Ostsächsische Sparkasse Dresden

Pressemitteilung

Online-Banking wird noch sicherer

Dresden, 17. Juli 2023

Die Sparkasse führt im Online-Banking eine weitere Sicherheitsvorkehrung ein: die Geräteerkennung. So verfügt jetzt auch das Online-Banking über eine 2-Faktor-Authentifizierung.

Ab 18. Juli 2023 werden Kundinnen und Kunden der Ostsächsischen Sparkasse Dresden beim Login in ihr Online-Banking am PC neben ihren Anmeldedaten nach einer TAN gefragt. Dies ist Teil des neueingeführten zweistufigen Anmeldevorgangs. Im Internetbrowser können von den Kunden Geräte dann als „vertrauenswürdig“ gespeichert werden, damit wird eine TAN Eingabe nur noch aller 180 Tage notwendig. So wird das Online-Banking über einen Internetbrowser noch sicherer.

Die Sparkasse stellt so sicher, dass Kundinnen und Kunden im Online-Banking einen Überblick behalten, über welche Geräte sie sich einloggen. Zukünftig wird bei allen unbekannten Geräten (außer beim Login in der App) immer eine TAN gefordert– so sollen ungewollte Logins in die Online-Banking-Zugänge der Kunden unterbunden werden.

Kriminelle melden sich am Wochenende

Betrüger setzen derzeit vermehrt auf gefälschte SMS und Anrufe, um Kunden der Sparkasse zu täuschen und finanziell zu schädigen. Dabei versenden sie vor allem am Wochenende SMS im Namen der Sparkasse mit der Aufforderung, einem Link zu folgen und persönliche Daten einzugeben. Haben Kunden auf die SMS reagiert und persönliche Informationen eingegeben, erhalten sie in der Regel anschließend einen Anruf. Dieser kommt augenscheinlich von der Sparkasse, da die Betrüger mit gefälschter Nummer anrufen. Ab hier geht alles ganz schnell: Die Kriminellen täuschen vor, dass beispielsweise eine falsche Überweisung sehr schnell rückgängig gemacht oder ein neues Sicherheitssystem sofort bestätigt werden muss. Kunden werden aufgefordert, mehrere TANs zu nennen. Damit nehmen die Täter dann aber Überweisungen von den Konten der Kunden vor. So kann ein erheblicher finanzieller Schaden entstehen.

Tipp: Ihre Daten gehören nur Ihnen und nicht in fremde Hände. Wenn Sie keine Daten weitergeben, kann nichts passieren.

Kunden sollten regelmäßig ihr Online-Banking-Passwort ändern. Hier sollte kein Standard-Passwort gewählt werden, sondern immer eine Kombination aus Groß- und Kleinschreibung, Zahlen und Sonderzeichen. Auch kann die Einrichtung des Kontoweckers helfen, über Bewegungen auf dem Konto auf dem Laufenden zu bleiben.

Sicherheitschecks werden missbraucht

Die Inhalte der betrügerischen SMS sind vielfältig: Kunden werden darüber "informiert", dass ihre pushTAN-Registrierung abläuft, dass sie ihren S-ID-Check der Kreditkarte

aktualisieren sollen oder dass andere Daten überprüft werden müssten. In jedem Falle gelangt der Kunde über den angegebenen Link auf eine gefälschte Seite, die der Homepage der Sparkasse zum Verwechseln ähnlich sieht und auf der er sensible Daten eingeben soll. Im Anschluss kommt ein Anruf der Betrüger.

Tipp: Handeln Sie bedacht und lassen Sie sich nicht unter Druck setzen. Oft wird am Telefon eine mutmaßliche Notfallsituation vorgegeben, bei der Sie schnell handeln sollen. Vereinbaren Sie gegebenenfalls mit Angehörigen eine individuelle Sicherheitsfrage, um sicherzugehen, dass Sie wirklich mit Ihnen bekannten Personen telefonieren.

Wir fragen NICHT nach sensiblen (Konto-)Daten!
Die Sparkasse, die Polizei oder auch andere seriöse Firmen (z.B. Autohäuser oder Energieunternehmen) fragen am Telefon, per Email oder SMS niemals nach persönlichen Kontodaten oder fordern auf, TANs am Telefon zu nennen. Die betrügerischen Anrufe kommen oft abends oder am Wochenende, also außerhalb der Geschäftszeiten der Sparkasse, damit Kunden keine Möglichkeit haben, bei ihrer Sparkasse nachzufragen.

Seien Sie misstrauisch!
Die Sparkasse aktualisiert das Online-Banking regelmäßig, um die Konten und Daten ihrer Kundinnen und Kunden bestmöglich zu schützen. Eine ganze Abteilung der Sparkasse ist nur dafür zuständig, aktuelle Betrugsmethoden zu identifizieren und Gegenmaßnahmen zu ergreifen. Um ihr Konto zu schützen, geben Kundinnen und Kunden am besten die URL ihrer Sparkasse direkt in den Browser ein und gehen nicht über Google oder andere Links.

Bekannte Betrügerkonten werden direkt von der Sparkasse gesperrt. Auch betrügerische Websites, die im Rahmen von Phishing-SMS oder E-Mails auffallen, werden vom zentralen Sparkassensicherheitszentrum gesperrt. So fallen Überweisungen an diese Adressen direkt auf und werden von unserem Sicherheitssystem gestoppt.

Alle Infos zur Einführung Geräteerkennung gibt's auf unserer Homepage:
www.ostsaechsische-sparkasse-dresden.de/de/home/aktionen/geraeteerkennung.html

www.ostsaechsische-sparkasse-dresden.de/de/home/service/s-cert-meldungen.html

Rückfragen:

Linda Menzel
Stellvertretende Unternehmenssprecherin
Tel. 0351 – 455 16516
linda.menzel@sparkasse-dresden.de