APPS

NUR EIN SPIEL?

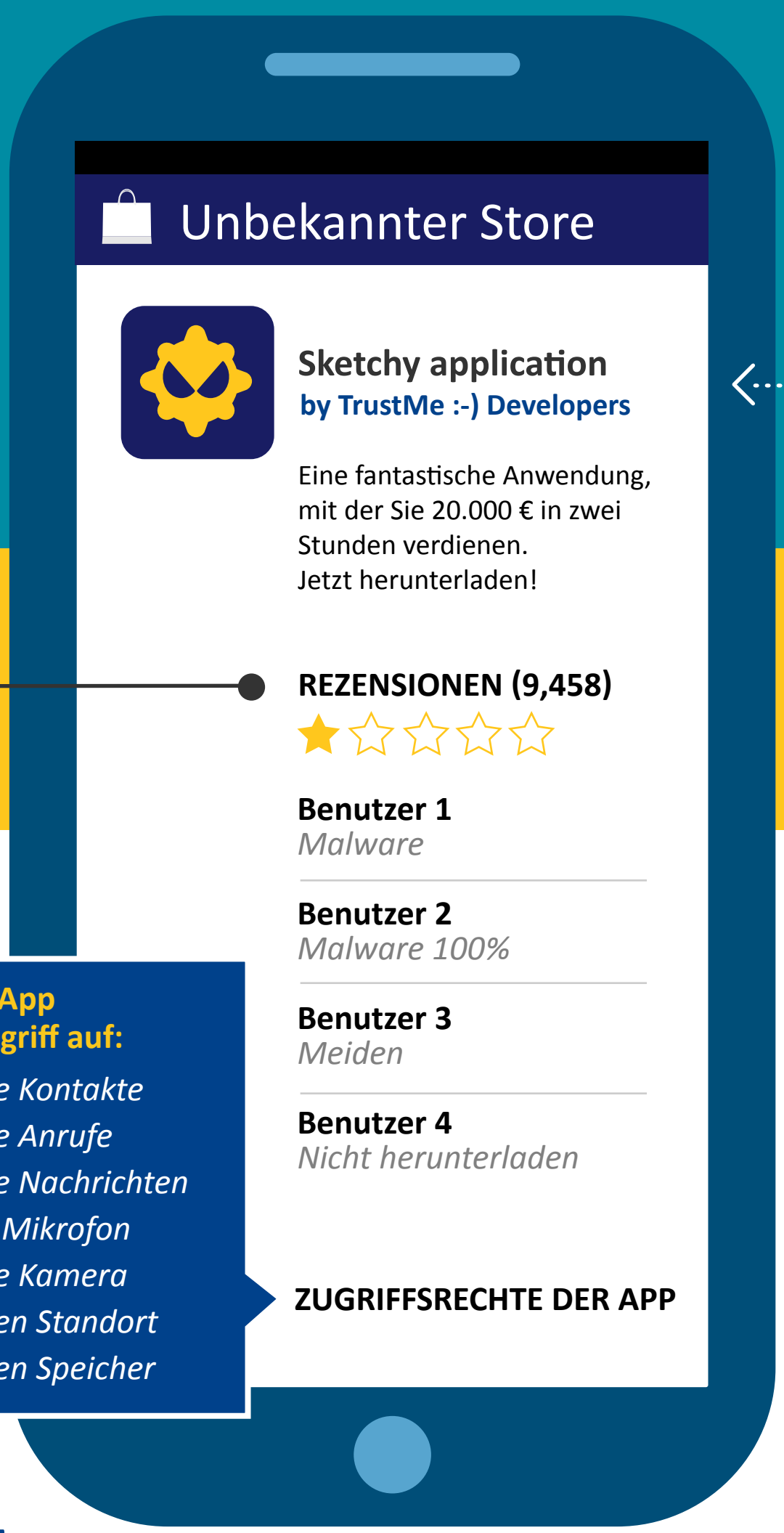
Installieren Sie nur Apps aus offiziellen App Stores

Informieren Sie sich über die App und deren Herausgeber, bevor Sie die App herunterladen. Seien Sie vorsichtig mit 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

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. Sind all diese Zugriffsrechte notwendig? Falls nicht, die App nicht herunterladen.



