NACHRICHTEN
Österreich

Achtung! Betrügerische E-Mails bedrohen ING-Kunden – So schützen Sie sich!

ING-Kunden sollten vorsichtig sein: Gefälschte E-Mails drohen mit Kontosperrung und fordern zur Datenpreisgabe auf.

Leer, Deutschland -

Aktuell müssen sich Kunden der ING-Bank in Acht nehmen, da sie mit gefälschten E-Mails konfrontiert werden. Diese Phishing-Versuche haben den Betreff „Aktualisieren Sie Ihr Konto | Letzte Mahnung“ und fordern die Empfänger auf, ein neues „Tan-App-Sicherheitssystem“ zu aktivieren. Die Verbraucherzentrale warnte vor dieser betrügerischen Masche, die darauf abzielt, persönliche Daten zu erlangen und Konten zu leerräumen.

In den E-Mails wird den Nutzern angedroht, dass sie keinen Zugriff mehr auf ihr Konto für Bankgeschäfte haben, wenn das Update nicht bis zum 5. Januar erfolgt. Um ihre Daten zu aktualisieren, werden die Empfänger aufgefordert, auf einen Button mit der Aufschrift „Klicken Sie hier“ zu klicken. Experten verweisen auf mehrere Anzeichen, die auf Phishing-Mails hindeuten, darunter unpersönliche Anrede, unseriöse Absenderadresse, verdächtige Links innerhalb der E-Mail und auffällige Rechtschreib- sowie Satzbaufehler.

Warnung vor Phishing-Versuchen

Die Verbraucherzentrale empfiehlt, solche E-Mails zu ignorieren

und sie in den Spam-Ordner zu verschieben. Zudem sollen die Nutzer in der offiziellen ING-App oder auf der Homepage nach ähnlichen Aufforderungen suchen. Der aktuelle Vorfall ist nicht der erste seiner Art: Im Februar 2024 waren bereits ING-Kunden von einer ähnlichen Betrugsmasche betroffen, und im Dezember 2024 warnte die Verbraucherzentrale vor einer Betrugswelle, die 12 Millionen Kunden anvisierte.

Wie **watson.de** berichtet, sind Phishing-Angriffe eine häufige Betrugsmethode, um persönliche und finanzielle Informationen zu stehlen. Kriminelle nutzen dabei täuschend echte E-Mails oder gefälschte Webseiten. Die Verbraucherzentrale weist ausdrücklich darauf hin, dass seriöse Banken niemals zur Preisgabe sensibler Daten via Link auffordern.

Bei verdächtigen E-Mails wird geraten, den Mauszeiger über den Link zu positionieren, um die Ziel-URL zu überprüfen, und den Link nicht anzuklicken. Verdächtige E-Mails können zur Auswertung an die Verbraucherzentrale weitergeleitet werden, wobei die personenbezogenen Daten anonymisiert werden.

– Übermittelt durch **West-Ost-Medien**

Details	
Vorfall	Betrug
Ursache	Phishing
Ort	Leer, Deutschland
Quellen	• **www.merkur.de** • **www.watson.de**