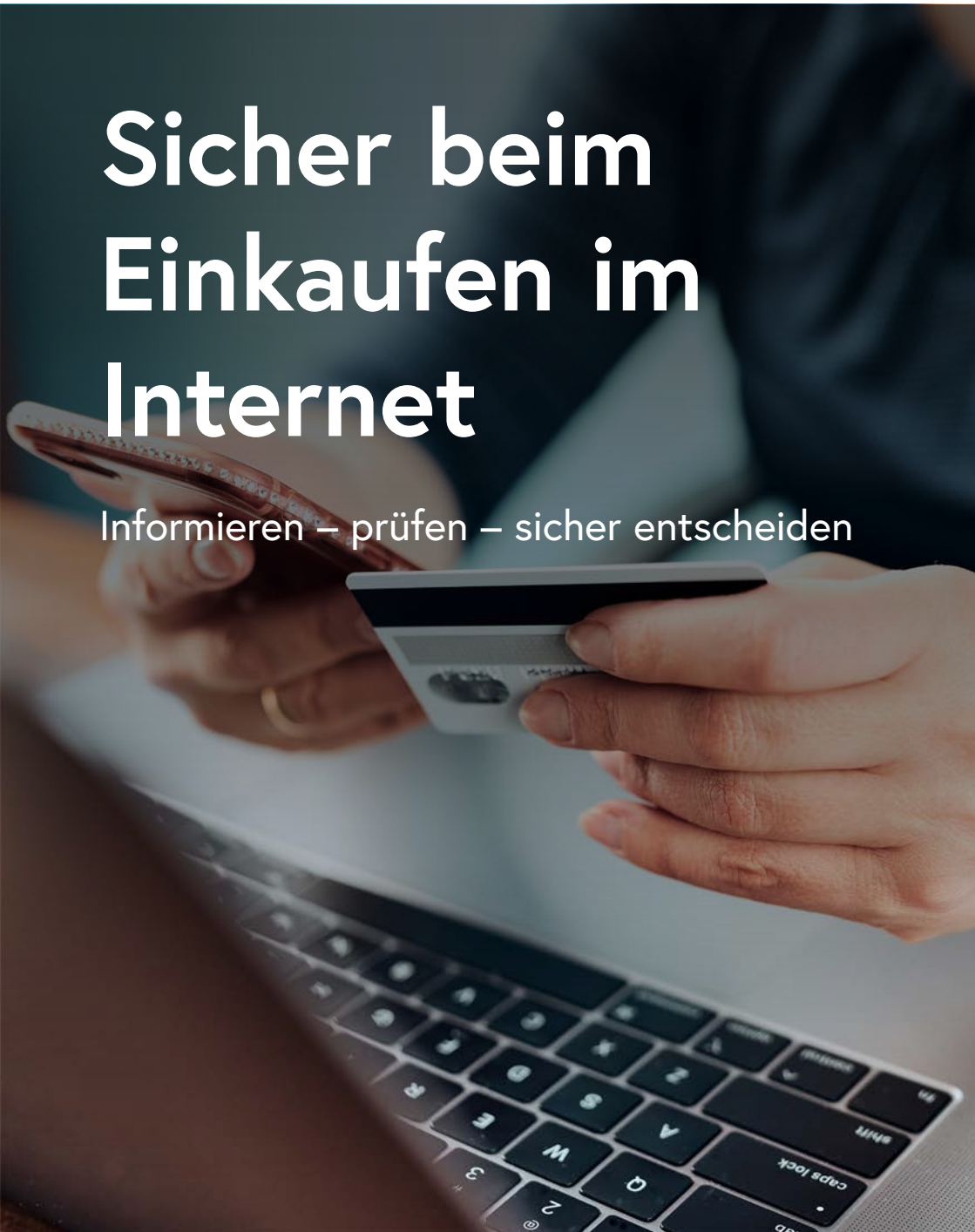
Bundesministerium
Inneres
Bundeskriminalamt

