Anzeige

Betrug:

Banken und Sparkassen fragen nie nach geheimen Daten!

„Social Engineering“ – dieser Begriff rückt immer stärker in den Fokus bei betrügerischer Abzocke mit ständig neu auftauchenden Varianten. Was steckt dahinter? Ziel der Angriffe ist es, Menschen so zu manipulieren, dass sie persönliche, finanzielle oder sicherheitsbezogene Informationen preisgeben. Dabei bauen Kriminelle unter dem Deckmantel einer Autorität wie Polizei, BKA, Bank/Sparkasse oder einer nahestehenden Person Druck auf und nutzen Stressreaktionen, Ängste oder Hilfsbereitschaft der potenziellen Opfer aus.

Das Internetportal kartensicherheit.de berichtet regelmäßig über Social-Engineering-Attacken wie z. B. Phishing, Smishing und Vishing. Alle Methoden haben das gleiche Ziel: Durch Täuschung, Irreführung und Lügen an sensible Daten wie PINs, TANs, Konto- oder Kreditkartennummern zu kommen.

Doch was sind die Unterschiede? kartensicherheit.de klärt auf:

„Phishing“ per E-Mail

Kriminelle versuchen mittels gefälschter E-Mails persönliche Zugangsdaten abzugreifen. Es wird dringender Handlungsbedarf vorgetäuscht, zum Beispiel „Konto wurde vorübergehend gesperrt“. Mit dem Klick auf einen Weblink und Eingabe der Daten landen diese in den Händen der Betrüger:innen. Oftmals beinhalten die E-Mails auch schädliche Anhänge, die weiteren Zugang zu wertvollen Daten liefern.

„Smishing“ per Textnachricht

Es wird eine SMS verschickt, mit der Aufforderung einem Link zu folgen oder eine Telefonnummer anzurufen. Dabei soll beispielsweise das Konto „geprüft“ werden. Der Link führt zu einer gefälschten Webseite oder ein Anruf zu einer Person, die sich als vermeintliches Teammitglied eines tatsächlich existierenden Unternehmens ausgibt.

„Vishing“ per Telefon

Der Kontakt läuft übers Telefon. Die Anrufer:innen wirken sehr vertrauenswürdig und geben vor, dass sie vermeintliche (Sicherheits-) Probleme lösen müssten. Auf mögliche Einwände und Zweifel reagieren sie mit glaubwürdigen Argumenten.

Wie können sich Verbraucher:innen schützen:

- Banken und Sparkassen, Behörden oder seriöse Firmen bitten Sie niemals darum, vertrauliche Informationen weiterzugeben – weder telefonisch noch digital!
- Folgen Sie keinen Links, bei denen zur Eingabe von PINs, TANs, Passwörtern, Konto- oder Kreditkartennummern aufgefordert wird. Auch dann nicht, wenn die Aufforderung noch so echt und dringlich erscheint.
- Reagieren Sie nicht auf unübliche E-Mails, SMS oder Anrufe. Anhänge, Links und Bilder sollten Sie nicht öffnen, ohne vorher genau zu prüfen, wer der Absender ist. Am besten löschen Sie verdächtige E-Mails sofort.
- Nehmen Sie sich Zeit und lassen Sie sich nicht unter Druck setzen! Fragen Sie im Zweifel direkt beim genannten Unternehmen oder bei Ihrer persönlichen Kundenberatung der Bank oder Sparkasse nach. Der Kontakt sollte nicht über die verdächtige Nachricht oder der darin genannten Rufnummer erfolgen.
- Kontrollieren Sie regelmäßig die Umsätze Ihres Bankkontos.
- Sollten Sie persönliche Daten weitergegeben haben, sperren Sie umgehend das Online-Banking bzw. die Karte(n). Entweder direkt bei Ihrem Kreditinstitut oder beim Sperr-Notruf 116 116*.

kartensicherheit.de
Aufklärung, Vernetzung, Information

Aktuelle Informationen und Präventionstipps finden Verbraucher:innen auf **www.kartensicherheit.de.**

Der monatliche kostenlose Newsletter bietet zudem spannende, informative Artikel, wichtige Neuigkeiten rund um das Thema Bezahlen und vieles mehr.

* 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 können Gebühren anfallen. Sollte der Sperr-Notruf in seltenen Fällen aus dem Ausland nicht erreicht werden können, gibt es alternativ die Rufnummer +49 (0) 30 40504050.