

Finanzen im Netz – Sicher durch den digitalen Alltag

Auszug der Präsentation

Katja Plieninger, freie Vortragsreferentin im Auftrag des DSGV e.V.

EIN ANGEBOT VON GELD UND HAUSHALT



**FINANZ
BILDUNG**
für alle.

Digitaltag 2026

Dieser Online-Vortrag findet im Rahmen des Digitaltags statt.

Der Digitaltag ist ein bundesweiter Aktionstag, der Menschen zusammenbringt, um die Digitalisierung erlebbar zu machen und die digitale Teilhabe zu fördern.

Er findet unter der Schirmherrschaft des Bundesministeriums für Digitales und Staatsmodernisierung statt.

www.digitaltag.eu

The logo for Digitaltag 2026 features the word "Digitaltag" in a playful, multi-colored font where each letter is a different color (purple, blue, green, yellow, red, pink, black). Below the "tag" part, the year "2026" is written in a smaller, pink font.



**Die Aufzeichnung bzw. der Mitschnitt
des Präsenz- oder Online-Vortrags in
Bild und/oder Ton ist nicht gestattet.**

Beratungsdienst Geld und Haushalt

- 1958 als Einrichtung des Deutschen Sparkassen- und Giroverbandes gegründet
- Bildungsangebote zur Vermittlung von **Finanzwissen** sowie **Stärkung von Handlungskompetenzen** in der Alltags- und Lebensökonomie privater Haushalte
- **Neutral, werbefrei, kostenfrei**
- Angebote stehen **allen Bürgerinnen und Bürgern** offen
- Auch Einrichtungen der Schuldner- oder Sozialberatung und Lehrkräfte im Bildungsbereich können Angebote nutzen
- **www.geld-und-haushalt.de**

Bild: Geld und Haushalt

Geld und Haushalt fördert lebensbegleitendes Lernen

Multimediale Angebote für jedes Alter und alle Lebenslagen



Vorträge

zu Verbraucher- und Rechtsthemen von Onlineshopping über Geld in der Familie bis hin zu Pflege und Erbe. Vorträge sind in Präsenz und als Online-Vortrag möglich, kostenfrei buchbar durch nicht kommerzielle Einrichtungen und Sparkassen



Ratgeber

Breites Informationsangebot mit Ratgebern zur Budgetplanung sowie zur Vorbereitung von Finanzentscheidungen. Versand erfolgt direkt an Verbraucher:innen oder an Multiplikator:innen, Beratungseinrichtungen und Sparkassen



Onlineplaner

Vier praktische Tools, darunter ein Online-Haushaltsbuch und eine Haushaltsbuch-App, ein Check-up für die Gesamtfinanzen, sowie Referenzbudgets – ein statistischer finanzieller Vergleich mit ähnlichen Haushalten

