Hackerangriffe auf mobile Geräte

Der smarte Ratgeber zum Schutz von Smartphones, Tablets und Laptops

HACKER FINDEN.DE Powered by Audat

Disclaimer

Haftungsausschluss
Die dargestellten Inhalte werden mit größtmöglicher Sorgfalt zusammengestellt. Dennoch müssen wir die Haftung für die Vollständigkeit, Richtigkeit und Aktualität der eigenen Informationen, die auf der Website zur Nutzung bereitgehalten werden, ausschließen, es sei denn, wir handeln vorsätzlich oder grobfahrlässig. Der Haftungsausschluss gilt auch für Linksammlungen, die zurzeit Bestehen oder in Zukunft bestehen werden.

Rechtlicher Hinweis
Alle Informationen auf den Seiten dieser Website dienen der allgemeinen Information. Sie stellen keine Rechtsberatung im Einzelfall dar, können und sollen diese auch nicht ersetzen. Alle Informationen auf den Seiten dieser Website dienen der allgemeinen Information. Sie stellen keine Rechtsberatung im Einzelfall dar, können und sollen diese auch nicht ersetzen.

Die Inhalte unserer Website sind urheberrechtlich geschützt. Soweit Sie die Inhalte für Ihre eigenen beruflichen oder persönlichen Zwecke benötigen, räumen wir Ihnen das Recht ein, die bereitgestellten Texte ganz oder teilweise zu speichern und zu drucken.

Die Speicherung und Vervielfältigung von Bildmaterial oder Grafiken aus unserer Website ist nicht gestattet.

Wenn Sie weitere Fragen oder Anmerkungen haben, kontaktieren Sie uns per Mail: hilfe@hacker-finden.de

Handy und Tablets

Das Smartphone ist das wichtigste Gerät im Leben vieler Menschen. Deshalb ist es unglaublich wichtig, dass es richtig gesichert ist, egal ob Sie ein Android-Gerät oder ein iPhone besitzen.

Kaufen Sie ein iPhone

Okay, das klingt vielleicht ein bisschen direkt, aber iPhones sind im Allgemeinen sicherer als Android-Geräte. Deshalb haben Menschen, die dem Risiko ausgesetzt sind, gehackt zu werden, wie Anwälte und Politiker, in der Regel ein iPhone.
iPhones erhalten außerdem garantiert fünf Jahre lang nach ihrer Veröffentlichung Updates.

Die sichersten Android-Geräte sind die von Google hergestellten Pixel-Telefone (früher Nexus genannt).

Aktualisieren Sie so bald wie möglich

Dieser immer wiederkehrende Tipp steht nach wie vor ganz oben auf der Liste: Aktualisieren Sie Ihre mobilen Geräte immer so schnell wie möglich. Updates beheben Sicherheitslücken, die es Hackern ermöglichen, Ihr Smartphone oder Tablet zu durchdringen.
Aktualisieren Sie auch regelmäßig Ihre Apps. Auch diese können Sicherheitslücken enthalten, die Hackern den Zugriff auf Ihre privaten Daten ermöglichen.

Aktivieren Sie die Verschlüsselung

Die Verschlüsselung sorgt dafür, dass Ihre Daten, z. B. Ihre Nachrichten und Bilder, in einem digitalen Tresor gespeichert werden. Bei allen iPhones und den meisten Android-Telefonen ist die Verschlüsselung standardmäßig aktiviert, aber bei einigen Android-Telefonen müssen Sie die Verschlüsselung manuell einschalten.

Die Option zum Einschalten der Verschlüsselung finden Sie unter Einstellungen > Sicherheit.

Was ist, wenn jemand Ihr Telefon findet und es mit einem Computer verbindet?

Die Verschlüsselung stellt sicher, dass diese Person nicht in der Lage ist, alle Ihre Chatprotokolle und Bilder zu sehen. Diese können nur eingesehen werden, wenn der richtige Passcode eingegeben wird, der der Schlüssel zu Ihrem eigenen digitalen Tresor ist.
Deshalb ist es sehr wichtig, dass Sie Ihre mobilen Geräte mit einem Passcode sperren, wenn Sie sie nicht benutzen.

Verwenden Sie einen sechsstelligen Code und den Fingerabdruckscanner

Durch die **Verwendung eines Codes** verhindern Sie, dass andere auf Ihr Telefon oder Tablet zugreifen. Wählen Sie einen sechsstelligen Code, den nur Sie kennen, und keinen Standardcode wie 0-0-0-0-0-0, 1-2-3-4-5-6 oder 1-1-2-2-3-3.

Es ist auch **nicht** empfehlenswert, Ihr Geburtsdatum zu verwenden, genau wie jede andere Kombination, die auf persönlichen Informationen basiert.
iPhones und einige Android-Telefone ermöglichen es Ihnen auch, eine Option zu aktivieren, die alle Inhalte des Telefons vollständig löscht, wenn der falsche Code mehr als zehnmal eingegeben wird. Dies kann als zusätzliche Sicherheitsmethode dienen, kann aber auch ziemlich riskant sein, wenn Sie keine Sicherungskopie Ihres Geräts haben.

