kartensicherheit.de
Aufklärung, Vernetzung, Information

EURO KARTENSYSTEME

Presseinformation

Die Vertrauensfalle: Betrug im Namen bekannter Marken

Frankfurt, 6. Mai 2026 – Ob vermeintliche E-Mail der Hausbank, SMS vom Paketdienst oder Schreiben einer Behörde: Was seriös wirkt, kann häufig auch ein Betrugsversuch sein. Aktuelle Sicherheitsanalysen[1] bestätigen, dass Social Engineering – also die gezielte Manipulation von Menschen – mittlerweile zu den häufigsten Einfallstoren für Finanzbetrug zählt. Statt technische Schutzsysteme zu knacken, unterwandern Kriminelle gezielt bestehendes Vertrauen.

Durch den Einsatz Künstlicher Intelligenz können diese Maschen deutlich an Qualität zunehmen. Angreifende nutzen KI für:

- Täuschend echte E-Mails ohne sprachliche Auffälligkeiten, personalisierte Anschreiben und originalgetreue Kopien offizieller Webseiten.
- Betrügerische Anrufe oder Videobotschaften, bei denen Stimmen und Aussehen von Vertrauenspersonen oder Vorgesetzten imitiert werden, so genannte Deepfakes.
- Manipulierte Rufnummern, sodass bei SMS und Anrufen offizielle Behörden- oder Institutsnummern im Display erscheinen (SMS- und Call-ID-Spoofing).

Das Ziel bleibt stets dasselbe: Das Abgreifen sensibler Daten sowie das Auslösen direkter Zahlungen oder die Übernahme von Online-Banking-Identitäten. Um sich gegen diese psychologischen Tricks zu wappnen, rät kartensicherheit.de zu folgenden Verhaltensregeln:

Inhalt hinterfragen statt Absender vertrauen

Entscheidend ist nicht die vermeintlich seriöse Aufmachung, sondern was verlangt wird. Banken, Sparkassen und Behörden fordern niemals zur Preisgabe von Passwörtern, PINs oder TANs auf.

Zeitdruck als Warnsignal erkennen

Kriminelle nutzen emotionale Stresssituationen oder drohende Konsequenzen (z. B. Kontosperrung), um schnelles Handeln zu erzwingen. Ein Moment des Innehaltens genügt oft, um die Strategie der Täterinnen und Täter zu erkennen und auszuhebeln.

Unabhängige Verifizierung

Im Zweifel hilft die Prüfung über einen sicheren Kanal. Links oder Kontaktangaben aus der Nachricht sind nicht vertrauenswürdig. Daher am besten eine bekannte Nummer anrufen, etwa die Servicehotline oder die Rufnummer von der offiziellen Webseite der jeweiligen Institution. Wichtig: Die Webadresse manuell in den Browser eingeben.

Im Ernstfall sofort handeln

Wurden sensible Daten versehentlich weitergegeben, zählt jede Minute. Zahlungskarten und Online-Banking-Zugänge lassen sich rund um die Uhr über den Sperr-Notruf 116 116* oder direkt beim Kreditinstitut sperren. Alternativ steht die kostenlose SperrApp zur Verfügung.

[1] EAST Fraud Update 1-2026

* Der Service des Sperr-Notrufs ist kostenlos. Auch der Anruf bei der 116 116 aus dem deutschen Festnetz ist gebührenfrei. Aus dem Mobilnetz und aus dem Ausland (+49 116 116) können Gebühren anfallen. Sollte der Sperr-Notruf in seltenen Fällen nicht erreichbar sein, gibt es alternativ die Rufnummer +49 (0) 30 40504050.

Tipps zum richtigen Umgang mit Karte und PIN hat die EURO Kartensysteme GmbH in Zusammenarbeit mit der Deutschen Kreditwirtschaft im Internetportal www.kartensicherheit.de zusammengestellt. Hier finden Verbraucherinnen und Verbraucher viele interessante Informationen zu bargeldlosen Zahlungsmitteln und einen SOS-Infopass mit den wichtigsten Sperrnummern für den Notfall als Download.

EURO Kartensysteme GmbH | Solmsstraße 6 | D-60486 Frankfurt am Main | **T** +49 (0) 69/9 79 45-0 | **F** +49 (0) 69/9 79 45-48 88 | **W** www.eurokartensysteme.de
Vorsitzende des Aufsichtsrats Tanja Müller-Ziegler | **Geschäftsführung** Oliver Hommel (Vorsitzender), Susanne Raupbach | **Steuernummer** 045 232 54053
Umsatzsteuer ID DE257820111 | **Handelsregister** Frankfurt am Main, HRB 80376 | **Bankdaten** Deutsche Bank AG | **IBAN** DE78 5007 0010 0092 5974 00 | **BIC** DEUTDEFFXXX

EURO Kartensysteme GmbH
Sandra Königstein
Teamleiterin Aufklärung & Prävention
Sicherheitsmanagement
Tel.: +49 (0)69 / 97945-4552
sandra.koenigstein@eurokartensysteme.de

Schwarz & Sprenger - Agentur für Öffentlichkeitsarbeit GmbH
Anja Schneider
Geschäftsführerin
Tel.: +49 (0)89 / 21537887-1
anja.schneider@schwarz-sprenger.de