KRIMINAL
PRÄVENTION

Sicher beim Einkaufen im Internet

Informieren – prüfen – sicher entscheiden



Sicher beim Einkaufen im Internet

Informieren – prüfen – sicher entscheiden

Wien, 2026

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
Bundeskriminalamt
Josef-Holaubek-Platz 1, 1090 Wien
www.bmi.gv.at
Autorinnen und Autoren: Bundeskriminalamt – Kriminalprävention und Opferhilfe
Layout: BMI I/C/10/a – Strategische Kommunikation und Kreation
Druck: BMI Digitalprintcenter
Foto Titelbild: © Adobe Stock/Przemek Klos
Wien, 2026

Inhalt

1 Betrügerische Online-Shops („Fake Shops“) 5

2 Betrug auf Verkaufsplattformen 7

3 Das Gütesiegel 9

4 Zahlungssicherheit beim Online-Einkauf 10

5 Identitätsmissbrauch 12

6 Hilfe im Schadensfall 14

7 Fünf kompakte Tipps 15

8 Weitere Informationen 16

Der Einkauf im Internet boomt und damit auch der digitale Betrug. Online-Shops bieten Waren zu Schnäppchenpreisen an. Tatsächlich wird aber das Geld der Kundinnen und Kunden abkassiert oder die eigenen Daten dreist missbraucht.

© Adobe Stock/Daniel

1 Betrügerische Online-Shops („Fake Shops“)

Online-Shopping ist bequem, aber auch ein häufiges Einfallstor für Betrug. Besonders sogenannte Fake-Shops wirken auf den ersten Blick seriös, bieten attraktive Preise und nutzen täuschend echte Webseiten. Ziel ist, Kundinnen und Kunden zur Zahlung zu bewegen, ohne die Ware zu liefern.

Betrugsseiten erkennen – so geht‘s

- Ungewöhnlich günstige Preise (deutlich unter Marktwert)
- Nur Vorkasse möglich (kein Kauf auf Rechnung oder sichere Zahlungsarten)
- Negative oder fehlende Bewertungen im Internet
- Unklare oder fehlende Kontaktmöglichkeiten
- Fehlendes oder unvollständiges Impressum
- Druck durch angebliche „letzte Stücke“ oder Countdown-Timer
- Webadresse wirkt ungewöhnlich oder leicht verfälscht (z. B. bekannte Marke mit Tippfehler)

Präventionsempfehlungen der Polizei

- Preise vergleichen und bei extremen Schnäppchen skeptisch bleiben
- Nur sichere Zahlungsarten nutzen (z. B. Kauf auf Rechnung, Kreditkarte mit Käuferschutz) – Achtung bei Vorkasse
- Bewertungen und Erfahrungen anderer Käuferinnen und Käufer recherchieren
- Impressum und Anbieter genau prüfen (Adresse, Firma, Kontakt)
- URL genau kontrollieren (Tippfehler oder verdächtige Domains)
- Im Zweifel auf bekannte und etablierte Shops zurückgreifen
- Konto- und Zahlungsbewegungen regelmäßig überprüfen
- Verdächtige Shops melden (z. B. Watchlist Internet)

© BMI/Tobias Bosina

2 Betrug auf Verkaufsplattformen

Kleinanzeigenplattformen im Internet funktionieren wie digitale Flohmärkte und bieten Privatpersonen die Möglichkeit, gebrauchte Gegenstände zu verkaufen oder günstig zu erwerben. Gleichzeitig nutzen Betrügerinnen und Betrüger diese Plattformen gezielt: Sie kassieren Zahlungen ohne Lieferung, bieten mangelhafte Ware an oder täuschen als Käuferin bzw. Käufer eine Zahlung vor, um an die Ware zu gelangen. Besonders risikoreich sind Situationen, in denen die Kommunikation auf externe Kanäle verlagert wird, Zahlungen ins Ausland erfolgen sollen oder komplizierte Zahlungs- und Versandmodalitäten gefordert werden.

Typische Maschen:

Vorkasse-Betrug

Käuferinnen und Käufer werden zur Vorauszahlung aufgefordert, die Ware wird jedoch nie geliefert. Häufig wird Druck aufgebaut und eine persönliche Abholung ausgeschlossen.

