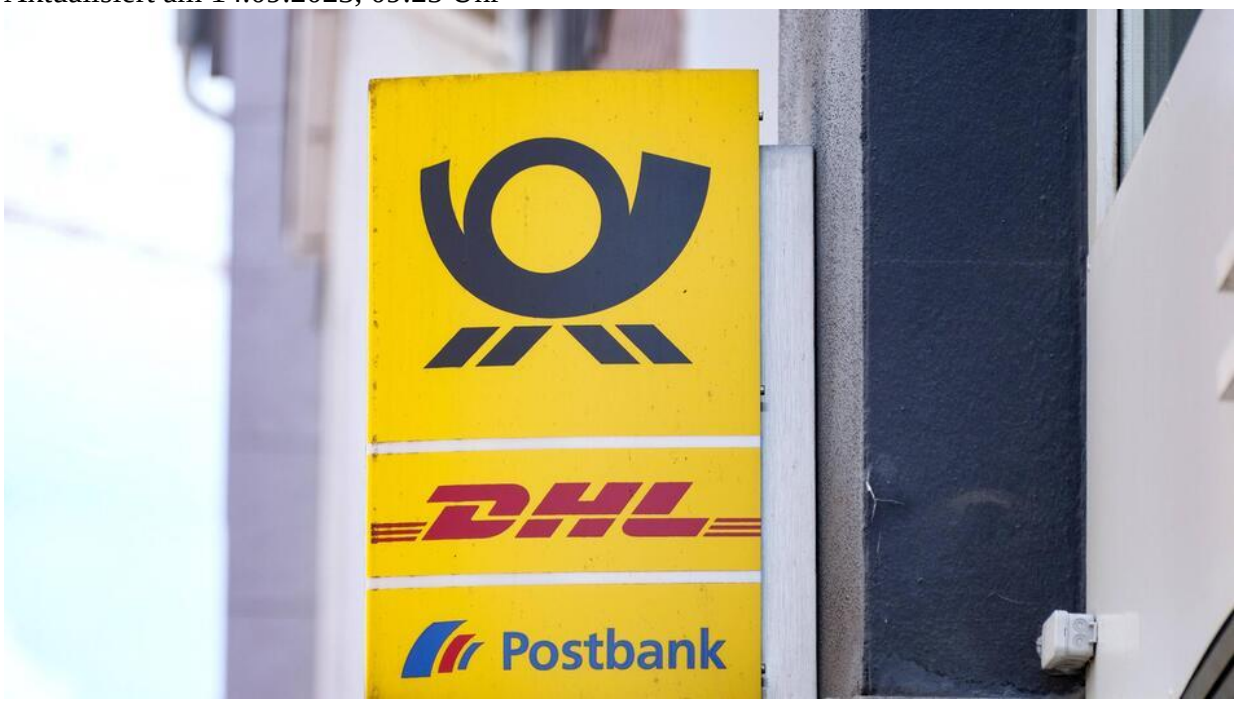
DIETMAR WALKER - PC-BLITZHELFER-NOTDIENST
Nationalgasse 14 • 72124 Pliezhausen • ∅ Tel. 07127 / 890 729 - Fax 89118
Internet: http://www.pc-blitzhelfer.de – Mobil 0172-882 79 55

Anleitung Aktuelle Betrugsmaschen

Aktuelle Betrugsmaschen: Angeblicher Kundendienst der Deutschen Post fordert Zollgebühr

Aktualisiert am 14.09.2023, 09:25 Uhr



Kunden der Deutschen Post erhalten derzeit wieder vermehrt Phishing-Mails.

Sie gehen mit großer Raffinesse vor: Betrüger, die ihre Opfer am Telefon, im Netz oder an der Haustür um ihr Geld bringen. Um gewarnt zu sein, sollte jeder von den folgenden aktuellen Betrugsmaschen gehört haben.

