Internetsicherheit für Einsteiger: Sicherer Online-Einkauf

Grundlagen und Tipps für sicheres Einkaufen im Internet

Agenda zum sicheren Online-Einkauf für Senioren

- **Einführung in die Internetsicherheit für Senioren**
- **Typische Betrugsformen und wie man sie erkennt**
- **Sichere Online-Shops und vertrauenswürdiges Einkaufen**
- **Sicheres Bezahlen im Internet**
- **Technische Schutzmaßnahmen für sicheres Online-Shopping**
- **Im Ernstfall richtig handeln**
- **Abschluss und Wiederholung**

Zum Nachdenken

Woran erkennen Sie persönlich, ob ein Online-Shop vertrauenswürdig ist?

Prüfen Sie Impressum, HTTPS, echte Siegel, faire Preise, externe Bewertungen und mehrere Zahlungsmethoden.

BSI+2Wikipedia+2polizei-praevention.de+2Onlinesicherheit+1BSI+1

Was glauben Sie: Wie viele Menschen in Deutschland wurden allein im letzten Jahr beim Online-Shopping betrogen?

Über 300.000 Personen (Nur bekannte) und nur 49 % der Verbraucher fühlen sich sicher

sicher-im-netz.de; 3bitkom.org; 3boniversum.de

Einführung in die Internetsicherheit

Bedeutung der Internetsicherheit für Senioren

Gefahr durch Betrug

Senioren sind häufig Ziel von Online-Betrug und müssen besonders vorsichtig sein, um sich zu schützen.

Schutz persönlicher Daten

Sicheres Verhalten bewahrt persönliche Informationen und finanziellen Besitz vor Verlust und Missbrauch.

Risikoverständnis fördern

Das Verstehen von Online-Risiken hilft Senioren, sich sicher und selbstbewusst im Internet zu bewegen.

Häufige Bedrohungen und Betrugsarten

„Im Internet gibt’s nicht nur Schnäppchen, sondern auch jede Menge Schwindler.“

Gefälschte Online-Shops: Die Seite sieht super aus, aber die **Ware kommt nie** – und das Geld ist weg.

Phishing-E-Mails: E-Mails, die angeblich von der Bank, Post oder einem Online-Shop kommen – aber in Wirklichkeit nur eins wollen: Ihre **Zugangsdaten** oder Ihr Geld.

Fake-Rechnungen oder Mahnungen: Sie bekommen eine Rechnung für etwas, das Sie nie gekauft haben – und sollen **schnell** überweisen.

Telefonbetrug mit „Support“ oder „Polizei“: Da ruft jemand an und behauptet, der Computer sei **gehackt** worden – oder das Konto sei **gesperrt**.

Liebesbetrug („Love Scamming“): Jemand gibt sich online als Traumpartner aus – am Ende geht’s um **Geld**, nicht um Gefühle.

Falsche Gewinnspiele: „Sie haben gewonnen!“ – aber erst mal soll man **Gebühren** zahlen oder persönliche Daten rausrücken.

Unterschiedliche Arten von Bedrohungen (1)

Betrug ohne Lieferung

- **Ziel:** Geld kassieren, ohne jemals Ware zu versenden.
- **Merkmale:**
  - Extrem günstige Preise, oft deutlich unter Marktwert.
  - Fehlendes oder gefälschtes Impressum.
  - Keine oder nur sehr eingeschränkte Zahlungsmethoden mit Käuferschutz (meist nur Vorkasse oder Kryptowährungen).
  - Keine echte Warenverfügbarkeit – Bilder und Texte oft kopiert von anderen Shops.
- **Risiko:** Reiner finanzieller Verlust, Ware kommt nie an.

Unterschiedliche Arten von Bedrohungen (2)

Problematische, aber „echte“ Händler

- **Ziel:** Verkauf findet statt, aber mit mangelhaften Bedingungen.
- **Merkmale:**
  - Lieferung zwar vorhanden, aber Ware defekt, falsch oder stark abweichend von der Beschreibung.
  - Schlechte oder unfaire Rückgabe- und Garantiebedingungen (z. B. Rücksendung nur auf eigene Kosten ins Ausland, keine Rückerstattung).
  - Überlange Lieferzeiten ohne klare Kommunikation.
  - Aggressive AGB, die Verbraucherrechte einschränken sollen.
- **Risiko:** Ärger, Qualitätsmängel, aufwendige Reklamation, möglicher Teil- oder Totalausfall des Geldes.

Unterschiedliche Arten von Bedrohungen (3)

Kategorie	Betrug ohne Lieferung	Problematischer, aber „echter“ Händler
Ziel	Geld kassieren, ohne Ware zu versenden	Verkauf findet statt, aber unter schlechten Bedingungen
Typische Merkmale	- Keine echte Warenverfügbarkeit	- Ware wird geliefert, aber defekt oder abweichend
	- Preise deutlich unter Marktwert	- Schlechte Rückgabe- und Garantiebedingungen
	- Fehlendes oder gefälschtes Impressum	- Überlange Lieferzeiten
	- Nur unsichere Zahlungsmethoden (z. B. Vorkasse, Kryptowährung)	- Aggressive AGB, die Verbraucherrechte einschränken
	- Kopierte Produktbilder und -texte	- Unklare oder teure Rücksendungen ins Ausland
Risiko für Käufer	- Reiner finanzieller Verlust	- Ärger und zusätzlicher Aufwand
	- Ware kommt nie an	- Teil- oder Totalausfall des Kaufpreises
		- Langwierige Reklamationen
Warnsignale	- Kein Käuferschutz möglich	- Negative Bewertungen zu Qualität und Service
	- Kein Impressum oder falsche Kontaktdaten	- Viele Berichte über Reklamationsprobleme
	- Extrem günstige Preise	- Ungewöhnlich lange Lieferzeiten

Typische Betrugsformen und wie man sie erkennt

Phishing, Quishing und Fake-Nachrichten

Phishing und Quishing Methoden

Phishing nutzt E-Mails, Quishing nutzt SMS, um Nutzer zur Preisgabe sensibler Daten zu verleiten.

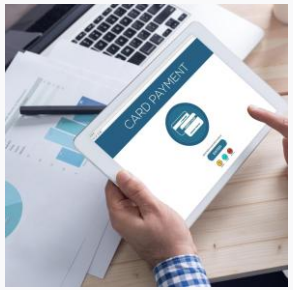
Warnzeichen erkennen

Unverschlüsselte Links, Rechtschreibfehler und ungewöhnliche Absender sind typische Hinweise auf Betrugsnachrichten.

Sicherheitsverhalten

Niemals vertrauliche Daten eingeben oder Links anklicken, wenn Zweifel an der Echtheit der Nachricht bestehen.

Fake-Shops erkennen: Impressum, Bewertungen, DSGVO

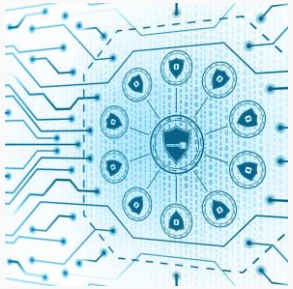


Vollständiges Impressum

Seriöse Online-Shops verfügen über ein vollständiges Impressum mit klaren Kontaktinformationen und rechtlichen Angaben.

Echte Kundenbewertungen

Authentische Kundenbewertungen sind ein wichtiges Merkmal seriöser Shops und helfen bei der Vertrauensbildung.

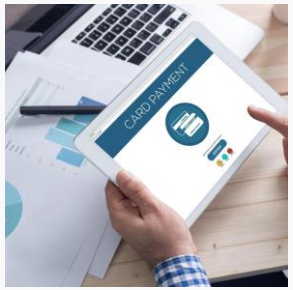


DSGVO-Konformität

Die Einhaltung der Datenschutz-Grundverordnung (DSGVO) schützt die Nutzerdaten und signalisiert Seriosität.

Fake-Shops erkennen: Impressum, Bewertungen, DSGVO

Achtung!
Nur gültig bei EU - Shops

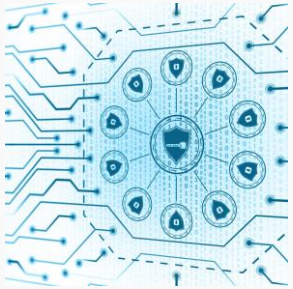


Vollständiges In

Seriöse Online-Shops v Kontaktinformationen und rechtlichen Angaben.

Echte Kundenbewertun

Authentische Kundenbewertunge öser Shops und helfen bei der Vertrauensbildung.



DSGVO-Konformität

Die Einhaltung der Datenschutz-Grundverc VO) schützt die Nutzerdaten und signalisiert Seriosität.

Achtung bei Shops außerhalb der EU

So prüfen Sie internationale Online-Anbieter auf Seriosität

So prüfen Sie internationale Online-Anbieter auf Seriosität

- **Kein EU-Verbraucherschutz:** Bei Händlern außerhalb der EU gilt oft kein Widerrufsrecht oder Käuferschutz nach EU-Standard.
- **Impressum & Adresse prüfen:** Gibt es eine klare Firmenadresse? Prüfen Sie die Existenz über Google Maps.
- **AGB & Datenschutz vorhanden?:** Seriöse Anbieter nennen klar ihre Rückgabe- und Datenschutzregeln – auch auf Englisch (**Terms & Conditions**).
- **Vorsicht bei Vorkasse:** Fehlt PayPal oder Kreditkarte mit 2FA, ist das Risiko bei Fake-Shops deutlich erhöht.

