Mobile Banking und Mobile Payment

So verwenden Sie Ihr Mobilgerät im Zahlungsverkehr sicher!

Ihre Polizei und die Schweizerische Kriminalprävention (SKP) – eine interkantonale Fachstelle der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)

Sie tätigen Bankgeschäfte auf Ihrem Tablet und bezahlen an der Kasse am liebsten bargeldlos mit Ihrem Smartphone?

Mobile Banking und Mobile Payment sind bereits heute zwei weit verbreitete Anwendungen auf Mobilgeräten. Aber, was gilt es betreffend Sicherheit zu beachten und wie können finanzielle Schäden vermieden werden?

Die Vorteile von Mobilgeräten wie Smartphones und Tablets liegen auf der Hand: Sie sind handlich, immer dabei und mit dem Internet verbunden. Wie bei Ihrem Computer zuhause gibt es Risiken bei der Nutzung von Mobilgeräten. Die folgenden Tipps zeigen, wie Sie Ihr Mobilgerät möglichst gut schützen können.

Halten Sie Ihr Mobilgerät aktuell und sauber!

- **Installieren Sie nur Apps aus dem offiziellen Store!** Laden Sie nur Apps aus dem Apple App Store oder Google Play Store herunter. Seien Sie dabei misstrauisch gegenüber Apps mit fehlenden Bewertungen. Informieren Sie sich vor der Installation über den Anbieter der App, wenn Ihnen dieser unbekannt ist.
- **Machen Sie regelmässig Updates!** Aktivieren Sie die automatische Update-Funktion auf Ihrem Mobilgerät und installieren Sie umgehend die verfügbaren Updates für das Betriebssystem und die installierten Apps. Deinstallieren Sie veraltete oder nicht mehr benötigte Apps, um Sicherheitsrisiken zu vermeiden.
- **Seien Sie beim Öffnen von Nachrichten unbekannter Absender vorsichtig!** Klicken Sie nicht auf Links und laden Sie in E-Mails, Messenger-Nachrichten (z. B. WhatsApp) sowie MMS keine Anhänge von unbekannten Absendern herunter. Dahinter könnte sich Schadsoftware (Malware) verstecken. Installieren Sie auf Ihrem Android-Gerät ausserdem eine Virenschutz-App. Bei iOS-Geräten ist dies nicht möglich, aber auch nicht erforderlich.
- **Lassen Sie nur benötigte und vertrauenswürdige Verbindungen zu!** Ihr Mobilgerät kann sich via WiFi/WLAN, NFC, Bluetooth, Infrarot, 3G/4G/5G, USB etc. mit dem Internet oder anderen Geräten verbinden. Aktivieren Sie immer nur die Verbindungsart, die Sie nutzen möchten und akzeptieren Sie keine Verbindungsanfragen von unbekannten Geräten.

Beachten Sie gewisse Grundregeln bei den Einstellungen Ihres Mobilgerätes!

- **Beschränken Sie die Zugriffsrechte der jeweiligen App!** Prüfen Sie, ob eine App die Zugriffsrechte zum Erfüllen der Funktionalität benötigt und deaktivieren Sie die nicht benötigten Rechte. Umfassende Rechte, wie z. B. der Zugriff auf Standortdaten, die Kamera oder das Adressbuch sind nicht für jede App notwendig.
- **Seien Sie mit der Weitergabe Ihrer Ortsangaben zurückhaltend!** Verwenden Sie Lokalisierungsdienste mit Bedacht und speichern Sie keine Positionsangaben in Fotos, die Sie z. B. auf Social Media hochladen.
- **Speichern Sie keine Zugangsdaten auf Ihrem Mobilgerät oder in der Cloud!** Speichern Sie Zugangsdaten wie PIN, TAN und Passwörter, die Sie im Browser oder Store verwenden, niemals auf Ihrem Mobilgerät und in der Cloud. Nutzen Sie einen Passwortmanager und deaktivieren Sie die automatische Speicherung von Passwörtern auf Ihrem Mobilgerät.

Schützen Sie Ihr Mobilgerät vor unbefugten Zugriffen!

