POLIZEI
Nordrhein-Westfalen
Dortmund

Fakeshops

Quelle: adobe stocks (Polizei NRW)

Die „fast perfekte Täuschung“

Das Einkaufen über Online-Shops bietet in der heutigen Zeit viele Vorteile und ermöglicht den Einkauf von Waren und Dienstleistungen ohne das Haus verlassen zu müssen.

Die Jagd nach Schnäppchen, dass Verlangen, hochwertige Markenprodukte zu günstigen Preisen zu ergattern sowie fehlende Internetrecherche führen allerdings dazu, dass immer mehr Verbraucher auf sogenannte Fakeshops hereinfallen.

Definition & Vorgehensweise

Fakeshops sind gefälschte Internet-Verkaufsplattformen, die auf den ersten Blick nicht als solche zu erkennen sind. Sie sind teilweise Kopien real existierender Websites und wirken daher seriös und lassen beim Käufer selten Zweifel an ihrer Echtheit aufkommen. Dabei werden nicht selten Domainnamen, also die „www-Adresse“ der Internetseiten durch Cyberkriminelle eingerichtet, welche dem Originalnamen einer Firma ähneln, sodass der Unterschied lediglich in der Domainendung, also zum Beispiel „.info“ anstatt „.de“ liegt. Auch Bilder und Beschreibungen können ganz leicht kopiert werden. Dadurch wird der Bezug zur Originalseite einer Firma hergestellt.

Das Ziel der Betrüger ist es, mit falschen Produktbildern, einem gefälschten Impressum, falschen Gütesiegeln, sehr günstigen Preisen und professionell angelegten Allgemeinen Geschäftsbedingungen das Vertrauen von Online-Shoppern zu gewinnen und sie zum Kauf zu animieren.

Wenn ein Käufer dann Ware bestellt, sind die Kriminellen am Zug. Sie verschicken dann minderwertige Ware zu einem überhöhten Preis oder liefern nach Vorauszahlung die Ware erst gar nicht. Oftmals werden auch Lieferschwierigkeiten vorgetäuscht, um die Betroffenen daran zu hindern, bereits getätigte Überweisungen rückgängig zu machen.

Von den Tätern werden vermehrt auch bereits gekündigte Webseiten anderer Nutzer reaktiviert und im Anschluss daran Fakeshops eingerichtet. Dies können dann Websites ehemaliger Apotheken, Sportvereine, Anwälte, Architekten usw. sein, die dann plötzlich Designerartikel oder andere Waren anbieten.

Woran erkennt man Fakeshops?

POLIZEI Nordrhein-Westfalen Dortmund

Fakeshops sind nicht immer gleich auf den ersten Blick zu erkennen. Auch die Cyberkriminellen haben sich im Laufe der Jahre immer wieder neue Strategien und Betrugswege überlegt, um arglose Käufer zu überlisten.
So verwenden die Täter mittlerweile auch zertifizierte- und verschlüsselte Datenübertragung (https) um Sicherheit zu suggerieren. Des Weiteren sind die meisten Shops mittlerweile sprachlich fehlerfrei und innovativ gestaltet.

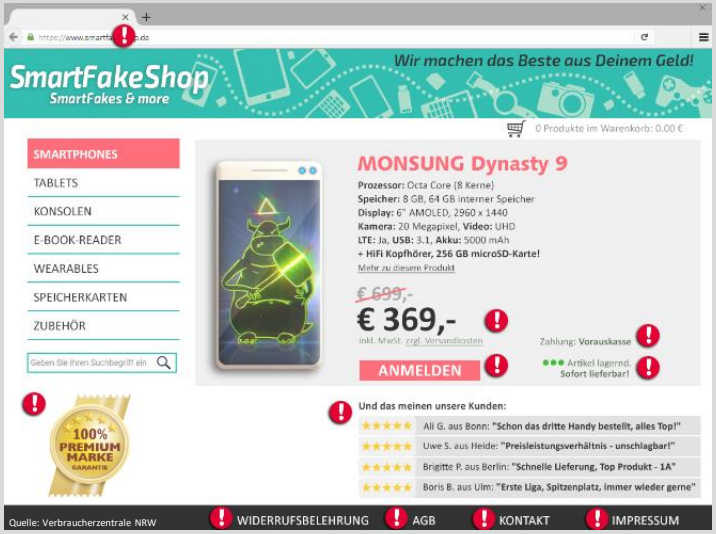
Wesentliche Merkmale für Fakeshops:

