

Wie sicher ist Ihr Mobilgerät?

Die meisten Leute haben ein Smartphone, aber die wenigsten denken an die Sicherheitsbedrohungen, die mit der Nutzung dieser Mobilgeräte verbunden sind. Mobilgeräte sind anfällig für ganz unterschiedliche Bedrohungen. Cyberkriminelle greifen immer häufiger Mobilgeräte an und versuchen, Smartphones mit schädlichen Anwendungen zu infizieren. Sie können dann ohne Ihr Wissen personenbezogene Daten oder Geschäftsgeheimnisse stehlen.

Das gilt selbst dann, wenn Sie eine Sicherheits- oder Antivirus-App installiert haben. Für den Schutz Ihres Smartphones müssen Sie mehr tun. Gewöhnen Sie sich am besten Praktiken zum Schutz Ihres Mobilgeräts an, um Probleme mit Datenschutz oder Sicherheit im Voraus abzuwenden.

Welche Praktiken zum Schutz von Mobilgeräten sind sinnvoll?

Mithilfe dieser Best Practices können Sie das Risiko von Exploits auf Ihren Mobilgeräten minimieren:

1. **Stellen Sie sicher, dass das Betriebssystem Ihres Smartphones immer auf dem neuesten Stand ist.** Für Betriebssysteme werden häufig Updates bereitgestellt, die Sicherheitslücken schließen. Auf Mobilgeräten mit veralteten Betriebssystemen können diese Sicherheitslücken für Angriffe ausgenutzt werden.
2. **Laden Sie nur vertrauenswürdige Apps aus Ihrem App-Store herunter.** Offizielle App-Stores entfernen in der Regel Anwendungen, die Malware enthalten. Manchmal schaffen es solche gefährlichen Apps jedoch durch die Kontrollen und werden von nichts ahnenden Personen heruntergeladen. Informieren Sie sich, lesen Sie die Bewertungen und achten Sie auf die Anzahl der Downloads. Laden Sie niemals Anwendungen von anderen Quellen als offiziellen App-Stores herunter.
3. **Überprüfen Sie die Berechtigungen von Apps.** Gewähren Sie nur Berechtigungen, die für die Funktion der App relevant sind. Anwendungen fordern gewöhnlich Berechtigungen für den Zugriff auf Dateien, Ordner, andere Anwendungen und Daten an, bevor sie heruntergeladen werden können. Gewähren Sie diese Berechtigungen nicht blindlings. Wenn zu viele unnötige Berechtigungen angefordert werden, suchen Sie sich eine andere App aus dem App-Store aus.
4. **Legen Sie ein sicheres Passwort fest.** Viele Leute sperren ihr Smartphone noch immer nicht mit einem Passwort. Wenn das Gerät verloren geht oder gestohlen wird, können die Diebe ganz einfach auf die auf dem Smartphone gespeicherten Informationen zugreifen.
5. **Seien Sie bei der Nutzung öffentlicher WLAN-Netzwerke vorsichtig.** Cyberkriminelle verwenden Technologie, mit der sie Ihre Onlineaktivitäten ausspionieren können. Unterlassen Sie es daher, in öffentlichen WLAN-Netzwerken sensible Transaktionen vorzunehmen.



Das KnowBe4 Security Team