Photo by Roman Kraft on Unsplash

So erkennen Sie unseriöse oder gefälschte Internet-Shops

Fehlende Kontaktinformationen

Unseriöse Shops bieten oft keine oder unvollständige Kontaktinformationen, was Misstrauen wecken sollte.

Unrealistisch günstige Preise
Extrem niedrige Preise können auf gefälschte Shops hinweisen und sollten skeptisch betrachtet werden.

Schlechte Webseite und Design
Eine schlecht gestaltete Webseite deutet häufig auf einen unseriösen oder gefälschten Internet-Shop hin.

Fehlende Sicherheitszertifikate
Ohne SSL-Zertifikate oder Sicherheitskennzeichen sollten Sie keine Einkäufe tätigen.

So erkennen Sie unseriöse oder gefälschte Inte

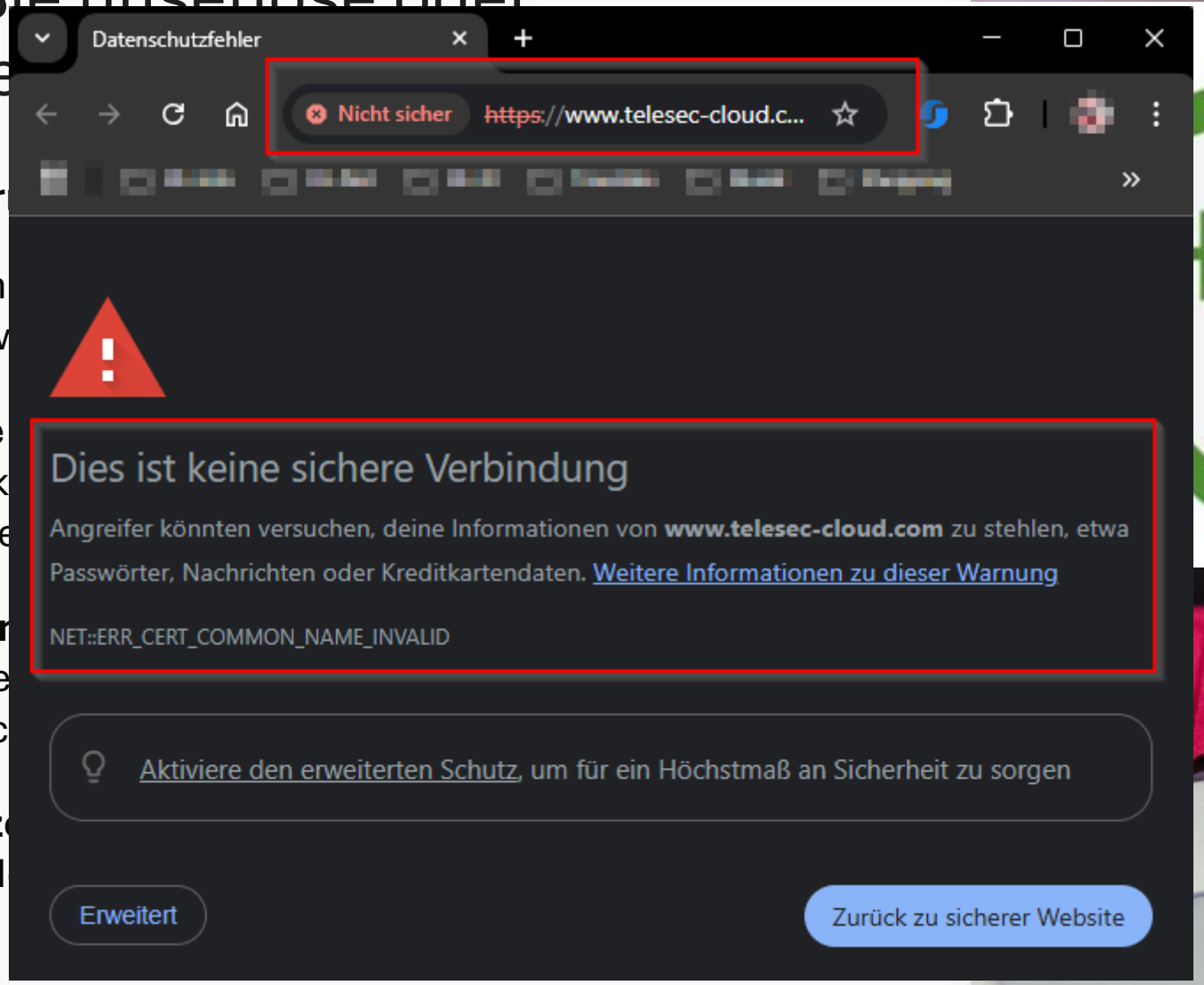
Fehlende Kontaktinfor

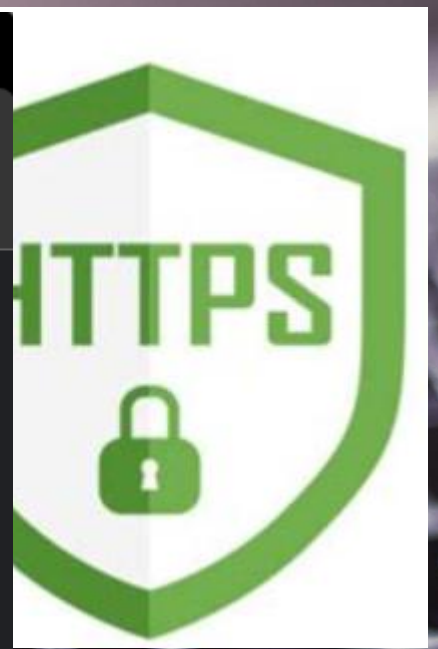
Unseriöse Shops bieten
Kontaktinformationen, v

Unrealistisch günstige
Extrem niedrige Preise k
und sollten skeptisch be

Schlechte Webseite ur
Eine schlecht gestaltete
unseriösen oder gefälsc

Fehlende Sicherheitsz
Ohne SSL-Zertifikate od
keine Einkäufe tätigen.





Sichere Online-Shops und vertrauenswürdiges Einkaufen

Vertrauenswürdige Shops: bekannte Anbieter und Prüfsiegel

Bekannte Anbieter

Etablierte Online-Shops sind vertrauenswürdig und bieten sichere Einkaufserfahrungen für Kunden.

Prüfsiegel Bedeutung

Prüfsiegel wie **TÜV**, **EHI-Gütesiegel** und **Trusted Shops** signalisieren geprüfte Sicherheit und Seriosität von Online-Händlern.

Sicher einkaufen

Kunden sollten **Prüfsiegel** kontrollieren und bevorzugt bei Händlern mit etabliertem Ruf einkaufen.

Verwendung von sicheren Internetseiten beim Einkaufen

HTTPS als Sicherheitsmerkmal

HTTPS in der URL zeigt an, dass die Verbindung zum Online Shop verschlüsselt ist und Daten geschützt werden.

Schloss-Symbol im Browser

Das Schloss-Symbol signalisiert dem Nutzer, dass die Webseite eine sichere Verbindung verwendet.

Beispiel anhand der offiziellen Internet-Seite der Raiffeisenbank Buch-Eching eG

Verwendung von sicheren Interne

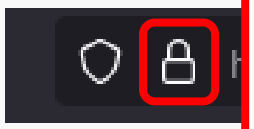
HTTPS als

HTTPS in d
Shop versc

Schloss-S

Das Schlos
Webseite e

Beispiel a
Raiffeisen



Wichtig:

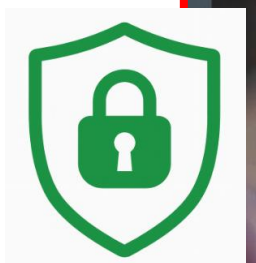
- Kein „**HTTP**“ ohne „**S**“

  (HTTPS://WWW.sichere-Seite.de)

- Wenn die Adresse „**komisch**“ aussieht ist sie es auch“

  → Nicht anklicken!

