INTERNETKRIMINALITÄT

SHOPS AUS FERNOST, PHISHING, ONLINE-BETRUG

Als regionale Anbieter getarnte Shops aus Fernost, Phishing-Versuche, überteuerte Online-Dienste und gehackte Accounts – Beschwerden zu Internetkriminalität und Abzocke nehmen deutlich zu. Um nicht hereinzufallen, hilft nur eines: Angaben vorab überprüfen, Warnhinweise ernst nehmen. Doch genau das wissen unseriöse Anbieter zu erschweren. Mit manipulativen Designs, professioneller Gestaltung sowie Werbebannern und erkauften Platzierungen verleiten sie Kundinnen und Kunden gezielt zum schnellen Klick.

Getarnte Shops aus Fernost: Rücksendung? Fehlanzeige!

Getarnte Shops aus Fernost werben mit hochwertigen Produkten zu Schnäppchenpreisen. Die Websites sind professionell gemacht, deutsche Namen und Städte in der Shop-URL erwecken den Eindruck von Regionalität. Wird die Ware geliefert, fühlen sich Verbraucherinnen und Verbraucher oft getäuscht: Die Qualität ist schlecht, Widerruf und Reklamation schlagen fehl. Erst bei der Suche nach einer Rücksendeadresse fällt auf: Die Ware wird aus China verschickt.

Beispiele: **beckerhannover.de** und **hoffmannbremen.de** (gleicher Betreiber)

Überteuerte Online-Dienste: Anzeigen führen in die Kostenfalle

Führungszeugnis beantragen, Nachsendeantrag einrichten oder dem Rundfunkbeitragsservice eine Änderung mitteilen? Wer online danach sucht, landet schnell bei Drittanbietern, die ihre Angebote mit Anzeigen prominent platzieren. Ihr Konzept: Sie lassen sich kostenlose oder günstige Leistungen teuer bezahlen. Die Websites ähneln dem Original. Bemerken Verbraucherinnen und Verbraucher den Irrtum, ist es meist zu spät: Damit der Auftrag direkt ausgeführt wird, mussten sie auf ihr Widerrufsrecht verzichten.

Beispiele:

amtsweg.info/fuehrungszeugnis (26 Euro für ein **eBook** zur Beantragung des Führungszeugnis)
nachsendeauftrag-direkt.com (99,90 statt 28,90 Euro für sechs Monate)
service-rundfunkbeitrag.de (29,99 statt 0 Euro – allein für die Weiterleitung von Daten)

Phishing-Versuche: FTI-Insolvenz für Betrug genutzt

Gefälschte Paketbenachrichtigungen, vermeintliche Nachrichten der eigenen Bank: Per SMS und E-Mail versuchen Kriminelle, Verbraucherinnen und Verbraucher zum Anklicken von Links und Eingabe persönlicher Daten auf nachgebauten Websites zu verleiten. Aktuell wird die FTI-Insolvenz von Betrügern missbraucht, warnt der Deutsche Reisesicherungsfonds (DRSF). Die Masche: Per SMS und E-Mail werden Verbraucherinnen und Verbraucher aufgefordert, für die Erstattung des Reisepreises ihre Bankdaten zu übermitteln.

Warnung unter: drsf.reise

INTERNETKRIMINALITÄT

GEHACKTE ACCOUNTS, SCHUTZ & TIPPS

Gehackte Accounts: Im Betrugsfall muss es schnell gehen

Wenn sich Fremde Zugang zu Online-Konten verschaffen, auf Daten zugreifen oder für weiteren Betrug missbrauchen, ist schnelles Handeln entscheidend. Betroffene sollten **Anzeichen** daher **ernst nehmen** – etwa geänderte Daten, unklare Bestellbestätigungen oder Hinweise auf Anmeldeversuche über fremde Endgeräte. Wurde das Konto gehackt, gibt es zwei Möglichkeiten:

1) Selbst versuchen, die Kontrolle zurückzuerlangen. Für nahezu jedes Online-Konto lässt sich ein neues Passwort anfordern. Das geht etwa über die Funktion „Passwort vergessen“ oder „Neues Passwort anfordern“. Eine zentrale Rolle spielt dabei die im Online-Konto hinterlegte E-Mail-Adresse. Dorthin werden die Anforderungen und Informationen versendet.

Wichtig: Bevor ein Passwort geändert wird, immer erst das Endgerät auf Schadsoftware prüfen, damit das neue Passwort nicht wieder ausgespäht werden kann. Wenn möglich eine **Zwei-Faktor-Authentifizierung** für den Account **einrichten**.

Tipp: In Banking-Apps lassen sich Bankkarten oft per Klick temporär sperren. Alternativ geht das auch über die Rufnummer 116 116. So kann Betrügern der Geldhahn zugedreht werden.

