Sparkasse Nürnberg

Medieninformation vom 02.11.2022

Warnung vor Betrugsmasche

Sparkasse fragt keine TAN´s oder Online-Banking-Daten am Telefon ab

Nürnberg (SN). **Derzeit versuchen Bertrügerinnen und Betrüger vermehrt Daten, PIN´s sowie TAN´s zum Online-Banking von Kundinnen und Kunden zu erfragen oder diese zur Digitalisierung der Sparkassencard und der Registrierung der Kreditkarte im S-ID-Check-Verfahren zu bewegen. Sparkassenmitarbeitende rufen niemals Kundinnen und Kunden an und fordern sie telefonisch zur Angabe von Online-Banking-Daten, PINs oder TAN´s auf. Die Sicherheit des Online Bankings der Sparkassen steht damit jedoch nicht zur Debatte, für die missbräuchlichen Zugriffe ist die Mithilfe der Kundinnen und Kunden Voraussetzung. Deshalb warnt die Sparkasse davor, sensible Daten am Telefon herrauszugeben. Stattdessen rät sie, bei entsprechenden Anrufen aufzulegen und ihr Finanzinsitut zu kontaktieren.**

Die Betrügerinnen und Betrüger rufen meist außerhalb der Öffnungszeiten unter der Telefonnummer der Sparkasse Nürnberg bei den Kundinnen und Kunden an. Unter dem Vorwand, dass „sonst nichts mehr funktionieren würde“ bauen die Anruferinnen und Anrufer Druck auf. Den betroffenen Kundinnen und Kunden ist nicht klar, dass sie durch die Mitteilung der TAN Überweisungen oder sogar den Zugriff auf das gesamte Online Banking bis hin zur Änderung der Zugangsdaten ermöglichen. Mit der missbräuchlichen Digitalisierung der Sparkassencard wird das Mobile Bezahlen freigeschalten und somit sind Bargeldverfügungen und Abbuchungen – meist in Supermärkten – für die Betrügerinnen und Betrüger möglich. Dadurch entstehen oft massive finanzielle Schäden

bei den Betroffenen, die nicht über das Sicherheitspaket zum Online Banking von der Sparkasse Nürnerg gedeckt sind, da die Kundinnen und Kunden die Daten selbst weitergegeben haben.

Phishing Versuche auch per SMS

Eine weitere Betrugsmasche erreicht die Kundinnen und Kunden per SMS. Die Betrügerinnen und Betrüger schicken Nachrichten mit der Sparkasse als angebliche Absenderin und nutzen verschiedene Vorwände, um sensible Daten abzugreifen: „*Ihre Synchronisierung zu den PSD2/EU-Richtlinien steht weiter aus […]*“, „*Ihr TAN-Gerät läuft heute aus. Bitte verlängern Sie dieses unter […]*“ oder „*Ihr TAN-Verfahren läuft am […] ab. Bitte verlängern Sie Ihre Legitimation unter […]*“. Kundinnen und Kunden sollen nicht auf die in den Nachrichten enthaltenen Link klicken und auch keine Daten auf der verlinkten Seite eingeben, um so Schadensfälle zu vermeiden.

Das sollten Kundinnen und Kunden im Schadensfall tun

Betroffene Kundinnen und Kunden sollten im ersten Schritt ihre digitalen Karten im Online Banking löschen und den Online-Banking-Zugang bei ihrem Finanzinsitut sperren lassen. Anschließend sollten sie eine Anzeige bei der Polizei tätigen.

Kontakt:

Sarah Schmoll
Referentin Unternehmenskommunikation
Telefon: 0911 230 2642
sarah.schmoll@sparkasse-nuernberg.de