



Sicherheit im Internet und beim Bezahlen



Stadtsparkasse
Mönchengladbach

Das Wichtigste für den Umgang im Netz: Teilen Sie niemals Ihre Passwörter oder persönlichen Informationen. Sie sind genau so wertvoll zu behandeln wie Bargeld oder die PIN Ihrer Bankkarte.

Kontaktieren Sie bei jeglichem Verdacht oder Zweifel gerne unser KundenServiceCenter 02161/279-0 (täglich von 8.00 bis 18.00 Uhr erreichbar)! Sperren Sie ggf. selbst Ihren Zugang in Ihrem Online-Banking!

Zur Sperrung Ihrer Karten und des Online-Bankings bei Verlust, Diebstahl oder Verdacht auf Missbrauch, können Sie außerdem rund um die Uhr den Sperr-Notruf +49 116 116 kontaktieren!

Betrügerische Anrufe

- Die Täter versuchen, durch vermeintlich von der Sparkasse stammende Anrufe TAN-Freigaben und/oder sicherheitsrelevante Informationen zu erhalten.
- Die Anzeige tatsächlich existierender Telefonnummern unseres Hauses ist dabei gefälscht.
- Oft haben die Betrüger sich durch eine unten beschriebene Phishing-Nachricht bereits persönliche Daten beschafft.
- Die Betrüger versuchen unter Angabe falscher Vorwände Ihre Daten zu erhalten oder Sie zu Freigaben zu Zahlungen oder Vorgängen im Online-Banking zu drängen:
 - Online-Banking-Daten werden abgefragt.
 - Kreditkarten- und/oder Sparkassen-Card-Daten werden abgefragt.
 - Es werden TAN-Freigaben im Online-Banking oder über die S-ID-Check-App angefordert.
 - Weitergabe von SMS/E-Mail/WhatsApp-Links während des Telefonats.



Legen Sie bei einem Verdacht sofort auf! Wir werden Sie niemals auffordern Links zu kopieren/anzuklicken, eine TAN weiterzugeben bzw. etwas in der pushTAN-App freizugeben!

Falsche Sparkassen-Nachrichten / Sparkassen-E-Mails

- Die Täter versuchen von Ihnen durch vermeintlich von der Sparkasse stammende Nachrichten (E-Mail, SMS, WhatsApp o. ä.) sicherheitsrelevante Informationen zu halten.
- Häufig wird ein Link mitgeschickt, der auf eine gefälschte Seite der Sparkasse verlinkt, auf der Sie Informationen wie Anmeldename, Online-Banking PIN, Karten-Nr. oder persönliche Daten eingeben oder bestätigen sollen.
- Ggf. werden diese Informationen für einen oben beschriebenen Anruf mit falschen Sparkassen-Mitarbeitenden genutzt.
- Folgende Vorwände sind dabei geläufig:
 - Ablaufende Online-Banking/pushTAN-Registrierung
 - Akzeptanz von Bedingungen



Weder die Sparkasse noch Ihr Händler werden Sie per E-Mail o. ä. auffordern, Ihre persönlichen Daten preiszugeben!

Sicherheit im Internet und beim Bezahlen

Betrugsmasche ebay-Kauf/Verkauf

- Betrug bei Käufen und Verkäufen insbesondere über ebay-Kleinanzeigen (aber auch anderen Handelsplattformen).
- Die Bezahlweise „Sicheres Bezahlen“ wird vom Betrüger angeboten (auch wenn Sie Verkäufer sind).
- Sie werden aufgefordert sich über einen Link (per WhatsApp oder SMS versandt) für die Bezahlweise zu registrieren.
- Die Seite sieht der Handelsplattform täuschend ähnlich.
- Auf der Seite werden Sie aufgefordert Ihre Kreditkartendaten anzugeben.
- Im selben Moment versuchen die Betrüger sich mit Ihren Daten für den S-ID-Check zu registrieren.
- Unter dem Vorwand, dass Sie sich gerne für „Sicheres Bezahlen“ registrieren, versuchen die Betrüger eine TAN bzw. eine Freigabe in der pushTAN- oder S-ID-Check-App zu erhalten.



Durch eine Freigabe ermöglichen Sie den Betrügern sich unter Ihrem Namen für den S-ID-Check zu registrieren und mit Ihrer Kreditkarte zu bezahlen. Weichen Sie auf andere Bezahlmethoden aus und melden Sie die Betrüger bei der Handelsplattform!

Tipps für den Umgang mit der PIN Ihrer Sparkassen-Card/ Sparkassen-Kreditkarte

Halten Sie Ihre PIN geheim!

- Geben Sie Ihre PIN niemals an andere weiter.
- Schreiben Sie Ihre PIN unter keinen Umständen auf Ihre Karten.
- Achten Sie auf Sichtschutz bei der PIN-Eingabe.

Eigene PIN? Aber sicher!

- Sie können die Geheimzahl Ihrer Sparkassen-Card deutschlandweit an jedem Sparkassen-Geldautomaten selbst ändern.
- Wählen Sie keine PIN, die leicht zu erraten ist.
- Beziehen Sie die PIN nicht auf Ihren Geburtstag o. ä.



Bitte beachten Sie, dass Sie bei Verlust der Sparkassen-Card mit PIN ggf. vollständig für Ihren Schaden haften!

Ausführliche Informationen über Betrugsmaschen sowie aktuelle Sicherheitshinweise finden Sie unter folgender Adresse:

www.sskmg.de/sicherheit

Unsere Sicherheitsstandards gehen über die gesetzlichen und regulatorischen Anforderungen hinaus. Beim Trickbetrug allerdings – und damit ist gemeint, eine Person unter psychologischem Druck und einem Vorwand dazu verleiten, etwas zu tun, was er oder sie sonst nie gemacht hätte – ist es hilfreich, wachsam und vorsichtig zu sein und jeweilige Situationen kritisch zu hinterfragen.

Weil's um mehr als Geld geht.



Stadtsparkasse
Mönchengladbach