NACHRICHTEN AG

09. Mai 2025

Achtung ING-Kunden: Phishing-Welle bedroht Ihre Bankdaten!

Verbraucherzentrale warnt vor Phishing-E-Mails an ING-Kunden. Tipps zur Erkennung und Sicherheitsmaßnahmen im Artikel.

Ruhr, Deutschland - Die Verbraucherzentrale warnt eindringlich vor einer aktuellen Welle von Phishing-E-Mails, die sich gezielt an Kunden der ING-Bank richten. Diese gefälschten Nachrichten fordern die Empfänger dazu auf, ihre Banking-App zu aktualisieren, und beinhalten oft einen dubiosen Link anstelle von Verweisen zu offiziellen App-Stores. In den letzten Tagen haben zahlreiche Kunden solche betrügerischen E-Mails erhalten, die mit dem Betreff „[ING-Banking-to-go] – Es gibt neue Informationen in Ihrer Post-Box“ auf sich aufmerksam machen. Betrüger drohen sogar mit „Einschränkungen bei der Nutzung der ING App“, falls die Aufforderung nicht schnellstmöglich befolgt wird, was zusätzlichen Druck erzeugt.

Die E-Mails weisen mehrere charakteristische Merkmale auf, die auf Phishing hindeuten. Dazu gehören eine unpersönliche Anrede wie „Sehr geehrter Kunde“, sowie unseriöse Absenderadressen, die nicht zur offiziellen ING-Domain gehören. Zudem enthalten die E-Mails oft auffällige Fehler und erzeugen künstlich Dringlichkeit durch vage Fristen (**Ruhr24**, **Stuttgarter Nachrichten**).

Warnsignale und Schutzmaßnahmen

Die Verbraucherzentrale hat spezifische Tipps zur Erkennung von Phishing-Mails veröffentlicht. Empfänger sollten die Absenderadresse prüfen, unpersönliche Anreden identifizieren und Links vor dem Anklicken durch „Mouse-over“ kontrollieren. Zeitdruck und Drohungen sind ebenfalls alarmierende Hinweise. Zudem sollten Prüfsiegel in offiziellen Mails der ING ein Anzeichen für Echtheit sein. Verdächtige E-Mails empfiehlt die Verbraucherzentrale, in den Spam-Ordner zu verschieben und sich direkt über die offizielle Website oder App der Bank einzuloggen (**Ruhr24**, **Stuttgarter Nachrichten**).

Es gibt auch andere Methoden von Betrügern, die Verbraucher auf Trab halten: Dazu gehören gefälschte QR-Codes, die auf manipulierte Webseiten leiten, sowie falsche App-Installationen, die häufig Schadsoftware beinhalten. Wer mit der Situation konfrontiert wird, sollte umgehend seine Passwörter ändern und die Bank über den Vorfall informieren. Ein sofortiger Scan des Geräts auf Schadsoftware sowie die Erstattung einer Anzeige bei der Polizei können ebenfalls notwendig sein. Die ING versichert zudem, dass finanzieller Schaden bei Missbrauch von Zugangsdaten ersetzt wird (**Stuttgarter Nachrichten**).

Allgemeine Tipps zur Cyber-Sicherheit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt weitere Ratschläge zur Vermeidung von Phishing-Angriffen. Es wird geraten, keine vertraulichen Zugangsdaten per E-Mail weiterzugeben und Links in dubiosen E-Mails nicht anzuklicken.

Empfohlene Vorgehensweisen umfassen das Speichern häufig besuchter Login-Seiten in einer Favoritenliste sowie das Erreichen wichtiger Webseiten über die offizielle Startseite der jeweiligen Organisation. Bei Unsicherheiten sollte man sich telefonisch beim Anbieter vergewissern. Zudem empfiehlt das BSI, keine persönlichen Daten auf unverschlüsselten Webseiten einzugeben und regelmäßig den Kontostand sowie die Umsätze zu kontrollieren. Eine aktive Antivirus-Software und eine funktionierende Firewall sind ebenfalls entscheidend für den Schutz der eigenen Daten (**BSI**).

Insgesamt bleibt festzuhalten, dass Wachsamkeit und gesunder Menschenverstand entscheidend sind. Verdächtige E-Mails sollten ignoriere werden, um nicht Opfer von Cyberkriminalität zu werden.

Details	
Vorfall	Phishing
Ort	Ruhr, Deutschland
Quellen	• **www.ruhr24.de** • **www.stuttgarter-nachrichten.de** • **www.bsi.bund.de**