INSTALLIEREN SIE EINE MOBILE SECURITY APP (SICHERHEITSSOFTWARE)

Diese wird alle auf Ihrem Gerät installierten Apps, die Sie später installieren, überprüfen und Sie warnen, wenn Schadsoftware gefunden wird.

EUROPOL EC3 European Cybercrime Centre

Bundeskriminalamt

#MobileMalware

MOBILE BANKING-MALWARE (SCHADSOFTWARE)

MALWARE KANN SIE GELD KOSTEN

Mobile Banking-Malware wurde entwickelt, um die auf Ihrem Gerät gespeicherten sensiblen Informationen zu Ihren Finanzgeschäften zu stehlen.

WIE VERBREITET SIE SICH?

- Besuch infizierter Webseiten
- Herunterladen maliziöser Apps
- Phishing

WAS SIND DIE RISIKEN?

- Abgreifen Ihrer persönlichen Authentifizierungsdaten
- Unerlaubte Abbuchungen

WAS KÖNNEN SIE TUN?

- Laden Sie die offizielle App Ihrer Bank herunter und stellen Sie sicher, dass Sie immer die echte Webseite der Bank besuchen. (https://)
- Verhindern Sie automatisches Anmelden bei der Online-Banking-Seite oder -App.
- Bankkartennummer oder Passwort nicht teilen und niemandem zeigen.
- Falls verfügbar, installieren sie eine Mobile-Security-App, die Sie bei verdächtigen Aktivitäten warnt.
- Informieren Sie Ihre Bank, wenn Sie Ihr Smartphone verlieren oder Ihre Nummer ändern, damit Ihre Daten aktualisiert werden können.
- Teilen Sie keine Kontoinformationen über Textnachrichten oder E-Mail.
- Nutzen Sie immer ein sicheres WLAN-Netzwerk für den Zugang zur mobilen Seite oder App Ihrer Bank. Nutzen Sie dazu niemals ein öffentliches WLAN!
- Kontrollieren Sie Ihre Kontounterlagen regelmäßig.

EUROPOL EC3 European Cybercrime Centre

Bundeskriminalamt

#MobileMalware

MOBILE
RANSOMWARE

VERABSCHIEDEN SIE SICH VON IHREN DATEIEN

Ransomware verschlüsselt Ihr mobiles Endgerät sowie die darauf gespeicherten Daten und fordert die Bezahlung eines Lösegeldes.

WIE VERBREITET SIE SICH?

Besuch kompromittierter Webseiten.

Herunterladen von gefälschten Versionen legitimer Apps.

Klicken auf bösartige Links und Anhänge in Phishing-E-Mails.

WAS SIND DIE RISIKEN?

Sie müssen Ihr Gerät eventuell auf die Werkseinstellungen zurücksetzen, all Ihre Daten gehen verloren.

Ein Angreifer kann unbegrenzten Zugriff auf Ihr Gerät erhalten und Ihre Dateien/Daten mit Dritten teilen.

WAS KÖNNEN SIE TUN?

Sichern Sie Ihre Daten regelmäßig und halten sie all Ihre Apps und Ihr Betriebssystem auf dem aktuellen Stand.

Erwerben Sie Ihre Apps nicht in unbekannten App-Stores oder Stores von Drittanbietern.

Falls verfügbar, installieren Sie eine Mobile-Security-App, die Sie warnt, wenn Ihr Gerät kompromittiert wurde.

Setzen Sie im Umgang mit E-Mails und Webseiten Ihren gesunden Menschenverstand ein: Öffnen Sie keine verdächtigen oder unglaubwürdigen E-Mails, Links oder Anhänge.

Geben Sie niemandem Administratorrechte für Ihr Gerät.

Zahlen Sie das Lösegeld nicht. Sie finanzieren damit Kriminelle und ermutigen diese, ihre illegalen Aktivitäten fortzusetzen.

EUROPOL EC3 European Cybercrime Centre
Bundeskriminalamt

#MobileMalware

BEDROHUNGEN AUS DEM WEB

GENAU HINSCHAUEN, BEVOR SIE KLICKEN

Sie könnten Ihr Geld, Ihre persönlichen Informationen und sogar Ihre gespeicherten Daten verlieren, wenn Ihr Gerät nicht mehr funktioniert.

WIE KANN DAS PASSIEREN?

