



POLIZEI
Nordrhein-Westfalen
Bonn

bürgerorientiert · professionell · rechtsstaatlich

Newsletter



Polizeipräsidium Bonn - Kriminalkommissariat Kriminalprävention/Opferschutz

Präventionstipps für Bürgerinnen und Bürger

Themenreihe 2025

Waren-/Warenkreditbetrug

Ausgabe 1

„Fake-Shops - Vorsicht beim Onlinekauf“

Fake-Shops

Inhalte

1. Fake-Shops – was versteht man darunter und wie funktionieren sie?
2. Mögliche Gefahren durch Fake-Shops
3. Worauf müssen Sie achten, um Fake-Shops zu erkennen?
4. Gütesiegel für sichere Shops
5. Die SHS Regel und kleine Tipps in Sachen Fake-Shops
6. Was sollten Sie tun, wenn Sie auf einen Fake-Shop reingefallen sind?

1. Fakeshops – Was versteht man darunter und wie funktionieren sie?

Im Internet wimmelt es inzwischen von sog. Fake-Shops, die den Onlinehandel ernsthaft bedrohen.

Professionelle Fake-Shops sehen täuschend echt aus, gleichen seriösen Online-Shops fast bis auf das I-Tüpfelchen und suggerieren Kaufwilligen: Auf dieser Plattform sind gewünschte (Marken-) Produkte (sehr) günstig erhältlich.

Die Bandbreite der Produktpalette reicht von Uhren, Schmuck über Kleidung, Pflegeprodukten, Haushaltsgeräte, Werkzeuge, Smartphones, Laptops bis hin zu Unterhaltungselektronik aller Art, die zu einem deutlich reduzierten Preis angeboten werden.

Bei der Schnäppchenjagd nach begehrten Produkten geraten Kund*innen schneller als ihnen lieb ist auf gefälschten oder imitierenden Internetseiten. Die Angaben über einen angeblich „geringen Bestand“ oder „letztes Exemplar“ suggerieren den Nutzer*innen die Notwendigkeit einer schnellen Kaufentscheidung.

Oft unterschieden sich seriöse und imitierte Online-Shops nur durch ein Sonderzeichen oder die Endung im Domainnamen, z.B. „.info“ statt „.de“. In vielen Fällen wird die Existenz eines realen Shops nur vorgetäuscht.

Cyberkriminelle übernehmen zuweilen entweder gekündigte Webseiten Dritter (ehemaliger Vereine, Apotheken, Sportgeschäfte, Restaurants, etc.), reaktivieren diese wieder und starten den Verkauf von Luxusartikel, die man mit dem Webseitenamen eigentlich nicht in Verbindung bringen würde.

Manchmal werden auch aktive Webseiten übernommen und in deren Unterverzeichnissen eigene Fake-Shopseiten eingebettet.

Der Zugang zu diesen Bereichen erfolgt in der Regel durch Zusendung eines Links per (Werbe-)Mail oder durch Nutzung des Links nach Suche des Shops über Suchmaschinen.

2. Mögliche Gefahren durch Fake-Shops

- Sie leisten eine Kaufpreiszahlung und erhalten entweder keine Ware, minderwertige Ware oder gefälschte Markenartikel (Plagiate).
- Sie bekommen Ihr Geld nicht zurück.
- Ihre persönlichen Daten und Zahlungsdaten werden für weitere Betrugsdelikte gesammelt und später missbräuchlich eingesetzt.
- Fake-Shop-Domainnamen werden mit missbräuchlich erlangten privaten Daten angelegt.
- Ihre Überweisung geht u.U. an sog. Finanzagenten mit deutschen Bankkonten. (Ein Finanzagent stellt nur das eigene Girokonto für Überweisungen zur Verfügung und soll eingehende Geldbeträge Dritter möglichst umgehend per Bargeldversand oder über Finanztransferdienstleister (wie z.B. Western Union) an eine im Ausland befindliche Person transferieren. Für diese Tätigkeit winkt eine Beteiligung zwischen fünf und 20 Prozent, die vom Überweisungsbetrag einbehalten werden darf.)
- Die Ware wird Ihnen aus dem Ausland zugesandt und der Zoll beschlagnahmt die von Ihnen bestellte Ware (z.B. bei Fälschungen).