In vielen Fällen ist es einfacher, den **Fingerabdruckscanner** zu verwenden. Er funktioniert schneller und ist sicherer, weil jemand nicht einfach Ihren Fingerabdruck kopieren kann, um Ihr Telefon zu entsperren. Wenn Sie den Fingerabdruckscanner vorübergehend deaktivieren möchten, schalten Sie Ihr Gerät aus und wieder ein. Sie werden dann aufgefordert, Ihren Passcode einzugeben, um auf Ihr Gerät zuzugreifen. Wenn Sie keinen Fingerabdruckscanner auf Ihrem Android-Telefon haben, können Sie auch ein Muster erstellen, um es zu entsperren.

Auch Ihre **SIM-Karte** hat einen Code. Sie können diesen Code bearbeiten und ihn in den Einstellungen Ihres Smartphones in einen sechsstelligen Code ändern, anstatt den Standard 0-0-0-0 zu verwenden. Es ist ratsam, alle Ihre Kontakte auf Ihr Telefon zu übertragen und sie von der SIM-Karte zu entfernen. Wenn Sie Ihr Telefon verlieren, können die persönlichen Daten Ihrer Kontakte nicht von der SIM-Karte extrahiert werden.

Installieren Sie nur Apps aus dem App Store oder von Google Play

Die meisten Telefone, die Malware enthalten, werden durch Apps infiziert, die nicht über die offiziellen App-Stores installiert wurden. Dies geschieht in der Regel, wenn Menschen eine kostenpflichtige App oder ein Spiel kostenlos installieren wollen.

In dieser "kostenlosen" App kann Malware versteckt sein, die zum Stehlen von Kreditkartendaten verwendet wird. Dies gilt sowohl für Android- als auch für iOS-Telefone.

Android stellt ein weiteres Risiko dar: Im Google Play Store gibt es viele Apps, die zwar legitim erscheinen, aber dennoch Malware enthalten. Stellen Sie sicher, dass Sie sich vor dem Herunterladen einer App gründlich informieren. Googeln Sie den Namen der App, lesen Sie Bewertungen und prüfen Sie, wie oft die App bereits installiert wurde. Kurz gesagt: Installieren Sie nicht einfach irgendeine App auf Ihrem Android-Telefon oder -Tablet.

Es ist auch wichtig, die Berechtigungen einer App zu überprüfen. Eine Taschenlampen-App zum Beispiel sollte keinen Zugriff auf Ihre Kontakte benötigen. Sie können die Berechtigungen von Apps sowohl auf iOS als auch auf Android überprüfen und bearbeiten. Bei Android gehen Sie zu Einstellungen > Apps und bei iOS zu Einstellungen > Datenschutz.

Antivirus für ihr Mobilgerät 

Android-Nutzer sollten ein Virenschutzprogramm auf ihrem Smartphone oder Tablet installieren.
ESET (15€ pro Jahr), **BitDefender** (15€ pro Jahr) und **Kaspersky** (15€ pro Jahr) sind allesamt eine ausgezeichnete Wahl.
Von den beiden letztgenannten können Sie kostenlose Versionen herunterladen, die jedoch weniger Funktionen bieten.

Die Installation eines Virenschutzes auf Ihrem iOS-Gerät ist sinnlos. Das Apple-Betriebssystem gewährt diesen Anwendungen nicht die erforderlichen Berechtigungen, um Ihr Telefon oder Tablet auf Viren zu überprüfen. Installieren Sie stattdessen die App **iVerify** (2,99€), die Ihr Betriebssystem auf Anomalien überprüft, die darauf hindeuten, dass Ihr Gerät möglicherweise kompromittiert wurde. iVerify bietet außerdem eine Reihe nützlicher Anleitungen, um die Sicherheit Ihres iPhones oder iPads zu erhöhen.

Zusätzlich zum Virenscan gibt es eine Möglichkeit, zu überwachen, welche Apps auf Ihrem Android-Gerät eine Verbindung zum Internet herstellen. Sie können herausfinden, welche Daten von Ihrem Telefon oder Tablet gesendet werden. Glasswire, die Firewall für Windows, hat auch eine Android-App (5€ pro Jahr), mit der Sie den Zugriff auf das Internet durch invasive oder bösartige Apps blockieren können.

Starten Sie Ihr Gerät neu

Ein Neustart Ihres Telefons oder Tablets ist eine gute Möglichkeit, Ihr Gerät vor Hackern zu schützen. In vielen Fällen wird durch einen Neustart jegliche Malware entfernt, die zuvor installiert wurde. Hacker werden es schwer haben, nach einem Neustart Zugriff auf Ihr Gerät zu erhalten. Ein regelmäßiger Neustart Ihres Telefons oder Tablets (einmal pro Woche) hat noch einen weiteren Vorteil: Das Betriebssystem wird weiterhin reibungslos funktionieren.