Mehr zum Thema Verbraucher

+++ Dieser Artikel wird regelmäßig aktualisiert +++

Angeblicher Kundendienst der Deutschen Post fordert Zollgebühr

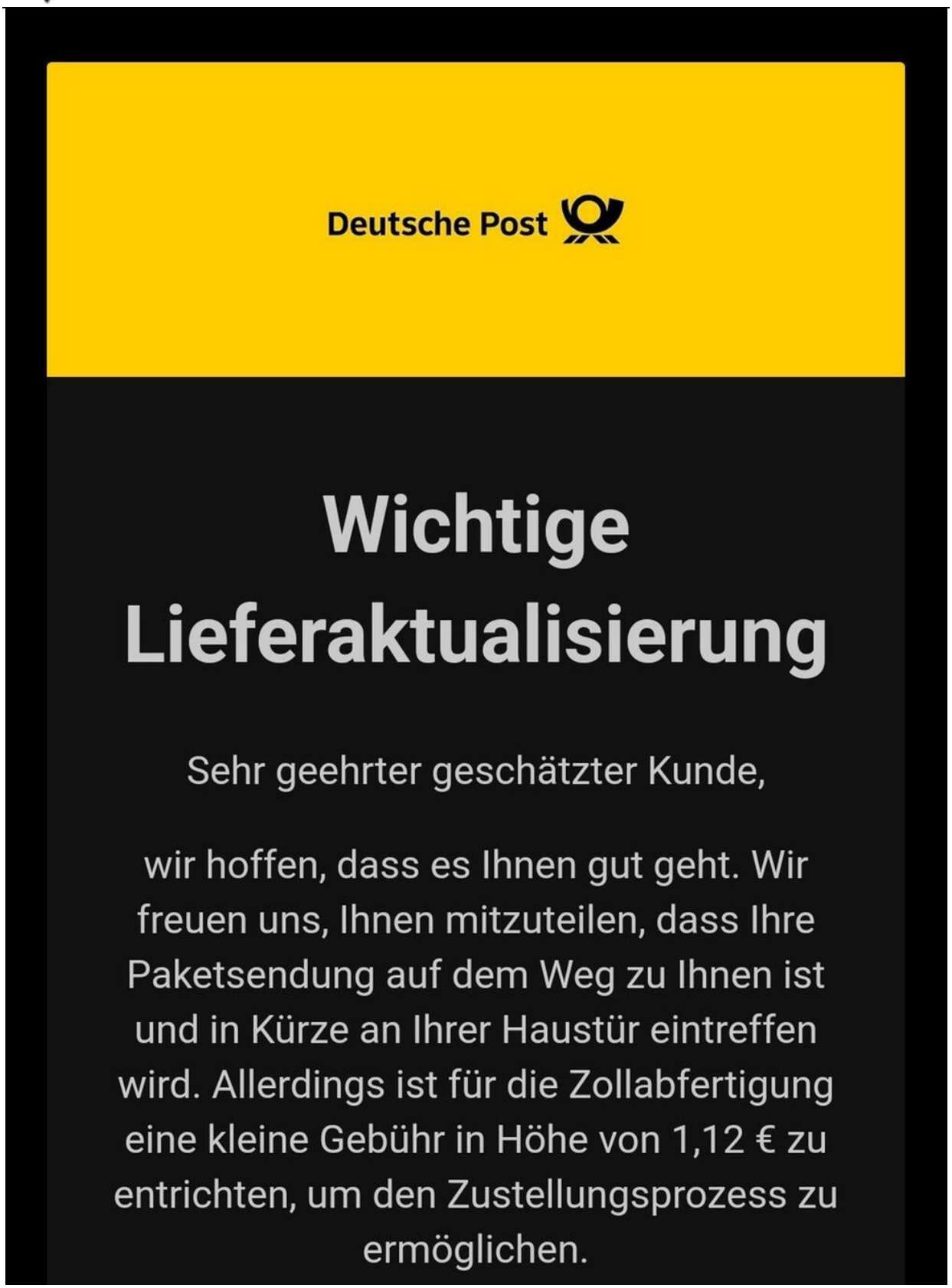
Update vom 14. September: Eine betrügerische E-Mail versucht derzeit Kundinnen und Kunden der Deutschen Post zu verunsichern.

Der Absender nennt sich "Kundendienst" und behauptet, dass eine Zollgebühr für die Versendung des Pakets nötig wäre. Durch das Einfügen des Logos der Deutschen Post wirkt die Mail auf den ersten Blick vertrauenerweckend. Die unpersönliche Ansprache sowie die unten angegebene australische Adresse lassen jedoch schnell auf einen Betrug schließen.

Außerdem typisch für eine Phishing-Mail: Die Betrüger bauen Druck auf, in welchem Zeitraum die Zahlung über einen Link getätigt werden muss.

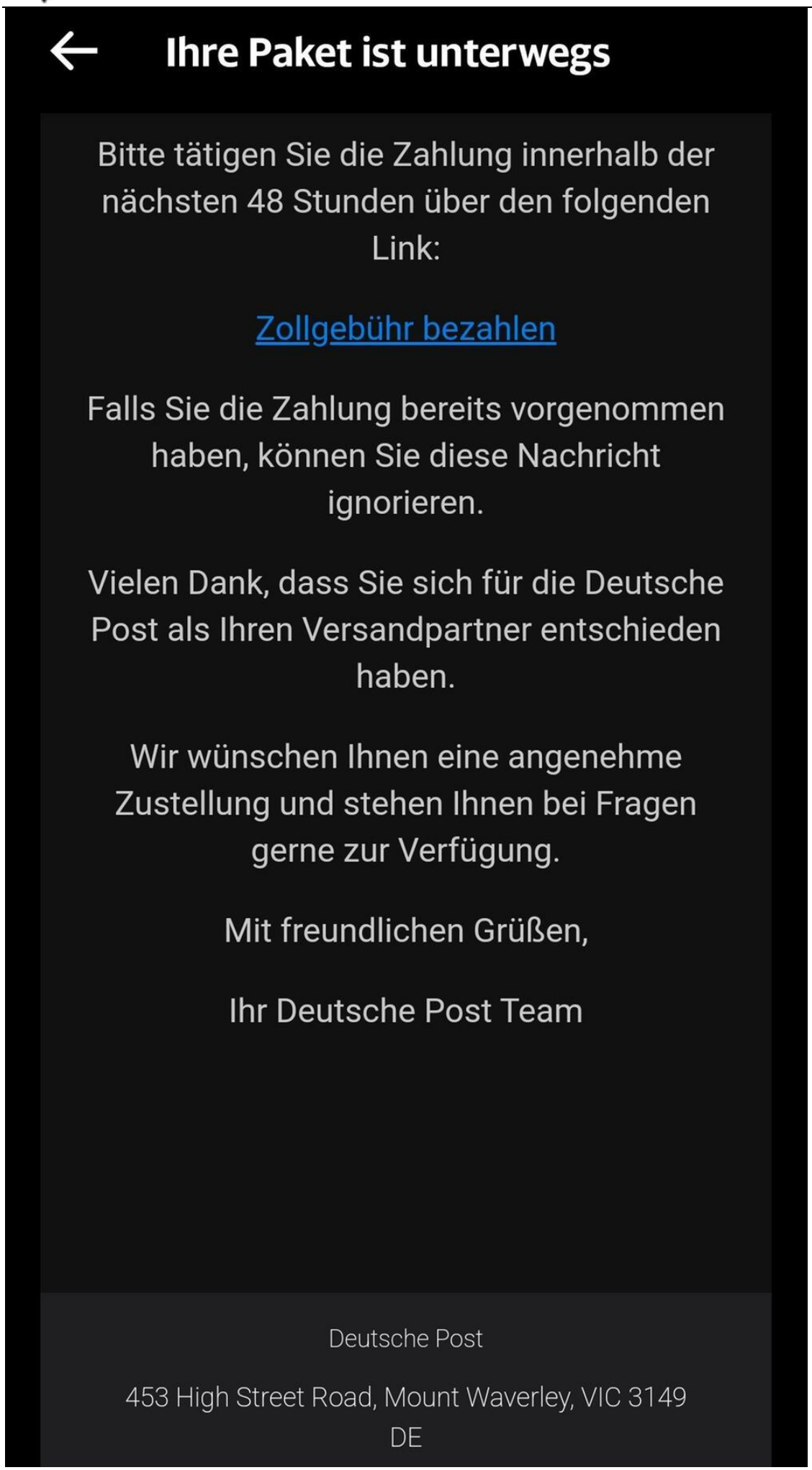
Wir empfehlen Ihnen auf keinen Fall auf den Link zu klicken und die E-Mail unbeantwortet in den Spam-Ordner zu verschieben.