- Hoher Aufwand und hohe Kosten beim Rückversand minderwertiger/falscher Ware, wenn diese aus scheinbar deutschen Shops kommen (z.B. Vortäuschen mit Domain-Endung)
- Domain-Spoofing - hierbei fälschen Kriminelle einen Website-Namen oder eine E-Mail-Domain, um Internetuser zu täuschen. Ziel ist es, die Nutzer dazu zu verleiten, dass sie mit einer böswilligen E-Mail oder einer Phishing-Website so umgehen bzw. kommunizieren, als ob diese legitim seien und sie sich sicher wähnen. [Domain-Spoofing näher erläutert](#)

3. Worauf müssen Sie achten, um Fake-Shops zu erkennen?

- Achten Sie auf auffällige Webadressen - der Teufel steckt häufig im kleinsten Detail - achten Sie bei einer bekannten Domain auf plötzliche zusätzliche Endungen z.B. „de.com“ statt „de“
- Stimmen URL und Inhalt überein, d.h. stimmen Shop-Adresse und Ihre Erwartung vom Inhalt auf der Webseite überein? Nein - dann bitte Finger weg.
- Die Preise sind zu schön, um wahr zu sein, d.h. die Ware wird außergewöhnlich, eigentlich schon unrealistisch günstig angeboten. Nehmen Sie Abstand - niemand will Ihnen etwas schenken.
- Die Ware scheint entweder immer verfügbar zu sein oder ist (angeblich nur noch) in geringer Stückzahl vorhanden.
- Als Bezahlmöglichkeit besteht beim Abschluss der Bestellung nur (noch) die Option der Vorkasse, obwohl anderes zu Beginn des Bestellvorgangs angeboten wurde. Dann auch hier besser Finger weg - brechen Sie den Kauf ab. Seriöse Shops bieten immer mehrere Zahlungsmöglichkeiten an, darunter sichere Optionen wie PayPal oder Kreditkarte. Diese bieten einen Käuferschutz im Falle eines Betrugs.
- In früheren Zeiten fehlten oftmals Abbildungen von Produkten, zugehörige Informationen, Impressum oder wichtige AGB. Diese Informationen waren ggf. unvollständig, unklar bzw. schlecht formuliert, fehlerhaft oder wurden von fremden Seiten kopiert. Mittlerweile sind auch solche Angaben so gut aufbereitet, dass Fälschungen nur schwer zu erkennen sind.
- Weitere Bereiche der Internetseite (Unterseiten) sind leer oder mit unsinnigen Fülltexten angereichert.
- Sie erhalten keine korrekte Bestellbestätigung.
- Sie bekommen ungewöhnliche Bankverbindungen genannt, die eher nach privaten Bankkonten aussehen.
- Zweifeln Sie Kundenrezensionen in Online-Shops grundsätzlich an.

4. Gütesiegel für sichere Shops

- Wichtig zu wissen: Es gibt leider kein einheitliches Gütesiegel für Online-Shops und nicht jeder Online-Shop, der über kein Gütesiegel verfügt, ist unbedingt sofort als unseriös zu bewerten. Mit den einzelnen Gütesiegeln sind unterschiedliche Überprüfungsverfahren sowie Qualitätsanforderungen für Webshops verbunden.
[Näheres s. Initiative D21](#)
- Wenn ein Gütesiegel vorhanden ist, achten Sie darauf, dass das Siegel nicht nur als Bilddatei angezeigt wird.
- Bei einigen betrügerischen Fake-Shops werben die Betreiber wahlweise auch mit frei erfundenen oder auch unrechtmäßig mit bekannten Gütesiegeln.
- Überprüfen Sie das Gütesiegel eines Shops, indem Sie darauf klicken. Ein echtes Siegel führt Sie durch Mausclick auf die Internetseite des Gütesiegelbetreibers, wo Ihnen das gültige Prüfzertifikat des Anbieters angezeigt wird.
- Lesen Sie alle Angaben genau. Das Gütesiegel muss Bezug nehmen auf den konkreten Shop.
- Welche Gütesiegel bei Online-Shops seriös sind und worauf sie detailliert achten sollten, erfahren Sie unter: [Trusted Shops, EHI & Co](#)

5. Die SHS Regel und kleine Tipps in Sachen Fake-Shops

Sie gehen Betrüger*innen beim Onlineshopping nicht so schnell auf den Leim, wenn Sie sich an der **SHS-Regel** zu orientieren:

- **Stoppen**
Seien Sie kritisch, handeln Sie nicht vorschnell auf der Jagd nach Schnäppchen, kennen Sie die Risiken, prüfen Sie und wägen Sie ab.
- **Hinterfragen**
Prüfen Sie die Kriterien, die einen sicheren Web-Shop ausmachen und hinterfragen Sie einen unrealistischen Preis.
- **Sich und andere Schützen**
Haben Sie durch die ersten beiden Schritte eine Betrugsmasche erkannt, dann sollten Sie das umgehend melden: am besten an die Betreiber der Plattform, bei der der Betrug stattfindet sowie auch bei der Polizei.

