sie die App nicht herunter.

2 Klicken Sie nicht auf Links oder Anhänge in unerwünschten E-Mails oder Textnachrichten



- **Vertrauen Sie Links in unerwünschten E-Mails oder Textnachrichten** (SMS und MMS) **nicht** — Löschen Sie diese sofort nach Erhalt.
- **Überprüfen Sie verkürzte URLs und QR-Codes genau** — sie könnten auf schädliche Websites weiterleiten oder direkt Malware auf Ihr Gerät herunterladen. Bevor Sie auf den Link klicken, sollten Sie sich eine URL-Vorschauseite anschauen, um sich zu vergewissern, dass die Webadresse seriös ist. Wählen Sie einen QR-Reader, der Ihnen eine Vorschau auf die eingebettete Webadresse zeigt, bevor Sie den QR-Code scannen, und benutzen Sie Mobile-Security-Software, die Sie vor verdächtigen Links warnt.

3 Melden Sie sich auf Webseiten ab, nachdem Sie eine Zahlung getätigt haben

- **Speichern Sie niemals Benutzernamen und Passwörter** — Wenn Sie Ihr Smartphone oder Tablet verlieren oder es gestohlen wird, kann sich der neue Besitzer bei Ihren Konten anmelden. Wenn die Transaktion beendet ist, melden Sie sich ab und schließen Sie nicht nur einfach den Browser.
- **Tätigen Sie Ihre Bankgeschäfte und Online-Einkäufe nicht über öffentliche WLAN-Netzwerke** — Online-Bankgeschäfte und Transaktionen sollten Sie nur über Netzwerke tätigen, die Sie kennen und denen Sie vertrauen.
- **Überprüfen Sie die URL der Seite genau** — Stellen Sie sicher, dass die Webadresse stimmt, bevor Sie sich anmelden oder vertrauliche Informationen senden. Laden Sie eventuell die offizielle App Ihrer Bank herunter, um sicherzugehen, dass Sie immer eine Verbindung zu der echten Seite herstellen.

4 Aktualisieren Sie Ihr Betriebssystem und Ihre Apps regelmäßig

- **Laden Sie Software-Updates für das Betriebssystem Ihrer mobilen Geräte herunter, sobald Sie dazu aufgefordert werden** — Die neuesten Updates gewährleisten nicht nur mehr Sicherheit sondern auch eine bessere Leistung Ihrer Geräte.

5 Schalten Sie WLAN, Ortungsdienste und Bluetooth aus, wenn Sie diese nicht benutzen

- **Schalten Sie WLAN aus, wenn Sie es nicht benutzen** — Cyberkriminelle können auf Ihre Informationen zugreifen, wenn die Verbindung nicht sicher ist. Falls möglich, nutzen Sie eine 3G- oder 4G-Datenverbindung anstelle von Hotspots. Eine weitere Option ist die Nutzung eines VPN-Services (Virtual Private Network) zur Verschlüsselung Ihrer Daten unterwegs.
- **Lassen Sie Apps nicht auf Ihre Ortungsdienste zugreifen, es sei denn es ist notwendig** — Diese Informationen könnten geteilt oder preisgegeben und für standortabhängige „Push-Ads“ (Werbung) genutzt werden.
- **Schalten Sie Bluetooth aus, wenn Sie es nicht benutzen** — Stellen Sie sicher, dass es vollständig ausgeschaltet ist und nicht im Modus „unsichtbar“ steht. Die Standardeinstellungen sind oft so eingestellt, dass andere ohne Ihr Wissen eine Verbindung mit Ihrem Gerät herstellen können. Böswillige Benutzer könnten möglicherweise Ihre Dateien kopieren, auf angeschlossene Geräte zugreifen oder sogar Fernzugriff auf Ihr Telefon erlangen, um Gespräche zu führen und Textnachrichten zu senden, was hohe Kosten zur Folge haben kann.

6 Vermeiden Sie die Weitergabe persönlicher Informationen

- **Antworten Sie niemals mit persönlichen Informationen** auf Textnachrichten oder E-Mails, die angeblich von Ihrer Bank oder einem anderen legitimen Unternehmen stammen. Nehmen Sie stattdessen direkt mit dem Unternehmen Kontakt auf, um die Anfrage bestätigen zu lassen.
- **Überprüfen Sie regelmäßig Ihre Handy-Abrechnung in Bezug auf verdächtige Gebühren** — Falls Ihnen Leistungen in Rechnung gestellt werden, die Sie nicht in Anspruch genommen haben, setzen Sie sich sofort mit Ihrem Dienstanbieter in Verbindung.

7 Kein „Jailbreak/Rooting“ auf Ihrem Gerät

- „Jailbreaking“ oder „Rooting“ ist der Prozess, bei dem die vom Anbieter des Betriebssystems auferlegten Sicherheitsbeschränkungen aufgehoben werden, um vollständigen Zugriff auf das Betriebssystem und Funktionen zu erhalten. — **Ein Jailbreak auf Ihrem Gerät kann dessen Sicherheit erheblich beeinträchtigen und zu Sicherheitslücken führen,** die sonst nicht existieren.

8 Sichern Sie Ihre Daten

- **Viele Smartphones und Tablets sind in der Lage, ein Daten-Back-up drahtlos zu erstellen** — Informieren Sie sich über die von Ihrem Betriebssystem abhängigen Optionen. Wenn Sie ein Back-up für Ihr Smartphone oder Tablet erstellt haben, sind Sie in der Lage, Ihre persönlichen Daten wiederherzustellen, falls Sie das Gerät verlieren, es gestohlen oder unbrauchbar wird.

9 Installieren Sie eine Mobile Security App (Sicherheitssoftware)

- Alle Betriebssysteme sind anfällig für Infektionen. Falls verfügbar, **nutzen Sie eine Mobile-Security-Lösung** die Schadprogramme, Spyware und schädliche Apps entdeckt und blockiert und darüber hinaus Datenschutz- und Diebstahlschutzfunktionen bietet.