- Vorsicht bei **Warnmeldung** des Browsers



Wichtige Sicherheitszeichen und Siegel beim Online-Einkauf

Trusted Shop Siegel

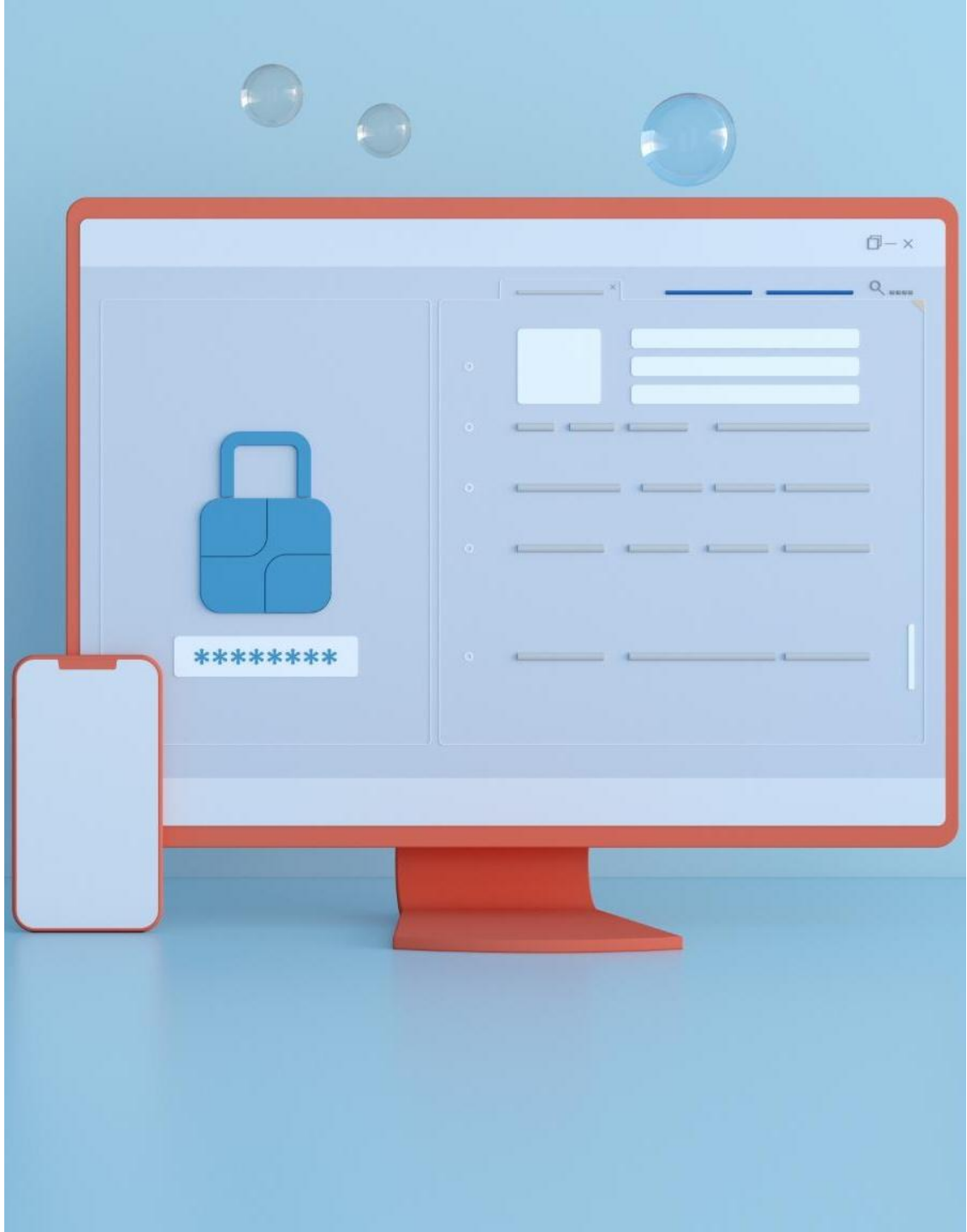
Weist auf geprüfte Anbieter mit Käuferschutz, Datenschutzkonformität und Kundenservice hin.

EHI-Gütesiegel

Zeigt, das rechtliche Vorgaben, Sicherheit und Transparenz kontrolliert wurden

Regelmäßige Prüfungen

Siegel erhalten nur Anbieter, die fortlaufend überprüft und zertifiziert werden



Woran erkenne ich echte Prüfsiegel?

- **Anklickbares Siegel:** Ein echtes Prüfsiegel ist immer verlinkt – z. B. zur Zertifikatsseite von Trusted Shops oder EHI.
- **Siegelgrafik nicht verpixelt:** Gefälschte Siegel sind oft unscharf, veraltet oder wirken optisch abgeschnitten.
- **Zertifikatsnummer & Gültigkeit:** Echte Siegel enthalten eine ID oder Gültigkeitsdatum, oft mit Prüfdatum.
- **Position im Shop-Layout:** Seriöse Shops platzieren Siegel meist unteren Seitenbereich oder auf Produktseiten – nicht übertrieben präsent.

Beispiele für unseriöse Online-Shops

Beispiel für eine fragwürdige Shop-Adresse:

🛑 www.nike-deutschland-**schnäppchen.store**

- Warum ist das verdächtig?
  - Die Adresse sieht auf den ersten Blick „seriös“ aus (Stichwort: bekannte Marke).
  - Sie enthält das Wort „Schnäppchen“ – ein Lockmittel. Die Endung **.store** wird oft bei Fake-Shops verwendet.
  - Es fehlt ein echtes Impressum oder die Firma dahinter.

Überprüfen von Shops

F-Secure:
https://www.f-secure.com/de/online-shopping-checker

Trusted Shops
https://www.trustedshops.de/fake-shops/

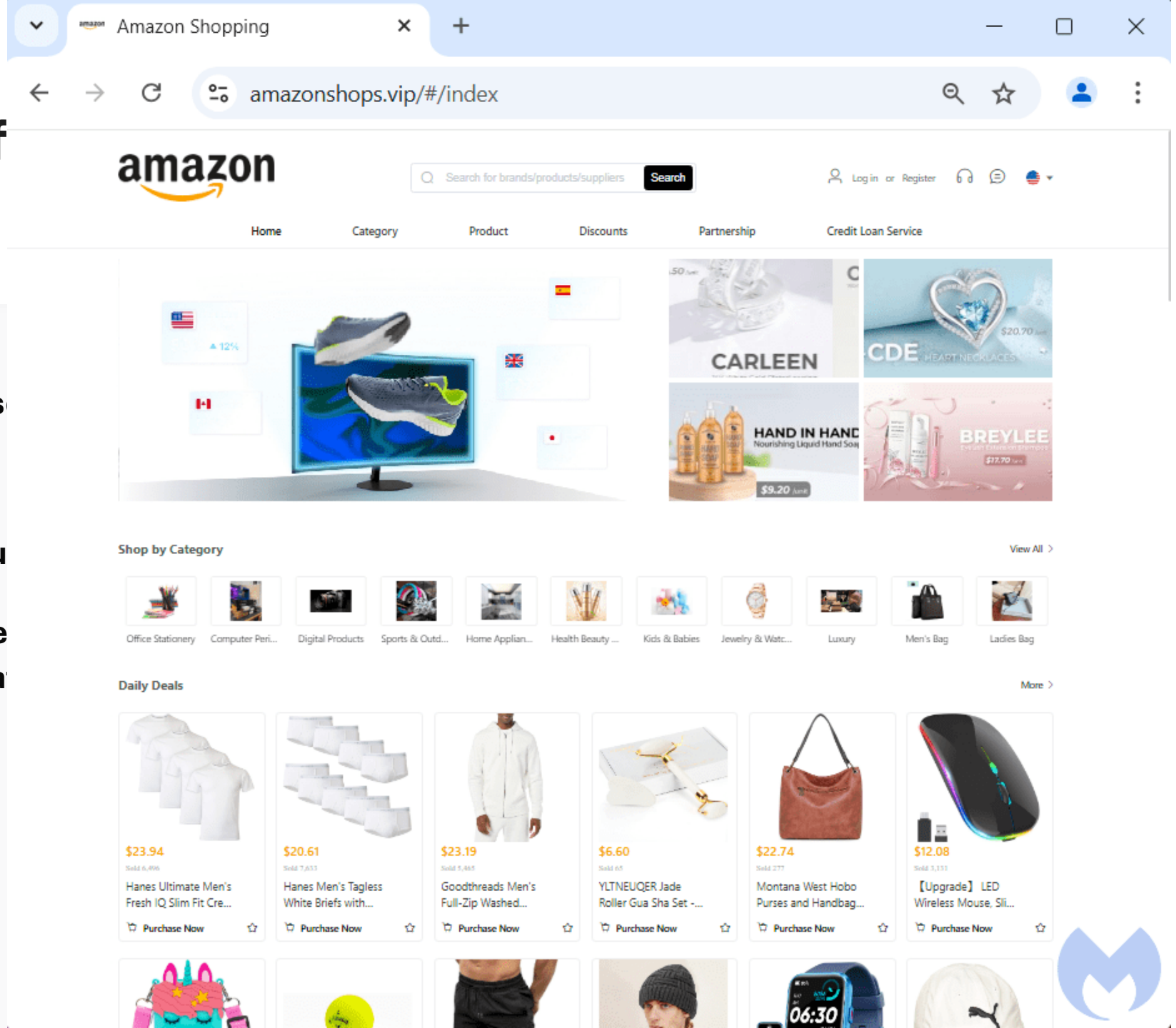
Österreichisches Institut für angewandte Telekommunikation
https://www.watchlist-internet.at/liste-betruegerischer-shops/

