Warum wir bei Fragen immer für Sie nah sind?

Weil Sie keinem Betrüger ins Netz gehen sollen

Wichtige Tipps und Hinweise zu unserem Online-Banking

LzO
meine Sparkasse

Online-Banking? Aber sicher!

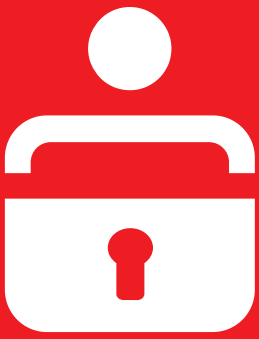
Immer wieder versuchen Betrüger, an Ihre persönlichen Daten zu gelangen – teilweise mit sehr geschickten Maschen. Damit Sie darauf nicht hereinfallen und Ihre Bankgeschäfte weiterhin sicher erledigen können, lesen Sie sich dieses Merkblatt bitte aufmerksam durch.

Kontrolle ist wichtig

Kontrollieren Sie Ihre Auftragsdaten in der pushTAN-App bzw. am TAN-Generator auf Richtigkeit, bevor Sie den Auftrag freigeben. Falls bei einer Überweisung Empfänger-IBAN oder Betrag nicht mit Ihren Daten übereinstimmen, brechen Sie die Transaktion sofort ab.

Betrügerische Anrufe

Anrufer geben sich als vermeintlicher LzO-Mitarbeitender, als Polizist oder Microsoft-Mitarbeiter aus und möchten mit Ihnen Online-Banking-Transaktionen ausführen. Geben Sie niemals Zugangsdaten für das Online-Banking, Transaktionsnummern (TAN), Kartennummern oder persönliche Daten per Telefon weiter. Legen Sie in so einem Fall bitte sofort auf!



Phishing-SMS

SMS-Nachrichten im Namen der Sparkasse werden unter dem Vorwand verschickt, dass das Online-Banking angeblich abgelaufen sei. Die Betrüger versuchen dadurch, Sie zum Aufruf einer betrügerischen Webseite (Phishing-Seite) zu bewegen. Dort werden Ihre Online-Banking-Zugangsdaten und weitere persönliche Daten erfragt. Zudem sollen Sie eine vermeintliche Testüberweisung durch Eingabe einer TAN gemäß des von Ihnen genutzten TAN-Verfahrens durchführen.

VORSICHT: Geben Sie keine Daten und keine TAN auf Phishing-Seiten ein. Diese werden von Betrügern für betrügerische Transaktionen genutzt.

Phishing-Mails

Täglich werden betrügerische E-Mails mit Bezug zur Sparkasse verteilt. Der Fantasie der Betrüger sind hier keine Grenzen gesetzt. Es ist die Rede von vermeintlichen Bedingungsänderungen, angeblichen Sperrungen Ihres Zugangs oder der Bestätigung Ihrer Kundendaten. Lassen Sie sich nicht verwirren.

Sie werden von uns niemals solche E-Mails erhalten. In Wirklichkeit handelt es sich immer um den Versuch, dass Sie auf einer gefälschten Sparkassen-Internetseite Ihre Online-Banking-Zugangsdaten, persönliche Daten sowie TAN eingeben.

Hierdurch kann es zu betrügerischen Online-Banking-Überweisungen kommen. Löschen Sie solche Mails bitte umgehend!

Regelmäßiger Passwort-Wechsel

Ändern Sie regelmäßig die PIN für Ihr Online-Banking.

Auf der richtigen Seite

Achten Sie stets auf die richtige Adresse, die in Ihrem Browser angezeigt wird, wenn Sie die LzO-Seite besuchen. Dort muss immer **https://www.lzo.com/**... stehen.

Im Fall der Fälle

Sollten Sie doch einmal auf einen Betrugsversuch hereingefallen sein, rufen Sie bitte umgehend den kostenfreien **Sperrnotruf unter 116 116** an. Sie können Ihren Zugang auch ganz einfach über **lzo.com/sperre** selber sperren.

Weitere Informationen und Warnungen zu aktuellen Betrugsmaschen finden Sie auf **lzo.com/sicherheit**

Wir sind für Sie da

Unsere Beratungszeiten
Montags bis freitags von 8–20 Uhr
Einfach Termin in der Filiale vereinbaren.

KundenServiceCenter
Hier erreichen Sie uns montags bis freitags
von 8–20 Uhr telefonisch oder online.

Unsere Kollegen vom Video-Service Amelie
sind montags bis freitags von 9–18 Uhr für Sie da.

Telefon: 0441 2300
Text-Chat: lzo.com/chat
lzo.com · lzo@lzo.com

Unsere Nähe bringt Sie weiter.

LzO
meine Sparkasse

2101096 / 01.22