Bilder: iStock: Halfpoint; Geld und Haushalt

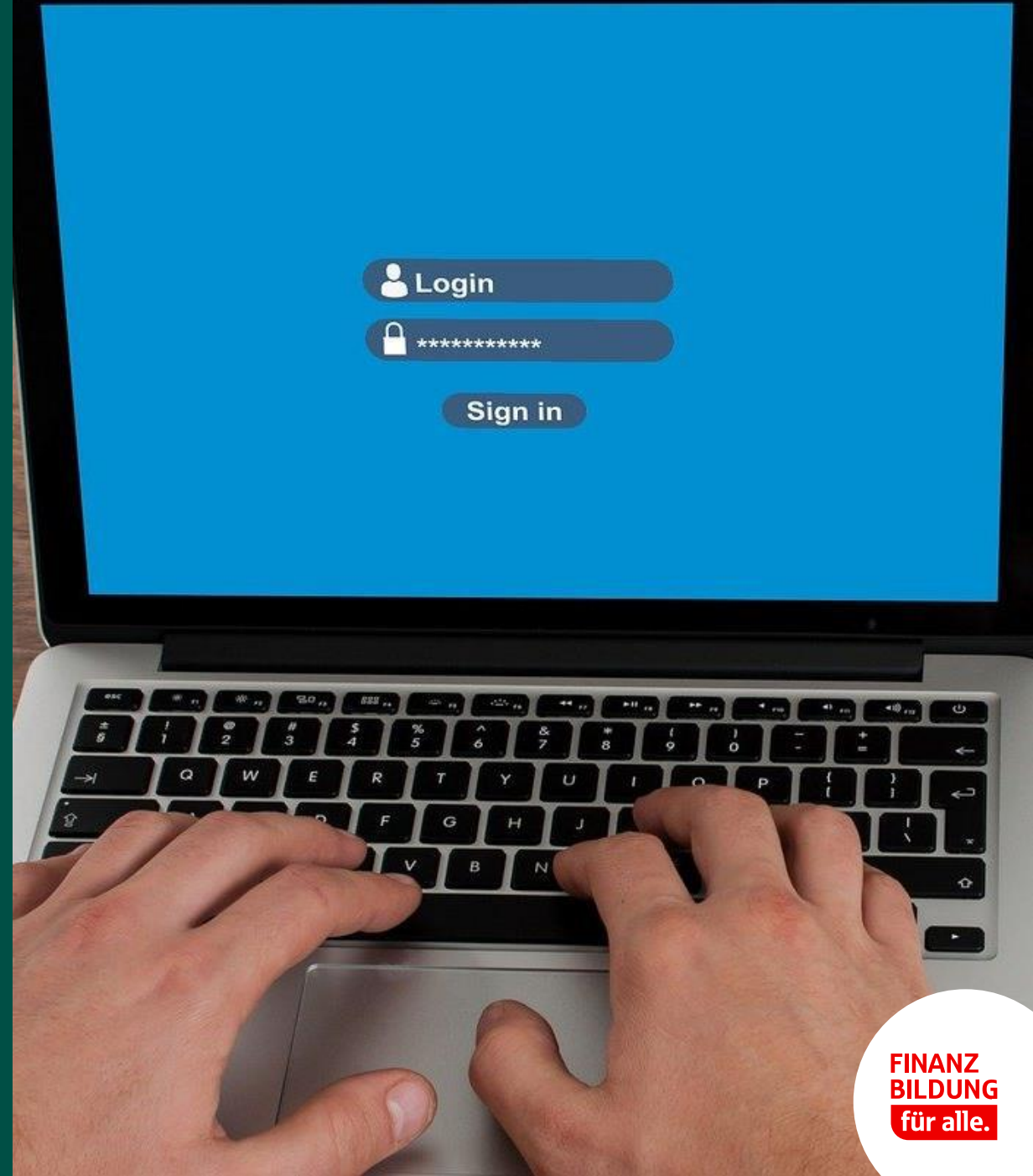
EIN ANGEBOT VON GELD UND HAUSHALT

Inhalte

1. Zahlen und Fakten rund um Cybersicherheit
2. Die häufigsten Betrugsmaschen
3. Wie kann ich mich schützen?
4. Was tun, wenn ich Opfer von Cyberkriminalität wurde?

1.

Zahlen und Fakten rund um Cybersicherheit



1. Zahlen und Fakten rund um Cybersicherheit

Cybersicherheitsmonitor 2026

Jede und jeder vierte Deutsche war schon einmal von Cyberkriminalität betroffen.

Häufigste Straftaten:

- 22 % wurden Opfer von Betrug bei Online Shopping
- 14 % erlebten einen Fremdzugriff auf einen Account
- 13 % erlebten Betrug beim Onlinebanking
- 12 % wurden Opfer von Phishing
- 7 % fanden Schadsoftware auf einem ihrer Geräte
- 2 % zusätzlich Ransomware

Quelle und Bild: BSI und Polizeiliche Kriminalprävention der Länder
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Leistungen-und-Kooperationen/Digitaler-Verbraucherschutz/Digitalbarometer/digitalbarometer_node.html