Hier sehen Sie Screenshots der Phishing-Mail.



© privater Screenshot

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



© privater Screenshot

(mak)

+++

Amazon-Prime-Kunden sollen Zahlungsdaten eingeben - Vorsicht!

Update vom 10. September: Wieder gibt es eine aktuelle Warnung der Verbraucherzentrale an Amazon-Nutzer. Derzeit kursiert eine Phishing-Mail, die sich an Prime-Kunden richtet.

Der Betreff lautet "Aktuelle Info: Aktivitätszugriffsinformationen – \"Um unbefugte Bestellungen zu verhindern, wurde Ihr Konto für mehrere Aktivitäten gesperrt". Der Inhalt der Mail passt dazu nicht ganz, denn darin geht es dann nicht um Fremdzugriff, sondern um die Aktualisierung der Zahlungsinformationen: Ein zu zahlender Betrag sowie anfallende Steuern seien fällig, heißt es, weshalb "Mitgliedschaftsvorteile" zurückgestellt worden seien. User werden aufgefordert, ihre Daten innerhalb von sechs Tagen über einen Link einzugeben. Hier sollten alle Alarmglocken schrillen. Solche E-Mails gilt es immer sofort in den Spam-Ordner zu verschieben.

+++

Millionärsfamilie Geiss warnt vor Betrug auf Instagram

Update vom 6. September 2023: Es klingt zu gut, um wahr zu sein - und das ist es wie so oft leider auch. Wenn Sie Prominenten auf Instagram folgen, hat Sie vielleicht schon einmal eine der Nachrichten erreicht, vor denen aktuell die Millionärsfamilie des Unternehmers Robert Geiss warnt (bekannt aus der TV-Serie "Die Geissens – Eine schrecklich glamouröse Familie").

Empfohlener externer Inhalt

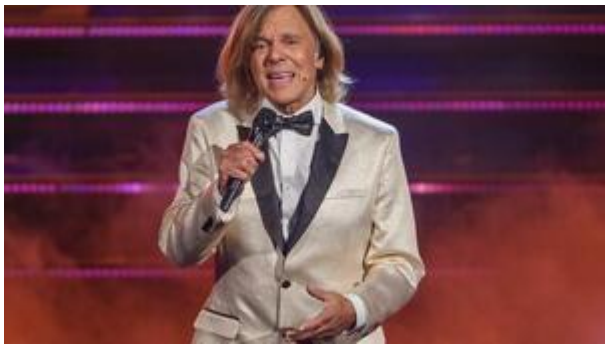
Mit einem Klick können Sie die Instagram-Beiträge anzeigen lassen oder wieder ausblenden.
Externe Inhalte anzeigen

Ich bin damit einverstanden, dass mir externe Inhalte angezeigt werden. Damit können personenbezogene Daten an Drittplattformen übermittelt werden. Mehr dazu in unserer Datenschutzerklärung und Zustimmungen zu externen Inhalten.

Bei der Masche gibt sich jemand als Mitarbeiter eines Promis aus und gaukelt dem Follower vor, der Prominente wolle nun Kontakt mit seinem Fan aufnehmen. Am Beispiel der Geiss-Tochter Davina heißt es in der Nachricht: "Sie wurden aufgrund Ihrer Likes und Kommentare auf den verifizierten Seiten von @davinageiss ausgewählt. (...) Sie möchte gerne mit Ihnen als Fan sprechen." Laut Robert Geiss gibt es "zurzeit mehrere Accounts, die behaupten, in unserem Namen mit Fans und Followern Kontakt aufzunehmen.“

Die Polizei rät, solche Nachrichten zu ignorieren, das Profil zu melden und den Absender zu blockieren. "Das Ziel ist immer dasselbe", warnt die Polizeiliche Kriminalprävention der

Länder und des Bundes auf Anfrage unserer Redaktion, "die Betrüger wollen auf unterschiedlichste Art und Weise an Kontodaten oder Geld gelangen und hoffen, dass die potenziellen Betroffenen auf die prominenten Namen hereinfallen und reagieren". (af)



Schlager

"Achtung! Betrug!": Jürgen Drews warnt Fans vor Fake-Profil

26. August 2022

+++

Netflix-Abonnement läuft bald ab - angeblich

Update vom 5. September: Aktuell meldet die Verbraucherzentrale, dass wieder eine Fake-Nachricht im Umlauf ist, die angeblich von Netflix stammt. Es handele sich um einen eindeutigen Betrugsversuch, was sich schon an der Absender-Adresse erkennen ließe, die nicht dem echten Streaming-Anbieter zuzuordnen ist. In der Mail heißt es dann: "Dein Netflix-Abonnement läuft bald ab" - mit Angabe eines konkreten Datums samt Uhrzeit.