- Ungewöhnlich günstige Preise für Markenartikel, wobei sich bei neueren Fakeshops mittlerweile auch Artikel zu Normalpreisen finden lassen, um so die Shops „echter“ wirken zu lassen
- Das Impressum des Onlineshops fehlt komplett, ist unvollständig oder die Inhalte sind nicht korrekt dargestellt, welches durch Suchmaschinen-Recherche oder Kartendienste kontrolliert werden kann. Auch der Verweis auf das Handelsregister mit entsprechender Nummer kann geprüft werden
- Die Ware kann nur gegen Vorkasse bezahlt werden. Weitere Zahlungsmöglichkeiten werden zwar im Vorfeld per Logo suggeriert, sind später bei der Bezahlung aber nicht mehr auswählbar
- Gütesiegel wurden nur als Bild auf die Seite hineinkopiert und sind nicht überprüfbar. Zertifizierte „Trusted Shops“ können per Mausklick auf das Siegel überprüft werden
- Die Allgemeinen Geschäftsbedingungen sind fehlerhaft/unvollständig oder fehlen komplett. Hier werden oftmals schlecht übersetzte AGB von Übersetzungsprogrammen verwendet
- Der Domainname ergibt keinen logischen Sinn; ein Luxusuhrenhersteller verkauft beispielsweise keine Computer
- Die Ware ist „immer“ verfügbar oder es werden Counter eingesetzt welche herunterzählen, um den potentiellen Käufer unter Druck zu setzen
- Es werden ungewöhnliche Bankverbindungen angezeigt, die entweder privat aussehen oder ins Ausland verzweigen

Woran erkennt man Fakeshops?

POLIZEI Nordrhein-Westfalen Dortmund

- Der Käufer bekommt keine korrekte Bestellbestätigung und der Kontakt findet nur auf Englisch oder in schlechtem Deutsch statt
- Auf den Seiten des Fakeshops finden sich nur überaus gute Kundenbewertungen. Diese werden in der Regel von den Kriminellen künstlich erzeugt, um gute Erfahrungen vorzugaukeln



Neben den hier aufgeführten Merkmalen, sollte man auch die folgenden Punkte beachten:

- Prüfen Sie die Firmenadresse des Anbieters mithilfe von Suchmaschinen, Kartendiensten, Onlinetelefonbüchern oder über Online-Bewertungsportale
- Überprüfen sie die eingebundenen Links des Onlineshops zu Social Media-Kanälen wie Instagram, Facebook, Twitter und ähnlichen Plattformen; oftmals wird nur zu der Startseite dieser Kanäle verlinkt
- Die Angaben von Handelsregisternummern können auf www.handelsregister.de überprüft werden; eine Prüfung der Umsatzsteuer-ID ist über https://ust-id-pruefen.de möglich
- Testen sie die Telefon-/Hotline-Nummern, falls diese in Deutschland angegeben sind; meistens laufen diese Nummern ins Leere oder werden an Sprachdienste weitergeleitet

Risiken und Schutz

POLIZEI
Nordrhein-Westfalen
Dortmund

Wie kann ich mich vor Fakeshops schützen?

- Wenn sie unsicher sind, nehmen Sie Kontakt mit dem Shop Betreiber auf
- Recherchieren sie im Internet nach dem Shop
- Überprüfen sie die Gütesiegel des Shops per Mausklick
- Nutzen Sie nur ihnen bekannte Bezahldienste oder den Kauf auf Rechnung
- Seien Sie misstrauisch, wenn die Kommunikation nur über E-Mail erfolgen kann
- Kontrollieren Sie den Domain-Namen des Onlineshops
- Folgen Sie keinen Links aus Spam-Mails zu den Seiten des angebotenen Shops
- Vermeiden sie Käufe und Überweisungen außerhalb der Geschäftszeiten ihrer Bank um im Notfall einen Ansprechpartner zu haben

Was kann passieren, wenn Sie auf einen Fakeshop hereingefallen sind?