Überprüf

F-Secure:
https://www.f-s

Trusted Shops
https://www.tru

Österreichische
https://www.wa



15.08.2025

Sicheres Bezahlen im Internet

Sichere Zahlungsmethoden: Käuferschutz, PayPal, Kreditkarte

Sicherheit durch Käuferschutz

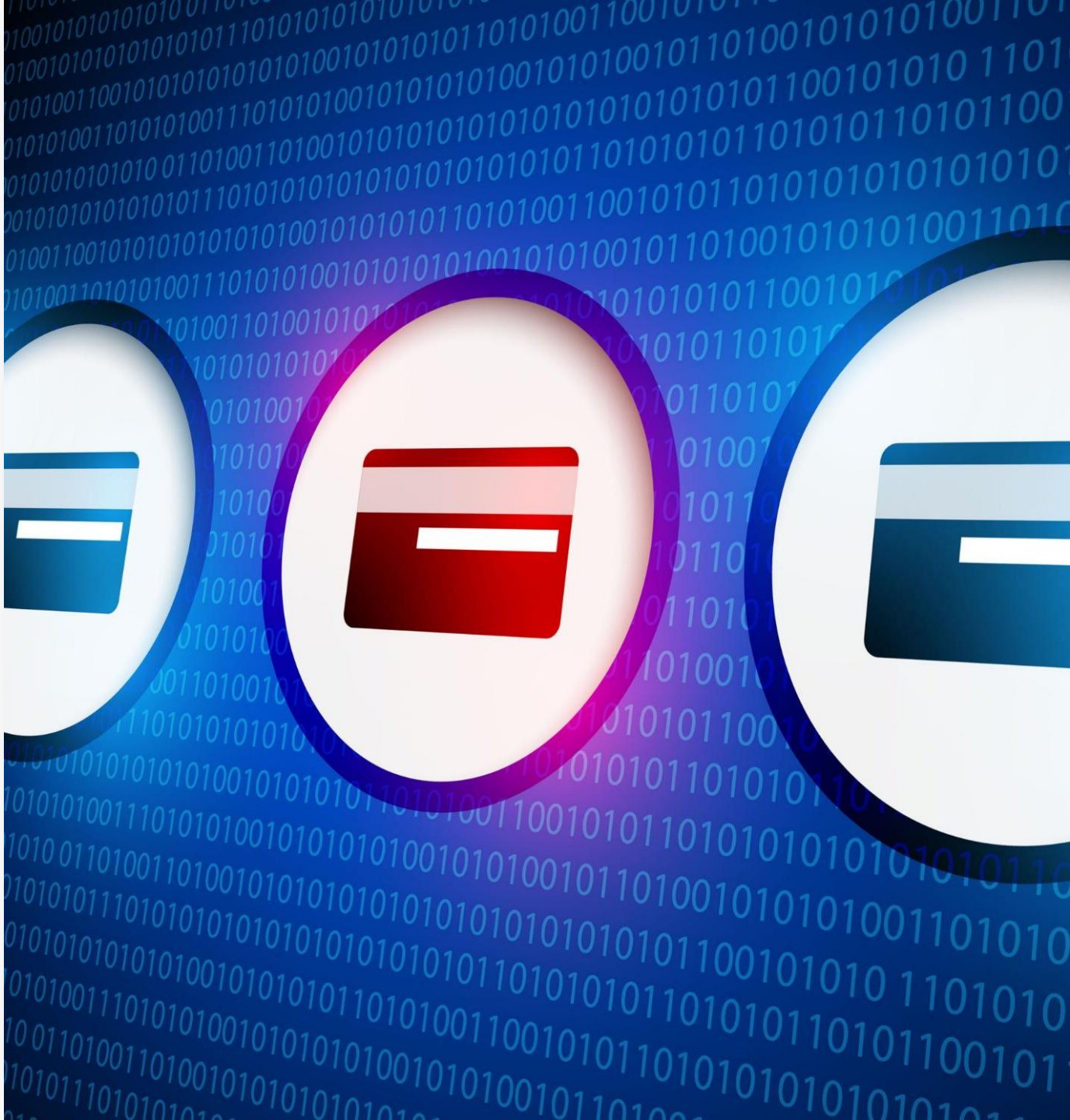
Käuferschutz sorgt für Sicherheit bei Onlinezahlungen und schützt vor betrügerischen Transaktionen.

PayPal als sichere Zahlungsmethode

PayPal ermöglicht sichere Zahlungen mit schneller Rückerstattung bei Problemen oder Betrug.

Kreditkarten mit Rückbuchung

Kreditkartenzahlungen bieten Käuferschutz durch Rückbuchungen bei Streitfällen mit Händlern.



Typische Merkmale von Käuferschutz

Erstattung des Kaufpreises bei Nichtlieferung oder Falschlieferung

Fristen für die Meldung eines Problems (oft 30–180 Tage nach Kauf)

Zwischenstelle (Zahlungsdienstleister) vermittelt zwischen Käufer und Verkäufer

Keine direkte Preisgabe sensibler Bank- oder Kreditkartendaten an den Verkäufer

Zahlungsmethoden mit und ohne Käuferschutz

Zahlungsmethode	Käuferschutz vorhanden?	Bemerkung
PayPal	✅ Ja	180 Tage Frist, Erstattung bei Nichtlieferung oder abweichender Ware
Kreditkarte	✅ Ja (Chargeback)	Rückbuchung möglich, wenn Ware nicht geliefert wird oder Betrug vorliegt
Klarna Rechnung / Ratenkauf	✅ Ja	Zahlung erst nach Erhalt, Konfliktlösung über Klarna
Amazon Pay	✅ Ja	Schutz wie bei direktem Amazon-Kauf
eBay-Zahlungsabwicklung	✅ Ja	Käuferschutz für viele Kategorien, inkl. internationale Bestellungen
Apple Pay / Google Pay	✅ Indirekt	Schutz hängt von hinterlegter Karte (Chargeback) ab
Giropay mit Händlergarantie	✅ Teilweise	Nur, wenn Händler im Garantieprogramm ist
Banküberweisung (SEPA)	❌ Nein	Kein Käuferschutz, nur freiwillige Rückzahlung durch Verkäufer
Vorkasse / Barzahlung	❌ Nein	Hohes Risiko bei unbekannten Verkäufern
Western Union / MoneyGram	❌ Nein	Kein Schutz, hohe Betrugsgefahr

Technische Schutzmaßnahmen für sicheres Online-Shopping

Passwörter und Zwei-Faktor-Authentifizierung

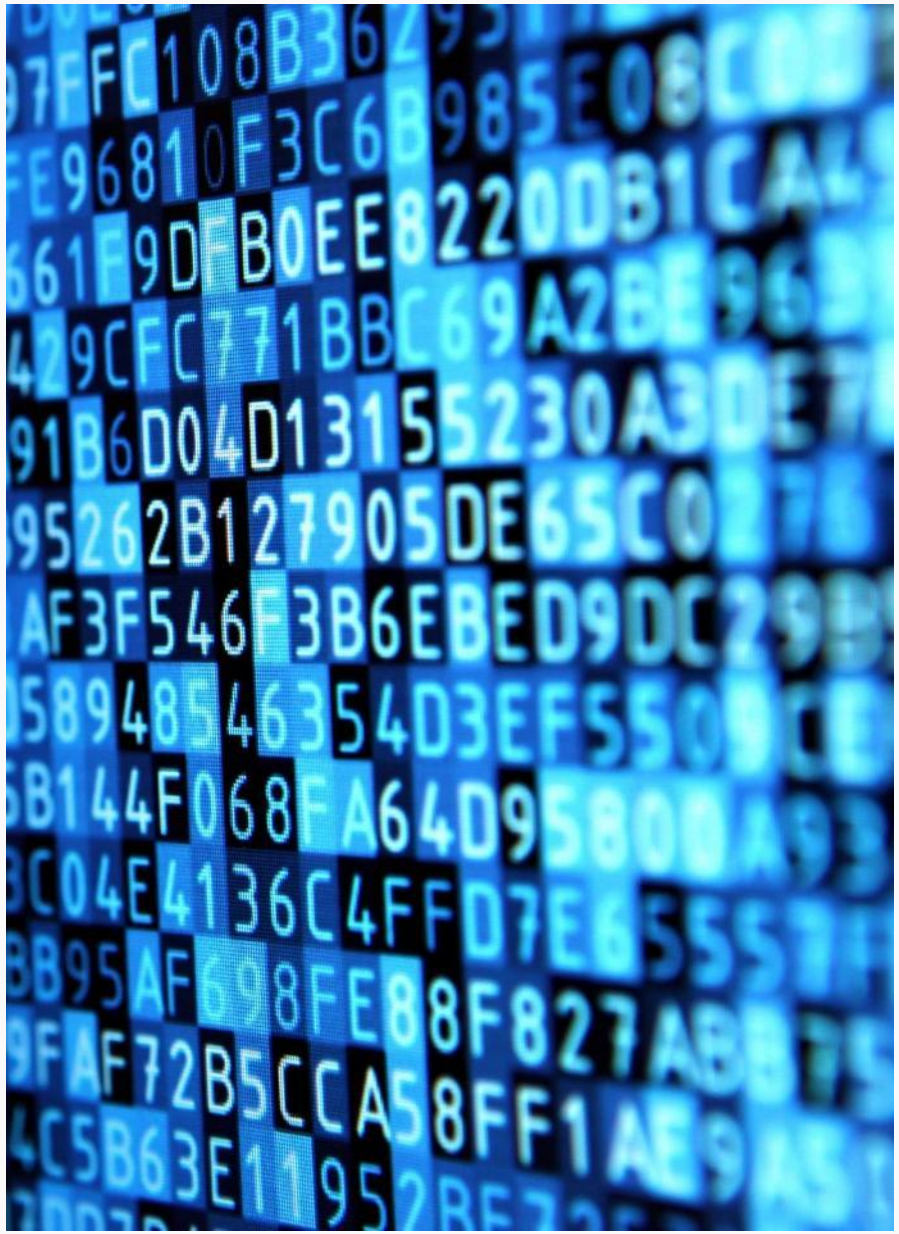
Starke individuelle Passwörter

Starke Passwörter sind lang, komplex und einzigartig für jedes Konto, um unbefugten Zugriff zu verhindern.

Zwei-Faktor-Authentifizierung aktivieren

Die Zwei-Faktor-Authentifizierung stärkt die Kontosicherheit durch eine zusätzliche Verifizierungsebene.