Typisch an dem Phishing-Versuch ist laut den Verbraucherschützern auch, dass die Adressaten zu unüberlegtem Handeln gedrängt werden mit Sätzen wie "Verpasse nicht deine Lieblingsserien und Filme!". Der User soll auf einen Link klicken, um sein Abo zu erneuern. Wer dort allerdings seine Daten eingibt, überlässt sie den Betrügern. Wer also eine solche Mail erhält, verschiebt sie am besten sofort unbeantwortet in den Spam-Ordner. (af)

Vorsicht, Betrug

Betrugsversuche im Juli 2023: Warnung vor "Quishing" per E-Mail

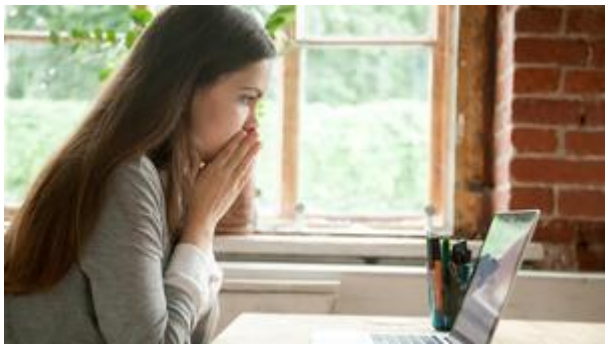
vor 8 Tagen

+++

Commerzbank im Fokus: Phishing-Mails kündigen "unterhaltsamen" Vorgang an

Update vom 31. August: Derzeit steht die Commerzbank wieder im Fokus von Kriminellen, das teilt die Verbraucherzentrale mit. Kundinnen und Kunden erhalten vermehrt E-Mails mit den Worten "dringende Aufgabe" im Betreff. Demnach soll es ein Photo-TAN-Update geben. Um dieses Update durchführen zu können, müssen Betroffene auf einen Link in der Mail klicken. Ziel ist es, an Ihre sensiblen Daten zu kommen.

Der Phishing-Versuch ist nicht gerade ausgefeilt und schnell erkennbar: Nicht nur die indirekte Anrede und die kontextlosen Sätze sind ein Indiz für den Betrug. Die Commerzbank würde Sie auch nie per Mail zur Preisgabe Ihrer sensibelsten Daten, wie Ihrem Aktivierungsbrief, auffordern. Außerdem schreiben die Kriminellen, der Vorgang sei "kurz und unterhaltsam". So würde sich die Bank in einer offiziellen Nachricht nicht ausdrücken. (ff)



Betrugsmaschen

Mit diesen Betrugsmaschen versuchen es Kriminelle immer wieder

04. Juli 2023 von Antonia Fuchs

+++

Echt wirkende E-Mail verunsichert Kunden der Deutschen Bank

Update vom 28. August: Kundinnen und Kunden sollten sich von einer aktuell kursierenden Phishing-Mail nicht aus der Ruhe bringen lassen – auch, wenn sie auf den ersten Blick echt wirkt. Im Betreff heißt es "Ihr photoTAN-Aktivierungsbrief ist ungültig!", was auch mit dem Inhalt der E-Mail übereinstimmt. Die Verbraucherzentrale erklärt, dass die Mail schon deshalb zu einer der besseren Fälschungen gehört. Auch die Aufmachung der gesamten Mail wirkt seriös, vom Logo der Deutschen Bank bis hin zu den entsprechenden Firmenfarben auf dem

Link-Button. Wie so oft bei Phishing-Versuchen im Namen einer Bank, geht es auch hier um die Sicherheit der Kundschaft.

Die Betrüger behaupten, dass ein sogenannter "photoTAN-Aktivierungsbrief" nur 120 Tage gültig sei und nun erneuert werden müsse. Die Mail wirkt umso seriöser, da sie eine europäische Richtlinie zitiert, die ein gültiges TAN-Verfahren als notwendig bezeichnet. Es wird behauptet, dass ein Aktivierungscode für die Aktivierung des photoTAN-Verfahrens erforderlich sei. Diesen erhalten die Kundinnen und Kunden, die Online-Banking nutzen, angeblich über den beigefügten Link. Die Verbraucherzentrale warnt vor einem Klick auf den Link, da die Absenderadresse sowie die unpersönliche Anrede stark auf einen Phishing-Versuch hindeuten. (mak)

+++

Sparkasse: Diese Phishing-Mail sieht täuschend echt aus

Update vom 25. August: Bei dieser Mail der Sparkasse müssen Kundinnen und Kunden zweimal hinschauen, denn sie sieht täuschend echt aus. Es handelt sich aber um einen Phishing-Versuch. Wie immer gilt daher: Löschen Sie die Mail oder verschieben Sie sie in den Spam-Ordner.

Empfohlener externer Inhalt

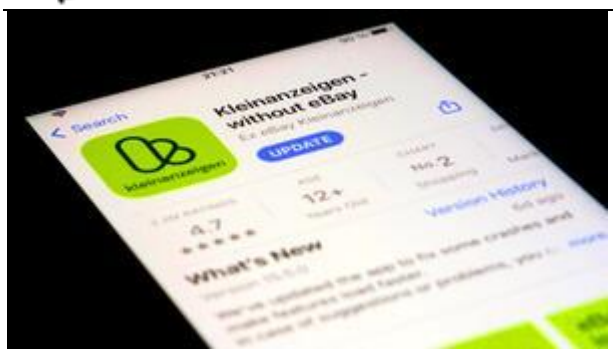
Mit einem Klick können Sie die Twitter-Beiträge anzeigen lassen oder wieder ausblenden. Externe Inhalte anzeigen

Ich bin damit einverstanden, dass mir externe Inhalte angezeigt werden. Damit können personenbezogene Daten an Drittplattformen übermittelt werden. Mehr dazu in unserer Datenschutzerklärung und Zustimmungen zu externen Inhalten.