EIN ANGEBOT VON GELD UND HAUSHALT



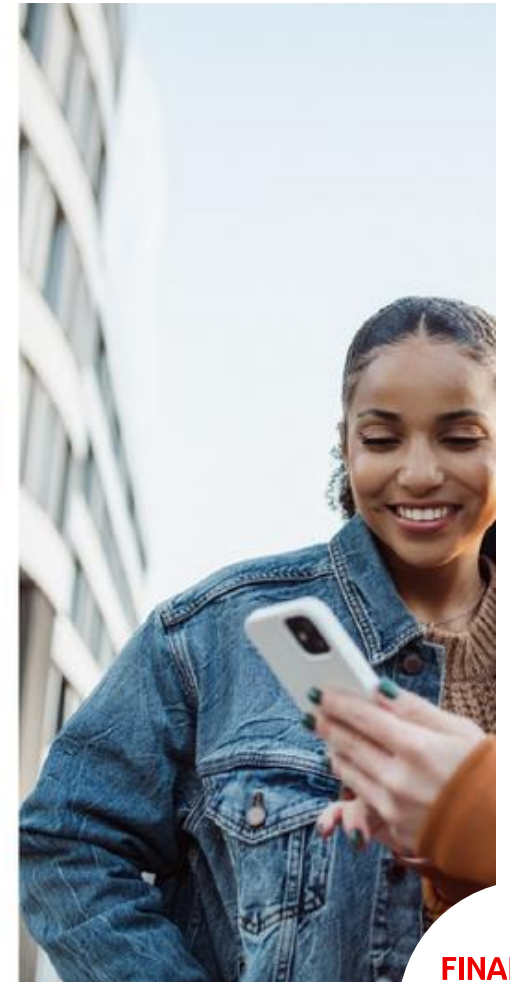
Befragung

zur Cybersicherheit

2026

 **CyMon**
Der Cybersicherheitsmonitor

Kurzbericht zur Studie der Polizeilichen
Kriminalprävention der Länder und des
Bundes (ProPK) und des Bundesamtes für Sicherheit
in der Informationstechnik (BSI)



**FINANZ
BILDUNG**
für alle.

2. Die häufigsten Betrugsmaschen

EIN ANGEBOT VON GELD UND HAUSHALT



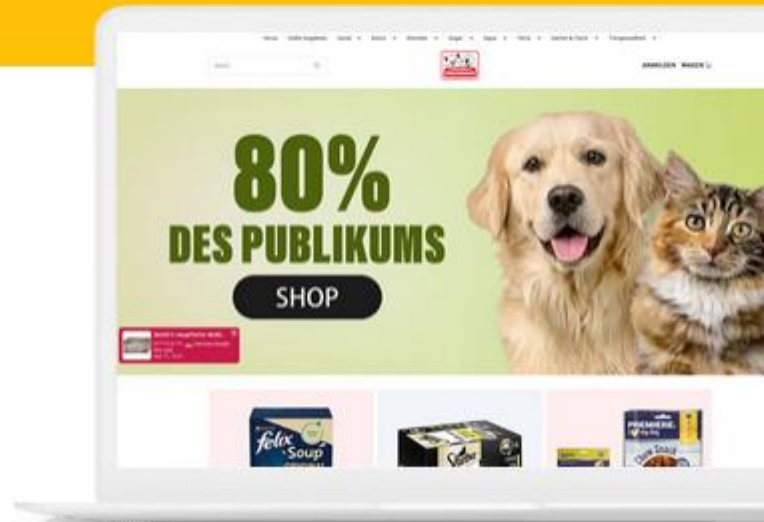
2. Die häufigsten Betrugsmaschen

Fakeshops

online seit 11.12.2023

Achtung Fake-Shop: fressnapfs.shop

Kriminelle schalten auf Facebook und Instagram Werbung für einen betrügerischen Fressnapf-Online-Shop. Der gefälschte Online-Shop sieht dem echten Shop zum Verwechseln ähnlich. Auch die Internetadresse „fressnapfs.shop“ scheint plausibel. Wenn Sie beim Fake-Shop bestellen, verlieren Sie Ihr Geld und erhalten keine Lieferung!



Kriminelle werben mit Angeboten auf Social Media

Betrogene Kund:innen berichten, dass Sie über eine Werbung auf Facebook oder Instagram im betrügerischen Fressnapf-Shop gelandet sind. Eine Anzeige, die wir über eine Recherche in der Meta Werbebibliothek gefunden haben, verspricht einen Rabatt von 60 %. Die betrügerische Werbung führt dann in den Fake-Shop fressnapfs.shop.