Wie lange brauchen Hacker, um Ihr Password zu hacken?				
Anzahl Zeichen	Nur Kleinbuchstaben	Mindestens 1 Großbuchstabe	mindestens 1 Großbuchstabe + Zahl	mindestens 1 Großbuchstabe + Zahl + Sonderzeichen
1	Sofort	Sofort	-	-
2	Sofort	Sofort	Sofort	-
3	Sofort	Sofort	Sofort	Sofort
4	Sofort	Sofort	Sofort	Sofort
5	Sofort	Sofort	Sofort	Sofort
6	Sofort	Sofort	Sofort	Sofort
7	Sofort	Sofort	1 Minute	6 Minuten
8	Sofort	22 Minuten	1 Stunde	8 Stunden
9	2 Minuten	19 Stunden	3 Tage	3 Wochen
10	1 Stunde	1 Monat	7 Monate	5 Jahre
11	1 Tag	5 Jahre	41 Jahre	400 Jahre
12	3 Wochen	300 Jahre	2.000 Jahre	34.000 Jahre
13	1 Jahr	16.000 Jahre	100.000 Jahre	2 Millionen Jahre
14	51 Jahre	800.000 Jahre	9 Millionen Jahre	200 Millionen Jahre
15	1.000 Jahre	43 Million Jahre	600 Millionen Jahre	15 Milliarden Jahre
16	34.000 Jahre	2 Milliarden Jahre	37 Milliarden Jahre	1 Billiarde Jahre



Sichere Passwörter

✅ **So machen Sie Ihr Passwort sicher:**

- Mindestens 12 Zeichen
- Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen verwenden
- Keine Namen, Geburtstage oder einfache Wörter
- Idealerweise für jeden Dienst ein eigenes Passwort

Sehr gutes Passwort:

IJ1973fid1MnP!

Ein Trick für sichere **UND** merkbare Passwörter ist die **Eselsbrücke**:

Merksatz: **I**m **J**ahr **1973** **f**uhr **i**ch **d**as **e**rste **M**al **n**ach **P**aris**!**

Passwort: **I J 1 9 7 3 f i d 1 M n P !**

14 Zeichen

Schutz am Gerät: Browser, Updates, Virenschutz

Browser und Betriebssystem aktuell halten

Regelmäßige Updates von Browser und Betriebssystem schließen Sicherheitslücken und verbessern den Schutz vor Schadsoftware.

Virenschutz verwenden

Ein aktueller Virenschutz erkennt und blockiert Schadsoftware effektiv und schützt persönliche Daten.

Sicheres Online-Shopping

Schutzmaßnahmen wie Updates und Virenschutz gewährleisten sichere Datenübertragung beim Online-Shopping.

Vorsicht bei öffentlichem WLAN und QR-Codes

Risiken beim öffentlichen WLAN

Öffentliche WLAN-Netzwerke sind oft unsicher und können persönliche Daten beim Online-Einkauf gefährden.

Vorsicht bei QR-Codes

Gefälschte QR-Codes können auf betrügerische Webseiten führen und persönliche Daten stehlen.

Im Ernstfall richtig handeln

Handlung bei Betrugsverdacht: was tun?

Sofortige Meldung

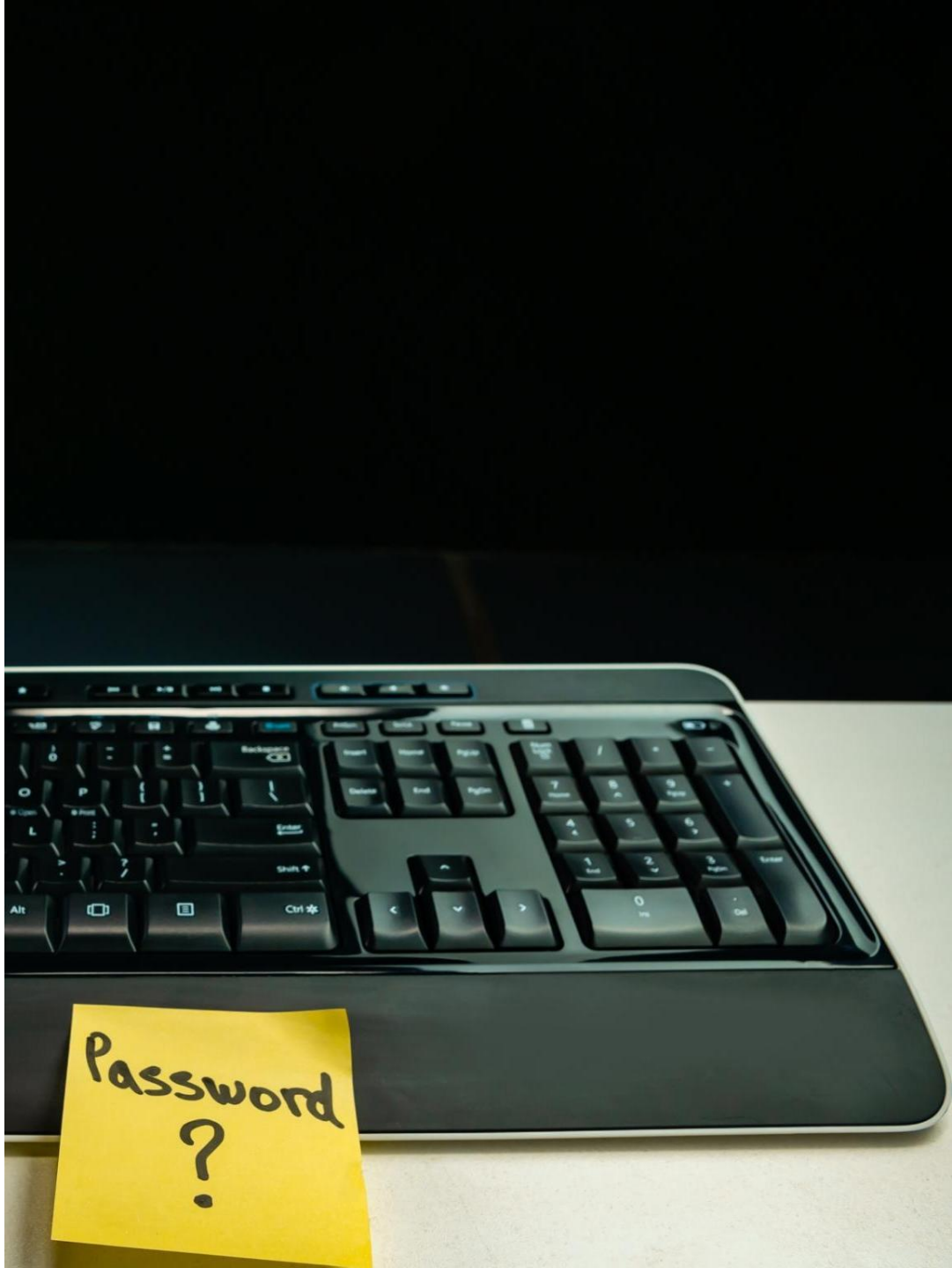
Betrugsfälle sollten unverzüglich der Bank, dem Online-Shop und der Polizei gemeldet werden, um schnellen Schutz zu gewährleisten.

Passwörter ändern

Nach einem Betrugsverdacht ist es wichtig, alle Passwörter sicher zu ändern, um weitere Zugriffe zu verhindern.

Sicherheitsmaßnahmen informieren

Informieren Sie sich über zusätzliche Sicherheitsmaßnahmen, um künftig Betrugsfälle zu vermeiden und den Schutz zu erhöhen.



Abschluss und Wiederholung

Abschluss und Checkliste (Handout-Folie)

Sorgfältige Shop-Prüfung

Überprüfen Sie Online-Shops gründlich, um Betrug zu vermeiden und sichere Einkäufe zu gewährleisten.

Sichere Zahlungsmethoden

Nutzen Sie vertrauenswürdige und geschützte Zahlungsoptionen beim Online-Einkauf.

Geräteschutz

Schützen Sie Ihre Geräte mit aktueller Software, um Risiken beim Online-Shopping zu minimieren.

Schnelles Handeln bei Verdacht

Reagieren Sie umgehend bei verdächtigen Aktivitäten, um Schäden zu verhindern.

Zusammenfassung: Sicher online einkaufen

Bewusstes Einkaufen

Senioren sollten beim Online-Shopping stets aufmerksam und vorsichtig sein, um Risiken zu vermeiden.

Technische Schutzmaßnahmen

Der Einsatz von Sicherheitssoftware und sicheren Netzwerken schützt vor Betrug und Datenverlust.

Vertrauenswürdige Shops

Nur geprüfte Online-Shops und sichere Zahlungsmethoden garantieren einen sicheren Einkauf.

Wie erkenne ich eine sichere Internetverbindung?

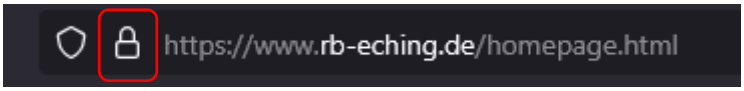
Wenn Sie eine Webseite besuchen – etwa Ihre Bank, eine Einkaufseite oder Ihr E-Mail-Konto – möchten Sie sicher sein, dass Ihre Daten **geschützt** sind. Eine sichere Internetverbindung sorgt dafür, dass niemand mitlesen kann, was Sie dort eingeben, z. B. Passwörter oder Kreditkartennummern.

Aber woran erkennt man, **ob eine Webseite sicher ist**?

