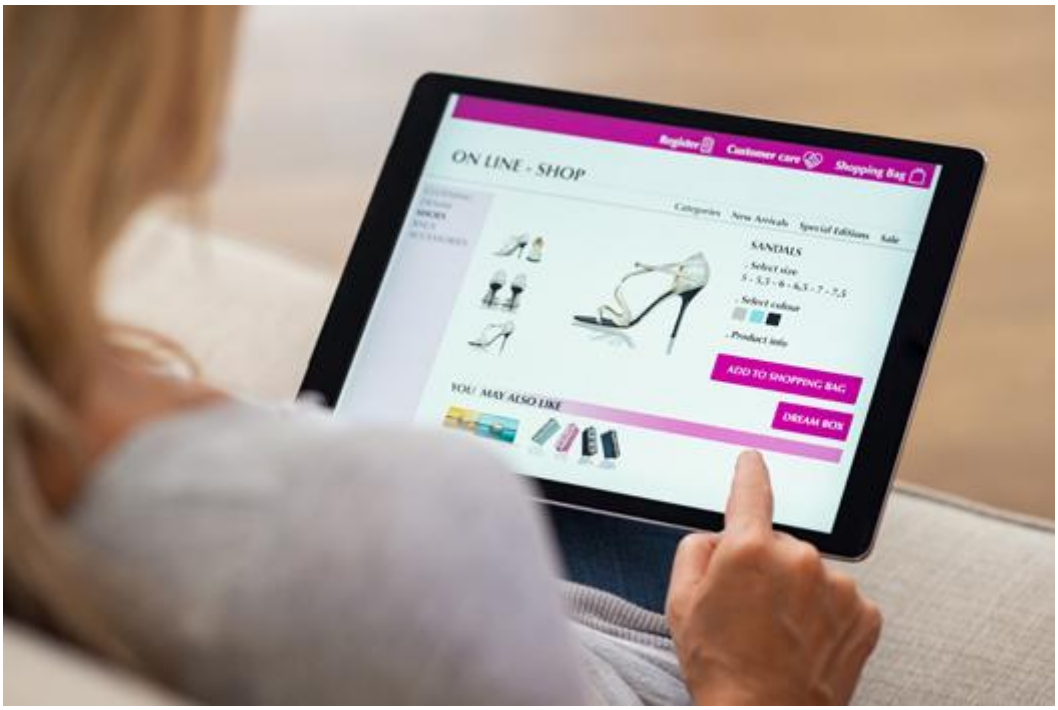
Hetze im Netz ist strafbar >
< Kontaktloses Bezahlen

Bestellt und nichts geliefert

Fakeshops in der Hand von internationalen Täterbanden



Die Webseiten der Betrügershops sehen oft täuschend echt aus

Die Polizei im Rhein-Sieg-Kreis nahm im Frühjahr 2018 vier Betrüger fest. Sie hatten über den Fakeshop „oneupyou.com“ Elektroware im Wert von über 300.000 Euro verkauft, aber nicht verschickt. Die Männer mit türkischen Wurzeln versuchten, ihre wahre Identität mit gefälschten Pässen zu verschleiern. Rund ein Jahr später wurde der Hauptverdächtige zu einer fünfjährigen Haftstrafe verurteilt. Groß angelegte Online-Abzocken auf gefälschten Verkaufsplattformen nehmen immer weiter zu. Hans-Joachim Henschel vom LKA Niedersachsen klärt über die neuen Tricks der Täter und über die Fahndungsarbeit der Polizei auf und gibt hilfreiche Tipps, wann man beim Online-Shopping misstrauisch werden sollte.

Der Wolf im Schafspelz

Sie machen einen seriösen Eindruck, haben eine „.de“-Domain und sogar ein Impressum, das keine Rechtschreibfehler enthält: Fakeshops werden immer professioneller. Das macht es für Verbraucher schwieriger, sie zu erkennen. Sicherheits-Checks, auf die man sich bisher verlassen konnte, reichen oft nicht mehr aus. „Fakeshops sind leider immer noch im Umlauf“, bestätigt Kriminalhauptkommissar Hans-Joachim Henschel vom Landeskriminalamt Niedersachsen. Erkennbar sind sie aber häufig daran, dass sie Markenware mit hohen Rabatten anbieten. Als Zahlungsart ist oft nur Vorkasse möglich. „Viele Fakeshop-Betreiber nutzen für ihren Webauftritt Daten existierender Firmen. So verstecken sich Fakeshops beispielweise in Unterverzeichnissen von aktiven Webseiten eines Vereins oder Restaurants. Hierbei nutzen die Täter Sicherheitslücken in der Programmierung oder schlecht gesicherte Webseiten aus, die