Die Anrede gibt bereits den ersten Hinweis. Sie beginnt mit Frau/Herr und dahinter steht der Nachname des Betroffenen, wie die Verbraucherzentrale mitteilt. In der E-Mail geht es darum, dass angeblich eine Geräteerkennung eingeführt worden ist und man sich nur noch mit dem hinterlegten Gerät anmelden könne.

Der Prozess, der schnell durchführbar sein soll, müsse allerdings bis zum 25. August bestätigt werden, da sonst einige Kontofunktionen nicht mehr genutzt werden könnten. Zu diesem Zweck solle man auf einen Link innerhalb der Mail klicken und auf der sich öffnenden Seite persönliche Daten eingeben. Dabei ist das Layout der Seite sehr professionell und auch den Prozess der Geräteerkennung gibt es grundsätzlich.

Aber: Die Sparkasse würde Sie niemals per Mail dazu auffordern, Ihre Daten preiszugeben. Werfen Sie einen Blick auf den Absender der Mail, wird schnell klar, dass es sich um einen Fake handelt. Sind Sie sich unsicher, können Sie aber auch immer bei Ihrer Bank nachfragen. (ff)



Kleinanzeigen

Plötzlich muss Verkäufer bezahlen: Betrugsmasche kann Tausende Euros kosten

vor 22 Tagen 38 Kommentare

+++

Mail spricht von "Abrechnungsproblemen" bei Disney+

Update vom 24. August: Die Verbraucherzentrale warnt aktuell Kundinnen und Kunden des Streaming-Anbieters Disney+ vor einer Phishing-Mail. Diese E-Mail deutet schon von Beginn an auf einen Betrug hin, da sie keine Anrede enthält und direkt auf ein vermeintliches Abrechnungsproblem hinweist. Besagte Abrechnungsprobleme werden jedoch nicht weiter erläutert.

Stattdessen gibt es einen Link-Button, über den Nutzerinnen und Nutzer ihre Daten aktualisieren sollen - angeblich aus Sicherheitsgründen. Weiter wird gedroht, dass der Streaming-Dienst ohne eine Aktualisierung nicht weiter genutzt werden könne. Sollten Sie eine solche Mail erhalten, schieben Sie sie am besten unbeantwortet in den Spam-Ordner - und klicken Sie erst recht nicht auf den Link-Button. (mak)

+++

Ungewöhnliche Phishing-Attacke auf Kunden der Commerzbank

Update vom 21. August: Die Verbraucherzentrale (VZ) berichtet aktuell von einer "ungewöhnlichen Betrugsmasche" im Namen der Commerzbank. In der Mail mit "unüblichem Vorwand" würden die Empfängerinnen und Empfänger nämlich nicht direkt aufgefordert, ihre Daten einzugeben oder zu bestätigen. Stattdessen winkt eine vermeintliche Rückerstattung wegen einer Doppelbelastung der Kreditkarte.

Die Rückerstattung bekomme man über ein Erstattungsformular, das in der Mail verlinkt ist. Dabei handelt es sich dann aber um den Phishing-Versuch, den Link sollte man daher auf

keinen Fall anklicken. Die Betrugsabsicht, die Daten der Nutzerinnen und Nutzer abzugreifen, wird nach Einschätzung der VZ durch dieses Ablenkungsmanöver verschleiert.

Empfohlener externer Inhalt

Mit einem Klick können Sie die Twitter-Beiträge anzeigen lassen oder wieder ausblenden.
Externe Inhalte anzeigen

Ich bin damit einverstanden, dass mir externe Inhalte angezeigt werden. Damit können personenbezogene Daten an Drittplattformen übermittelt werden. Mehr dazu in unserer Datenschutzerklärung und Zustimmungen zu externen Inhalten.

Zu erkennen sei der Betrugsversuch auch durch die "unseriöse Absenderadresse". Um diese zu sehen, könne man mit dem Mauszeiger über den Link gehen, ohne diesen aber zu klicken (sogenanntes Mouse-over). Der Rat der VZ lautet in jedem Fall, die Mail unbeantwortet in den Spam-Ordner zu schieben oder direkt zu löschen. (cze)

+++

Phishing-Mails im Namen von WEB.DE

Update vom 16. August: In den Postfächern der Nutzerinnen und Nutzer von WEB.DE können derzeit E-Mails mit dem Betreff "E-Mail-Anfrage von web.de" eingehen. Die Userinnen und User werden darin darüber informiert, dass sie angeblich eine Anfrage zur Deaktivierung ihres Kontos eingereicht haben. Über einen beigefügten Link sollen sie die angebliche Anfrage stornieren.

Diese Aufforderung ist nicht echt, die Kontolöschung wurde nie beantragt. Die Mails sollten daher am besten sofort unbeantwortet in den Spam-Ordner verschoben oder gelöscht werden. Es handelt sich um Phishing, um an persönliche Daten zu gelangen, wie die Verbraucherzentrale berichtet.

