OstseeSparkasse Rostock

PRESSEINFORMATION **11. Oktober 2022**

OstseeSparkasse Rostock warnt vor Online-Banking Betrugsmaschen

Phishing im Internet, per E-Mail oder SMS

Immer häufiger werden der OSPA und örtlichen Polizei Betrugsversuche und Schadensfälle im Online-Banking gemeldet. Derzeit sind der OSPA ca. ein Dutzend Fälle bekannt. Zuletzt wurden zahlreiche betrügerische SMS vermeintlich im Namen der Sparkasse wahllos an Kunden wie auch Nicht-Kunden verschickt. Ein Datenleck oder eine Sicherheitslücke auf Seiten der Sparkassen ist dabei ausgeschlossen. Für die Speicherung und Verarbeitung kundenbezogener Daten gelten höchste Sicherheitsstandards. Das Abgreifen persönlicher Kontaktdaten (z. B. Telefonnummer oder E-Mailadresse), welches nicht speziell auf Sparkassenkunden ausgerichtet ist, erfolgt zumeist im Vorfeld über sog. Phishing-Seiten oder Datenklau im Internet (z. B. nach freiwilliger Angabe in Online-Shops).

Im Rahmen der aktuellen Betrugsmasche werden die abgegriffenen Mobilfunknummern zum Versand von Massen-SMS durch die Betrüger genutzt.

Quelle: Polizeiinspektion Rostock

Die SMS beinhaltet eine Aufforderung und einen Link. Dieser führt zu einer täuschend echten Sparkassen-Webseite, auf der der Nutzer zur Auswahl seines betreuenden Instituts aufgefordert wird, um im Anschluss seine Online-Banking Zugangsdaten einzugeben. In diesem Schritt greifen die Betrüger die persönlichen Anmeldedaten ab. Nach vermeintlicher Verifizierung über Informationen wie Geburtsdatum und Kontonummer erfolgt eine Aufforderung zur Bestätigung per TAN-Verfahren. Gibt der Kunde diese Bestätigung aktiv frei, erhalten die Betrüger zusätzlich Zugriff auf das TAN-Verfahren im Online-Banking und können eigenständig Aufträge auslösen und freigeben. Ein telefonischer Kontakt erfolgt bei dieser Betrugsmasche nicht.

OstseeSparkasse Rostock

Berichte betroffener Kunden verdeutlichen die Professionalität dieser Masche. *„Ich hätte nie gedacht, dass mir das passiert! Ich mache schon seit vielen Jahren Online-Banking und obwohl ich weiß, dass man auf solche Links nicht klicken darf, bin ich in einem unachtsamen Moment einfach der Aufforderung gefolgt. Die gefälschte Webseite sah täuschend echt aus, so dass ich keinen Verdacht schöpfte. Mir ist bewusst, dass ich einen Fehler gemacht habe. Im Anschluss habe ich direkt meinen ganzen Bekanntenkreis informiert, damit nicht noch mehr Menschen auf diese Betrüger reinfallen.“* (OSPA Kunde, - anonym -)

Die maßgeblichen Sorgfaltspflichten des Kunden im Online-Banking ergeben sich aus § 675 l BGB in Verbindung mit den Sonderbedingungen für das Online-Banking. Hat der Kunde grob fahrlässig gegen diese Sorgfaltspflichten verstoßen, indem er personalisierte Sicherheitsmerkmale (PIN/ TAN) außerhalb des Online-Banking Verfahrens herausgegeben hat, besteht kein Anspruch auf Wiedergutschrift missbräuchlich verfügter Beträge. Vor diesem Hintergrund ist verstärkte Wachsamkeit und Skepsis geboten.

Grundsätzlich gilt: Für den sicheren Zugang zum OSPA Online-Banking sollten ausschließlich folgende zwei Wege genutzt werden:

1) Eigen- und vollständige Eingabe der Internetadresse www.ospa.de in der Adresszeile des Browsers oder wahlweise abspeichern der genannten URL unter den persönlichen Favoriten. Auf Suchmaschinen wie Google oder die Ausfüllhilfen moderner Browser sollte unbedingt verzichtet werden.
2) Nutzung der S-App auf dem persönlichen mobilen Endgerät

Bei Unsicherheiten oder Auffälligkeiten können Kunden sich umgehend unter 0381 643-0 im Kundenservice der OSPA über die Rechtmäßigkeit eines Vorgangs informieren.

In keinem Fall sollten Links geklickt werden, die einem unaufgefordert im Internet, per E-Mail oder SMS angezeigt werden. Auf diese Weise umgehen Kunden die Gefahr, durch gefälschte Suchmaschinenanzeigen oder ähnlich lautende Web-Adressen auf Phishing-Seiten umgeleitet zu werden, die täuschend echt die Nutzeroberfläche des Sparkassen Online-Bankings imitieren.

Ausführliche Informationen zum Thema Datendiebstahl und Phishing sowie Sicherheitstipps stellt die Sparkasse verunsicherten Kunden auf https://www.ospa.de/de/home/service/datendiebstahl-phishing.html zur Verfügung.

Medienvertreter:innen können zudem jeder Zeit im Presse-Center der OSPA unter www.ospa.de/presse Informationen abrufen, inkl. Mediathek mit Downloadbereich (Pressefotos und Logodateien).