- **Nutzen Sie die vorhandenen Sicherheitseinstellungen Ihres Gerätes!** Aktivieren Sie die Bildschirmsperre mit einem starken Passwort, Fingerabdruck oder Gesichtserkennung. Geben Sie Ihre Zugangsdaten nicht weiter.
- **Sperren Sie Ihr Mobilgerät bei Diebstahl oder Verlust sofort!** Verlorene oder gestohlene Mobilgeräte können Sie mithilfe verschiedener Apps aus der Ferne sperren. So sind Ihre persönlichen Daten nicht mehr abrufbar. Lassen Sie ausserdem die SIM-Karte von Ihrem Provider sperren.
- **Setzen Sie Ihr Mobilgerät vor dem Verkauf oder der Entsorgung auf die Werkeinstellung zurück!** Wenn Sie Ihr Gerät zurücksetzen, geraten die auf Ihrem Mobilgerät gespeicherten Daten nicht in falsche Hände. Entfernen und vernichten Sie ausserdem die SIM-Karte, wenn Sie diese nicht mehr benötigen.

Mobile Banking

Unter Mobile Banking wird das Abwickeln von Bankgeschäften mit Hilfe von Mobilgeräten bezeichnet. Dafür können die Apps der jeweiligen Finanzinstitute verwendet oder das E-Banking-Portal des Finanzinstituts im Browser aufgerufen werden. Auf die Sicherheit hat die Form des Mobile Banking keinen Einfluss, falls die vorherigen Tipps beachtet werden.

Beim Mobile Banking sollten Sie ausserdem ...

- **eine sichere Verbindung wählen.** Verwenden Sie im WLAN eine WPA2- oder WPA3-Verschlüsselung, die Sie bei Ihrem WLAN-Router aktivieren können.
- **bei der Zwei-Faktor-Authentifizierung ein separates Gerät verwenden.** Beim Mobile Banking auf dem Mobilgerät in Verbindung mit dem mTAN- oder PhotoTAN-Verfahren fehlt der zweite unabhängige Kommunikationskanal. Verwenden Sie deshalb ein weiteres für diesen Zweck eingesetztes Gerät, wie z. B. ein altes Handy oder ein TAN-Gerät Ihrer Bank.

Mobile Payment

Unter Mobile Payment wird das bargeld- und kontaktlose Bezahlen mit Mobilgeräten verstanden. Die Sicherheit von Mobile Payment wird oft hinterfragt: Was passiert mit meinen Daten? Ist die Verbindung sicher? Sind die Transaktionen verschlüsselt? Das Wichtigste ist, dass die Kunden- und Bezahldaten getrennt sind. So sollte der Betreiber der App (z. B. Twint oder Apple Pay) nicht erfahren, was der Kunde wo gekauft hat; und der Händler sollte nicht erfahren, wie hoch der Kontostand seines Kunden ist. Ob das so ist, lässt sich nur schwer überprüfen, kann aber beim Betreiber der App abgeklärt werden.

Bezahlen Sie sicher bargeld- und kontaktlos, indem Sie die vorherigen Tipps beachten und …

- **nur die wirklich notwendigen Daten der Mobile Payment App preisgeben.** Die Gefahr des Datenmissbrauchs entsteht durch eine mögliche Verknüpfung von Zahlungs- und Einkaufsdaten mit Nutzungs- und Standortdaten zu aussagekräftigen Nutzerprofilen.
- **den Zugang zur Mobile Payment App schützen.** Aktivieren Sie die Sicherheitseinstellungen der App. Richten Sie die automatische Sperre mittels Code, Passwort, Fingerabdruck oder Gesichtserkennung ein.

Weitere Informationen: **www.ebas.ch/mobilebanking**

Frühling 2019

SKPPSC

Schweizerische Kriminalprävention
Haus der Kantone
Speichergasse 6
3001 Bern

www.skppsc.ch

Dieses Faltblatt entstand in Zusammenarbeit mit
der **Hochschule Luzern** und **«eBanking – aber sicher!».**

www.ebas.ch | www.ebankingabersicher.ch

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

eBanking aber sicher!