Überzahlungs-Masche

Eine angebliche Käuferin bzw. ein angeblicher Käufer überweist zu viel Geld oder sendet eine gefälschte Zahlungsbestätigung und fordert die Rücküberweisung des „Überschusses“. Die ursprüngliche Zahlung ist jedoch nicht echt oder wird rückgebucht.

Betrugsangebote erkennen – so geht‘s

- Wechsel der Kommunikation auf WhatsApp, SMS oder private E-Mail
- Verständigung nicht in der Sprache des Angebots
- Ausschließlich Vorkasse oder ungewöhnliche Zahlungsarten
- Zeitdruck („schnell entscheiden“, „sofort überweisen“) Aufforderung zu Versand, Zahlung oder Abwicklung ins Ausland
- Keine persönliche Abholung möglich oder ausdrücklich unerwünscht
- Unstimmige Zahlungsdaten (z. B. abweichender Kontoinhaber)
- Verwendung angeblicher Treuhandservices über zugesandte Links

Präventionsempfehlungen der Polizei

- Skeptisch bei ungewöhnlich günstigen Angeboten bleiben
- Kommunikation ausschließlich über die Plattform führen
- Bevorzugt persönliche Übergabe mit Barzahlung nutzen
- Sich nicht unter Zeitdruck setzen lassen
- Keine Vorkasse bei unbekannten Personen leisten
- Keine Zahlungen oder Lieferungen ins Ausland ohne Absicherung
- Keine sensiblen Daten oder Dokumente weitergeben
- Zahlungseingänge tatsächlich am Konto prüfen (nicht auf Bestätigungen verlassen)

3 Das Gütesiegel

Gütesiegel können beim Online-Einkaufen eine hilfreiche Orientierung bieten, um seriöse Anbieter zu erkennen. Viele vertrauenswürdige Shops lassen sich freiwillig zertifizieren und erfüllen bestimmte Qualitäts- und Sicherheitsstandards. In Österreich sind z. B. das Österreichische E-Commerce-Gütezeichen oder das von „Trusted Shops“ verbreitet.
Allerdings nutzen auch Betrügerinnen und Betrüger gefälschte oder kopierte Siegel, um Seriosität vorzutäuschen. Deshalb ein wichtiger Hinweis: Echte Gütesiegel sind anklickbar und führen direkt zur offiziellen Prüfseite, auf der der Shop gelistet ist.

Vorteile von Gütezeichen:

- ein klar nachvollziehbarer Bestellprozess
- umfassende Angaben zu Preisen, Vertragsbedingungen, Lieferung usw.
- der Schutz persönlicher Daten
- sichere Zahlung im Shop

4 Zahlungssicherheit beim Online-Einkauf

Beim Einkaufen im Internet kann man leicht Geld verlieren, wenn man eine unsichere Bezahlmethode benutzt. Deshalb sollte man nur sichere Zahlungsarten wählen und vorsichtig sein. Besonders Vorkasse-Zahlungen per Überweisung sind problematisch, da das Geld nach der Zahlung meist nicht mehr zurückgeholt werden kann. Betrügerinnen und Betrüger nutzen solche Zahlungsarten, weil sie schwer nachvollziehbar sind. Deutlich mehr Sicherheit bieten hingegen Zahlungsmethoden mit Käuferschutz oder Rückbuchungsmöglichkeiten. Daher ist ein bewusster Umgang mit der gewählten Zahlungsart notwendig.

