



Guten Tag,

Sie und Ihr Vermögen zu schützen, liegt uns sehr am Herzen. Gerne informieren wir Sie deshalb über aktuelle Betrugsmaschen:

- Anrufe vermeintlicher Sparkassenmitarbeiter:innen – es sollten Online-Zugänge bestätigt werden
- Vermeintliche Kaufinteressenten bei Kleinanzeigen oder Vinted, die Ihre Kreditkartennummer per WhatsApp erfragen, um darauf das Geld zu überweisen
- Anschreiben mit gefälschtem QR-Code
- Gefälschte Webseiten beim Kauf von Vignetten

Mit dem Online-Banking, der S-PushTAN-App oder der S-ID-Check App, zur Freigabe von Online-Zahlungen, bieten wir Ihnen bereits ein hohes Maß an Sicherheit. Mit folgenden Tipps können Sie sich zusätzlich schützen:

- Achten Sie generell bei Zahlungen über Links (PayPal, Klarna, etc.) darauf, dass Ihnen diese über die Webseite bzw. Plattform des Händlers angezeigt werden. Reagieren Sie nicht auf Links, die Sie per WhatsApp oder ähnlichen Messenger-Diensten erhalten.
- Bei einem privaten Verkauf über ein Online-Portal, wie Kleinanzeigen oder Vinted, ist die Weitergabe Ihrer Kartendaten nicht nötig. Lassen Sie sich bitte auf keine Unterhaltung zur Kaufabwicklung außerhalb der Plattform ein.
- Prüfen Sie vor Freigabe der Transaktion, ob Sie wirklich eine Zahlung an den angegebenen Empfänger/die angegebene Empfängerin veranlassen wollen. Im Zweifel brechen Sie den Vorgang ab. Zur Annahme einer Zahlung/Überweisung müssen Sie keine Freigabe erteilen!
- Geben Sie niemals persönliche Daten bekannt. Betrugsversuche erfolgen auf unterschiedlichen Wegen, z.B. per WhatsApp, E-Mail, Post oder Telefon. Geben Sie Ihre Passwörter und Daten nicht auf einer Internetseite ein, wenn Sie durch einen Link in einer E-Mail oder einem Messenger-Dienst dazu aufgefordert werden.
- Achten Sie bei den angezeigten Links auf ungewöhnliche Endungen wie z.B. ufzyc.com/jylix/ oder Schreibfehler (info@sparkasse.de). Diese weisen häufig auf gefälschte E-Mails hin.
- Prüfen Sie genau, ob das Schreiben mit dem erhaltenen QR-Code plausibel ist. Stimmen die angegebenen Daten (z. B. der Name des Vorstands Ihrer Sparkasse)? Wurden Sie persönlich angesprochen oder steht in der Anrede „Sehr geehrter Kunde?“. Fragen Sie im Zweifelsfall lieber bei Ihrer Sparkasse nach.

Wir empfehlen Ihnen auch den Kreditkartenwecker Ihrer Sparkasse zu nutzen, um sofort über Zahlungen, die Ihrem Kreditkartenkonto belastet werden, informiert zu werden. Wenn Ihnen etwas ungewöhnlich vorkommt, lassen Sie Ihre Kreditkarte bitte umgehend unter der Notfallhotline unseres Dienstleisters qards GmbH unter der Telefonnummer +49 89 411 116 446 sperren. Die Hotline ist rund um die Uhr für Sie da. Wir empfehlen Ihnen, diese Nummer auf Ihrem Handy zu speichern. Die Mitarbeitenden dort können Ihre Karte sofort sperren, so dass weiterer Betrug oder Missbrauch verhindert werden kann.

Gehen Sie mit Ihren Kreditkartendaten um, als würde es sich um Bargeld handeln. Dann haben Sie auch in Zukunft viel Freude beim Kaufen und Bezahlen kleinerer und größerer Lieblingsstücke. Bei Fragen ist Ihr Berater/ Ihre Beraterin gerne für Sie da.