



Grundlegende Sicherheitsvorkehrungen für Benutzer von 3CX Apps

Vorsicht ist besser als später das Nachsehen zu haben. Wer grundlegende Schritte für die Sicherheit und den Datenschutz aller Informationen auf seinem Gerät unternimmt, der vermeidet böse Überraschungen.

Dieser Beitrag stellt einige grundlegende Sicherheitsmaßnahmen zur Stärkung der Informationssicherheit für die wachsende Anzahl an 3CX Android und iOS Anwendern vor, damit Ihre Daten außer Reichweite für unbefugte Dritte bleiben.

Die folgenden Hinweise sind abhängig vom Gerät, Modell und Betriebssystem. Beispielsweise befinden sich die Sicherheitseinstellungen für einige Android-Geräte unter *“Sicherheit“*, für andere unter *“Sicherheit & Datenschutz“*. Für Apple-Geräte gibt es nur wenige Unterschiede zwischen den einzelnen iOS-Versionen. Wir empfehlen Ihnen, Ihr Gerät zu erkunden, um die passende Option zu finden.

1 Sichern Sie den Zugriff auf ihr Gerät mittels Passcode oder biometrischem Merkmal

Verwenden Sie immer einen komplexen, aber einprägsamen Entsperrcode, ein Muster, oder alternativ eine biometrische Sicherheitsfunktion wie die Fingerabdruck-, Iris- oder Gesichtserkennung.

Android: Gehen Sie zu *“Einstellungen > Sicherheit > Sperrbildschirm-passwort“* und legen Sie ein komplexes Muster oder ein starkes Passwort fest, welches Sie sich merken können. Für die alternative biometrische Zugangsbeschränkung tippen Sie auf *“Fingerabdruckverwaltung“* oder *“Fingerabdruck-ID“*.

iOS: Gehen Sie zu *“Einstellungen > Touch ID & Code“* bzw. *„Face-ID & Code“* und wählen Sie die gewünschte Sicherungsmethode. Folgen Sie anschließend den Anweisungen auf dem Bildschirm.

2 Lassen Sie Ihr Gerät nicht unbeaufsichtigt und aktivieren sie die Bildschirmsperre

Es ist selbsterklärend, dass vor allem an öffentlichen Orten für unbeaufsichtigte Telefone Ärger vorprogrammiert ist. Bewahren Sie Ihr Gerät bei Nichtgebrauch besser außer Sichtweite auf und stellen Sie sicher, dass der Bildschirm Ihres Telefons schnell gesperrt wird.

Android: Aktivieren Sie die Option *“Bildschirmsperre“* unter *“Einstellungen“* und stellen Sie eine kurze Zeitspanne (z.B. 30 Sekunden) ein, bevor das Gerät in den Ruhemodus wechselt und gesperrt wird.

iOS: Die sicherste Option ist es, die Einstellung *“Passwort anfordern“* auf *“Sofort“* zu setzen. Dann muss das Passwort völlig unabhängig davon wann Sie Ihr Telefon zuletzt entsperrt haben eingegeben werden.

3 Lehen Sie Apps aus unbekanntem Quellen ab

Die Installation oder das Sideloaden von nicht verifizierten Anwendungen kann der kürzeste Weg zu einer Malware-Infektion sein, welche im Nu auf Ihr Telefon und Ihre Informationen übergreift. Installieren Sie daher auf Ihrem Android-Telefon lediglich Apps über den offiziellen Google Play App Store, da dieser Apps regelmäßig in Sachen Sicherheit und Datenschutz überprüft. Verifizieren Sie auch unter *“Einstellungen > Sicherheit“*, dass die Option zur Installation von Apps aus *“externen/unbekannten Quellen“* deaktiviert ist.

iOS ist in dieser Hinsicht viel restriktiver: Um tatsächlich eine App von unbekannter Quelle installieren zu können, muss zuerst das iPhone *“gerootet“* werden – das wird nicht empfohlen.