Quelle: https://www.watchlist-internet.at/news/achtung-fake-shop-fressnapfsshop/?sword_list%5B0%5D=fake&sword_list%5B1%5D=shop&no_cache=1

EIN ANGEBOT VON GELD UND HAUSHALT

2. Die häufigsten Betrugsmaschen

Was ist ein Fakeshop?



Merkmale u.a.:

- Professionelle Website mit sehr günstigen Preisen
- Liefert keine / gefälschte Ware
- Oft nur Vorkasse / seltsame Zahlungsmöglichkeiten
- **KEIN/ Merkwürdiges Impressum**
- Unklare Lieferzeiten (5 – 30 Tage)
- Fehler Website (Fressnapfs.shop)
- Negative Berichte im Internet:
„Name Shop + Erfahrungen“ in Suchmaschine eingeben
- Keine sichere Datenübertragung (Schlosssymbol im Browser/httpS)

Bild: KI generiert (ChatGPT)



Fakeshop-Finder

Ist dieser Online-Shop seriös?

Shop-URL prüfen**URL prüfen und Ergebnis erhalten**

2. Die häufigsten Betrugsmaschen

Fakeshops erkennen

Mit dem Fakeshop-Finder der Verbraucherzentralen seriöse und unseriöse Online-Shops prüfen.

- www.verbraucherzentrale.de/fakeshopfinder-71560
- URL eingeben
- Ergebnis erhalten

Bild: www.verbraucherzentrale.de/fakeshopfinder-71560

Was ist Phishing?



- Betrugsversuch im Internet
- Kriminelle wollen z.B. an folgende Informationen kommen
 - Passwörter
 - Bankdaten
 - Zugangsdaten
- Vom englischen „fishing“ = angeln
- Kriminelle werfen den Köder aus, und warten dass jemand anbeißt

Bild: Pixabay

2. Die häufigsten Betrugsmaschen

Verhalten der Nutzer:innen

- Etwa jede Dritte unerwünschte E-Mail beinhaltet einen Phishing-Versuch¹
- 41 % nutzen ihre Passwörter für mehrere Konten¹
- Klickrate bei Phishing Mails²

18- bis 39-Jährige: 29 Prozent

Über 50-Jährige: 19 Prozent

1 Studie der Polizeilichen Kriminalprävention der Länder und des Bundes und des Bundesamtes für Sicherheit in der Informationstechnik; 2 SoSafe Security Awareness

Bild: Pixabay



Abgrenzung Phishing/Spam

Phishing

- Kriminelle versuchen an Ihre Daten zu kommen
- Oft mit gefälschten Mails/SMS
- Unbekannter Absender
- Rechtschreibfehler
- Kopiert aus Chatgpt
- Drohungen (Konto wird gesperrt, Bilder werden gelöscht)
- Aufforderung, Daten einzugeben

SPAM

- Unerwünschte Nachrichten
- Per E-Mail, SMS, Messenger
- Werbung
- Beispiel: Nur noch heute 70% Rabatt auf Babbel Sprach App

Smishing???
Quishing???

2. Die häufigsten Betrugsmaschen

Quishing

- Phishing per QR Code
- QR Codes werden überklebt (Ladesäulen, Parkscheinautomaten, Speisekarte/Tische in Restaurants, Öffentliches WLAN)
- Briefe, Flyer im Briefkasten
- QR Code führt zu gefälschten Websites mit Zahlungsaufforderungen
- Oft mit Lockangeboten

→ Immer Link prüfen!

Bild: Pixabay

EIN ANGEBOT VON GELD UND HAUSHALT



2. Die häufigsten Betrugsmaschen

Enkeltrick 2.0 – Deepfakes

Deepfake = Mit Hilfe von künstlicher Intelligenz erzeugtes Bild, Video oder Sprachaufnahme.

Betrüger:innen können:

- Stimmen nachahmen
- Fotos/Videos fälschen

Enkeltrick 2.0

„Oma ich hatte einen Unfall. Bitte überweise mir Geld.“

Stimme klingt echt, erstellt mit KI aus Videos/Sprachnachrichten



Wie schützen?