- Sie erhalten keine Ware
- Sie erhalten gefälschte Markenartikel
- Es wird minderwertige Ware versendet
- Sie bekommen ihr Geld nicht wieder
- Der Zoll beschlagnahmt Ihre Ware
- Ihre persönlichen Daten werden für weitere Betrügereien verwendet

Was sollten Sie tun, wenn sie Opfer eines Fakeshops geworden sind?

- Haben Sie schon Geld überwiesen, sollten sie umgehend ihre Bank kontaktieren, um die Zahlung zu stoppen
- Sammeln Sie alle Belege von der Online-Bestellung (Screenshots, Bestellbestätigung, …)
- Stellen Sie unbedingt Strafanzeige bei der Polizei

Starke Passwörter verwenden

Stark ist ein Passwort, wenn es aus mindestens 10 Zeichen unter Nutzung von Klein- und Großbuchstaben, Ziffern und Sonderzeichen besteht. Bitte keine Namen, Geburtsdaten oder Passwörter aus dem Wörterbuch verwenden und auf keinen Fall an Dritte weiter geben. Es wird empfohlen, für verschiedene Onlinezugänge auch unterschiedliche Nutzernamen und Passwörter zu verwenden. Diese Passwörter sollten auch an geeigneten Stellen und vor Dritten geschützt aufbewahrt werden. Optimal ist auch die Verwendung eines Passwortmanagers mit Schlüsselbundfunktion.

Verwenden Sie keine Passwörter, die in der Vergangenheit schon einmal benutzt wurden und vermeiden Sie die „Passwort merken“-Funktion von Anwendungen im Browser und in Applikationen (Apps). Bevorzugt werden sollten auch Dienste, welche die Zwei-Faktor-Authentifizierung unterstützen.

Privatsphäre schützen

Richtige Sicherheitseinstellungen auf den Endgeräten sowie in den Sozialen Medien reduzieren das Risiko, zu viele Informationen von sich selbst preiszugeben. Ein sorgfältiger Umgang mit seinen Profildaten und Bildern ist unerlässlich.

=> Seien Sie sparsam mit der Weitergabe Ihrer persönlichen Daten!

[Profilbild, personenbezogene Daten, Freunde-Einstellungen, öffentliche-Daten, Selfies, Likes]

Misstrauisch sein

Bei Anfragen von Unbekannten immer misstrauisch sein! Cyberkriminelle verstecken sich in erster Linie hinter anonymen, gefälschten und unseriösen Profilen. Aus diesem Grund sollte jede Kontaktanfrage immer kritisch hinterfragt und keine sensiblen Daten herausgegeben werden. Auch E-Mails von Unbekannten sollten weder geöffnet, noch sollten Anhänge und Links in keinster Weise angeklickt werden. Hier verbirgt sich oftmals Schadsoftware, mit der Absicht Passwörter zu erbeuten, um weitere, kriminelle Handlungen durchzuführen. Oftmals lassen sich Betrüger auch durch die unkorrekte Schreibweise der E-Mailabsenderadresse, deren Inhalt, falsche Umlaute, kryptische Buchstaben oder anhand der Linkadresse erkennen.

Wo gibt es Hilfe?

POLIZEI
Nordrhein-Westfalen
Dortmund

Wenn Sie Opfer von Cybercrime geworden sind, stehen Ihnen die gleichen umfangreichen Hilfs- und Unterstützungsangebote zur Verfügung, wie den Opfern von Straftaten in der realen Welt.

Bei akuter Bedrohung, wählen Sie 110! Die Polizei wird alles Erforderliche tun, um Sie zu schützen.

- Zeigen Sie die Straftat bei der Polizei an (Strafanzeige ist bei jeder Polizeidienststelle möglich)
- Existierendes Datenmaterial, wie z. B. E-Mails, Chat-Verläufe in Messenger-Diensten, digitale Fotos oder Videos sind wichtige Beweismittel, die Sie bis zum ersten Kontakt mit der Polizei bestenfalls komplett unverändert lassen.
- Bringen Sie das gesicherte Beweismaterial am besten gleich zur Anzeigenerstattung mit. Das ist wichtig für die weiteren Ermittlungen, um den Verlust von Spuren im Netz zu vermeiden.