4 Verschlüsseln Sie Ihre Festplatte

Dies kommt insbesondere zum Tragen, wenn Ihr Gerät verloren geht oder gar gestohlen wird. Ihre Daten können so nicht ohne Weiteres von jedem wiederhergestellt werden, der physischen Zugriff auf Ihr Telefon hat. Da es sich um eine in das jeweilige Gerät integrierte Funktion handelt, müssen Sie Ihr aktuelles Gerät auf Kompatibilität prüfen oder im Fall einer geplanten Neuanschaffung diese Funktion Ihrer persönlichen Features-Checkliste hinzufügen:

Android: Entscheiden Sie sich für ein Handy mit Android 7+ wie zum Beispiel Google's Pixel und das neueste Galaxy von Samsung. Diese Modelle verfügen standardmäßig über eine dateibasierte AES (Advanced Encryption Standard) 256-Bit-Verschlüsselung. Manche Geräte, darunter das Blackberry KEY2, integrieren eine vollständige Festplattenverschlüsselung mit AES 128 Bit.

iOS: Alle iOS-Geräte von Apple verfügen über eine vollständige Festplattenverschlüsselung und eine zusätzliche Verschlüsselungsebene für den Schlüsselbund des Benutzers, welcher die sensibelsten Informationen, z.B. Passwörter und Kreditkartendaten, speichert.

5 Verwerfen Sie nicht-vertrauenswürdige Verbindungen

Wenn Sie eine Verbindung zu einem öffentlichen drahtlosen Netzwerk herstellen müssen, dann stellen Sie zumindest sicher, dass Sie diese Verbindung trennen, sobald Sie fertig sind. Unsichere Netzwerke können leicht kompromittiert werden – und damit auch alle Geräte, welche sich mit diesen verbinden, einschließlich Ihrem Handy.

6 Sichern Sie Ihre Backups

Smartphones enthalten mittlerweile unsere wichtigsten Daten, sei es privat oder geschäftlich. Die Sicherung der Daten auf Ihrem Telefon hilft Ihnen dabei, diese bei Verlust oder Beschädigung wiederherzustellen. Gleichzeitig liegt hier jedoch auch eine Schwachstelle, wenn Backups in die falschen Hände geraten.

Um dieses Risiko zu minimieren, ist es wichtig, dass Sie Ihre Backups schützen:

Android: Ab Android 9 (Pie) verschlüsselt Google standardmäßig die gesicherten Daten Ihres Geräts und speichert diese im von Ihnen gewählten Google Mail-Konto. Wenn Sie benutzerdefinierte Geräte-Backups erstellen, dann stellen Sie sicher, dass diese verschlüsselt und/oder passwortgeschützt sind.

iOS: Stellen Sie in iTunes unter den Sicherungseinstellungen für Ihr Gerät die Option *“iPhone Backup verschlüsseln”* ein. Sie müssen zunächst ein neues Passwort für das iTunes-Backup wählen, bevor Sie ein verschlüsseltes Backup erstellen können. iCloud-Backups werden automatisch verschlüsselt.

6 Seien Sie misstrauisch

Seien Sie besonders vorsichtig, wenn Sie Links und Anhänge von Dritten erhalten. Überprüfen und verifizieren Sie diese, da der Absender – unbeabsichtigt oder absichtlich – versuchen kann, Malware zu installieren, persönliche Daten zu löschen oder Sie anderen Bedrohungen und Betrügereien auszusetzen.

Einige “beliebte” Beispiele:

“DRINGEND! Klicken Sie hier, um zu prüfen, ob Ihr Konto gehackt wurde: [<https://clickme.kom/and/get/your/poison>]”

“Dein Konto ist jetzt gesperrt! Klicken Sie hier und geben Sie Ihre PIN ein, um dieses freizuschalten.”

7 Halten Sie Ihr Telefon auf dem neuesten Stand

Unabhängig von den Unterschieden zwischen Google und Apple unterstützen beide ihre jeweiligen mobilen Plattformen durch regelmäßige Sicherheits- und Stabilitäts-Updates.

Android: Überprüfen Sie auf mögliche Updates unter *“Einstellungen>System>Software-Update”*, um auf Android 7 oder höher zu aktualisieren. Beachten Sie, dass frühere Android- Versionen weniger sicher und anfälliger für Sicherheitsbedrohungen sind. Entscheiden Sie sich für Geräte von Herstellern, die regelmäßig Sicherheits- und Stabilitäts-Updates anbieten, damit Ihr Gerät stets auf dem neuesten Stand bleibt.

iOS: Prüfen und aktivieren Sie die automatischen Updates unter *“Einstellungen>Allgemein>Software-Update”*. Es ist empfehlenswert, auf iOS 12 oder noch besser auf 13 zu aktualisieren. Während die Version 12 über ausreichende Sicherheits- und Datenschutzfunktionen verfügt, führt iOS 13 eine detaillierte App-Standortsteuerung, das Blocken von WiFi- und Bluetooth-Tracking sowie Berechtigungen pro Website ein.