Verwenden Sie eine Mobile Banking App

Über die Hälfte aller E-Banking Transaktionen werden mit dem Smartphone oder Tablet abgewickelt. Meist kommt dabei eine App des jeweiligen Finanzinstituts zum Einsatz. Mobile Banking hat viele Vorteile, birgt aber auch Gefahren.

So verwenden Sie eine Mobile Banking App sicher:

- Schützen Sie Ihr Mobilgerät mit unseren «5 Schritten für Ihre digitale Sicherheit» (https://www.ebas.ch/5-schritte-fuer-ihre-digitale-sicherheit/) . Nur ein sauberes und sicheres Gerät ermöglicht auch ein sicheres Mobile Banking.
- Übertragen Sie mit Mobile Banking Apps grössere Geldbeträge nicht über die Senden-Funktion, sondern immer nur über die Anfordern-Funktion. So kommt nämlich bei einem Tippfehler etc. nicht das Geld, sondern nur die Anforderung beim falschen Empfänger an.
- Installieren Sie die Mobile Banking App sowie alle anderen Apps nur aus dem offiziellen Store.
- Installieren Sie nur wirklich benötigte Apps und deinstallieren Sie alle nicht (mehr) verwendeten Apps.
- Beschränken Sie die Zugriffsrechte aller Apps aufs Nötigste.
- Verbinden Sie Ihr Gerät unterwegs nur mit vertrauenswürdigen Netzwerken.
- Lassen Sie Ihr Gerät bei Verlust sofort sperren, und setzen Sie es vor Verkauf oder Entsorgung korrekt zurück.

Gefahren und Vorteile von Mobile Banking Apps

Smartphones und Tablets sind (kleine) Computer und damit ähnlichen Gefahren wie klassische Computer ausgesetzt: Datenverlust oder -diebstahl, Malwarebefall, unberechtigter Zugriff usw. Beim mobilen Einsatz kommen darüber hinaus Risiken wie Verlust oder Diebstahl hinzu.

Demgegenüber stehen Vorzüge wie Mobilität und Platzbedarf. Bei der Verwendung einer Mobile Banking App kommt ein weiterer entscheidender Vorteil hinzu: **Im Gegensatz zum klassischen E-Banking mittels Browser erhält der Kunde vom Finanzinstitut eine vorgefertigte und speziell fürs elektronische Banking zugeschnittene Software, welche entsprechend gut abgesichert ist.**

Damit entfallen für den sicherheitsbewussten Anwender ungeliebte Aufgaben wie die manuelle Eingabe der Bankadresse im Browser und die Überprüfung der sicheren Verbindung. Denn im Gegensatz zum Browser erledigt eine Banking App diese Aufgaben im Hintergrund automatisch, und minimiert damit die Gefahr von typischen Anwendungsfehlern wie Tippfehlern sowie Phishing –vorausgesetzt, der Benutzer hält sich an einige Grundregeln.

Sichere Verwendung einer Mobile Banking App

Grundschutz erstellen

Als Erstes müssen die allgemeinen Gefahren bei der Verwendung eines mobilen Geräts minimiert werden. Befolgen Sie dazu auch für mobile Geräte unsere «5 Schritte für Ihre digitale Sicherheit» (https://www.ebas.ch/5-schritte-fuer-ihre-digitale-sicherheit/) . Vergewissern Sie sich insbesondere, dass die automatische Bildschirmsperre mittels Code, Passwort, Fingerabdruck oder Gesichtserkennung eingeschaltet ist.

Das Gebot der Wachsamkeit gilt bei Smartphones und Tablets im Besonderen: Lassen Sie Ihr Gerät nicht unbeaufsichtigt. Achten Sie darauf, dass Sie Ihre Zugangsdaten wie PIN, TAN und Passwörter niemandem mitteilen, immer verdeckt eingeben, und dass Ihnen dabei niemand über die Schulter blickt. Seien Sie vorsichtig beim Öffnen von E-Mails, Anhängen, Messenger-Nachrichten (z.B. WhatsApp) sowie MMS. Auch über MMS und WhatsApp kann Malware verbreitet werden. Klicken Sie auf keine unbekannten Links und löschen Sie Nachrichten von unbekannten Absendern sofort. Prüfen Sie unbekannte Rufnummern vor dem Rückruf.