PHISHING ANGRIFFE: Verleiten Benutzer dazu, persönliche Informationen preiszugeben, indem sie sich als vertrauenswürdige Institution ausgeben. Sie verbreiten sich über E-Mail, Textnachrichten oder Social Media Plattformen.

WEBSITE BROWSING: Ihr mobiles Gerät kann bereits durch den Besuch einer unsicheren Website infiziert werden.

DATEIDOWNLOAD: Bösartige Links und Anhänge können direkt in eine E-Mail eingebettet sein.

WARUM IST DAS SO EFFEKTIV?

Mobile Geräte sind **STÄNDIG VERBUNDEN** mit dem Internet.

Die **REDUZIERTE GRÖSSE DES GERÄTBILDSCHIRMS** ist eine generelle Einschränkung. Mobile Browser zeigen URLs auf eingeschränktem Bildschirmplatz, wodurch schwer zu erkennen ist, ob es sich um eine legitime Domain handelt.

VORBEHALTLOSES VERTRAUEN DER NUTZER in den persönlichen Charakter eines mobilen Geräts.

WAS KÖNNEN SIE TUN?

Seien Sie misstrauisch, wenn Sie eine SMS oder einen Anruf erhalten, in dem nach persönlichen Informationen gefragt wird. Sie können feststellen, ob die Nachricht/der Anruf echt ist, indem Sie das Unternehmen direkt unter der offiziellen Nummer anrufen.

Wenn Sie mit Ihrem mobilen Gerät im Internet surfen, vergewissern Sie sich, dass die Verbindung über HTTPS gesichert ist. Das können Sie am Anfang der URL kontrollieren.

Klicken Sie nie auf einen Link/Anhang in einer unerwünschten E-Mail oder SMS. Löschen Sie diese sofort.

Seien Sie vorsichtig, wenn Sie auf einer Seite mit schlechter Grammatik, Rechtschreibfehlern oder geringer Auflösung landen.

Falls verfügbar, installieren sie eine Mobile-Security-App, die Sie bei verdächtigen Aktivitäten warnt.

EUROPOL EC3 European Cybercrime Centre

Bundeskriminalamt

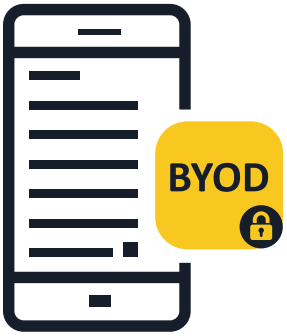
#MobileMalware

MOBILE MALWARE

TIPPS UND HINWEISE FÜR UNTERNEHMEN

1 Informieren Sie Ihre Mitarbeiter über die Risiken

- Mobiles Arbeiten lässt die Grenzen zwischen geschäftlicher und privater Nutzung verschwimmen. Unternehmen können durch einen Angriff, der zunächst gegen das mobile Gerät eines Einzelnen gerichtet war, erheblich getroffen werden. Ein mobiles Gerät ist ein Computer und sollte dementsprechend abgeschirmt werden.

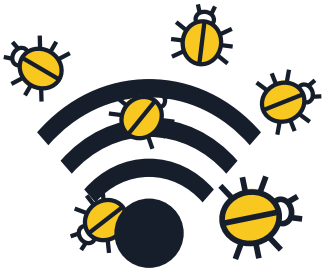


2 Legen Sie unternehmensinterne Richtlinien für Bring Your Own Device (BYOD) fest

- Mitarbeiter und Mitarbeiterinnen, die ihre eigenen mobilen Geräte (BYOD) benutzen, um auf Unternehmensdaten und -systeme zuzugreifen (auch wenn es sich nur um E-Mail, Kalender oder Kontaktdaten handelt) sollten Unternehmensrichtlinien folgen. Wählen Sie die Technologien, die zum Managen und zur Sicherung mobiler Geräte gewählt werden, sorgfältig aus und bringen Sie Ihre Mitarbeiter dazu, umsichtig zu handeln.