Achten Sie auf das Schloss-Symbol 🔒

In der Adresszeile Ihres Browsers (also oben, wo die Internetadresse steht), sollte ein kleines Schloss-Symbol erscheinen. Es zeigt an, dass die Verbindung verschlüsselt, ist. Das bedeutet: Die Daten werden beim Versenden „verpackt", sodass niemand mitlesen kann.

Beispiel anhand der offiziellen Internet-Seite der Raiffeisenbank Buch-Eching eG im Browser **Firefox:**



⚠️ **Beispiel:** Gefälschte Adresse einer bekannten Bank

Stellen Sie sich vor, Sie möchten die Internetseite der **Sparkasse** besuchen. Die **echte** Adresse lautet:

☑ **https://www.sparkasse.de**

Nun erhalten Sie eine E-Mail, in der steht:

"Bitte melden Sie sich dringend über folgenden Link bei Ihrer Sparkasse an, um Ihr Konto zu schützen!"

Der Link in der Mail sieht so aus:

❌ **https://sparkasse-konto.sicher-login.info**

Oder auch:

❌ **https://sparkasse.de-kundensicherheit.net**

Beide Adressen **sehen auf den ersten Blick vertrauenswürdig aus**, sind aber **gefälscht**. Die Betrüger nutzen bekannte Namen und fügen z. B. „sicher", „login", „kundensupport" oder „konto" hinzu. Dadurch wirken die Seiten offiziell, sind aber **nicht von der echten Bank**.

🕵️ **So erkennen Sie den Unterschied:**

Die echte Adresse endet bei .de oder .com – und hat nichts Zusätzliches davor oder danach.

- → www.sparkasse.de ✅
- → www.sparkasse.de-login.net ❌

Gefälschte Seiten enthalten oft ungewöhnliche Wörter, viele Bindestriche oder fremde Domains (z. B. .info, .biz, .ru).

Prüfen Sie bei Unsicherheit immer direkt über die offizielle Startseite der Bank – geben Sie die Adresse von Hand ein oder speichern Sie sie als Lesezeichen.

Was ist ein Zertifikat auf einer Webseite?

Ein Zertifikat (genauer: ein SSL-/TLS-Zertifikat) ist ein digitales Dokument, das bestätigt, dass eine Webseite sicher ist und wirklich demjenigen gehört, der sie betreibt.

👉 Wichtig:

Wenn eine Webseite ein solches Zertifikat hat, wird die Verbindung zwischen deinem Gerät und der Webseite verschlüsselt. Das bedeutet: Niemand kann mitlesen – weder Passwörter noch persönliche Daten.

🔒 **Wie erkenne ich, ob eine Webseite ein gültiges Zertifikat hat?**

Du kannst das leicht in der **Adresszeile deines Internetbrowsers** erkennen (z. B. in Chrome, Firefox, Safari):

☑ **Zeichen für eine sichere Webseite:**

1. **Schloss-Symbol** links neben der Internetadresse
2. Die Adresse beginnt mit **https://** (das „s" steht für „secure" = sicher)

❌ **Zeichen für eine unsichere Webseite:**

- Kein Schloss
- Warnhinweis wie „Nicht sicher"
- Adresse beginnt nur mit **http://** (ohne „s")

🔍 **Wie prüfe ich das Zertifikat genauer?**

Wenn du wissen willst, **wer das Zertifikat ausgestellt hat** und ob es gültig ist:

So geht's in den gängigen Browsern:

🧿 **Google Chrome oder Microsoft Edge:**

1. Klicke auf das **Schloss-Symbol** links neben der Adresse.
2. Wähle „Zertifikat ist gültig" oder „Sicherheitsdetails".
3. Dort steht:
    - Für **welche Webseite** das Zertifikat gilt.
    - **Wer es ausgestellt hat** (z. B. DigiCert, Let's Encrypt).
    - **Bis wann es gültig ist**.

🦊 **Firefox:**

1. Klicke auf das **Schloss-Symbol**.
2. Dann auf „Verbindungsdetails" → „Weitere Informationen" → „Zertifikat anzeigen".

📱 **Auf dem Handy (z. B. im Chrome-Browser):**

- Auch hier kannst du auf das Schloss tippen – allerdings zeigen viele Smartphones nur eine einfache Sicherheitsinfo.

🕵 **Beispiele**

🔐 Sichere Webseite:

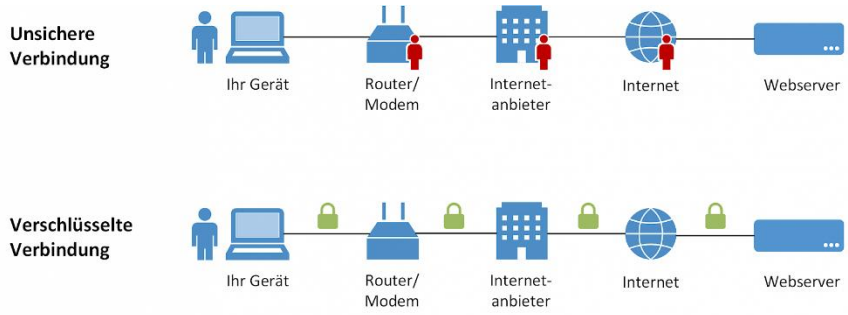
- https://www.deutsche-bank.de
  → Schloss-Symbol ✓
  → Adresse beginnt mit „https://“ ✓
  → Zertifikat: gültig und von einer offiziellen Stelle ✓

⚠️ Unsichere Webseite (Beispiel):

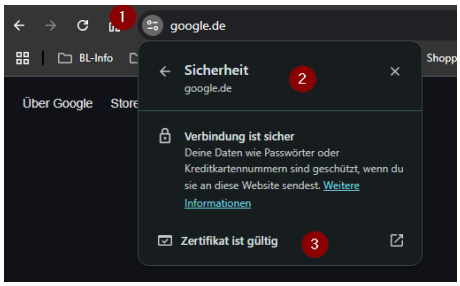
http://alte-beispielseite.de
→ Kein Schloss ❌
→ „Nicht sicher“-Hinweis ❌
→ Daten sind nicht geschützt ❌

So sehen beispielsweise sichere zertifizierte Seiten aus:

Unterschiede von unsichere und sicherer Verbindung:



Beispiel Google:



🧒💡 Tipps:

- **Nie persönliche Daten eingeben**, wenn kein Schloss zu sehen ist!

- Besonders bei **Online-Banking**, **Einkaufen** oder **E-Mails** immer auf das **https** und das **Schloss** achten.
- Bei Unsicherheiten lieber jemanden Fragen (Kinder, Enkel oder Nachbarn) oder die Seite meiden.

🧠 Merksatz:

"Wenn die Adresse komisch aussieht – nicht klicken!"

Achten Sie darauf, dass die Adresse mit https:// beginnt (nicht nur mit http://). Das „s" steht für „secure" – also „sicher".

⚠ Vorsicht bei Warnmeldungen

Moderne Browser wie Google Chrome, Firefox, Edge oder Safari warnen Sie oft, wenn eine Webseite unsicher oder sogar gefährlich ist. Dann sehen Sie z. B. eine rote Warnseite mit dem Hinweis „Diese Verbindung ist nicht sicher".

🧒 Tipp für Senioren:

Wenn Sie sich bei einer Seite nicht sicher sind, schließen Sie sie lieber und öffnen Sie sie später über eine vertrauenswürdige Quelle – z. B. die Startseite Ihrer Bank.

💡 Nutzen Sie keine öffentlichen WLANs für sensible Dinge

Öffentliche WLAN-Netze (z. B. im Café oder Bahnhof) sind oft nicht ausreichend gesichert. Vermeiden Sie darin:

- Online-Banking
- Einkäufe mit Kreditkarte
- Eingabe von Passwörtern
- Wenn Sie solche Dinge erledigen möchten, nutzen Sie lieber Ihr Heim-WLAN oder das mobile Netz Ihres Smartphones.

🛠 Noch sicherer mit diesen Tipps:

- **Halten Sie Ihren Browser immer aktuell.**
- **Installieren Sie ein gutes Virenschutzprogramm.**
- **Geben Sie vertrauliche Daten nur auf bekannten Seiten ein.**

🛍 Quellen & Empfehlungen:

BSI – Sicher im Netz: www.bsi-fuer-buerger.de

Verbraucherzentrale – Sichere Webseiten erkennen: www.verbraucherzentrale.de

Wie kann ich sicher im Internet einkaufen?

Sicheres Einkaufen im Internet ist wichtig, um persönliche Daten und Zahlungsmethoden zu schützen. Hier sind einige bewährte Schritte, die Sie befolgen können:

1. Verwendung von vertrauenswürdige Websites

Achten Sie auf die URL: Stelle sicher, dass die Webseite eine sichere Verbindung hat, indem die URL mit "https" beginnt (das "s" steht für Sicherheit).

Reputation prüfen: Kaufen Sie nur bei bekannten und vertrauenswürdigen Online-Shops oder großen Plattformen (z.B. Amazon, Zalando, eBay). Nutzen Sie Bewertungen und Rezensionen, um die Seriosität der Seite zu überprüfen.

Datenschutzerklärung lesen: Informieren Sie sich über die Datenschutzrichtlinien der Webseite, um sicherzustellen, dass Ihre persönlichen Daten geschützt sind.

