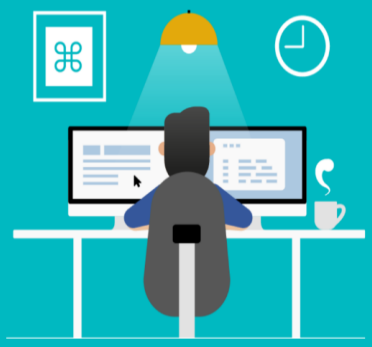
STAY SECURE AS A REMOTE WORKER



SECURITY COURSES
WORK FROM HOME

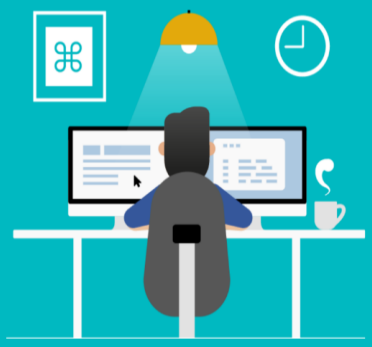
TIPPS ZUR SICHERUNG IHRER MOBILEN GERÄTE

Smartphones und Tablets speichern so viele persönliche und Unternehmensinformationen, dass es sehr schlecht wäre, wenn sie verloren gehen oder gestohlen, gehackt oder auf andere Weise kompromittiert werden. Im Folgenden finden Sie einige grundlegende Tipps, mit denen Sie Ihre mobilen Geräte schützen können, wenn Sie nicht im Büro arbeiten:

✓ LEGEN SIE EIN STARKES PASSWORT FEST

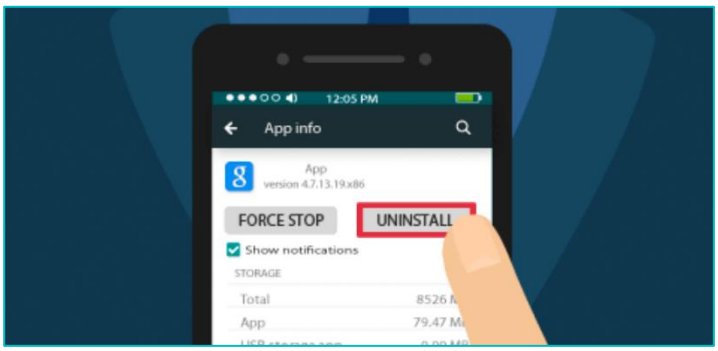
Wie ein Computer benötigt auch ein mobiles Gerät ein sicheres Passwort / eine sichere PIN, um die Inhalte zu schützen. Ohne Passwort kann jeder das Gerät entsperren und Ihre Dateien und gespeicherten Informationen durchsuchen. Stellen Sie sicher, dass Sie eine zufällige Kombination aus Klein- und Großbuchstaben, Zahlen und Symbolen verwenden, und versuchen Sie, für jedes Gerät und Konto ein einzigartiges Passwort zu verwenden.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES WORK FROM HOME

✓ NICHT VERWENDETE APPS LÖSCHEN

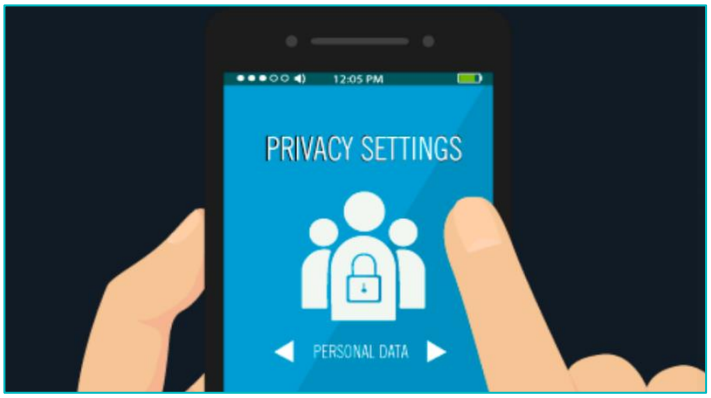


Unordnung ist niemals eine gute Praxis - nicht bei Ihnen zu Hause und schon gar nicht bei Ihren Geräten. Behalten Sie also keine Apps, die in Ihrem Leben und Ihrer Arbeit keine Anziehungskraft mehr haben und/oder nicht mehr verwendet werden. Gehen Sie regelmäßig Ihre App-Liste durch und entfernen Sie diejenigen, die nur Staub sammeln.