<https://www.polizei-beratung.de/themen-und-tipps/sicher-handeln/>

<https://www.polizei-beratung.de/themen-und-tipps/sicher-handeln/die-shs-regel/>

[Hinweise Landeskriminalamt NRW \(LKA NRW\)](#)

[Hinweise Landeskriminalamt Niedersachsen \(LKA NI\)](#)

- Vorhängeschloss in der Browserzeile und „https://“ waren ehemals noch Hinweise auf eine sichere Verbindung. Mittlerweile nutzen auch Fake-Shops immer häufiger sichere Verbindungen.
- Manches Mal unterscheiden sich seriöse URL von gefälschten nur durch ein Zeichen, in der Hoffnung, dass dies von Ihnen überlesen wird.
- Ein vollständiges Impressum enthält die Identität und die Kontaktmöglichkeit des Anbieters. Unternehmen/verantwortliche Person müssen transparent sein, inklusive Adresse (nicht nur Postfach), E-Mail, telefonischer Erreichbarkeit, Fax, Rechtsform und Handelsregisternummer, die Sie auf [Gemeinsames Registerportal](#) überprüfen können. Sofern das Angebot einer Zulassung bedarf z. B. Apotheker bedarf es auch der Angabe der Aufsichtsbehörde
- Der Shop benutzt ein bekanntes Gütesiegel (s.o.).
- Das Angebot enthält eine realistische Preisgestaltung. Auch Versandkosten, Rücksendekosten und mögliche Zusatzkosten sind transparent und in der Höhe nachvollziehbar.
- Es existiert ein eindeutiger Bestellbutton (herkömmlich: „Zahlungspflichtig bestellen“/„Jetzt kaufen“)
- Die allgemeinen Geschäftsbedingungen sind zur Einsicht verfügbar. Das Kleingedruckte ist aber oft lang und nicht leicht verständlich formuliert. Viele stimmen den AGB einfach nur zu, ohne sie zu lesen. [Wissenswertes zu AGB und wie man sie richtig liest](#)
- Die Informationen zum Datenschutz und Datensicherheit sind verfügbar.
- Angaben zum Widerrufsrecht, Rückgaberecht und der Kaufpreiserstattung sind verfügbar und rechtskonform.
- Sie können zwischen verschiedenen Zahlungsmöglichkeiten (Vorkasse, Rechnung, Lastschrift, Kreditkarte, seriöser Online-Bezahldienst,...) wählen.
- Sie erhalten eine verkehrsübliche E-Mail-Bestätigung des Bestellvorgangs.

6. Was sollten Sie tun, wenn Sie auf einen Fake-Shop reingefallen sind?

- Handeln Sie schnell! Kontaktieren Sie umgehend Ihre Bank und bitten Sie darum, die Überweisung oder den Zahlungsvorgang zu stoppen (bei eingereichtem Überweisungsträger) bzw. rückgängig zu machen.

Dies ist ggf. noch in einer kurzen Zeitspanne möglich - nicht aber bei Echtzeitüberweisungen! Bei anderen Zahlungsarten kontaktieren Sie bitte entsprechend den Dienstleister.

- Sichern Sie den kompletten Bestellvorgang Ihres Onlinekaufs: alle E-Mails, Bestellbestätigungen, Screenshots der Websites und den dort abgebildeten Angeboten sowie erhaltene Zahlungsbelege.
- Erstellen Sie Strafanzeige bei der Polizei! Auch, wenn die Täter aus dem Ausland agieren, sollten Sie auf keinen Fall von einer Anzeige absehen. Nur dann können Löschungen von Fake-Shops vorangetrieben werden.

Weiterführende Informationen zu Fake-Shops finden Sie auch hier:

[Polizei-Beratung.de](https://www.polizei-beratung.de)

[Bundesamt für Sicherheit in der Informationstechnik:](https://www.bsi.bund.de)

[BSI](https://www.bsi.bund.de)

[Verbraucherzentrale NRW](https://www.verbraucherzentrale-nrw.de)

[DENIC \(Registrierungsstelle für Domains\)](https://www.denic.de)

[Verbraucherzentrale-Marktbeobachtung](https://www.verbraucherzentrale.de)

[Verbraucherzentrale-Fakeshopfinder](https://www.verbraucherzentrale.de)

Impressum

Herausgeber

Polizeipräsidium Bonn

Kommissariat Kriminalprävention/Opferschutz

Königswinterer Str. 500

53227 Bonn

Tel.: 0228 - 157676

E-Mail: KKKPO.Bonn@polizei.nrw.de