Sicherheitshinweise für Online-Banking mit dem Smartphone, z.B. der Sparkassen-App

Wer viel unterwegs ist braucht eine flexible Möglichkeit, seine Bankgeschäfte immer und überall erledigen zu können.
Mit den Sparkassen eigenen Apps (**Sparkassen-App** und **S-pushTAN**) ist dies leicht möglich.
Dennoch gibt es einige wichtige Punkte, die Sie beachten sollten.

1. **Ihre Anmeldedaten**
   Vergeben Sie sichere Zugangsdaten.
   Neben Ihren persönlichen Anmeldedaten benötigen Sie noch ein Master-Passwort, das Sie IMMER eingeben müssen, um die Sparkassen-App zu öffnen.

2. **Sichere Quellen**
   Laden Sie Apps nur aus vertrauenswürdigen Quellen.
   (z.B. App-Store, Google-Play-Store)

3. **Sicherer Umgang mit IOS und Android**
   Jailbreaken Sie Ihr iPhone nicht. Dadurch wird das verschlossen IOS System aufgebrochen. Schadsoftware gelangt so viel leichter auf Ihr Smartphone.

   Achten Sie bei Android darauf Ihr Smartphone regelmäßig mit einem aktuellen Virenscanner zu überprüfen.
   Apps die über einen Screenreader verfügen, sollten Sie ebenfalls nicht nutzen, da diese die S-pushTAN App blockieren.

4. **Bankdaten niemals weitergeben**
   Öffnen Sie nur Mailanhänge von Ihnen bekannten Absendern. Auch Smartphones sind nicht generell vor Viren, Trojanern etc. geschützt. Schützen Sie Ihr Android Gerät mit einer Antiviren-Software.
   Leiten Sie uns „Sparkassen-Spam-Mails“ formlos an warnung@sparkasse.de weiter.

5. **Anmeldedaten nicht speichern. Passwort Manager „S-Trust“ nutzen.**
   Speichern Sie Ihre Anmeldedaten oder Ihr Master-Passwort für das Mobile Banking niemals auf dem Smartphone (auch nicht getarnt als Kontakt im Adressbruch).

   Unter www.s-trust.de finden Sie den Dokumenten- und Passwort-Manager der Sparkasse. Die Basisversion erhalten Sie kostenlos.

6. **Öffentliche Netzwerke**
   Vermeiden Sie es Mobile Banking über öffentliche Netzwerke oder während Bluetooth eingeschaltet ist zu nutzen. Hacker haben dann leichteren Zugriff auf Ihr Smartphone.

7. **Aktualisierungen**
   Halten Sie ihr Betriebssystem und die Apps auf dem aktuellen Stand. Nur so werden die Sicherheitseinstellungen auf einem aktuellen Stand gehalten.

8. **Sperren**
   Aktivieren Sie die automatische Sperrfunktion Ihres Smartphones. Dadurch hat nicht gleich jeder Zugriff.

9. Die TAN Verfahren

Prüfen Sie die Anzeige auf oder Ihrem Smartphone oder dem TAN-Generator immer sorgfältig.
Bevor Sie eine TAN eingeben, prüfen Sie stets, ob die Anzeige im Display Ihres Gerätes tatsächlich den Daten entspricht, die Sie zuvor selber in der Überweisung eingegeben haben.

10. Empfehlungen für vorsichtige pushTAN-User

Beim pushTAN-Verfahren kann das Online-Banking über den PC oder ein anderes zweites Gerät (z. B. Tablet) abgewickelt werden, nur die push-App wird über das Smartphone genutzt. Damit erfolgt eine Kanaltrennung.

11. Digitalisierung Ihrer Sparkassen-Card bzw. Kreditkarte für das Bezahlen per Smartphone oder Smartwatch im Einzelhandel („Apple Pay“ oder „Mobiles Bezahlen mit Android“)

In letzter Zeit kam es vor, dass Betrüger Phishing-Angriffe und Fake-Anrufe dafür nutzten, digitale Karten auf ihren eigenen Smartphones hinzuzufügen.
Bestätigen Sie die Digitalisierung Ihrer Karte deshalb nur, wenn Sie diese Aktion gerade selber durchführen.
Erzeugen Sie keine TAN, sofern Sie keine Digitalisierung durchführen möchten.

12. Im Notfall: Sperren Sie Ihren Online-Banking-Zugang.

Dazu

- rufen Sie Ihren Berater, unser Service-Center (02451 600) oder 116 116 an
- oder Sie sperren Ihren Zugang selber sofort: Geben Sie 3 x eine falsche PIN ein!

Stand 01/2023