- Auch vertraute Stimmen prüfen
- Auflegen, persönlich zurückrufen
- Fragen stellen z.B.
 - Wie heißt mein/dein Haustier?
 - Wo haben wir letztes Weihnachten gefeiert?
 - Was habe ich dir letztes Jahr zum Geburtstag geschenkt?

3. Die häufigsten Betrugsmaschen

Identitätsdiebstahl

Kriminelle nutzen persönliche Daten einer anderen Person, um sich als diese auszugeben.

- Name und Adresse
- Geburtsdatum
- Telefonnummern
- E-Mailadresse
- Fotos
- Kontonummern

Für z.B.: Bestellungen, Vertragsabschlüsse, Kontoeröffnungen, gefälschte Profile in sozialen Medien

Bild: Pixabay

EIN ANGEBOT VON GELD UND HAUSHALT



3.

Wie kann ich mich schützen?

EIN ANGEBOT VON GELD UND HAUSHALT



3. Wie kann ich mich schützen?

Kriterien für ein sicheres Passwort

- 12 – 16 Zeichen, je länger desto besser
- Groß- und Kleinbuchstaben
- Sonderzeichen
- Zahlen
- Sätze/Affirmationen:
Ich **s**chaue **j**eden **D**onnerstag um 20 Uhr **d**en
Bergdokter!**=** IsjDu2dB!
Ich **g**laube **a**n **m**ich **u**nd **b**in **e**in **w**undervoller **M**ensch **!=**
lgamub1wM!
- Für jedes Konto eigenes Passwort
- Tipp: Passwortmanager



3. Wie kann ich mich schützen?

Zwei Faktor Authentifizierung

Zwei Nachweise erforderlich



Etwas, das man weiß:

- PIN
- Passwort, Code

Etwas, das man dabei hat

- Smartphone (Coder per App oder SMS)
- Fingerabdruck
- Gesichtserkennung

3. Wie kann ich mich schützen?

Passwortmanager

Tresor für Passwörter

- Daten werden verschlüsselt gespeichert
- Man muss sich nur ein „Masterpasswort“ merken
- Starke Passwörter können automatisch erstellt werden
- Kostenfreie und kostenpflichtige Anbieter

Nachteile

- Wenn Masterpasswort weg, dann alle Passwörter weg
- Cyberangriff möglich?

Wichtig

- Zwei Faktor Authentifizierung (2FA) möglich?
- Wo werden die Daten gespeichert? Lokal oder in einer Cloud und wenn in einer Cloud, in welchem Land?
- Kein Browser Passwortmanager nutzen

3. Wie kann ich mich schützen?

Tipp vom BSI (Bundesamt für Sicherheit in der Informationstechnik)

1. Teil des Passworts merken



- Für jeden Account gleich
- Ohne persönlichen Bezug
- Mindestens acht Zeichen lang
- Besteht bspw. aus zwei ausgedachten, aneinander gereihten Wörtern
(tisch-himmel)



2. Teil des Passworts in Liste eintragen



- Für jeden Account anders
- Entweder kurz und komplex oder besonders lang
- Besteht bspw. aus willkürlich aneinander gereihten Zeichen oder aus vier Wörtern, die durch Sonderzeichen getrennt sind
(Berg_spät_hüpfen_Kühlschrank)



Sichere Passwörter für jeden Account

(tisch-himmelBerg_
spät_hüpfen_Kühlschrank)

Quelle:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Umgang-mit-Passwoertern/umgang-mit-passwoertern_node.html



3. Wie kann ich mich schützen?

Sicherheitstipps

- Virenschutz, Firewall
- Geräte mit PIN sichern (auch Tablets, PC)
- Sicheres Passwort, Zwei Faktor Authentifizierung
- Software aktuell halten, Updates machen
- Kein öffentliches WLAN beim Banking!
- Bluetooth, NFC, Öffentliches WLAN nur bei Gebrauch aktivieren
- Verfügungslimit beim Online-Banking einrichten
- Keine verdächtigen Anhänge/Links öffnen
- Niemals PIN/TAN weitergeben
- Absender:in kontaktieren z.B. Bank

Bild: Pexels: Pixabay

3. Wie kann ich mich schützen?

An wen können Sie sich wenden?

