

## Achtung: Neue PayPal-Betrugsmasche mit gefälschten Rechnungen!

Achtung vor PayPal-Betrug: Verbraucherzentrale warnt vor gefälschten Rechnungen und Phishing-Mails. Schützen Sie Ihre Daten!



**Luxembourg, Luxembourg** - Aktuell gibt es einen alarmierenden Betrugsversuch, der sich gegen PayPal-Nutzer richtet. Ermittlungen der Verbraucherzentrale zeigen, dass Betrüger versuchen, mit gefälschten Rechnungen Nutzer zu täuschen. Eine besonders auffällige E-Mail fordert die Empfänger auf, eine angebliche Airbnb-Buchung über 1481,04 Euro zu stornieren. Die Verbraucherzentrale warnt eindringlich vor dieser betrügerischen Masche und gibt wichtige Hinweise zur Identifikation der Phishing-Mail. Insbesondere sollten Nutzer darauf achten, dass die Absenderadresse nicht von PayPal stammt und die E-Mail häufig fehlerhafte Groß- und Kleinschreibung aufweist.

In der fraglichen E-Mail wird ein Button mit der Aufschrift „Transaktion Stornieren“ eingefügt, der Nutzer dazu verleiten soll, darauf zu klicken. Ein Klick auf diesen Button führt zur gefälschten Webseite, auf der die Nutzer dazu aufgefordert werden, ihre PayPal-Login-Daten einzugeben. Ziel der Betrüger ist es, an persönliche Kontodaten zu gelangen. Die Verbraucherzentrale rät dringend davon ab, auf links in der E-Mail zu klicken oder persönliche Informationen preiszugeben.

## **Wichtige Merkmale von Phishing-Mails**

Wie die Verbraucherzentrale weiter berichtet, gibt es einige Kennzeichen, an denen Phishing-Mails erkannt werden können:

- Unseriöse Absenderadresse, die nicht von PayPal stammt.
- Fehlerhafte Groß- und Kleinschreibung.
- Verdächtige Links oder irrelevante Informationen über Transaktionen.

Solche E-Mails verlangen oft nicht direkt eine Aktion, sondern ermutigen die Empfänger, eigenständig zu handeln. In diesem Fall sollten Nutzer immer in ihrem PayPal-Konto nachsehen, ob es tatsächlich eine Abbuchung gab. Die Verbraucherzentrale gibt den wichtigen Tipp, bei Zweifeln nicht auf Links zu klicken. Stattdessen sollten E-Mails, die verdächtig erscheinen, in den Spam-Ordner verschoben werden.

## **Präventive Maßnahmen und Vorgehen bei Verdacht**

Um präventiv gegen Phishing vorzugehen, empfiehlt die Verbraucherzentrale folgende Schritte:

- Keine persönlichen Daten eingeben.
- Die Mail unbeantwortet in den Spam-Ordner verschieben.

- Bei Verdacht auf Datenmissbrauch das PayPal-Passwort umgehend ändern und den Support kontaktieren.

Ein Anstieg solcher Phishing-Versuche hat in letzter Zeit beobachtet werden können. Betrüger verwenden automatisierte Systeme, um zufällige E-Mail-Adressen zu generieren und innerhalb kurzer Zeit eine große Anzahl von Spam-Mails zu versenden. Das Phänomen tritt häufig in Schüben auf, gefolgt von Ruhephasen. Die Verbraucherzentrale betont, dass jeder Verbraucher misstrauisch sein sollte, insbesondere gegenüber unbekanntem Absendern und unerwarteten Rechnungen.

Wie Experten berichten, sind gefälschte E-Mails aber nicht die einzige Methode, um an persönliche Daten zu gelangen. Phishing kann auch über SMS, QR-Codes und sogar Telefonanrufe erfolgen. Daher sollten Verbraucher stets wachsam sein und keine sensiblen Informationen leichtfertig preisgeben, egal in welcher Form die Anfrage kommt. Wer Opfer eines Phishing-Versuchs wird, sollte umgehend seine Bank informieren und seine Konten sperren.

Für weiterführende Informationen über die Erkennung von Phishing-Mails und wie man sich schützen kann, verweist die Verbraucherzentrale auf ihre Website, wo umfassende Ratschläge zu finden sind. Es ist unerlässlich, in der heutigen digitalen Welt die eigenen Daten zu schützen und betroffene Nachrichten unverzüglich zu melden, um weitere Schäden zu vermeiden.

Details	
<b>Vorfall</b>	Betrug
<b>Ursache</b>	Phishing
<b>Ort</b>	Luxembourg, Luxemburg
<b>Schaden in €</b>	1481
<b>Quellen</b>	<ul style="list-style-type: none"> <li>• <a href="http://www.ruhr24.de">www.ruhr24.de</a></li> <li>• <a href="http://www.focus.de">www.focus.de</a></li> <li>• <a href="http://www.ndr.de">www.ndr.de</a></li> </ul>

**Besuchen Sie uns auf: [n-ag.de](http://n-ag.de)**