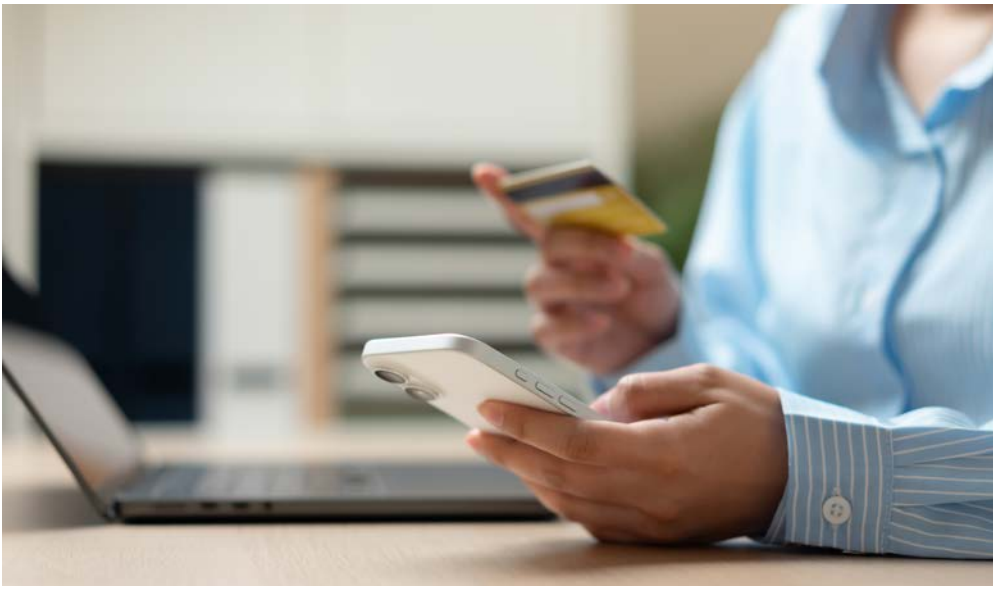
Zahlungsbetrug erkennen – so geht‘s

- Druck, schnell zu bezahlen
- Ausschließlich Vorkasse (Überweisung vor Warenerhalt)
- Aufforderung zur Zahlung mit Kryptowährungen
- Nutzung von Geldtransferdiensten
- Keine Option für Kauf auf Rechnung oder Käuferschutz
- Ungewöhnliche oder komplizierte Zahlungsabwicklung
- Zahlung an ausländische oder unbekannte Konten

Präventionsempfehlungen der Polizei

- Kauf auf Rechnung bevorzugen (Bezahlung erst nach Erhalt der Ware)
- Kreditkarte nutzen (gute Rückholmöglichkeit)
- Etablierte Bezahldienste mit Käuferschutz verwenden (z. B. PayPal)
- SEPA-Lastschrift als sichere Alternative in Betracht ziehen
- Keine Vorkasse bei unbekannten oder unseriösen Anbietern leisten
- Keine Zahlungen mit Kryptowährungen oder Bargeldtransferdiensten durchführen
- Zahlungsbedingungen vor dem Kauf genau prüfen

© Adobe Stock/Father_Studio



5 Identitätsmissbrauch

Der Online-Kauf ist zwar bequem, birgt jedoch Risiken durch Datenmissbrauch. Kriminelle nutzen täuschend echte Nachrichten, um an persönliche Daten zu gelangen und diese für betrügerische Bestellungen zu verwenden. Häufig geschieht dies über „Phishing“ (E-Mail) oder „Smishing“ (SMS), bei denen ein dringender Handlungsbedarf vorgetäuscht wird – etwa eine angeblich fehlgeschlagene Paketzustellung oder Aktualisierung ihres Benutzerkontos. Die enthaltenen Links führen zu gefälschten Webseiten, auf denen Sie Ihre persönlichen Daten (Name, Adresse, Geburtsdatum oder Bankverbindungen) eingeben und diese abgegriffen werden. Die Folgen reichen von unberechtigten Abbuchungen bis hin zu Bestellungen im Namen der Betroffenen.

Datenklau: Warnhinweise

- Unerwartete Nachrichten zu angeblichen Bestellungen oder Lieferproblemen
- Dringender Handlungsdruck oder Drohungen („sofort bestätigen“, „sonst Rücksendung“)
- Die E-Mail oder SMS enthält Links zu Webseiten
- Aufforderung zur Eingabe von Zugangsdaten oder Bankdaten
- Unpersönliche Anrede („Sehr geehrter Kunde“)

