tgbw
Türkische Gemeinde in Baden-Württemberg e.V.

Sicherer Umgang
mit dem Smartphone

Unser Alltag ist geprägt von Smartphones: Nachrichten austauschen, Videos anschauen oder kurz im Internet nach etwas surfen. Ein Leben ohne Smartphones ist nicht mehr wegzudenken. Smatphone-Nutzer sollten einige Dinge beachten, um vor bösen Überraschungen wie z.B. Angriffe auf Ihre Daten geschützt zu bleiben.Wir haben für Sie die wichtigsten Tipps zur sicheren Nutzung von Smartphones zusammengestellt.

Unsere Tipps

Bildschirmsperre als Basisschutz

Ihr Smartphone beinhaltet wichtige Informationen. Richten Sie die Bildschirmsperre Ihres Smartphones ein. So schützen Sie Ihre sensiblen Daten vor Ihrem Umfeld und neugierigen Findern oder Dieben. Unbefugte können Ihr Gerät nicht benutzen, auf Ihre Daten zugreifen und weitere Sicherheitsprogramme wie z.B. eine Fernortungs-App nicht deaktivieren.

Offizielle App-Store benutzen

Drittanbieter-Apps können oft mit Schadsoftware verseucht sein. Wenn Sie eine App herunterladen möchten, benutzen Sie den offiziellen App-Store Ihres Smartphones. Bewertungen können dabei Ihnen Hinweis darüber geben, ob die App seriös ist.

Verwendung aktuellster Software

Die Aktualisierung des Betriebssystems und den Apps bringen nicht nur neue Funktionen für das Smartphone, sondern schließen auch entdeckte Sicherheitslücken. Bieten Hersteller neue Updates an, installieren Sie diese umgehend. Denn viele Angriffe zielen auf bekannte Schwachstellen ab, die erst durch Updates der Hersteller geschlossen werden.

Rechte der Apps

Für die Nutzung vieler Apps werden den Anbietern sämtliche Zugriffsrechte wie Standort, Adressbuch oder Kamera vergeben, die nicht bei der App zwingend notwendig sind. Überprüfen Sie kritisch die Zugriffsrechte, die Sie Apps einräumen und schalten Sie diese gegebenfalls aus.

Vorsicht vor öffentlichen WLAN-Netzwerken

Cafés, Züge, Restaurants, Flughäfen bieten kostenlose WLAN-Verbindungen an. In der Regel sind solche WLAN-Netzwerke nicht verschlüsselt. Das bedeutet, dass sich jeder andere Nutzer zwischen Ihr Gerät und den Zugriffspunkt schalten und Ihre Daten mitlesen kann. Löschen Sie die gespeicherten Netzwerke auf Ihrem Gerät. Surfen Sie, wenn möglich nur auf verschlüsselten Seiten. Die verschlüsselten Seiten beginnen mit https:// unverschlüsselte hingegen mit http://

Zwei-Faktor-Authentifizierung

Ob bei Google, Facebook, WhatsApp oder Dropbox – viele Online-Dienste sind voller sensibler Daten. Im Zweifelsfall können Hacker auf Ihre Daten zugreifen. Einige Online-Dienste wie Facebook bieten die Zwei-Faktor-Authentifizierung an: Nachdem Sie sich wie gewohnt mit Name und Passwort angemeldet haben, fragt Sie der Online-Dienst nach einer PIN. Diese bekommen Sie meist als SMS auf Ihrem Gerät. So sperren Sie die Hacker aus. Selbst dann, wenn sie Ihr Passwort geknackt haben.