Sparkasse Nürnberg

Medieninformation vom 23.10.2024

Warnung vor Phishing

Aufmerksam sein und Schäden vermeiden

Nürnberg (SN). **Sie erhalten eine SMS oder E-Mail mit dem Hinweis *„Aktualisieren Sie Ihre Daten“* oder *„Ihr PushTAN läuft ab“,* in der Sie dazu aufgefordert werden, den enthalten Link, der Sie auf eine Phishingseite führt, anzuklicken. In der Folge erhalten Sie einen Anruf eines falschen Bank- bzw. Sparkassenmitarbeitenden. Der angebliche Mitarbeitende aus der Sicherheitsabteilung Ihres Finanzinstituts informiert Sie über Probleme im Online Banking oder über auffällige Buchnungen auf Ihren Konten. Anschließend will der Anrufende die Probleme gleich am Telefon mit Ihnen lösen und fordert Sie auf, die Anmeldedaten für Ihr Online Banking zu nennen bzw. Transaktionen in der PushTAN-App freizugeben. So oder so ähnlich sehen gängige Phishing-Maschen aus. Ohne die Mithilfe von Kontoinhaberinnen und -inhabern, haben die Betrügerinnen und Betrüger allerdings keine Chance.**

Die Sparkasse Nürnberg macht regelmäßig über verschiedene Kanäle auf aktuelle Betrugsmaschen aufmerksam, um ein Bewusstsein bei Verbraucherinnen und Verbrauchern dafür zu schaffen und präventiv zu informieren. Fallen Kundinnen oder Kunden auf die Maschen der Betrüger herein, können massive finanzielle Schäden für die Betroffenen entstehen. Aktuelle Sicherheitswarnungen finden Kundinnen und Kunden unter: www.sparkasse-nuernberg.de/sicherheitshinweise

Das sollten Kundinnen und Kunden tun, um Schäden zu vermeiden

- Prüfen Sie SMS oder E-Mail-Nachrichten sorgfältig, auch wenn der Absender angeblich ihre Hausbank ist.

- Klicken Sie nicht auf die enthaltenen Links.
- Melden Sie sich über Ihren Browser direkt im Online-Banking an oder rufen Sie direkt Ihre Sparkassen-App auf.
- Vertrauen Sie nicht darauf, dass Sie wirklich ihre Bank oder Sparkasse anruft, auch wenn die angezeigte Rufnummer dies suggeriert. Die angezeigte Rufnummer kann mit einer entsprechenden Software manipuliert werden.
- Geben Sie niemals Aufträge in der Push-TAN-App frei, die Sie nicht vorher selbst im Online-Banking erfasst haben. Prüfen Sie die in der App angezeigten Daten immer gründlich, bevor Sie die Freigabe erteilen.
- Bei auffälligen Anrufen von vermeintlichen Sparkassen- oder Bankmitarbeitenden legen Sie auf und rufen Ihr Finanzinstitut unter den Ihnen bekannten Rufnummern an. Sperren Sie vorsichtshalber Ihren Online-Banking-Zugang.

Das ist im Schadensfall zu tun

Betroffene Kundinnen und Kunden sollten im ersten Schritt ihren Online-Banking-Zugang sperren (lassen). Anschließend sollten sie ihr Finanzinstitut informieren und eine Anzeige bei der Polizei stellen.

Kontakt:

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