Präventionsempfehlungen der Polizei

- Links in E-Mails oder SMS nicht unüberlegt anklicken
- Absender und Internetadresse genau prüfen
- Webseiten von Online-Shops oder Paketdiensten direkt im Browser aufrufen
- Bei Unsicherheit Kontakt über offizielle Kanäle aufnehmen
- Keine sensiblen Daten bei unbekannten oder verdächtigen Seiten eingeben
- Nicht unter Druck setzen lassen
- Regelmäßig Konto- und Kreditkartenbewegungen kontrollieren
- Zwei-Faktor-Authentifizierung nutzen
- Verdächtige Nachrichten löschen und melden

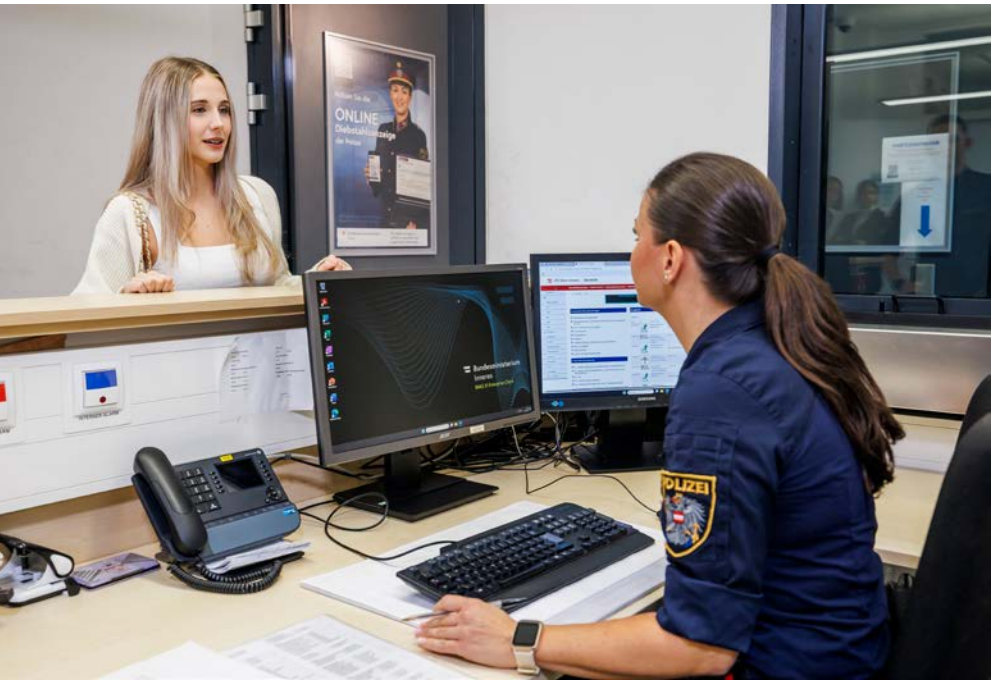
© Adobe Stock/fadfebrian

6 Hilfe im Schadensfall

- Umgehend Bank/Kreditkartenanbieter/Zahlungsdienst informieren
- Versuch der Rückbuchung (Chargeback) einleiten
- Sofort Anzeige bei der Polizeiinspektion erstatten
- Alle Unterlagen sichern und mitnehmen (wie Bestellbestätigungen, E-Mails, Screenshots, Zahlungsnachweise – möglichst im Original)
- Sollte ein technisches Gerät betroffen sein, bringen Sie es nach Möglichkeit mit zur Polizei (z. B. Handy, Laptop etc.)
- Kontobewegungen laufend kontrollieren

Schnelles Handeln erhöht die Chance auf Schadensbegrenzung und Rückerstattung!

© BMI/Gerd Pachauer



7 Fünf kompakte Tipps

1. Nur bei vertrauenswürdigen Online-Shops einkaufen
2. Preise vergleichen und unrealistische Angebote meiden
3. Bewertungen und Erfahrungen anderer Käuferinnen und Käufer prüfen
4. Auf sichere Zahlungsmethoden und HTTPS achten
5. Persönliche Daten sparsam weitergeben

8 Weitere Informationen

www.onlinesicherheit.gv.at
www.oesterreich.gv.at
www.watchlist-internet.at
www.guetezeichen.at
www.konsument.at
www.ombudsstelle.at
www.arbeiterkammer.at
www.trustmark-austria.at