Empfohlener externer Inhalt

Mit einem Klick können Sie die Twitter-Beiträge anzeigen lassen oder wieder ausblenden.
Externe Inhalte anzeigen

Ich bin damit einverstanden, dass mir externe Inhalte angezeigt werden. Damit können personenbezogene Daten an Drittplattformen übermittelt werden. Mehr dazu in unserer Datenschutzerklärung und Zustimmungen zu externen Inhalten.

WEB.DE selbst bietet zusätzlich ein Tool an, mit dem man testen kann, ob eine Mail tatsächlich von dem Mailanbieter kommt. Auch die Nutzerinnen und Nutzer von GMX haben in der Vergangenheit solche Mails erhalten - siehe Eintrag in diesem Artikel am 13. Juli. (mak)

Offenlegung: Die Redaktion gehört wie die Mail-Anbieter WEB.DE und GMX zum Unternehmen United Internet.

+++

Abzocke mit Nahrungsergänzungsmitteln

Update vom 14. August: Die Verbraucherzentrale warnt aktuell vor Abzocke mit Nahrungsergänzungsmitteln. Dabei gibt sich der Anrufer oder die Anruferin offenbar häufig als Apotheke aus und bietet Nahrungsergänzungsmittel, zum Beispiel gegen Gelenkschmerzen oder für die Gedächtnisleistung, an. Und das günstiger als zum sonstigen teuren Apothekenpreis.

Nach dem Anruf erhalten die Betroffenen dann zunächst eine kostenlose Probepackung - dabei haben die meisten einer Lieferung nicht einmal zugestimmt. Was vielen nicht klar ist: Mit der Zusendung "kommt aus Sicht des Unternehmens ein Abonnement zustande", wie es bei der Verbraucherzentrale heißt. Es folgen Rechnungen in dreistelliger Höhe und nach einigen Monaten eine weitere Lieferung.

Die Verbraucherzentrale rät, nach Erhalt des Päckchens dem angeblichen Vertragsschluss so schnell wie möglich ausdrücklich zu widersprechen. Auch wenn Sie einer Belieferung zugestimmt haben, können Sie dies innerhalb von zwei Wochen widerrufen. Auf der Seite der Verbraucherzentrale finden Sie für beide Fälle einen Musterbrief.

Bei unerwünschten Werbeanrufen gilt generell: Am besten schützen Sie sich, indem Sie sofort auflegen. (ff)

Vorsicht Telefon-Betrug: Auf dieses Wort warten die Kriminellen

Aktualisiert am 04.03.2022, 14:07 Uhr
Die Verbraucherzentrale warnt jetzt vor einer neuen Betrugsmasche, die kaum zu durchschauen ist. Die Betrüger versuchen den Betroffenen ein einfaches Wort zu entlocken.

+++

KI-Betrug mit Gesicht und Stimme von "Tagesschau"-Sprecher

Update vom 11. August: Im Internet, unter anderem bei Facebook, kursiert derzeit ein Video, in dem "Tagesschau"-Sprecher André Schünke angeblich Online-Finanzprodukte empfiehlt. Das Video ist allerdings nicht echt, offenbar handelt es sich um ein mittels Künstlicher Intelligenz (KI) erstelltes Fake-Video.

Bei diesem sogenannten Deepfake missbrauchten Betrüger das Gesicht und die Stimme des 43-Jährigen und ließen ihn so scheinbar aus dem "Tagesschau"-Studio heraus dubiose Finanztipps für eine Plattform namens "Quantum" geben.

Dabei wurde der Werbetext offenbar aus Text- und Bildschnippseln aus der "Tagesschau" zusammengesetzt. Schünke selbst weist bei Instagram darauf hin, dass es sich dabei um einen KI-Fake handelt.

Empfohlener externer Inhalt

Mit einem Klick können Sie die Instagram-Beiträge anzeigen lassen oder wieder ausblenden.
Externe Inhalte anzeigen

Ich bin damit einverstanden, dass mir externe Inhalte angezeigt werden. Damit können personenbezogene Daten an Drittplattformen übermittelt werden. Mehr dazu in unserer Datenschutzerklärung und Zustimmungen zu externen Inhalten.

Der "Bild"-Zeitung sagte Schünke, in dem aktuellen Fall sei die Fälschung wegen der "komischen Betonung" zu erkennen. "Aber wenn die KIs noch weiter lernen, erleben wir in Zukunft noch krassere Fakes. Wenn die Programme zum Beispiel lernen, die Sprache anders zu betonen, weiß ich nicht, wie man in Zukunft Original und Fälschung auseinanderhalten soll", sagte er weiter.

In dem Video taucht auch angeblich der aus den Medien bekannte Lottomillionär Chico auf, der sich dank der Finanzprodukte endlich einen Porsche leisten könne.

Was Deepfakes genau sind und wie man sie erkennen kann, erklärt unter anderem die Initiative Klicksafe für mehr Sicherheit im Internet auf ihrer Seite.

(cze)

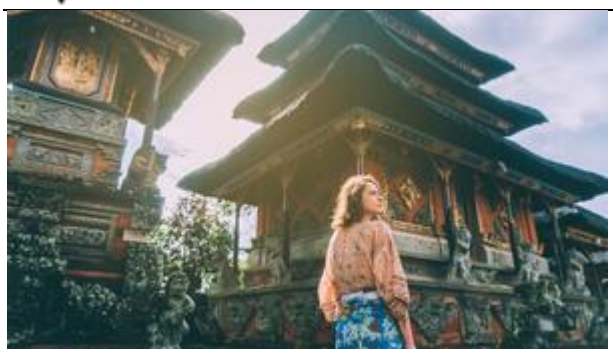
+++

Betrug im Urlaub: Banken geben simplen, aber wichtigen Tipp

Update vom 10. August: Im Urlaub können Girocard und Kreditkarte bei all den anfallenden Zahlungen schon mal glühen. Betrüger nutzen gerade bei Touristen gern die Gelegenheit und buchen zu viel ab.

