

Achtung, Sparkassen-Kunden: Neue Phishing-Masche bedroht dein Geld!

Achtung Sparkassen-Kunden: Betrüger nutzen neue Phishing-Mails, um sensible Daten zu stehlen. Jetzt handeln und Online-Banking schützen!



Nachrichten AG

Dortmund, Deutschland - Immer mehr Cyber-Betrüger nehmen gezielt Sparkassen-Kunden ins Visier. Wie **Berlin Live** berichtet, kommt es derzeit zu einer Welle von Phishing-Attacken, die dazu führen, dass ahnungslose Nutzer glauben, ihre Bank benötige wichtige Informationen. Dabei wird vorgespielt, dass eine dringende Aktualisierung der „PushTan“-App notwendig sei, um den Zugang zum Online-Banking aufrechtzuerhalten. In einer solchen Situation sollten Kunden jedoch dringend darauf achten, keine sensiblen Daten preiszugeben.

In den gefälschten Nachrichten, die viele Sparkassen-Kunden erreichen, wird behauptet, dass eine Untersuchung im Hinblick

auf Sicherheitsverfahren notwendig ist. Die Betrüger fordern die Nutzer auf, einen Link zu klicken, der sie auf eine manipulierte Website führt. Dort sollen sie die Online-Banking-Zugangsdaten sowie persönliche Informationen eingeben. „Es wird versucht, Sie zum Aufruf einer betrügerischen Webseite zu bewegen“, warnt die Sparkasse. Das Geldinstitut rät eindringlich, solche Anfragen ernst zu nehmen und keine sensiblen Informationen preiszugeben.

Risiken und Folgen

Die Gefahren solcher Phishing-Attacken sind immens. Wer in die Falle tappt und seine Daten eingibt, erleichtert es Betrügern, auf sein Konto zuzugreifen. Im schlimmsten Fall könnte dies zu erheblichen finanziellen Verlusten führen. Die Sparkasse macht Kunden darauf aufmerksam, dass diese Daten auch für betrügerische Anrufe verwendet werden können, in denen sich Betrüger als Bankmitarbeiter ausgeben und versuchen, die Opfer weiter zu manipulieren. **Ruhr24** führt aus, dass Kriminelle in den Mails sogar das offizielle Design der Bank imitieren, was das Erkennen von Betrug zusätzlich erschwert.

Besonders perfide ist, dass die Mails mit Betreffzeilen wie „Aktualisierung unseres Sicherheitsverfahrens – Prüfen Sie jetzt“ versehen sind. Kunden sollten hierbei besondere Vorsicht walten lassen und in keinem Fall auf Links in solchen E-Mails klicken oder gar persönliche Daten eingeben. Die Sparkasse rät, verdächtige Mails direkt in den Spam-Ordner zu verschieben und im Ernstfall sofort zu handeln: Sollte man bereits Daten übermittelt haben, ist es ratsam, umgehend den Online-Banking-Zugang zu sperren und eventuelle Schäden zu melden.

Schutzmaßnahmen

Um sich vor solchen Angriffen zu schützen, empfiehlt die Sparkasse, regelmäßig auf Aktualisierungen der Bank-Apps zu achten und im Zweifel immer direkt bei der Bank nachzufragen, wenn eine E-Mail ungewöhnlich erscheint. Insbesondere sollten

Kunden nie auf Links aus E-Mails klicken, die sie nicht erwartet haben, und bei Ansprüchen auf persönliche Daten äußerst skeptisch reagieren.

Die reiterierten Warnungen mahnen Kunden dazu, aufmerksam und vorsichtig zu sein, um nicht Opfer der ausgeklügelten Betrugsmaschen zu werden, die immer wieder neue Formen annehmen. Damit so viele Menschen wie möglich informiert werden, sollte jeder, der solche Mails erhält, dies auch in seinem Umfeld kommunizieren.

Details	
Vorfall	Betrug
Ursache	Phishing
Ort	Dortmund, Deutschland
Quellen	<ul style="list-style-type: none">• www.berlin-live.de• www.ruhr24.de

Besuchen Sie uns auf: n-ag.de