✓ AKTIVIEREN SIE „FIND YOUR DEVICE"

„Find your device", zum Aufspüren ihres Geräts, ist eine sehr praktische Funktion, die in allen gängigen Betriebssystemen integriert ist. Falls Sie Ihr Gerät nicht finden können, können Sie es mit dieser Funktion in Echtzeit verfolgen. Wenn der Standort keine Zuversicht aufkeimen lässt, können Sie außerdem aus der Ferne alle Inhalte löschen, damit vertrauliche Informationen nicht in falsche Hände geraten.

✓ SICHERHEITSEIN-STELLUNGEN KONFIGURIEREN

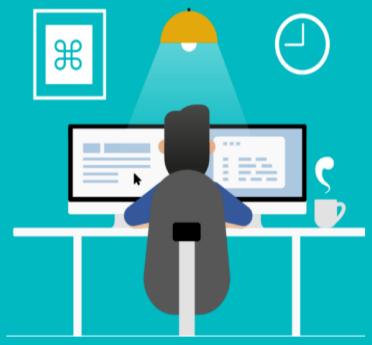


Stellen Sie sicher, dass Sie die Sicherheits- und Datenschutzeinstellungen für jedes Konto auf öffentlichen Webseiten, Apps und in sozialen Netzwerken genau abstimmen. Auf diese Weise können Sie verwalten, was über Sie geteilt wird und wer es sehen kann.

✓ LADEN SIE APPS NUR AUS VERTRAUENSWÜRDIGEN QUELLEN HERUNTER

Wenn Sie eine neue App benötigen, suchen Sie sie bevorzugt im Apple App Store oder im Google Play Store. Diese Plattformen listen nur Apps auf, die deren Standards und Filter erfüllt haben, wodurch die Wahrscheinlichkeit, eine mit Malware infizierten App herunterzuladen, erheblich minimiert wird.

STAY SECURE AS A REMOTE WORKER



SECURITY COURSES WORK FROM HOME

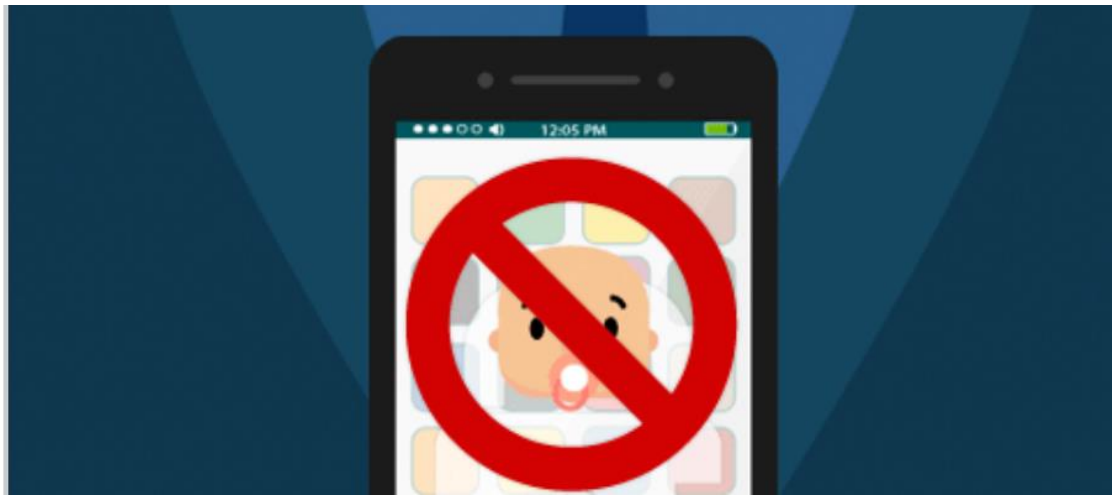
✓ SICHERN SIE IHRE DATEN

Machen Sie es sich zur Gewohnheit, regelmäßig alle auf Ihren Geräten gespeicherten Daten mittels Back-up zu sichern. Im Falle eines Verlusts oder Diebstahls sind die Daten nicht verloren.

✓ AUTOMATISCHE SPERRE EINRICHTEN

Alle Ihre Geräte sollten sich nach kurzer Zeit automatisch sperren (30 Sekunden reichen für mobile Geräte aus) und erst nach Eingabe des richtigen Codes entsperrt werden.

✓ DAS GERÄT VON KINDERN FERNHALTEN



Erlauben Sie Ihren Kindern nicht, Ihr Mobilgerät zu verwenden. Sie könnten auf auffällige Anzeigen klicken oder ungewollt Apps herunterladen, die Ihr Gerät nur allzu leicht gefährden könnten.