2. Verwenden von sichere Zahlungsmethoden

Kreditkarte oder PayPal: Diese Zahlungsmethoden bieten in der Regel einen zusätzlichen Schutz. Besonders PayPal bietet Käuferschutz, falls etwas schief geht.

Keine Überweisungen an unbekannte Verkäufer: Vermeiden Sie direkte Banküberweisungen an unbekannte Händler, da dies bei Problemen schwer rückgängig gemacht werden kann.

Zwei-Faktor-Authentifizierung: Nutzen Sie, wenn möglich, eine zusätzliche Authentifizierungsmethode, wie eine TAN oder ein Fingerabdruck, um die Sicherheit deiner Zahlungen zu erhöhen. (Siehe auch nachfolgendes Kapitel: „Was ist Zwei-Faktor-Authentifizierung – und warum schützt sie mich?“

3. Achten auf Sicherheitszeichen

SSL-Zertifikate: Seiten mit einem SSL-Zertifikat (erkennbar an "https" und einem Schloss-Symbol in der URL-Leiste) bieten verschlüsselte Kommunikation, die Daten schützt.

Vertrauenssiegel: Achten Sie auf bekannte Vertrauenssiegel, wie z.B. "Trusted Shops" oder "EHI-Siegel". Diese zeigen, dass die Seite bestimmte Sicherheitsstandards erfüllt.

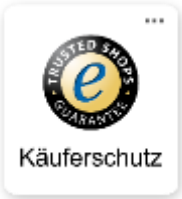
Was sind Trusted Shops?

Trusted Shops (Vertrauenswürdige Geschäfte) ist ein bekanntes Siegel, das Online-Shops in Europa erhalten können, um Vertrauen und Sicherheit zu vermitteln. Es stellt sicher, dass der Online-Shop bestimmte Sicherheits- und Qualitätskriterien erfüllt.

Wie funktioniert ein Trusted Shop?

Überprüfung des Shops: Trusted Shops prüft regelmäßig, ob ein Online-Shop sicher ist. Dazu gehören die Überprüfung von Datenschutzrichtlinien, allgemeinen Geschäftsbedingungen (AGB), Lieferbedingungen, Rückgaberechten und den Zahlungsmethoden. Ein Shop muss auch ein kundenfreundliches und faires Verhalten zeigen.

Das Trusted Shop Siegel sieht so aus:



Käuferschutz: Das Trusted Shops-Siegel bietet den Käufern zusätzlichen Schutz. Wenn Sie etwas bei einem zertifizierten Shop kaufen, sind Sie durch den Trusted Shops Käuferschutz abgesichert. Dies bedeutet, dass Sie Ihr Geld zurückerhalten können, wenn der Shop nicht liefert oder die Ware beschädigt ist. Der Käuferschutz greift auch bei Problemen mit der Rückerstattung von Rücksendungen.

Bewertungen: Trusted Shops ermöglicht es Käufern, Bewertungen abzugeben. Diese Bewertungen sind ein wichtiger Teil des Vertrauenssystems und helfen anderen Käufern, sich eine Meinung über den Shop zu bilden.

Zertifizierungskosten: Online-Shops müssen für die Zertifizierung durch Trusted Shops zahlen. Es gibt jedoch strenge Anforderungen, die erfüllt werden müssen, um das Siegel zu erhalten, was bedeutet, dass dieser Shop als vertrauenswürdig gilt.

Vorteile für den Verbraucher:

- **Käuferschutz**: Im Falle von Problemen bekommen Sie Ihr Geld zurück.
- **Vertrauen**: Das Trusted Shops-Siegel signalisiert, dass der Shop hohe Sicherheits- und Qualitätsstandards erfüllt.
- **Transparenz**: Trusted Shops bietet eine transparente Bewertung von Shops und Produkten.

EHI-Siegel

Was ist das EHI-Siegel? Das EHI-Siegel wird vom EHI Retail Institute, einer renommierten deutschen Forschungseinrichtung, vergeben. Es ist ein weiteres Sicherheitszeichen, das Online-Shops erhalten können, wenn sie hohe Anforderungen in Bezug auf Sicherheit, Service und Qualität erfüllen.

Das EHI-Siegel sieht so aus:

Wie funktioniert das EHI-Siegel?

Überprüfung und Zertifizierung: Das EHI-Siegel wird an Online-Shops vergeben, die sich einer umfassenden Prüfung unterziehen müssen. Diese Prüfung umfasst sowohl rechtliche als auch sicherheitstechnische Aspekte des Online-Shops. Dazu gehören Datenschutz, Versandbedingungen, Rückgaberechte, Zahlungsmethoden und die IT-Sicherheit.

Regelmäßige Audits: Ein EHI-zertifizierter Shop wird regelmäßig überprüft, um sicherzustellen, dass er weiterhin den hohen Standards entspricht.

Verbraucherschutz: Das EHI-Siegel steht für hohe Verbraucherfreundlichkeit. Shops, die dieses Siegel tragen, bieten transparente Geschäftsbedingungen und fairen Kundenservice. Dazu gehört auch ein klarer Prozess für Rücksendungen und Rückerstattungen.

Vorteile für den Verbraucher:

Rechtliche Sicherheit: Shops mit dem EHI-Siegel erfüllen die deutschen Verbraucherrechte, was dir als Käufer zusätzliche Sicherheit gibt.

Verbraucherschutz: Das Siegel stellt sicher, dass der Shop alle gesetzlichen Anforderungen im Hinblick auf Datenschutz, Preisangaben und Zahlungsbedingungen erfüllt.

Verlässlichkeit: EHI-zertifizierte Shops müssen regelmäßig Audits bestehen, was das Vertrauen in den Shop erhöht.

Unterschiede zwischen Trusted Shops und EHI-Siegel

Trusted Shops bietet in erster Linie Käuferschutz und ermöglicht die Abgabe von Bewertungen durch Kunden. Es ist stärker auf den Kundenschutz fokussiert und umfasst zusätzliche Dienste wie eine Geld-zurück-Garantie.

Das EHI-Siegel legt mehr Wert auf die Einhaltung von rechtlichen Anforderungen und den Verbraucherschutz. Es stellt sicher, dass der Shop die notwendigen gesetzlichen Vorschriften einhält und regelmäßig überprüft wird, bietet jedoch keinen expliziten Käuferschutz wie Trusted Shops.

Wie Sie das Siegel erkennen:

Trusted Shops: Sie finden das Trusted Shops-Siegel oft im Fußbereich der Seite oder auf Produktseiten. Es ist auch häufig als Logo mit der Aufschrift "Trusted Shops" sichtbar. Wenn Sie auf das Siegel klicken, bekommen Sie Informationen zur Zertifizierung des Shops. **Wichtiger Hinweis:** Das Siegel muss man anklicken können und dort auf die entsprechende Seite weitergeleitet werden, es darf **kein Bild** sein!

EHI-Siegel: Das EHI-Siegel ist ein rundes Logo mit dem Schriftzug "EHI geprüfter Online-Shop". Auch dieses Siegel ist meist am Ende der Seite oder auf der „Über uns"-Seite des Shops zu finden.

Wichtiger Hinweis: Das Siegel muss man anklicken können und dort auf die entsprechende Seite weitergeleitet werden, es darf **kein Bild** sein!

Fazit

Beide Siegel bieten zusätzliche Sicherheit beim Online-Einkauf. Trusted Shops eignet sich besonders, wenn Sie zusätzlichen Schutz für Ihren Einkauf suchen, während das EHI-Siegel Vertrauen in die Einhaltung rechtlicher und sicherheitsrelevanter Standards des Shops gibt. Beide Siegel tragen dazu bei, dass Sie mit einem sicheren Gefühl einkaufen können.

Wenn Sie beim Online-Shopping auf eines dieser Siegel stoßen, können Sie sicherer sein, dass der Shop überprüft wurde und hohe Standards in Bezug auf Service, Sicherheit und Verbraucherschutz einhält.

4. Achten Sie auf die Versand- und Rückgabebedingungen

Rückgaberecht: Überprüfen, ob der Online-Shop ein Rückgaberecht bietet, falls die Ware nicht Ihren Erwartungen entspricht oder defekt ist.

Lieferbedingungen: Achten Sie auf die Versandkosten und Lieferzeiten. Seriöse Shops bieten transparente Informationen zu diesen Themen.

5. So erkennen Sie einen Fake-Shop

Keine oder unvollständige Impressumsangaben

→ Ein seriöser Online-Shop hat ein vollständiges Impressum (mit Name, Adresse, Telefonnummer und E-Mail-Adresse).

Unglaubwürdig günstige Preise

→ Wenn Produkte deutlich unter dem Marktwert verkauft werden, ist das ein Warnzeichen.

Nur Vorkasse als Zahlungsmethode

→ Fehlen Optionen wie PayPal, Kreditkarte oder Kauf auf Rechnung, ist Vorsicht geboten.

Fehlende oder schlechte Kundenbewertungen

→ Prüfen Sie unabhängige Bewertungsseiten wie Trustpilot oder Google Reviews.

Fehlerhafte Sprache

→ Viele Fake-Shops haben schlecht übersetzte Texte oder ungewöhnliche Formulierungen.

Webadresse (URL)

→ Oft sind die Domains ungewöhnlich, z. B. mit exotischen Endungen oder Zahlencodes (z. B. shop12345.biz).