Die Gemeinschaftsunternehmen der deutschen Banken und Sparkassen, Euro Kartensysteme, rät zur Vorsicht: Gewöhnen Sie sich an, die Belege sämtlicher Ausgaben und Bargeldabhebungen zu behalten. So können Sie spätestens nach ihrer Rückkehr anhand der Unterlagen prüfen, ob es unberechtigte Buchungen gab.

Wer im Urlaub Opfer einer zu hohen Buchung geworden ist, sollte laut Euro Kartensysteme umgehend die Bank oder Sparkasse informieren und die Zahlungskarten vorsorglich sperren. Das geht bei vielen Instituten zum Beispiel im Onlinebanking oder in der Filiale. Außerhalb der Öffnungszeiten ist die Sperrung der Zahlungskarten auch rund um die Uhr über den Sperr-Notruf +49 116 116 möglich.



Reisen

Kennen Sie den Tempel-Trick? Achtung vor diesen Betrugsmaschen im Urlaub

17. Mai 2023 von Malina Köhn

+++

Vermeintlicher 1&1-Kundenservice will an Zahlungsdetails herankommen

Update vom 9. August: Ein angeblicher Kundenservice des Telekommunikationsanbieters 1&1 verschickt derzeit eine E-Mail an seine Kundschaft, die auffordert, die persönlichen Zahlungsdetails zu aktualisieren. Die Phishing-Mail läuft laut der Verbraucherzentrale unter dem Betreff "Vermeiden Sie den Verlust des Zugangs zu unserem Service" in das Postfach ein.

Als Vorwand wird erklärt, dass ein "technischer Ausbruch" für eine Beeinflussung der Genauigkeit der Zahlungsdetails verantwortlich wäre. Daher sollen Kundinnen und Kunden auf einen Button klicken, der sie auf eine Webseite leitet, wo sie ihre Zahlungsdetails angeben sollen. Dabei handelt es sich jedoch um keine offizielle Webseite, wie die Verbraucherzentrale warnt. Um das Abfangen Ihrer persönlichen Daten zu verhindern, verschieben Sie die Mail am besten unbeantwortet in den Spam-Ordner.

+++

Anrufe häufen sich: Deutsche Rentenversicherung klärt über Betrugsversuche auf

Update vom 8. August: Auch im Namen der Deutschen Rentenversicherung (DRV) versuchen es Betrüger immer wieder. Über täuschend echt wirkende Anschreiben und unangekündigte Besuche an der Haustür haben wir hier bereits mehrfach berichtet. Aktuell warnt die DRV vor allem vor dubiosen Anrufen, die sich offenbar gerade häufen.

- **Die Masche:** Trickbetrüger fordern am Telefon die Angerufenen dazu auf, ihre E-Mail-Adresse mitzuteilen. Im nächsten Schritt sollen die Opfer mehrere Tausend Euro für ein angeblich abgeschlossenes Gewinnspiel an eine Anwaltskanzlei überweisen - meist handelt es sich dabei um ein Konto im Ausland. "Es wird mit Rentenkürzungen, einem

Schufa-Eintrag oder anderen Sanktionen gedroht, wenn die Überweisung nicht erfolgt", klärt die DRV in einer Pressemitteilung weiter über die Details zum Betrug auf.

Die Deutsche Rentenversicherung Bund betont, dass es sich nicht um Anrufe von ihren Mitarbeitenden oder von ihr beauftragte Personen handelt. In keinem Fall sollten Betroffene aufgrund telefonischer oder per E-Mail gesendeter Aufforderungen Geld ins In- oder gar Ausland überweisen. "Auch telefonische oder digitale Angebote, Medikamente oder medizinische Hilfsmittel zu verkaufen, stammen nicht von der Deutschen Rentenversicherung", heißt es weiter.

In der Broschüre "Vorsicht Trickbetrug" informiert die DRV Kunden und Kundinnen zu weiteren gängigen Betrugsmaschen.

+++

Dreister Betrugsversuch im Namen von Booking.com

Update vom 7. August: In der Haupturlaubszeit kursiert eine E-Mail, die angeblich von Booking.com stammt und vor der die Verbraucherzentrale warnt. Sie enthält einige typische Kennzeichen einer klassischen Phishing-Mail. Der Betreff lautet: "Erinnerung: Aktualisierung Ihrer Informationen erforderlich." Die Kunden werden aufgefordert, ihre Daten über einen Link einzugeben und werden dabei massiv unter Zeitdruck gesetzt. Im konkreten Beispiel drohen die Betrüger, ohne eine Aktualisierung der Daten würde das Konto zwei Tage nach Versenden der E-Mail gelöscht. Sogar eine Gebühr (von 19,99 Euro) werde dann fällig.

Es folgt der Hinweis, dass die automatisierte Mail angeblich mit einer künstlichen Intelligenz versendet wurde, sodass eine Beantwortung nicht zweckmäßig sei. Die E-Mail endet mit dem Satz: "Sie haben diese E-Mail mit der Bitte erhalten, aktuelle Fehler in Ihrem Konto zu korrigieren."

Die Verbraucherschützer empfehlen, die E-Mail gleich in den Spam zu verschieben.

+++

Fake-E-Mail im Namen der Postbank im Umlauf

Update vom 4. August: Viele Kundinnen und Kunden der Postbank erhalten derzeit eine angeblich "automatisierte E-Mail", wie die Verbraucherzentrale informiert. In dieser steht, dass ihr Konto aus Sicherheitsgründen gesperrt worden wäre.