Wifi und Bluetooth

Schalten Sie WiFi und Bluetooth aus, wenn Sie sie nicht brauchen. *Dritte können Sie über WiFi und Bluetooth verfolgen*. Sie könnten zum Beispiel Ihren Weg zur Bushaltestelle verfolgen. Wenn Sie WiFi oder Bluetooth unterwegs nicht benötigen, sollten Sie sie in den Einstellungen Ihres Geräts vorübergehend ausschalten. So schützen Sie sich auch vor Angriffen über WiFi und Bluetooth.

Wenn Sie in der Vergangenheit eine Verbindung zu einem WiFi-Netzwerk hergestellt haben, verbindet sich Ihr mobiles Gerät automatisch mit diesem Netzwerk, wenn Sie in der Nähe sind. Dies birgt ein gewisses Risiko. Hacker erstellen oft gefälschte WiFi-Netzwerke mit Namen, die mit den Netzwerken identisch sind, mit denen Sie vielleicht schon einmal verbunden waren, z. B. Starbucks WiFi oder McDonald's Free WiFi. Da Ihr Mobilgerät diese Netzwerke erkennt, versucht es, sich automatisch mit ihnen zu verbinden. Dies ist nur eine weitere Möglichkeit für Kriminelle, zu überwachen, was Sie im Internet tun, und dabei Passwörter und andere persönliche Daten abzufangen.

Es ist ratsam, die Liste der vertrauenswürdigen WiFi-Netzwerke von Zeit zu Zeit zu bereinigen. Wenn Sie sich beispielsweise mit dem WiFi-Netzwerk eines Hotels verbinden, löschen Sie das Netzwerk anschließend aus dem Speicher Ihres Geräts. Öffnen Sie dazu die Einstellungen Ihres Geräts und drücken Sie auf Vergessen, nachdem Sie das betreffende WiFi-Netzwerk ausgewählt haben. Sie können Ihr Android- und iOS-Gerät in den WLAN-Einstellungen auch so einstellen, dass es sich nicht automatisch mit einzelnen WiFi-Netzwerken verbindet.

Benachrichtigungen

Keine Benachrichtigungsvorschau im Sperrbildschirm anzeigen

Benachrichtigungen können sensible Informationen enthalten, wie z. B. ein Passwort, das Ihnen ein Freund über WhatsApp geschickt hat, oder Anmeldecodes, die per Textnachricht verschickt wurden. Wenn Sie Benachrichtigungen auf dem Sperrbildschirm (Android, iOS) ausblenden, kann niemand den Inhalt sehen. Erst wenn Sie Ihr Telefon entsperren, können Sie sehen, was in den Benachrichtigungen steht.

Sichern Sie Ihre Geräte!

Backups sind unglaublich wichtig. Sollte Ihr Telefon gestohlen werden, können Sie die Sicherungskopie jederzeit auf einem anderen Telefon wiederherstellen. Google und Apple bieten Funktionen zur vollständigen Sicherung Ihres Telefons. Für viele Benutzer sind Bilder das Wichtigste auf ihrem Handy. Sichern Sie diese mit Diensten wie iCloud, Google Fotos und Dropbox. Vergessen Sie nicht, die Zwei-Faktor-Authentifizierung für diese Dienste zu aktivieren.

Fazit:

In der digitalen Welt kann es immer zu individuellen Problemen und Lösungen kommen. Wenn Sie schnell, einfach und diskret Handlungsempfehlungen erhalten und gemeinsam mit einem Experten das Problem lösen wollen, erhalten Sie hier eine kostenlose Ersteinschätzung: hilfe@hacker-finden.de.

IT-Hilfe von Experten erhalten

Schnell, einfach & diskret

Wurden Sie gehackt oder erpresst?
Haben Sie den Zugang zu Ihrem Konto verloren?
Müssen Sie sensible Bilder oder Videos entfernen?
Wurde Ihre ID missbraucht?
Wollen Sie eine Beweissicherung für Strafverfolgung?
Möchten Sie Cybermobbing stoppen?
Haben Sie ein Smartphone- oder Computerproblem?
Sind Sie Opfer von Online-Betrug?

Wir helfen Ihr Problem zu lösen

Bei Fragen oder IT-Notfällen einfach ein Online Videogespräch mit einem Experten buchen:
https://www.hacker-finden.de/kontakt/
oder schreiben Sie uns an hilfe@hacker-finden.de

Weitere e-Books: www.hacker-finden.de/ebooks
Weitere Informationen: www.hacker-finden.de

Es gibt Situationen, die sehr fortgeschritten sind und bei denen bestimmte Arten von Online-Schwachstellen oder Hacker-Angriffen die Schadensursache sein können. Wenn die Best-Practice-Schritte nicht zur Behebung führen oder Sie Informationen über den Täter herausfinden wollen, buchen Sie sich eine persönliche kostenlose Ersteinschätzung mit einen Experten:

JETZT STARTEN

HACKER FINDEN.DE Powered by Audat