Webseiten zur Shop-Überprüfung

www.watchlist-internet.at

- Bietet aktuelle Warnungen vor Fake-Shops.
- Möglichkeit zur Meldung und Prüfung verdächtiger Seiten.

www.fakeshop-finder.de (vom Bayerischen Verbraucherschutzministerium)

- Einfach URL eingeben → automatische Prüfung.
- Ampelsystem: grün = sicher, rot = gefährlich.

www.verbraucherzentrale.de

- Dort findest du eine Fake-Shop-Liste und weitere Ratgeber.
- Möglichkeit zur Meldung von Betrugsfällen.

◐ **Zusätzlicher Tipp**

Nutze beim Online-Shopping Browser-Add-ons, wie:

- Web of Trust (WOT) → bewertet Websites anhand von Nutzerfeedback.
- Trusted Shops Badge → Shops mit Gütesiegel sind meist geprüft.

Wie bezahle ich sicher mit PayPal oder anderen Online-Diensten?

Das Bezahlen mit PayPal und anderen Online-Zahlungsdiensten ist eine bequeme und sichere Möglichkeit, um Einkäufe im Internet zu tätigen. Allerdings gibt es bestimmte Maßnahmen, die Sie ergreifen können, um sicherzustellen, dass Ihre Zahlungen geschützt sind. Hier sind einige bewährte Schritte, die Sie befolgen können:

1. Verwendung vertrauenswürdiger Online-Zahlungsdienste

PayPal ist eine der beliebtesten und sichersten Zahlungsmethoden, da sie Ihren Zahlungsverkehr schützen und keine sensiblen Finanzdaten direkt an den Händler weitergibt. Auch andere Dienste wie Stripe oder Apple Pay bieten hohe Sicherheitsstandards.

Achten Sie auf die Qualität des Anbieters: Nutzen Sie nur bekannte Zahlungsdienste, die hohe Sicherheitsstandards haben und von großen Online-Shops oder etablierten Plattformen verwendet werden.

2. Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA)

Schützen Sie Ihr PayPal-Konto mit 2FA: Aktivieren Sie die Zwei-Faktor-Authentifizierung für Ihr PayPal-Konto, um zusätzliche Sicherheit zu bieten. So benötigen Sie neben Ihrem Passwort einen zusätzlichen Code (z.B. aus einer Authentifizierungs-App oder per SMS), um sich einzuloggen.

Schutz vor unbefugtem Zugriff: Wenn jemand Ihr Passwort stiehlt, ist der Zugriff auf Ihr Konto trotzdem durch den zweiten Faktor gesichert.

3. Nutzen Sie eine sichere Internetverbindung

WLAN und öffentliche Netzwerke: Vermeiden Sie es, Zahlungen über öffentliche WLAN-Netzwerke oder unsichere Verbindungen zu tätigen. Öffentliche Netzwerke sind anfällig für Angriffe, und ein Angreifer könnte versuchen, Ihre Zahlungsdaten abzufangen.

VPN verwenden: Wenn Sie von öffentlichen Netzwerken aus einkaufen, können Sie ein VPN (Virtual Private Network) verwenden, um Ihre Internetverbindung zu verschlüsseln und Ihre Daten zu schützen. Nützliche benutzerfreundliche VPN-Anbieter aus Deutschland oder mit deutscher Oberfläche:

- **CyberGhost** – deutschsprachig, sehr einsteigerfreundlich, viele Server.
- **ZenMate** – deutscher Anbieter, einfache Bedienung, gut für Alltagssurfer.
- **NordVPN** – international, aber komplett auf Deutsch verfügbar, viele Sicherheitsfunktionen.
- **Avira Phantom VPN** – vom deutschen Antivirus-Hersteller Avira, schlicht und leicht zu nutzen.

4. Achten Sie auf die Adresse der Webseite (URL)

HTTPS: Stellen Sie sicher, dass die Webseite, auf der Sie einkaufen, „https" in der URL verwendet und ein kleines Schloss-Symbol in der Adressleiste Ihres Browsers angezeigt wird. Dies bedeutet, dass die Verbindung verschlüsselt und sicher ist.

Kein **„http" ohne „s":** Webseiten, die kein „https" haben, sind nicht sicher, und deine Zahlungsdaten könnten abgefangen werden.

5. Zahlen Sie nur bei vertrauenswürdigen Händlern

Vertrauenssiegel und Bewertungen: Kaufen Sie nur bei Händlern, die gut bewertet sind und vertrauenswürdige Siegel wie Trusted Shops oder EHI-Siegel haben. Diese Siegel garantieren, dass der Händler geprüft wurde und Sie geschützt sind.

Überprüfen Sie den Händler: Wenn Sie bei einem unbekannten Online-Shop einkaufen, schauen Sie sich Kundenbewertungen an und prüfen, ob der Händler eine gültige Rückgabe- und Datenschutzrichtlinie hat.

6. Achten Sie auf die Sicherheit Ihrer PayPal- oder Kontoinformationen

Phishing vermeiden: Betrüger könnten versuchen, Sie mit gefälschten E-Mails oder Nachrichten dazu zu bringen, Ihre Login-Daten preiszugeben. PayPal und andere seriöse Zahlungsdienste werden Sie niemals per E-Mail auffordern, auf Links zu klicken oder sensible Informationen einzugeben.

Direkt einloggen: Gehen Sie immer direkt auf die Webseite von PayPal (oder dem Zahlungsdienst Ihrer Wahl), anstatt Links aus E-Mails zu folgen. Idealerweise haben Sie sich in dem Browser Ihre eigenen Favoritenliste gespeichert. So vermeiden Sie Phishing-Angriffe.

7. Nutzen Sie die Käuferschutzfunktionen

PayPal Käuferschutz: Einer der größten Vorteile von PayPal ist der Käuferschutz. Wenn etwas mit Ihrer Bestellung nicht stimmt (z.B. der Artikel kommt nicht an oder entspricht nicht der Beschreibung), können Sie eine Rückerstattung über PayPal beantragen.

Rückerstattung sicherstellen: Überprüfen, ob der Händler ebenfalls ein Rückgaberecht anbietet, um Sie abzusichern, falls der Artikel defekt ist oder nicht wie beschrieben.

8. Behalten Sie Ihre Kontobewegungen im Auge

Regelmäßige Kontrolle: Überprüfen Sie regelmäßig Ihr PayPal-Konto oder das Konto Ihres Online-Zahlungsdienstes auf ungewöhnliche Aktivitäten. Wenn Sie eine unbekannte Zahlung sehen, sollten Sie sofort reagieren und den Anbieter kontaktieren.

Benachrichtigungen aktivieren: Stellen Sie sicher, dass Sie Benachrichtigungen für alle Zahlungen und Transaktionen erhalten, sodass Sie sofort informiert werden, wenn es zu einer nicht autorisierten Zahlung kommt.

9. Vermeiden Sie das Speichern von Zahlungsinformationen

Nicht speichern lassen: Viele Online-Shops bieten an, Ihre Zahlungsinformationen für zukünftige Einkäufe zu speichern. Dies ist zwar bequem, aber es kann zu Sicherheitsrisiken führen, wenn ein Hacker Zugang zu Ihren Konto erhält. Geben Sie Ihre Zahlungsinformationen lieber jedes Mal manuell ein.

Alternativen wie virtuelle Kreditkarten: Sie könnenauch eine virtuelle Kreditkarte verwenden, die nur für einmalige Zahlungen verwendet wird und keine direkten Bankdaten speichert.

Beispiele zur sicheren Zahlung mit PayPal oder anderen Online-Diensten:

Beispiel 1: Einkauf bei einem bekannten Online-Shop (z.B. Amazon)

Sie möchten ein Produkt auf Amazon kaufen. Sie wählen PayPal als Zahlungsmethode und geben Ihre PayPal-Anmeldedaten ein.

Nachdem Sie Ihr Passwort eingegeben haben, erhalten Sie einen einmaligen Code auf Ihr Handy, den Sie eingeben (Zwei-Faktor-Authentifizierung).

Sie überprüfen die HTTPS-Verbindung der Amazon-Webseite (die URL beginnt mit „https://“ und es erscheint ein Schlosssymbol in der Browserleiste).

Ihre PayPal-Transaktion wird durch den Käuferschutz gesichert, falls etwas mit der Lieferung schiefgeht.

Beispiel 2: Bezahlung bei einem weniger bekannten Online-Shop

Sie sind auf einem Online-Shop, der PayPal als Zahlungsmethode anbietet. Sie überprüfen, ob die Webseite mit einem sicheren HTTPS-Protokoll verschlüsselt ist.

Nachdem Sie Ihre Bestellung abgeschlossen haben, werden Sie zur PayPal-Seite weitergeleitet. Sie geben Ihre PayPal-Anmeldedaten ein und bestätigen die Zahlung.

Falls der Artikel nie ankommt oder nicht wie beschrieben ist, können Sie den Käuferschutz von PayPal aktivieren, um Ihr Geld zurückzuerhalten.

Fazit:

Die Zahlung mit PayPal und anderen Online-Zahlungsdiensten ist eine sehr sichere Methode, um Einkäufe im Internet zu tätigen, wenn Sie einige grundlegende Sicherheitsvorkehrungen beachten. Durch die Zwei-Faktor-Authentifizierung, die Auswahl eines vertrauenswürdigen Händlers, und die Vermeidung von Phishing-Angriffen können Sie Ihre Zahlungen effektiv absichern. Die Käuferschutzfunktionen sorgen dafür, dass Sie im Fall von Problemen mit der Bestellung Ihr Geld zurückbekommen.