DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Anleitung Amazon Betrugs-Maschen in 07-2023

amazon.de

Betrüger:innen sind kreativ und entwickeln ständig neue Methoden, nutzen neue Technologien und ändern ihre Taktiken, um nicht entdeckt zu werden. Gehe auf Nummer sicher, indem du dich mit ihren aktuellsten Betrugsmaschen vertraut machst.

Betrug mit Bestellbestätigungen:

Dabei handelt es sich um unerwartete Anrufe/Textnachrichten/E-Mails, **die häufig auf einen nicht autorisierten** Kauf hinweisen und dich bitten, **dringend zu handeln**, **um den Kauf zu bestätigen oder zu stornieren**. Diese Betrüger versuchen, dich davon zu überzeugen, **Zahlungs- oder Bankkontoinformationen preiszugeben**, Software auf deinem Computer/Gerät zu installieren oder Geschenkkarten zu kaufen.

Amazon sendet dir keine Korrespondenz zu einer Bestellung, die du nicht erwartest. Bei Fragen zu einer Bestellung, überprüfe *Meine Bestellungen* immer auf *Amazon.de oder über die App „Amazon Shopping“. I*n deiner Bestellhistorie werden

nur ordnungsgemäße Einkäufe angezeigt. Der Kundenservice steht dir rund um die Uhr zur Verfügung, um dir zu helfen.

Betrug mit Zahlungsinformationen :

Betrüger:innen senden dir eine unerwartete **Aufforderung zur Aktualisierung deiner Zahlungsinformationen** oder zur Zahlung einer ausstehenden Rechnung für ein Produkt oder eine Dienstleistung, **die du nicht bestellt hast**. Sie drohen damit, den fälligen Betrag einzutreiben, wenn du deine Zahlungs- oder Kontoinformationen nicht zur Verfügung stellst.

Amazon wird dich niemals bitten, Zahlungsinformationen, einschließlich *Geschenkkarten (oder „Bestätigungskarten“, wie sie von einigen Betrüger:innen* genannt werden), für Produkte oder Dienstleistungen telefonisch anzugeben oder per E-Mail.

Hier sind einige wichtige Tipps, um Betrug zu erkennen und dein Konto und deine Daten zu schützen :

1. Vertraue den Kommunikationskanälen von Amazon.

Gehe immer über die mobile Amazon-App oder die Website, wenn du den Kundenservice oder technischen Support erreichen oder Änderungen an deinem Konto vornehmen möchtest.

2. Sei misstrauisch bei falscher Dringlichkeit.

Betrüger:innen versuchen möglicherweise, ein Gefühl der Dringlichkeit zu erzeugen, um dich zu überreden, das zu tun, was sie verlangen. Sei vorsichtig, wenn jemand dich dazu drängt, sofort zu handeln.

3. Bezahle niemals telefonisch.

Amazon wird dich niemals dazu auffordern, telefonisch Zahlungsinformationen, einschließlich Geschenkkarten (oder „Bestätigungskarten“, wie sie von einigen Betrüger:innen genannt werden) für Produkte oder Dienstleistungen anzugeben.

4. Überprüfe zuerst den Link.

Legitime Amazon Websitelinks enthalten „amazon.de“. Gehe direkt auf unsere Website, wenn du Hilfe zu Amazon-Geräten/-Diensten oder Bestellungen benötigst oder du Änderungen an deinem Kundenkonto vornehmen möchtest.

Weitere Informationen zur Online-Sicherheit findest du unter Sicherheit und Datenschutz auf der Amazon-Kundenservice-Seite.

DIETMAR **W**ALKER - **P**C-**B**LITZHELFER-**N**OTDIENST
Nationalgasse 14 • **7**2124 **P**liezhausen • ∅ **T**el. 07127 / 890 729 - **F**ax 89118
Internet: http://www.pc-blitzhelfer.de – **M**obil 0172-882 79 55

Wenn du eine Mitteilung erhältst — per Anruf, Textnachricht oder E-Mail —, von der du glaubst, dass sie möglicherweise nicht von Amazon stammt, dann melde uns die verdächtige Kommunikation bitte hier.

Melde es uns

Um E-Mails von Amazon zu überprüfen, besuche das Message Center auf unserer Website.