App-Herkunft beachten

Installieren Sie nur wirklich benötigte Apps und achten Sie darauf, dass diese aus seriöser Quelle stammen, also aus dem offiziellen Store (z.B. Apple App Store oder Google Play Store).

Seien Sie misstrauisch gegenüber Apps mit geringer Reputation oder Empfehlungen von Unbekannten. Informieren Sie sich vor der Installation einer App, wenn Ihnen der Anbieter nicht bekannt ist.

Überprüfen Sie von Zeit zu Zeit auch, welche Apps Sie überhaupt noch verwenden, und deinstallieren Sie veraltete und nicht mehr benötigte Anwendungen – jede zusätzliche App ist eine mögliche Sicherheitslücke.

Melden Sie Fehlermeldungen und ungewöhnliche Funktionsweisen Ihrer Banking App umgehend Ihrem Finanzinstitut (https://www.ebas.ch/partner/) .

Zugriffsrechte beschränken

Viele Apps räumen sich ohne erkennbaren Grund umfassende Rechte ein. Ein Zugriff auf beispielsweise Standortdaten, Adressbuch oder den Telefonstatus ist nicht bei jeder App notwendig. Prüfen Sie daher kritisch, ob die Zugriffsrechte zum Erfüllen der Funktionalität wirklich notwendig sind, und deaktivieren Sie nach Möglichkeit alle nicht benötigten Rechte.

Netzwerk-Anbieter überprüfen

Ihr Smartphone oder Tablet kann auf verschiedene Arten eine Verbindung zu Ihrem Finanzinstitut herstellen. Unterwegs verbindet sich Ihr Gerät mit unterschiedlichen Netzen. Wenn eine WiFi- bzw. WLAN-Verbindung verwendet wird, sollten Sie deren Vertraulichkeit sicherstellen: Unseriöse Anbieter «kostenloser» WiFi-Netze könnten die Banking App zum falschen Server weiterleiten und Ihre eingegebenen Zugangsdaten abgreifen.

Bei Android-Geräten können Sie zusätzlich eine Firewall-App zur Überwachung und Absicherung der aktiven Verbindungen einrichten. Bei iOS-Geräten (iPhone / iPad) ist dies weder möglich noch erforderlich.

Verlust, Verkauf und Entsorgung korrekt abwickeln

Gerät Ihr Smartphone oder Tablet in falsche Hände, können darauf gespeicherte Dateien oder Zugangsdaten unter Umständen abgegriffen und missbraucht werden.

Verlorene oder gestohlene Geräte können Sie mithilfe verschiedener Apps aus der Ferne sperren. Dadurch sind Ihre persönlichen Daten auf dem Gerät gelöscht und nicht mehr aufzurufen. Nach erfolgter Geräte-Sperrung sollten Sie

auch die SIM-Karte bei Ihrem Telekom-Anbieter sperren lassen.

Wenn Sie nicht möchten, dass Ihre gespeicherten Daten beim Verkauf oder bei der Entsorgung Ihres Gerätes in falsche Hände geraten, sollten Sie bedenken, dass Datenspuren verbleiben können, wenn nicht vorher alle Datenspeicher sicher gelöscht wurden. Wie das funktioniert, ist zum Beispiel auf der Internetseite von Apple (https://support.apple.com/de-de/HT201274) sowie auf SRF (https://www.srf.ch/sendungen/kassensturz-espresso/services/handy-daten-sicher-loeschen-so-funktioniert-s) beschrieben. Die SIM-Karte sollten Sie natürlich ebenfalls entfernen und – falls Sie diese nicht weiterverwenden möchten – vernichten.

Unter «Mobile Banking» versteht man die Abwicklung von Bankgeschäften über mobile Geräte wie Smartphone oder Tablet.

Sie haben die Möglichkeit, mittels Browser oder immer öfter mit speziellen Apps auf Ihr E-Banking zuzugreifen.

Merkblatt: *Download (PDF) (https://www.ebas.ch/wp-content/uploads/2019/10/mobilebankingSKP_de.pdf)*