NACHRICHTEN AG

19. März 2025

Achtung, Amazon-Kunden! Betrugsmasche mit Phishing-Mails entdeckt!

Die Verbraucherzentrale warnt Amazon-Kunden vor aktuellen Phishing-Versuchen, die sensible Kontodaten abgreifen wollen.

Deutschland - Die Verbraucherzentrale warnt erneut Amazon-Kunden vor einem neuen Betrugsversuch, der gezielt auf sensible Kontodaten abzielt. Kriminelle versenden E-Mails, die behaupten, das Konto sei aufgrund ȣungewöhnlicher Aktivitätenȣ gesperrt worden. Diese Phishing-Versuche sind eine ernsthafte Bedrohung, da sie die Empfänger dazu auffordern, innerhalb von 48 Stunden ihre Zahlungsdaten zu aktualisieren. Wie Ruhr24 berichtet, sind Informationen wie der angebliche ȣletzte Loginversuchȣ und persönliche Anreden mit Vor- und Nachnamen dazu bestimmt, den Eindruck von Glaubwürdigkeit zu erwecken.

Die E-Mails enthalten oft Links, die die Empfänger zu gefälschten Anmeldeseiten führen. Hierbei zeigt sich, dass die Betrüger auch mittels vermeintlich harmloser Informationen, wie IP-Adressen, Ängste schüren. Die Verbraucherzentrale empfiehlt, solche Nachrichten im Spam-Ordner abzulegen. Daneben gibt es spezifische Hinweise, um Phishing-Mails zu erkennen: Echte E-Mails von Amazon sind mit einem Amazon Smile-Logo gekennzeichnet und die Absenderadresse muss ȣAmazon.deȣ enthalten. Betrügerische Mails hingegen weisen oft Rechtschreib- oder Grammatikfehler auf sowie Links, die auf fragwürdige Adressen verweisen. Jährlich entstehen durch Phishing Schäden in Millionenhöhe.

Erweiterte Betrugsmaschen

Die Warnungen beziehen sich nicht nur auf Amazon. Auch PayPal-Kunden sollten Vorsicht walten lassen. Laut einem Artikel auf t3n versuchen Betrüger, über gefälschte E-Mails Kontoinformationen zu stehlen. Diese E-Mails thematisieren häufig angebliche neue Anmeldungen von anderen Geräten und fordern ebenfalls zur Aktualisierung von Zahlungsdaten auf. Die Verbraucherzentrale empfiehlt, auch in diesen Fällen die E-Mails zu ignorieren und ins Spam-Ordner zu verschieben. Zudem sind Betrüger auch telefonisch aktiv, indem sie sich als Interpol, Europol oder Polizei ausgeben und vermeintliche Zahlungen ansprechen.

Diese Anrufe können über herkömmliche Telefonkanäle sowie über Messengerdienste erfolgen und dazu führen, dass dann Gesprächspartner zur Zahlung auf ausländische Konten oder zum Investieren in Kryptowährungen gedrängt werden. Die Verbraucherzentrale rät dazu, bei solchen Anrufen einfach aufzulegen und keine weiteren Informationen preiszugeben. Bei Verdacht auf Betrug sollte der Kundenservice über die offizielle App oder Webseite kontaktiert werden.

Aktuelle Kontext-Warnung

Phishing ist eine der größten Bedrohungen im Internet und zielt nicht nur auf große Unternehmen ab. Wie die Verbraucherzentrale in einem umfassenden Beitrag erklärt, nutzen Kriminelle häufig aktuelle Themen wie Inflation oder nationale Sicherheitsbedenken, um Verdacht zu erregen und Menschen zu manipulieren. Betrügliche E-Mails werden oft unter dem Vorwand verschiedener Behörden oder Institutionen versendet, um Daten zu stehlen. Einige bekannte Maschen beinhalten das Versenden von Bußgeldbescheiden oder Steuererstattungen, die in Wirklichkeit nicht existieren.

Betrügerische Kommunikation kann in Form von E-Mails, SMS oder gefälschten Internetseiten erfolgen. Die Verbraucher

werden ermutigt, verdächtige E-Mails an phishing@verbraucherzentrale.nrw weiterzuleiten, um das Bewusstsein für diese Bedrohungen zu schärfen und zu helfen, andere zu schützen. Für Verbraucher, die sich über Betrügsversuche informieren möchten, lohnt ein Blick auf die Verbraucherzentrale, die umfassende Informationen zu verschiedenen Betrugsmaschen anbietet.

Details	
Vorfall	Betrug
Ursache	Phishing
Ort	Deutschland
Quellen	• www.ruhr24.de • t3n.de • www.verbraucherzentrale.de