

WICHTIGER SICHERHEITSHINWEIS

für alle Kundinnen und Kunden der Sparkasse Berlin

Datum: 15. Januar 2025

Sehr geehrte Kundin, sehr geehrter Kunde,

die Sicherheit Ihrer Finanzen hat für uns höchste Priorität. Aktuell beobachten wir eine Zunahme betrügerischer Aktivitäten, die darauf abzielen, an Ihre vertraulichen Bankdaten zu gelangen. Wir möchten Sie daher über die gängigsten Betrugsmaschen informieren und Ihnen Tipps zum Schutz geben.

1. Telefonbetrug („Vishing“ / Call-ID-Spoofing)

Betrüger rufen bei Kundinnen und Kunden an und geben sich als Sparkassen-Mitarbeiter aus. Dabei verwenden sie eine Technik namens „Call-ID-Spoofing“, mit der sie die angezeigte Rufnummer manipulieren können. Auf Ihrem Telefondisplay erscheint dann die echte Sparkassen-Nummer, obwohl der Anruf tatsächlich von Kriminellen stammt.

Die Anrufer behaupten typischerweise, es gäbe verdächtige Kontobewegungen oder Sicherheitsprobleme. Sie fordern Sie auf, eine TAN zu generieren und telefonisch mitzuteilen – angeblich zur „Verifizierung“ oder „Kontosperre“.

2. Phishing-E-Mails

Betrügerische E-Mails, die täuschend echt aussehen, fordern Sie auf, über einen Link Ihre Zugangsdaten einzugeben. Achten Sie auf: unpersönliche Anrede, Rechtschreibfehler, dringliche Aufforderungen, verdächtige Absenderadressen.

3. SMS-Phishing („Smishing“)

Sie erhalten eine SMS, die angeblich von der Sparkasse stammt, mit der Aufforderung, einen Link anzuklicken. Dieser führt zu einer gefälschten Webseite.

WICHTIG: Die Sparkasse Berlin wird Sie niemals telefonisch, per E-Mail oder SMS zur Eingabe von TANs, PINs oder Passwörtern auffordern.

So schützen Sie sich:

- Geben Sie **niemals** TANs, PINs oder Passwörter am Telefon, per E-Mail oder SMS weiter – auch nicht an vermeintliche Sparkassen-Mitarbeiter.
- Vertrauen Sie **nicht** der angezeigten Rufnummer. Telefonnummern können gefälscht werden.

- Legen Sie bei verdächtigen Anrufen auf und rufen Sie uns über die Ihnen bekannte Nummer zurück: 030-869869869.
- Prüfen Sie bei jeder TAN-Freigabe in der App **genau**, welche Transaktion Sie freigeben. Lesen Sie den **vollständigen** Anzeigetext.
- Klicken Sie **nicht** auf Links in E-Mails oder SMS, die Sie zur Eingabe von Zugangsdaten auffordern.
- Sperren Sie im Notfall Ihr Konto sofort über den Sperr-Notruf **116 116** (kostenlos, rund um die Uhr).

Bei Fragen oder Verdächtigungen wenden Sie sich bitte an Ihre Filiale oder unseren Kundenservice unter 030-869869869.

Mit freundlichen Grüßen

Ihre Sparkasse Berlin

*Dieser Sicherheitshinweis wird quartalweise an alle Kundinnen und Kunden versandt. Letzter Versand: 15. Oktober 2024.
Sparkasse Berlin · Alexanderplatz 2, 10178 Berlin · BLZ 100 500 00*