Finanzgruppe
Sparkassen- und Giroverband
für Schleswig-Holstein

Sparkassen- und Giroverband für Schleswig-Holstein | kommunikation@sgvsh.de

Dr. Kilian Lembke
Pressesprecher
Kommunikation und Gesellschaftliches Engagement
Fachbereichsleiter
Medien und Kommunikation
Telefon +49 431 5335 - 506
Mobil +49 151 688 705 46
kilian.lembke@sgvsh.de

Medieninformation

23. Juni 2022

Sparkassen Schleswig-Holsteins warnen vor aktueller Betrugsmasche beim Online-Banking

Die Sparkassen in Schleswig-Holstein warnen vor einer aktuellen Betrugsmasche im Online-Banking, die derzeit bundesweit auftritt. Diese betrifft ausschließlich Kundinnen und Kunden, die nicht die Sparkassen-App nutzen oder nicht direkt die URL-Adresse der (jeweiligen) Sparkasse verwenden, sondern diese über eine Suchmaschine ansteuern.

In diesen Fällen werden die Nutzerinnen und Nutzer zuerst auf eine falsche Internetseite gelenkt, die der der Sparkasse täuschend ähnlich aussieht. Dort werden sie wie üblich beim Online-Banking aufgefordert, ihre Zugangsdaten einzugeben, um sich in ihr Konto einzuloggen. Im aktuellen Fall der gefälschten Seiten taucht eine Fehlermeldung auf und eine angebliche Sparkassenmitarbeiterin ruft diese betroffenen Kundinnen und Kunden an, um den angeblichen Fehler zu beheben.

Die Betrüger erwecken einen vertrauensvollen Eindruck und täuschen beim Anruf teils auch die Telefonnummer der (jeweiligen) Bank oder Sparkasse vor. So gelingt es ihnen häufig, die Nutzer zur Eingabe von PIN und TAN zu bewegen und vermeintliche Testüberweisungen oder angebliche Stornierungsaufträge in großer Höhe durchzuführen. So werden insbesondere ältere Menschen um ihr Geld gebracht.

Dazu sagt Oliver Stolz, Präsident des Sparkassen- und Giroverbandes für Schleswig-Holstein: „Leider ist die Betrugsmasche bundesweit bekannt. Aktuell sind auch Kundinnen und Kunden in Schleswig-Holstein davon betroffen. Diese wollen wir bestmöglich schützen. Daher warnen wir in Beratungsgesprächen, über die Internetfilialen, Blogs, Social Media und über die Medien und rufen zur Vorsicht auf. Die Kundinnen und Kunden sollten dritten Personen niemals persönliche Zugangsdaten wie PIN- oder TAN-Nummern mitteilen. Sparkassenmitarbeiterinnen und -mitarbeiter erfragen diese nie am Telefon.“
Die Sparkassen raten dazu, bei verdächtigen Anrufen am besten gleich aufzulegen, keinesfalls Überweisungen o. Ä. auf Anweisung durchzuführen und sich auf keinen Fall unter Druck setzen zu lassen. Im Zweifelsfall sollte man seinen vertrauten Berater oder seine vertraute Beraterin in der Sparkasse anrufen, und zwar nur unter der jeweils bekannten Telefonnummer.

Das Online-Banking der Sparkasse ist sicher. Wer nicht die Sparkassen-App nutzt, sondern sich über die Internetfiliale anmeldet, sollte sich auf jeden Fall vergewissern, dass man die richtige Internetadresse gewählt hat.

Die korrekten Internetadressen (URL) und zentralen Telefonnummern der schleswig-holsteinischen Sparkassen sind unter https://www.sgvsh.de/sparkassen-schleswig-holsteins aufgelistet. Die jeweilige URL wird am besten direkt in die Adresszeile des Internetbrowsers eingegeben. Dabei sollte darauf geachtet werden, dass dort auch das geschlossene Schlosssymbol zu sehen ist.

Wer die Internetadresse stattdessen googelt und die ersten Ergebnisse in der Suchmaschine ungeprüft anklickt, läuft Gefahr, auf täuschend echt aussehenden, aber gefälschten Internetseiten zu landen. Diese sind zum Beispiel an einer anderen Schreibweise zu erkennen, teils mit Schreibfehlern, teils mit einer anderen Endung.

Sicherheitstipps der Polizei

- Grundsätzlich sollte die Internetadresse der Bank, die sogenannte URL, durch Eintippen in die Adresszeile im Internet eingegeben werden. Bei der Eingabe über eine Suchmaschine besteht das Risiko, auf eine gefälschte, täuschend echt aussehende Bankseite, einem sogenannten Fake, zu geraten.
- Bankmitarbeiter:innen werden niemals persönliche Daten oder Informationen über das Konto am Telefon erfragen und erst recht nicht nach der persönlichen Geheimzahl (PIN) oder nach der Transaktionsnummer (TAN).
- Ebenso wird niemals die Herausgabe von Bargeld oder Wertgegenständen verlangt.
- Behauptungen wie „Jemand hat Zugriff auf Ihr Konto“ oder „Das Geld ist bei der Bank nicht mehr sicher“, „Es muss zu Hause aufbewahrt oder in ein Schließfach gelegt werden“ stimmen nicht. Das gilt auch für die Aussage, dass Überweisungen gesperrt werden müssen.
- Lassen Sie sich nicht zeitlich durch Bemerkungen wie „sonst ist das Geld verloren“ unter Druck setzen. Bankmitarbeiter:innen würden ihre Kund:innen niemals am Telefon auffordern, Onlineüberweisungen oder Bargeld-Transaktionen vorzunehmen, auch nicht zu Testzwecken oder weil das Konto angeblich „gehackt“ wurde.
- Vergewissern Sie sich im Zweifel bei Ihrer Bank, ob ein Anruf tatsächlich von dort kommt. Die Betrüger:innen können bei Anrufen durch technische Manipulationen die echte Telefonnummer der Bank auf dem Display der Kund:innen erscheinen lassen. Wählen Sie bei einem Rückruf nur die Ihnen bekannte Telefonnummer der Bank und nutzen Sie keine Rückruffunktion.
- Sprechen Sie mit Familienangehörigen oder anderen Vertrauenspersonen über solche ungewöhnlichen Situationen und holen Sie sich Rat.
- Geben Sie auf keinen Fall private Daten wie Bankkontodaten, Kreditkartendaten, TAN-Nummern oder Zugangsdaten zu Kundenkonten, zum Beispiel PayPal, heraus.
- Erstatten Sie Anzeige bei der Polizei und melden Sie solche Vorfälle bei Ihrer Bank.
- Die Polizei ruft insbesondere ältere Menschen dazu auf, bei derartigen Anrufen hellhörig zu werden und umgehend die Polizei zu informieren. Darüber hinaus rät die Polizei jüngeren Familienangehörigen, ihre lebensälteren Verwandten und Bekannten für das Thema zu sensibilisieren.
- Wertvolle Sicherheitstipps für Senior:innen sind im dem Bereich Prävention der Website der Landespolizei Schleswig-Holstein zu finden.