NACHRICHTEN AG

27. Mai 2025

Achtung! Betrugswarnung für Klarna-Kunden: So schützen Sie Ihr Konto!

Verbraucherzentrale warnt vor neuen Phishing-Mails an Klarna-Kunden, die zur Herausgabe sensibler Daten auffordern.

Deutschland - In jüngster Zeit warnt die **Verbraucherzentrale** Klarna-Kunden vor gefährlichen Phishing-Mails. Diese betrügerischen Nachrichten zielen darauf ab, sensible Daten von Nutzern zu stehlen. Besonders auffällig ist der Betreff „Dringender Hinweis: Ihr Eingreifen ist gefragt!“, der hohe Alarmbereitschaft suggeriert. Empfänger werden aufgefordert, ihr Konto über einen bereitgestellten Link zu „bestätigen“.

Ein weiteres Indiz für den Betrug sind die fehlende persönliche Anrede und der Mangel an konkretisierten Dringlichkeiten. Darüber hinaus häufen sich Berichte über fragwürdige Absenderadressen. Das Risiko ist erheblich: Kriminelle erhalten möglicherweise Zugriff auf Klarna-Konten, was zu Konto-

Leerungen und Identitätsdiebstahl führen kann.

Warnung vor gefälschten Lastschriftmandats-Mails

Zusätzlich warnt **Computer Bild** vor einer anderen Betrugsmasche im Zusammenhang mit Klarna. Hierbei versenden Kriminelle gefälschte E-Mails mit dem Betreff „Lastschriftmandat erneuern“. Diese Mails erzeugen einen hohen Handlungsdruck und behaupten, dass das Lastschriftmandat abgelaufen sei.

Um die Dringlichkeit zu untermauern, warnen die Betrüger vor möglichen Gebühren für Rücklastschriften. Die E-Mails enthalten oft einen auffälligen pinkfarbenen Button mit der Aufschrift „Erneuern“, der einen zeitlich begrenzten Link zu beinhalten scheint. Anfangs seriös wirkende Nachrichten nutzen das Klarna-Logo sowie persönliche Anreden, um den Empfänger in Sicherheit zu wiegen.

Präventionsmaßnahmen und Verhaltenshinweise

Die **Bundesstelle für Sicherheit in der Informationstechnik (BSI)** gibt umfassende Empfehlungen zur Vermeidung von Phishing-Angriffen. Dazu gehört, dass kein seriöser Anbieter wie Klarna vertrauliche Zugangsdaten per E-Mail anfordert. Empfänger sollten immer die Adressleiste im Browser überprüfen und verdächtige Links meiden.

Einige der wichtigsten Ratschläge zur Sicherheit sind:

- Keine persönlichen Daten wie Passwörter oder Kreditkarteninformationen in E-Mails eingeben.
- Links nur über die offizielle Website des Anbieters aufrufen.
- Bei Unsicherheiten lieber telefonisch beim Anbieter

nachfragen.
- Regelmäßig Kontostände und Umsätze überprüfen.
- Geräte und Software aktuell halten, einschließlich sicherer Antivirus-Software.

Diese fortwährenden Cyber-Bedrohungen machen es unerlässlich, dass Nutzer stets wachsam bleiben und entsprechende Vorsichtsmaßnahmen ergreifen, um sich vor Betrug zu schützen. Die Verbraucherzentrale empfiehlt außerdem, verdächtige Mails in den Spam-Ordner zu verschieben und bei Verdacht auf Betrug die Polizei zu kontaktieren.

Details	
Vorfall	Betrug
Ursache	Phishing
Ort	Deutschland
Quellen	• **www.op-online.de** • **www.computerbild.de** • **www.bsi.bund.de**