

Fake-Shops entlarven

Hintergründe, Warnsignale und die schnelle Kontrolle vor dem Bezahlen.

Shop / Domain: _____

Datum: _____

Jede und jeder Vierte in Österreich war bereits von Cyberkriminalität betroffen. Fake-Shops sind nur eine ihrer Formen. Die Schadenssummen bewegen sich jährlich im zweistelligen Millionenbereich, und sie wachsen, weil der Vormarsch der künstlichen Intelligenz Menschen mit krimineller Energie immer schneller scheinbar perfekte Webseiten mit verlockenden Lockangeboten erstellen lässt.

Das Prinzip dahinter bleibt jedoch immer dasselbe: Ein unschlagbarer Preis, ein tickender Countdown, ein angeblich nur noch spärlich gefüllter Lagerbestand. All das soll unseren rationalen Verstand abschalten und unser Stammhirn übernehmen lassen, jene Instanz in uns, die Schnäppchen jagt wie einen schnellen Dopamin-Kick, ohne lange zu fragen, wer da eigentlich am anderen Ende der Leitung sitzt. Wer einmal bezahlt hat, meist per Vorkasse oder Sofortüberweisung, wartet oft für immer auf seine Ware, während der Shop längst wieder im digitalen Nirwana verschwunden ist.

Besonders perfide agieren Betrüger inzwischen auch über Social-Media. Meist sind es rührselige Geschichten von angeblich schließenden Familienunternehmen oder aber unglaubliche Rabatte auf Markenware, die selbst erfahrene Konsumentinnen und Konsumenten in die Falle locken. Auch auf privaten Verkaufsplattformen hat sich eine neue Masche etabliert: weg von der sicheren Plattform-Kommunikation, hin zu Nachrichtendiensten wie WhatsApp, wo Druck aufgebaut und zur Zahlung per „Freunde & Familie“ gedrängt wird. Der Käuferschutz ist dann verschwunden, noch bevor wir ihn gebraucht hätten.

Doch wir sind diesen Machenschaften nicht schutzlos ausgeliefert. Das Impressum ist und bleibt unser erster Realitätscheck. Fehlt es oder lässt es sich nicht anklicken, haben wir meist schon einen Fake-Shop entlarvt. Gütesiegel wie das Österreichische E-Commerce-Gütezeichen oder das Trusted-Shops-Siegel bieten zusätzliche Orientierung, vorausgesetzt, wir klicken sie auch tatsächlich an, denn selbst ein Siegel-Logo lässt sich leicht kopieren und auf einer betrügerischen Seite platzieren.

Und sollten wir trotz aller Vorsicht in die Falle tappen, entscheidet die gewählte Zahlungsart über unser Schicksal. Bei der Kreditkarte rettet uns oft das Chargeback-Verfahren, bei SEPA-Lastschrift können wir sogar acht Wochen lang ohne Angabe von Gründen widersprechen. Wichtig ist nur eines: rasch handeln, statt zu hoffen. Dabei helfen diese sieben Punkte, die betrügerische Shops entlarven können:

Quelle der Angabe zu Cyberkriminalität: Sicherheitsstudie 2025, Handelsverband Österreich — [PDF der Studie](#)

Die sieben Prüfpunkte

1. Impressum und Firma prüfen

☐

Ist ein vollständiges Impressum vorhanden und anklickbar? Passen Firmenname, Anschrift und Kontaktmöglichkeiten zum Shop?

2. Domain genau ansehen

☐

Achten Sie auf Tippfehler, zusätzliche Bindestriche, ungewohnte Domainendungen oder Zusätze wie „sale“ oder „outlet“, die bekannte Marken imitieren.

3. Zeitdruck hinterfragen

☐

Extrem kurze Angebotsfristen, ständig neu startende Countdown-Timer und angeblich fast ausverkaufte Ware sollen eine ruhige Prüfung verhindern.

4. Zahlungsarten kontrollieren

☐

Bleibt am Ende nur Vorkasse oder eine direkte Überweisung, fehlt im Betrugsfall oft eine einfache Rückbuchungsmöglichkeit. Wählen Sie möglichst eine Zahlungsart mit Käuferschutz.

5. Gütesiegel verifizieren

☐

Ein Bild eines Siegels ist kein Nachweis. Klicken Sie darauf und prüfen Sie, ob die Zertifikatsseite tatsächlich diesen Shop und diese Domain nennt.

6. Bewertungen kritisch lesen

☐

Viele sehr kurze, ähnlich formulierte und ausschließlich positive Bewertungen sind verdächtig. Suchen Sie zusätzlich nach unabhängigen Erfahrungen.

7. Shop vorab recherchieren

☐

Suchen Sie nach dem Shopnamen zusammen mit Begriffen wie „Betrug“, „Fake-Shop“ oder „Erfahrungen“ und prüfen Sie Warnungen seriöser Stellen.

Mein Prüfergebnis

■ UNAUFFÄLLIG

■ GENAUER PRÜFEN

■ NICHT BESTELLEN

Wenn Sie bereits bezahlt haben

1. Bank oder Zahlungsdienst sofort kontaktieren	Fragen Sie, ob eine Zahlung gestoppt, zurückgebucht oder über den Käuferschutz beanstandet werden kann. Handeln Sie möglichst sofort.
2. Alle Belege sichern	Bestellbestätigung, Rechnung, Zahlungsnachweis, E-Mails, Produktseite, Impressum und Screenshots des Shops speichern. Notieren Sie den zeitlichen Ablauf.
3. Zugangsdaten absichern	Falls Sie ein bereits anderweitig verwendetes Passwort eingegeben haben, ändern Sie es dort ebenfalls. Aktivieren Sie wenn möglich Zwei-Faktor-Authentifizierung.
4. Beratung und Anzeige prüfen	Unterstützung bieten unter anderem Watchlist Internet, die Internet Ombudsstelle, die Arbeiterkammer und bei Betrugsverdacht die Polizei.

Diese Belege sollten Sie sichern

■ Bestellbestätigung	■ Zahlungsnachweis	■ Produktseite / Angebot
■ Rechnung	■ E-Mail-Verlauf	■ Impressum und Kontaktdaten
■ Screenshots des Shops	■ Lieferangaben	■ Notizen zu Datum und Ablauf

Seriöse österreichische Anlaufstellen

Watchlist Internet	Aktuelle Warnungen und Informationen zu Internetbetrug	www.watchlist-internet.at
Internet Ombudsstelle	Kostenlose außergerichtliche Unterstützung bei Online-Problemen	www.ombudsstelle.at
Arbeiterkammer	Konsumentenberatung und Informationen zu Internetkäufen	www.arbeiterkammer.at
Polizei Österreich	Anzeige und Informationen bei Betrugsverdacht	www.polizei.gv.at