2) Anbieter kontaktieren und um Hilfe bitten. Wer alleine nicht weiterkommt – etwa, weil die hinterlegte E-Mail-Adresse geändert wurde oder kein Zugriff mehr zum Account besteht – ist auf die Hilfe des Anbieters angewiesen. Das Problem: Kontaktdaten sind oft nicht leicht zu finden.

Forderung: Anbieter müssen 24/7 Notfallhilfe vorhalten

Im Betrugsfall muss es schnell gehen. Hilfsangebote, Schritt-für-Schritt-Anleitungen und Kontaktmöglichkeiten sollten mit Suchbegriffen wie etwa „Konto gesperrt“ oder „Account gehackt“ auf der Website leicht zu finden sein. Das ist bei vielen Anbietern jedoch nicht der Fall. Hier sollten Anbieter nachbessern und klare „Notfall-Optionen“ bereitstellen, rund um die Uhr.

Ausführliche Tipps für Betroffene und Erste-Hilfe-Maßnahmen:
www.verbraucherzentrale-niedersachsen.de/erste-hilfe-bei-gehackten-online-konten

Schutz vor Online-Abzocke und Betrug:

- Angaben kritisch hinterfragen – die Endung „.de“ in der Shop-URL etwa bietet keine Sicherheit, dass der Shop aus Deutschland kommt. Vorab Impressum, Kontakt- und Rücksendeadresse prüfen, URL im Fakeshop-Finder eingeben (s. nächste Seite).
- Bei Online-Suchen die ersten Treffer in der Ergebnisliste (Anzeigen) meiden.
- Jede Abfrage persönlicher Daten kritisch hinterfragen. Änderungen nicht per Link-Klick übermitteln, sondern nach dem Einloggen direkt im Kunden-Account hinterlegen. Bestehen Zweifel: Bei Anbietern nachfragen, ob eine Anfrage echt ist.
- Im Betrugsfall: Strafanzeige stellen!

verbraucherzentrale Niedersachsen

FAKESHOP-FINDER

INTELLIGENTER SCHUTZ VOR ONLINE-BETRUG

Im Frühjahr Fahrräder und Gartenzubehör, im Sommer Mode und Reisen, zum Jahresende Brennholz, Elektroartikel und Parfum: Fakeshops nutzen saisonal nachgefragte Produkte und erfinden sich immer wieder neu. Aktuell wird auch die Fußball EM von Betrügern gern genutzt.

Professionell gemacht, sind Fakeshops mit bloßem Auge oft nicht erkennbar – und zunehmend eine Gefahr beim Online-Shopping. Schutz bietet der Fakeshop-Finder der Verbraucherzentralen. Dank KI sind Verbraucherinnen und Verbraucher den Betrügern damit einen Schritt voraus.

Erst checken, dann kaufen: per Klick zum Ergebnis

Der Fakeshop-Finder bietet schnell und unkompliziert Hilfe: Nach Eingabe der Shop-URL unter www.verbraucherzentrale-niedersachsen.de/fakeshop-finder erhalten Verbraucherinnen und Verbraucher innerhalb weniger Sekunden eine Einschätzung, ob sie dem Shop vertrauen können – oder von einer Bestellung lieber absehen sollten.

Basis des Fakeshop-Finders ist eine Domain-Datenbank, die mittels künstlicher Intelligenz stetig wächst. Wird eine Internetadresse eingegeben, die noch nicht bekannt ist, wird die Website auf verschiedene Merkmale gescannt. Dazu gehören auch technische Merkmale, die mit bloßem Auge nicht zu erkennen sind. Die daraus errechnete Wahrscheinlichkeit, ob es sich womöglich um einen unseriösen Anbieter handelt, gibt der Fakeshop-Finder in den Ampelfarben aus, verbunden mit Erklärungen und Hinweisen zu den überprüften Merkmalen.

Nutzung des Fakeshop-Finders nimmt zu

- Bis heute wurde der Fakeshop-Finder rund drei Millionen Mal genutzt (Start: 8/2022).
- Im Jahr 2023 wurde er durchschnittlich über 4.300 Mal pro Tag genutzt, im Gesamtjahr 1,6 Millionen Mal – aktuell (Jahr 2024) wird er bereits über 6.200 Mal pro Tag genutzt.
- Etwa 442.000 Shop-Seiten aus dem deutschsprachigen Raum sind zurzeit in der Datenbank erfasst, 62.500 davon als erkannte Fakeshops.
- Monatlich werden im Schnitt rund 2.000 neue Fakeshops erkannt!

Aktuelle Beispiele für Fakeshops

1. emsports.de
2. shop.soccerballofficial.com
3. dekanushop.com

verbraucherzentrale Niedersachsen