NACHRICHTEN AG

01. Juni 2025

Achtung! ING-Kunden im Visier: Phishing-E-Mails gefährden Ihr Geld!

Verbraucherzentrale warnt ING-Kunden vor aktuellen Phishing-E-Mails. Jetzt informieren und sensibel mit Daten umgehen!

Niederlande - Die Verbraucherzentrale warnt eindringlich vor aktuellen Phishing-E-Mails, die im Namen der niederländischen Bank ING versendet werden. Die betrügerischen Nachrichten fordern die Kunden zur „online Identifikation“ auf und geben an, dass diese bis zum 30. Mai 2025 abgeschlossen sein müsse. Bei Nichtbeachtung der Frist drohen die Betrüger mit der Sperrung bestimmter Dienstleistungen. **Ruhr24** berichtet, dass die Absender durch Zeitdruck die Kunden zu unüberlegten Handlungen drängen wollen.

Phishing ist ein Betrugsversuch, bei dem Kriminelle gefälschte E-Mails verwenden, die von vertrauenswürdigen Unternehmen zu stammen scheinen. Das übergeordnete Ziel ist der Diebstahl

sensibler Daten wie Passwörter. Die aktuellen E-Mails zeichnen sich durch Merkmale wie unseriöse Absenderadressen, unpersönliche Ansprachen, verdächtige Links, sowie drohende Fristen aus. Insbesondere Rechtschreibfehler im Betreff sind ein weiteres Indiz für deren Täuschungsabsicht.

Vorsicht vor Phishing-Mails

Neben der Warnung bezüglich der ING-E-Mails thematisiert die Bank selbst ähnliche Betrugsversuche. Laut **ING** erhalten die Kunden zurzeit E-Mails mit dem Betreff „Bestätigen Sie Ihre Kontodaten so schnell wie möglich!“. Diese Nachrichten behaupten, es sei erforderlich, ein neues Sicherheitssystem zu aktivieren und enthalten Links, über die sich die Empfänger anmelden sollen. ING weist jedoch darauf hin, dass alle sicherheitsrelevanten Informationen sicher in der Post-Box bereitgestellt werden, und niemals solche Umfragen über Links abgefragt werden.

Die Phishing-Mails sind oft schwer zu erkennen, denn sie sehen täuschend echt aus – die Betrüger ahmen die Kommunikation von Unternehmen nach und nutzen Layout und Sprache, um Vertrauen zu schaffen. Die Verbraucherzentrale empfiehlt daher, verdächtige E-Mails in den Spam-Ordner zu verschieben und keine Links zu klicken. Kunden sollten stets offizielle Kontaktwege nutzen, um die Echtheit von E-Mails zu überprüfen. Seriöse Banken fordern niemals per E-Mail zur Eingabe vertraulicher Daten auf.

Wichtige Maßnahmen bei Verdacht

Kunden, die bereits auf eine Phishing-Nachricht reagiert haben, sollten umgehend ihre Zugangsdaten ändern und die Bank kontaktieren. Diese Vorgehensweise ist entscheidend, um potenzielle Schäden durch den Verlust sensibler Daten zu minimieren.

Die Verbreitung von Phishing-Mails zeigt, wie wichtig es ist, sich

über diese Bedrohungen zu informieren. Auch andere Banken, wie die Commerzbank, warnen vor ähnlichen Betrugsversuchen. Die Verbraucherzentrale hat in ihrem **Phishingradar** aktuelle Warnungen, die auf unprofessionelle Aufmachungen und unseriöse Absenderadressen hinweisen.

In Anbetracht dieser Informationen ist es unerlässlich, stets wachsam zu bleiben und verdächtige E-Mails kritisch zu hinterfragen. Nur so können Kunden sich wirksam vor Betrugsversuchen schützen.

Details	
Vorfall	Betrug
Ursache	Phishing
Ort	Niederlande
Quellen	• **www.ruhr24.de** • **www.ing.de** • **www.verbraucherzentrale.de**

Besuchen Sie uns auf: n-ag.net