Berliner Sparkasse

## Vorwände, unter denen Betrüger Sie anrufen bzw. per Mail kontaktieren:

- Ihr TAN-Verfahren (pushTAN) verliert die Gültigkeit und eine neue App soll installiert werden
- Jemand hat im In- oder Ausland versucht Geld von Ihrem Konto abzuheben. Ihr Konto wurde vorübergehend gesperrt und soll nun gemeinsam mit Ihnen reaktiviert werden
- Sie erhalten einen Werbeanruf zu einem neuen TAN-Verfahren, das gleich im Gespräch aktiviert werden soll
- Die Täter möchten Ihre persönlichen Daten aktualisieren bzw. überprüfen und benötigen dazu Ihre TAN

## Aktuell erhöhte Vorsicht vor Betrugsversuchen am Telefon!

Sehr geehrte Kundinnen und Kunden,

zurzeit kommt es vermehrt zu Betrugsversuchen am Telefon. Daher möchten wir uns mit wichtigen Informationen zur Sicherheit Ihrer Konten an Sie wenden und mit diesem Schreiben um erhöhte Vorsicht bitten.

### Die Angriffe laufen meist wie folgt ab:

Die Betrüger rufen Sie über das Festnetz oder das Mobiltelefon an und geben sich als Mitarbeiter der Berliner Sparkasse aus. Dabei wird als Vorwand genannt, dass bestimmte Daten aus Sicherheitsgründen oder zur Aktualisierung abgeglichen werden müssen. Auch wurde vorgegeben, dass bereits versucht wurde Geld vom Konto abzubuchen oder eine Bargeldauszahlung verhindert werden konnte. Um die Glaubwürdigkeit dieser Vorgehensweise zu unterstreichen, werden persönliche Daten wie Adresse und Geburtsdatum genannt.

Nachdem hierdurch das Vertrauen gewonnen wird, werden kontobezogene Daten, wie beispielsweise Zugangsdaten, erfragt. Häufig wird anschließend um eine Freigabe mittels S-pushTAN-App oder um die Nennung von TANs von Zahlungsvorgängen gebeten. Auch wurde der Versuch durch den Anrufer unternommen, die S-pushTAN-App auf deren Gerat zu installieren, wofür eine empfangene SMS an den Anrufer weitergeleitet werden soll.

Wird dieser Aufforderung nicht folgegeleistet, drohen die Anrufer häufig mit angeblicher Kontosperrung oder hohen Gebühren.

Berliner Sparkasse

## Wie können Sie sich schützen?

### Lassen Sie sich nicht von der angezeigten Nummer in Ihrem Display täuschen!

Durch das sogenannte „Call lD Spoofing" sind Kriminelle in der Lage, die Rufnummernanzeige zu manipulieren und sich die Anzeige einer unserer Telefonnummern zu Eigen zu machen.

Auch wenn Sie auflegen und die angezeigte Nummer zurückrufen, werden Sie wieder mit den Betrügern verbunden.

### Lassen Sie sich nicht unter Druck setzen und geben Sie auf keinen Fall jegliche Art von Daten weiter!

Die Gesprächsverläufe der Kriminellen unterscheiden sich, aber eines ist immer gleich: Die Betrüger wollen an Ihre Daten gelangen. Dafür werden Zugangsdaten für das Online-Banking oder weitere sensible Daten verlangt.

Nennen Sie daher unter keinen Umständen sensible Daten wie Passwörter, PINs oder TANs, auch wenn Ihnen mit Kontosperrung gedroht wird.

### Beenden Sie das Gespräch unverzüglich und informieren Sie uns umgehend!!!

### Geben Sie niemals Ihre Zugangsdaten an andere Personen weiter!!

Keiner unserer Mitarbeiter wird Sie jemals nach Zugangsdaten für das Online-Banking, PINs oder TANs fragen. Diese Daten sind ausschließlich für Sie bestimmt.

Nutzen Sie diese Daten ausschließlich auf unseren offiziellen Seiten.

Geben Sie solche Daten auch niemals auf Internetseiten ein, die Ihnen durch Links in E-Mails, mittels SMS oder per Post zugeleitet wurden. Durch Phishing-Mails werden Sie teilweise auch aufgefordert, sich auf gefälschte Sparkassenseiten in Ihr Online-Banking einzuloggen. Ziel ist hier, an Ihre Zugangsdaten zu kommen.

Geben Sie ausschließlich die Adresse **www.berliner-sparkasse.de** in die Adresszeile Ihres Internet-Browsers ein, um Zugang zu unserer Internet-Filiale zu erhalten.

Unsere Sicherheitsmaßnahmen werden kontinuierlich weiterentwickelt. Aber für einen vollständigen Schutz Ihres Online-Bankings sind wir auf Ihre Aufmerksamkeit und Vorsicht angewiesen.

Halten Sie Firewall und Virenscanner zum Schutz ihres Computers immer aktuell, arbeiten Sie immer mit der aktuellsten Version Ihres Internetbrowsers und installieren Sie immer die neuesten Sicherheitsupdates der Sparkassen-Apps.

**Seien Sie aufmerksam. Geben Sie den Betrügern keine Chance!**