Um das Konto wieder freischalten zu können, müsse man seine Bankdaten überprüfen. Die Betrüger üben zusätzlichen Druck aus und behaupten, der Freischaltungsprozess sei "einfach" und in fünf bis zehn Minuten durchgeführt. Im Anschluss hätte die Kundin oder der Kunde wieder vollen Zugriff auf das eigene Konto.

Die Phishing-Mail, die im Namen der Postbank versendet wird, enthält zudem einen Link, über den die Dateneingabe erfolgen soll. Besagte E-Mail kann als Phishing identifiziert werden, da

in einem Absatz über einen untenstehenden Button gesprochen wird, sich dieser jedoch oberhalb dieses Absatzes befindet.

Besonders fies: Die Betrüger fügen der Mail hinzu, dass sich die Kundschaft bei "Fragen und Bedenken" jederzeit an den Kundenservice wenden könne. Tatsächlich können Sie sich bei Fragen und Bedenken an den echten Kundenservice der Postbank wenden, um die Echtheit einer solchen Mail zu überprüfen. Die Verbraucherzentrale empfiehlt, die Phishing-Mail unbeantwortet in den Spam-Ordner zu verschieben.

+++

Phishing im Namen der DKB

Update vom 3. August: Die Verbraucherzentrale warnt aktuell Kundinnen und Kunden der Deutschen Kreditbank (DKB) vor Phishing-Mails. In dieser Mail werden die DKB-Kunden dazu aufgefordert, ihre Handynummer aus Sicherheitsgründen über einen Link zu verifizieren.

Als Grund wird eine "steigende Zahl von Angriffen, die auf Sicherheitslücken bei bestimmten Mobilfunkanbietern" abzielen, genannt. Auf den ersten Blick erscheint die E-Mail, welche im Namen der DKB geschickt wird, aufgrund des authentisch wirkenden Layouts echt. Der Inhalt der E-Mail sowie die unpersönliche Anrede lassen jedoch auf eine Phishing-Mail schließen.

Die Verbraucherzentrale empfiehlt einen Blick auf die unseriöse Absender-Adresse zu werfen und die Mail unbeantwortet in den Spam-Ordner zu verschieben. Bei Unsicherheiten können Kundinnen und Kunden der Deutschen Kreditbank, die Echtheit der Mail bei der Bank verifizieren lassen.

+++

Betrüger schocken PayPal-Kunden mit E-Mail und ergaunern so ihre Daten

Update vom 2. August: Sehr viele Menschen erhalten derzeit eine gefälschte Zahlungsbestätigung von PayPal. "Die Verwunderung über die hohe Zahlungssumme kann schnell zu unüberlegten Handlungen führen", warnt die Verbraucherzentrale.

In einer aktuellen E-Mail wird beispielsweise behauptet, es sei eine Summe 853,67 Euro gesendet worden. Über einen Button "Zahlungen anzeigen oder verwalten" wird dann angeboten, die vermeintliche Zahlung zu stornieren - hierfür sollen User ihre persönlichen Anmeldedaten und Zahlungsdaten eingeben. Vorsicht: So fischen die Kriminellen hinter dieser Betrugsmasche Ihre Daten ab!

E-Mails mit diesem Betrugsversuch seien bereits mit unterschiedlichen Betreffzeilen im Umlauf, etwa "Bankdaten bestätigen" oder "Assistenz von Paypal.de – Aktualisierung für Ihr Konto erforderlich".

+++

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

Amazon warnt Kunden: Diese Betrugsmaschen sind gerade im Umlauf

Update vom 1. August: Onlineversandhändler Amazon warnt in einer aktuellen E-Mail Kundinnen und Kunden vor zwei Betrugsmaschen. Dabei versenden Kriminelle E-Mails, die angeblich von Amazon stammen. Tatsächlich versuchen die Betrüger so an Bankkontoinformationen zu gelangen.

Konkret macht Amazon jetzt auf diese Betrugsversuche aufmerksam:

- **Phishing mit Bestellbestätigung:** In der E-Mail geht es um eine Bestellung, die man selbst gar nicht aufgegeben hat. Man wird dazu aufgefordert, dringend zu reagieren, um den Kauf zu stornieren oder zu bestätigen. Den Betrügern geht es laut Amazon dabei um Zahlungs- und Bankinformationen, Softwareinstallationen zu installieren oder Gutscheine zu kaufen.
- **Betrug mit Zahlungsinformation:** Hier versuchen die Betrüger per Mail oder Telefon ebenfalls an Zahlungsinformationen zu gelangen. Der Vorwand ist eine angeblich offene Rechnung eines Produkts, das man gar nicht bestellt hatte, oder dass man seine Zahlungsangaben aktualisieren müsse.

Amazon rät Kundinnen und Kunden dazu, nie telefonisch Zahlungsangaben zu machen und nur über die App oder Website Kontoänderungen vorzunehmen und mit dem Kundendienst Kontakt aufzunehmen.

+++

Die Betrugsmaschen der vergangenen Monate:

- Juli 2023: Quishing" per E-Mail, angebliche Kontolöschung bei GMX und falsche Anrufe der Verbraucherzentrale
- Juni 2023: Nutzer von booking.com, PayPal und Netflix im Visier von Betrügern
- Mai 2023: Experten warnen Kunden von Amazon und Ebay vor Betrugsfallen

Verwendete Quellen:

- Polizeiliche Kriminalprävention der Länder und des Bundes
- Watchlist Internet
- Verbraucherzentralen
- Bundesnetzagentur
- Material der Deutschen Presse-Agentur (dpa)

Quelle: https://web.de/magazine/ratgeber/finanzen-verbraucher/betrug-angeblicher-kundendienst-deutschen-post-zollgebuehr-38599570