Ostsächsische Sparkasse Dresden

Pressemitteilung

„Achtung Betrug! Wir klären auf." Sparkasse informiert zu aktuellen Betrugsmaschen

Dresden, 16. Oktober 2025.

„Mir ist was ganz Blödes passiert." „Bei mir wurde Geld abgebucht, ich hab' gar nichts gemacht." „Ich habe doch nur etwas online verkauft." So oder ähnlich hört es sich an, wenn Kunden bei Antje Kramer und ihrem Team anrufen. Und meist ist damit nichts Gutes verbunden. Das Expertenteam rund um Prävention im Zahlungsverkehr der Ostsächsischen Sparkasse Dresden kommt immer dann ins Spiel, wenn Kunden mit hoher Wahrscheinlichkeit auf Betrüger hereingefallen sind – ob über gefälschte Zahlungslinks auf Verkaufsplattformen, Phishing-Mails oder vermeintliche Anrufer von Microsoft, die angeblich Schadsoftware beseitigen wollen.

Ihre Erfahrung zeigt: Die Betrugsfälle nehmen ebenso zu wie die Maschen der Kriminellen. Und die sind auf allen Kanälen. Das bestätigt auch die Statistik. Laut Branchenverband Bitkom sind die Schäden durch Cyberattacken 2024 auf 178 Mrd. Euro gestiegen. Nach wie vor zählen Phishing- und Ransomware-Angriffe, betrügerische Telefonanrufe sowie Manipulationen beim Online-Handel zu den größten Gefahren.

Aufklären und sensibilisieren: Bleiben Sie misstrauisch!

Die Ostsächsische Sparkasse Dresden reagiert mit einer klaren Botschaft: Aufklärung und Sensibilisierung sind der beste Schutz. Deshalb finden regelmäßig Veranstaltungen in Filialen statt. Dabei vermitteln die Experten, wie Kundinnen und Kunden Betrugsversuche rechtzeitig erkennen und sich davor schützen können. „Jeder kann Opfer werden – deshalb ist es wichtig, richtig informiert zu sein", sagt Antje Kramer, Leiterin Onlineservice der Ostsächsischen Sparkasse Dresden.

Thementag mit Online-Veranstaltung am 23. Oktober 2025

Am 23. Oktober 2025 widmet die Sparkasse nun einen speziellen Thementag der Prävention. Unter dem Motto „Achtung Betrug! Wir klären auf" stehen zwei Veranstaltungen – eine für Unternehmen und eine für Privatkunden – auf der Agenda.

Die Veranstaltung wird von hochkarätigen Experten begleitet: Tobias Schrödel, Comedyhacker und IT-Sicherheitsexperte, entführt ins Darknet und bringt auf humorvolle Weise Licht ins Dunkel der Cyberangriffe. Tobias Robra, Fachberater Prävention der Ostsächsischen Sparkasse Dresden, und Martin Klöden, IT-Sicherheitsexperte der axilaris GmbH, informieren über Phishing bei Unternehmen, aktuelle Betrugsszenarien und geben praxisnahe Tipps und Lösungen. Tipps zu

Schockanrufen und richtigem Verhalten gibt es auch von Dirk Möller, Leiter Sachgebiet Polizeiliche Beratung des Landeskriminalamts Sachsen.

Wer mehr zu aktuellen Betrugsszenarien erfahren möchte, kann sich für die Online-Veranstaltung über diesen Link anmelden: https://events.sparkasse.de/s/Achtung-Betrug-wir-klaeren-auf-online

Aktuelle Betrugsmethoden

Phishing über Handelsplattformen wie Kleinanzeigen, vinted und Co.

Kunden werden beim Verkauf von Artikeln in der Regel sehr schnell von einem Interessenten angeschrieben. Für die Bezahlung schickt der Interessent einen gefälschten Link an den Verkäufer, über den er angeblich sein Geld erhält. Wer dort seine Daten eingibt, öffnet den Betrügern den Zugang. Wenn dann noch eine TAN zur Freigabe gefordert wird, sollten unbedingt die Alarmglocken läuten.

Anlagebetrug

Angebote mit unrealistischen Anlageversprechen animieren z. B. auf Social Media auf Werbeanzeigen zu klicken, wo dann Kontaktdaten eingegeben werden sollen. Meist folgt der Anruf eines sogenannten Anlageberaters zu vermeintlich sicheren Investments u. a. in Kryptowährung. Anfangs wird meist ein kleinerer Startbetrag eingezahlt und später folgen weitere Zahlungen – oft auf Wallets oder Konten der Betrüger. Erst bei Auszahlungswünschen kommt der Betrug raus: Der Kontakt bricht ab, angebliche Gebühren werden fällig und weitere Gelder sollen zur Rettung gezahlt werden.

Vorsicht am Telefon

Auch Telefonbetrüger gehen geschickt vor: Mit manipulierter Rufnummernanzeige geben sie sich als z. B. als Bank-Mitarbeiter, Polizisten, Anwälte oder Familienmitglieder aus und drängen dazu, schnell zu handeln. Dabei wird Vertrauen erschlichen, um das Opfer zur Zahlung hoher Geldbeträge oder Auskunft persönlicher Daten zu bewegen. Am Ende sind die Täter unauffindbar und die Ersparnisse weg.

Die Grundregel lautet: Niemals sensible Daten wie PIN oder TAN auf Aufforderung weitergeben – weder online noch am Telefon. Am besten einfach auflegen.

Auf einen Betrug hereingefallen – so handeln Sie richtig

Wer dennoch Opfer wird, sollte schnell handeln: Unverzüglich die Sparkasse kontaktieren, Karten und Zugänge sperren lassen, ggf. Passwörter ändern und Anzeige bei der Polizei erstatten. So lassen sich Schäden in vielen Fällen begrenzen.

Die wichtigsten Tipps gegen Betrug

- Misstrauisch bei Links und Anhängen: Keine sensiblen Daten über E-Mail, SMS oder unbekannte Links eingeben.
- Am Telefon keine Daten preisgeben: Seriöse Banken fragen niemals nach Zugangsdaten fürs Online-Banking.
- Sicher handeln beim Online-Verkauf und -Kauf: Zahlungslinks und Bestätigungen genau prüfen, nur über offizielle Plattformen kommunizieren.
- Starke Passwörter nutzen: Lange Kombinationen aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen wählen – keine Namen oder Geburtstage.
- Passwörter regelmäßig ändern: Vor allem dann, wenn der Verdacht besteht, dass Daten kompromittiert wurden.
- Regelmäßig informieren: Aktuelle Betrugsmaschen werden auf der Website der Sparkasse veröffentlicht.

Aktuelle Sicherheitstipps und Betrugsfälle werden **auf der Website** der Ostsächsischen Sparkasse Dresden veröffentlicht: **Datendiebstahl/Phishing | Ostsächsische Sparkasse Dresden**

Rückfragen:
Petra Gehlich
Presse & Medien
Tel. 0351 – 455 16517
presse@sparkasse-dresden.de