Fragen zur IT-Sicherheit

Bundesamt für Sicherheit und Informationstechnik (BSI),
www.bsi.bund.de

- Servicetelefon: 0800 2741000
- Mo. bis Do. von 8-17 Uhr, Fr. 8-16 Uhr



4.

Was tun, wenn ich Opfer von Cyberkriminalität wurde?





Wo finde ich Hilfe? Cybersicherheits-Lotse

Universität Bonn



Wurden meine persönlichen Daten und Passwörter im Internet offengelegt?

➔ [Leakchecker Uni Bonn](#)

Hasso-Plattner-Institut



Wurden meine persönlichen Daten und Passwörter im Internet offengelegt?

➔ [Leakchecker Hasso Plattner Institut](#)

Verbraucherzentrale Niedersachsen



Online-Konto gehackt? Anleitungen für häufig genutzte Online-Accounts

➔ [Anleitungen zur Soforthilfe](#)

Verbraucherzentralen



Formen und Folgen von Identitätsdiebstahl im Internet

➔ [Verbraucherzentrale - Identitätsdiebstahl](#)

Polizeien der Länder



Opfer von Identitätsmissbrauch? Strafanzeige stellen bei den Onlinewachen

➔ [Polizei Onlinewachen](#)

Polizeiliche Kriminalprävention (ProPK)



Informationen und Hilfestellungen für Opfer von Cybercrime

➔ [Was tun im Ernstfall?](#)

Quelle: BSI

4. Was tun, wenn ich Opfer wurde?

Opfer geworden?

- Passwörter ändern/zurücksetzen wenn alternativer Weg möglich
- Aktive Sitzungen beenden (meistens in den Einstellungen)
- Ggf. Bank anrufen
- Beweise sichern (Screenshots)
- Verbraucherzentrale kontaktieren
- Polizeiliche Beratung, ggf. Anzeige erstatten
- Betrug auf Plattform melden
- ACHTUNG: Betrüger:innen melden sich oft ein zweites Mal

Tipp: www.bsi.bund.de
(Checklisten, Podcasts)

4. Was tun, wenn ich Opfer wurde?

Checklisten für den Ernstfall

Checklisten für Betroffene von Cyberkriminalität

- Identitätsdiebstahl
- Betrug beim Onlineshopping
- Gehackter Account
- Phishing
- ...

Weitere Informationen und kostenloser Download unter

**www.bsi.bund.de → Service → Publikationen →
Checklisten, Flyer & Schritt-für-Schritt-Anleitungen**

Quelle: Bundesamt für Sicherheit in der Informationstechnik

EIN ANGEBOT VON GELD UND HAUSHALT

BETRUG BEIM ONLINESHOPPING: CHECKLISTE FÜR DEN ERNSTFALL

Onlineshopping ist bequem und schnell, birgt jedoch auch Risiken: Nicht alle Anbieter im Netz sind vertrauenswürdig und Internetkriminelle nutzen jede Unachtsamkeit aus. Zu möglichen Betrugsfällen zählt etwa, dass bereits bezahlte Waren nicht, defekt bzw. falsch geliefert oder sensible Daten wie etwa Klarnamen in Verbindung mit Kreditkarteninformationen abgegriffen und missbraucht werden. Das kann sowohl bei größeren Onlineshops als auch auf Kleinanzeigenportalen oder in den Shops von Social-Media-Plattformen geschehen. Umso wichtiger ist es, beim Einkauf auf die Sicherheit zu achten.

- ✓ Wenn Sie Betrug durch einen anderen User z. B. auf einer Kleinanzeigen- oder einer Social-Media-Plattform erfahren haben, informieren Sie auch den Betreiber der Plattform.
- ✓ Beobachten Sie Ihre Kontobewegungen genau. Kontaktieren Sie bei unbekannten Abbuchungen Ihre Bank oder auch die Polizei.

