bankenverband

Blog

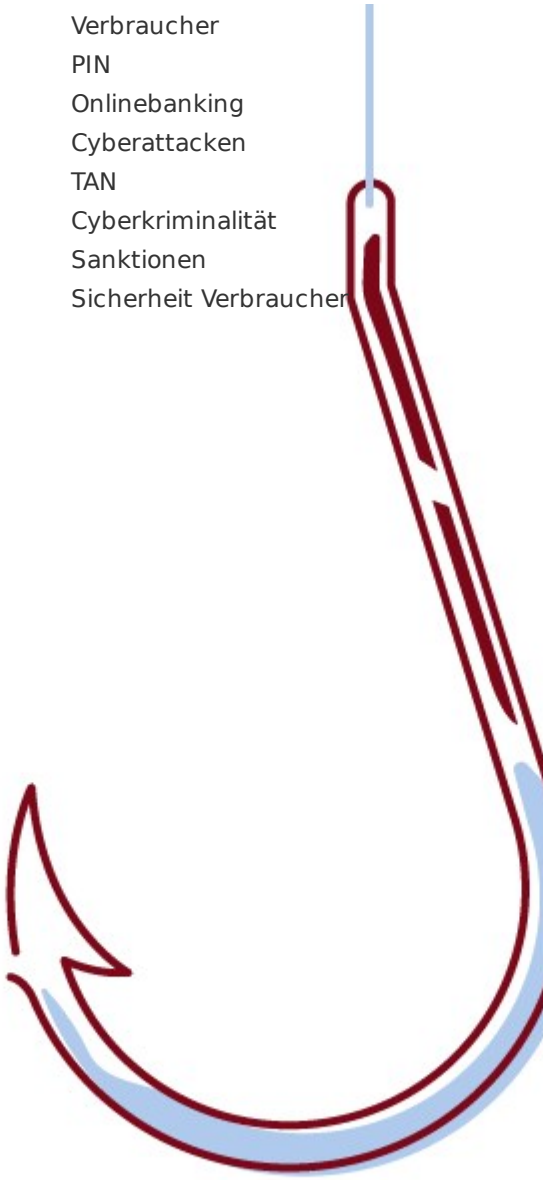
Achtung vor Zunahme von Phishing-Angriffen!

03.03.2022
von

Ernoult, Sylvie

Schlagworte

Phishing
Verbraucher
PIN
Onlinebanking
Cyberattacken
TAN
Cyberkriminalität
Sanktionen
Sicherheit Verbraucher



"Ihr Konto wird deaktiviert - Russland Sanktionen": So oder so ähnlich lautet der Betreff gefälschter Mails, die nach Aussage des Landeskriminalamts Niedersachen gerade von Betrügern in den Umlauf gebracht werden, denn unsichere Zeiten locken leider auch immer Kriminelle hervor. So behaupten die Betrüger, dass Finanzdienstleister zur Einhaltung der Russland-Sanktionen vertrauliche Kundendaten abfragen müssten und laden den Kunden dazu ein, auf einen Link zur Eingabe der Daten zu klicken.

Das Ziel eines solchen Angriffs ist das Abfischen von persönlichen Daten. Folgt das Opfer dem Link aus der gefälschten Mail, kann eine Schadstoffsoftware heruntergeladen werden oder man wird zu einer gefälschten Webseite weitergeleitet. Wird eine Telefonnummer angegeben, die man zurückrufen soll, um das eigene Konto zu „prüfen“, zu „aktualisieren“ oder zu „reaktivieren“ kann der Anruf zu einem Kriminellen, der sich als Angestellter des echten Unternehmens ausgibt, durchgestellt werden. Dabei wird das Opfer aufgefordert, seine persönlichen Daten offenzulegen. Beim vermeintlichen Abgleich der vorliegenden persönlichen Daten ergaunert sich dann der falsche Angestellte unter dem Vorwand von Sanktionsbestimmungen, wertvolle, vertrauliche Informationen.

Anbei finden Sie einige Tipps, um sich vor solchen Angriffen zu schützen!

Banking Apps nur aus autorisiertem App Store laden zum Schutz gegen Phishing

Banking Apps sollten ausschließlich aus dem autorisierten App Store des Smartphones oder Tablets installiert werden (Google Play Store/Apple App Store). Für die Installation sollte dabei keinen, möglicherweise gefälschten „Hinweisen“ zu einem Download aus werblichen E-Mails oder Webseiten nachgegangen werden.

Speichern Sie PINs, TANs und andere Zugangsdaten nicht

Kennwörter, persönliche Geheimzahlen (PINs) und Transaktionsnummern (TANs) sollten niemals unverschlüsselt in Apps, in einer Cloud oder auf der Festplatte gespeichert werden. Auch wenn sie als Telefonnummern im Adressbuch abgespeichert werden, bietet dies keinen ausreichenden Schutz. Zugangsdaten sollten zudem regelmäßig geändert werden. Dies gilt für die gesamten Nutzerkonten, nicht nur fürs Onlinebanking.

Schutz gegen Phishing: Prüfen Sie die Banking-Webseiten

Bei Phishing-Angriffen versuchen Betrüger unter anderem, ahnungslose Nutzer per E-Mail oder SMS auf eine vermeintliche Onlinebanking-Webseite der Bank zu locken, um die Daten abzufangen. Bevor Bankkunden sich einloggen, sollten

sie stets überprüfen, ob es sich wirklich um die verschlüsselte Seite der Bank handelt. Das ist unter anderem am „Schloss“-Symbol im Internet-Browser zu erkennen und daran, dass die Webadresse mit „https“ beginnt.

Bleiben Sie aufmerksam gegen Cybercrime

Auf E-Mails oder SMS der vermeintlich eigenen Bank, die zu einer Bestätigung der sensiblen Daten auffordern, etwa über die Abfrage von PINs oder TANs, sollte nicht geantwortet werden. Auf Links zu klicken, die zu einer weiteren Eingabeseite führen, sollte man ebenfalls unbedingt unterlassen. Banken fragen solche Daten niemals ab, weder per E-Mail oder SMS, aber auch nicht telefonisch. Wenn ein vermeintlicher Bankmitarbeiter anruft und dazu drängt, gemeinsam eine Transaktion vom Konto durchzuführen, sollte man das Gespräch umgehend beenden.