3 Nehmen Sie Richtlinien für mobile Geräte in Ihre Sicherheitsarchitektur auf

- Wenn ein Gerät die Sicherheitsrichtlinien nicht erfüllt, sollte eine Verbindung mit dem Unternehmensnetzwerk und Zugang zu Unternehmensdaten nicht gestattet werden. Unternehmen sollten Ihr eigenes Mobile Device Management (MDM) oder Enterprise Mobility Management (EMM) einsetzen.
- Ergänzend dazu ist es entscheidend, eine Mobile Threat Defence-Lösung zu installieren. Das sorgt für erhöhte Sichtbarkeit und kontextuelle Sensibilisierung für Gefahren auf App-, Netzwerk- und Betriebssystemniveau.

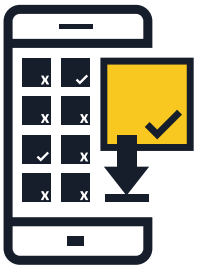


4 Seien Sie vorsichtig bei der Nutzung öffentlicher WLAN-Netzwerke für den Zugriff auf Unternehmensdaten

- Öffentliche WLAN-Netzwerke sind im Allgemeinen nicht sicher. Wenn ein Mitarbeiter/eine Mitarbeiterin am Flughafen oder in einem Café über eine kostenlose WLAN-Verbindung auf Unternehmensdaten zugreift, können die Daten böswilligen Benutzern ausgesetzt sein. Unternehmen wird geraten, Richtlinien zur Nutzung öffentlicher WLAN-Netzwerke zu entwickeln.

5 Betriebssysteme und Apps auf dem aktuellen Stand halten

- Empfehlen Sie Ihren Mitarbeitern, Software-Updates für das Betriebssystem Ihrer mobilen Geräte herunterzuladen, sobald Sie dazu aufgefordert werden. Informieren Sie sich, insbesondere für Android, über die Updaterichtlinien des Mobilfunkanbieters und Geräteherstellers. Die neuesten Updates gewährleisten nicht nur mehr Sicherheit sondern auch eine bessere Leistung des Geräts.



6 Installieren Sie Apps nur aus vertrauenswürdigen Quellen

- Unternehmen sollten für mobile Geräte, die Verbindungen zum Firmennetzwerk herstellen, nur die Installation von Apps aus offiziellen Quellen erlauben. Eine Alternative ist ein firmeneigener App Store, über den Endnutzer auf vom Unternehmen genehmigte Apps zugreifen und sie herunterladen und installieren können. Ihr Sicherheitsanbieter kann Sie bei der Einrichtung des Stores beraten, oder Sie lassen ihn betriebsintern entwickeln.

7 Verhindern Sie Jailbreaking/Rooting

- „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. Geräte mit Root-Zugriff sollten in der Unternehmensumgebung nicht zugelassen werden.

8 Erwägen Sie Cloud-Storage-Alternativen (Webbasierte Speicherung)

- Mobile Nutzer wollen häufig nicht nur über ihren Firmen-PC auf wichtige Dokumente zugreifen sondern auch über ihre privaten Telefone oder Tablets außerhalb des Büros. Unternehmen sollten die Verwendung eines sicheren Cloud-basierten Speichersystems und Daten-Synchronisierungsdienstes erwägen, um auf sichere Weise auf diese Bedürfnisse einzugehen.

9 Lassen Sie Ihre Mitarbeiter eine Mobile Security App (Sicherheitssoftware) installieren

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

EUROPOL EC3 European Cybercrime Centre

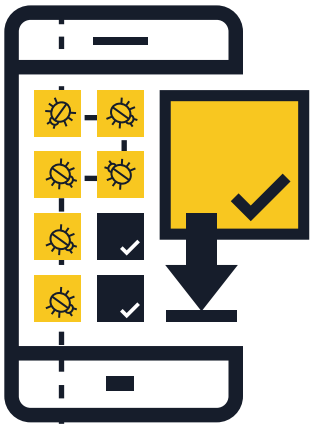
Bundeskriminalamt

#MobileMalware

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

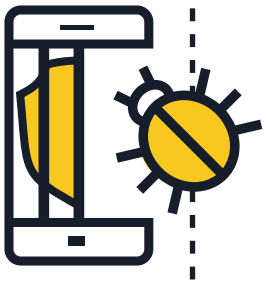
- **Laden Sie Software-Updates für das Betriebssystem Ihrer mobilen Geräte herunter, sobald Sie dazu aufgefordert werden** — Die neuesten Updates gewährleisten nicht nur mehr Sicherheit sondern auch eine bessere Leistung Ihrer Geräte.

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.