SO GEHEN SIE VOR, WENN SIE BEIM ONLINESHOPPING BETROGEN WURDEN

- ✓ Sollten Sie bereits Geld für Ihre Bestellung überwiesen haben, informieren Sie sich umgehend bei Ihrer Bank, ob Sie die Zahlung rückgängig machen können.
- ✓ Sollten Sie einen Zahlungsdienst wie z. B. PayPal, Klarna, Wero, Apple oder Google Pay nutzen, kontaktieren Sie sofort den Dienstleister und lassen ihn die Transaktion stoppen.
- ✓ Sichern Sie alle Beweise für Ihren Online-Kauf – ob Bestellbestätigung, Rechnung oder Versandbenachrichtigung.
- ✓ Erstellen Sie Anzeige bei der Polizei: Wenden Sie sich mit den gesicherten Unterlagen an Ihre lokale Polizeidienststelle oder an die **Online-Wachen der Polizei in der Länder**. Nur dann können z. B. Löschungen von Fake-Shops vorangetrieben werden.

SO SCHÜTZEN SIE SICH IN ZUKUNFT VOR BETRUG BEIM ONLINESHOPPING

- › Vergleichen Sie vor einem Kauf die Preise. Diese sollten realistisch sein und mit allen zusätzlichen Kosten, etwa Versand und Rücksendungsgebühr, ausgewiesen werden. Insbesondere Anbieter außerhalb der EU berechnen oftmals Zusatzkosten. Betrüger werben außerdem in vielen Fällen mit unrealistisch günstigen Angeboten.
- › Informieren Sie sich über die Seriosität des jeweiligen Onlineshops, zum Beispiel über Suchmaschinen, Erfahrungsberichte oder Foren.
- › Achten Sie darauf, welche Zahlungsmöglichkeiten zur Verfügung stehen: Betrüger bieten oft ausschließlich Vorkasse an. Wählen Sie Zahlungsarten wie Kauf auf Rechnung oder Lastschrift, da diese im Betrugsfall bessere Möglichkeiten zur Rückbuchung bieten. Nutzen Sie ausschließlich Bezahlmethoden, die einen wirksamen Käuferschutz bieten oder im Problemfall eine Rückerstattung ermöglichen.



4. Was tun, wenn ich Opfer wurde?

Die 6 wichtigsten Regeln

- Keine PINs/Tans rausgeben
- Kein Banking im öffentlichen WLAN
- Misstrauen bei Zeitdruck
- Im Zweifel zurückrufen
- QR-Codes und Links prüfen
- Regelmäßig informieren 😊



Bild: KI-generiert (ChatGPT)

EIN ANGEBOT VON GELD UND HAUSHALT

Danke.

Katja Plieninger
Freie Vortragsreferent:in im Auftrag des DSGV e. V.

+49 7181 2698665
katja.plieninger@guh-vs.de



Geld und Haushalt

**FINANZ
BILDUNG**
für alle.

Rechtliche Hinweise

Die Aufzeichnung bzw. der Mitschnitt des Präsenz- oder Online-Vortrags in Bild und/oder Ton ist nicht gestattet.

Diese Präsentation wurde mit größter Sorgfalt bearbeitet. Sie enthält jedoch lediglich unverbindliche Inhalte. Die Angaben beruhen auf Quellen, die als zuverlässig eingestuft werden, für deren Richtigkeit, Vollständigkeit oder Aktualität aber keine Gewähr übernommen werden kann.

Sämtliche in dieser Präsentation getroffenen Angaben dienen der Information. Sie dürfen nicht als Angebot oder Empfehlung für Anlageentscheidungen verstanden werden. Die Informationen oder Dokumente sind nicht als Grundlage für irgendeine vertragliche oder anderweitige Verpflichtung gedacht. Sie ersetzen keine (Rechts-, Steuer- und/oder Anlage-)Beratung.

Alle Abbildungen und Texte in dieser Präsentation sind urheberrechtlich und/oder markenrechtlich geschützt. Die Rechte liegen bei den Urhebern bzw. beim Markenrechtsinhaber. Jegliche externe Verwendung oder Reproduktion in elektronischer oder gedruckter Form bedarf der ausdrücklichen Zustimmung durch die Urheber bzw. Rechteinhaber.

Die Präsentation darf nicht für gewerbliche Zwecke verwendet werden. Eine Weitergabe an Dritte bedarf der schriftlichen Zustimmung des Urhebers.