über Standard-Passwörter oder Phishing leicht zu knacken sind.“ In den Unterverzeichnissen werden dann eigene Fakeshop-Seiten gespeichert. Diese Verkaufsbereiche sind nur über entsprechend angepasste Links erreichbar, die von den Opfern per Mail oder Suchmaschine angeklickt werden. Ruft man hingegen die ursprüngliche URL der Webseite auf, lässt sich nichts Auffälliges feststellen. „Betreiber und Besucher merken also in der Regel gar nicht, dass ein Fakeshop im Unterverzeichnis sein Unwesen treibt“, so Henschel. Auch übernehmen die Täter gekündigte Domains von Webseiten, die nicht länger benötigt werden – etwa, weil ein Geschäft Pleite gegangen ist oder sich ein Verein aufgelöst hat. „Die Täter kaufen die Domain auf und errichten dort ihren Fakeshop. So kann es sein, dass unter der ehemaligen Domain eines Architekten nun Smartphones verkauft werden. Schaut man sich den Domainnamen an, so passt dieser nicht unbedingt zu dem angebotenen Produkt“, erklärt der Experte.

„Nur noch 3 Stück auf Lager“

KHK Hans-Joachim Henschel

Landeskriminalamt Niedersachsen, © LKA Niedersachsen

Die Betrüger bieten insbesondere Artikel und Markenprodukte an, die bei Online-Shoppern beliebt, günstig, dauerhaft verfügbar und kurzfristig lieferbar sind. „Das können zum Beispiel trendige Schuhe, aktuelle Smartphones, hochwertige Küchenmaschinen, aber auch Eintrittskarten für Veranstaltungen sein, die bei den offiziellen Stellen ausverkauft sind“, erklärt Henschel. „Während andere Geschäfte den begehrten Artikel nicht mehr anbieten, gibt es diesen ‚einen‘ Shop, wo ich das Produkt noch bekomme.“ Zudem werde mit zeitlich beschränkten Rabatten, zum Beispiel einem Countdown auf der Webseite oder den Verweis auf einen geringen Bestand wie „nur noch 3 Stück auf Lager“ künstlicher Druck aufgebaut und ein unüberlegter Kauf verstärkt. Auch nutzen die Täter die verkaufsstarken Jahreszeiten wie Ostern und Weihnachten sowie Verkaufsevents wie den „Black Friday“ oder „Cyber Monday“, bei denen besonders viel Umsatz zu erwarten ist.

Den Tätern auf der Spur

Immer häufiger werden die Betrugsfälle aus dem Ausland gesteuert. Oft stammen und agieren die Täter aus unterschiedlichen Regionen und Ländern und nutzen alle ihnen zur Verfügung stehenden Mittel, um anonym zu bleiben. „In der Regel stecken hinter den Fakeshops keine Einzeltäter“, weiß Hans-Joachim Henschel. „Vielmehr teilen sich mehrere Täter die Aufgaben.“ Während einer beispielweise den Webshop programmiert, kümmert sich ein anderer um die Transaktionen. Zudem werden sehr häufig ahnungslose Finanzagenten eingesetzt, die sich auf ein unseriöses Jobangebot eingelassen haben und über deren Konten der Geldfluss erfolgt. Laufen die Shops über ausländische Server, können die Internet-Service-Provider zwar durch die entsprechenden polizeilichen Ermittlungsbehörden auf die Problematik mit strafbaren Handlungen im Zusammenhang mit einem Fakeshop auf ihren Servern hingewiesen werden. Es liegt jedoch im Ermessen der Provider, wie der Fall weiterbehandelt wird. Um insbesondere internationalen Tätern besser entgegenwirken zu können, benötige die Polizei unter anderem flachere Hierarchien bei internationalen Auskünften. Laut der Zentralstelle für Internetkriminalität des LKA Niedersachsen können weiterführende Maßnahmen erst getroffen werden, wenn Tatzusammenhänge erkennbar werden. Aufgrund der föderalen Struktur der Polizei in Deutschland kann das allerdings einige Zeit in Anspruch nehmen. Mit den Informationskanälen von Europol sei aber grundsätzlich ein Anfang gemacht. Allerdings sei für Inhaltsdaten von ausländischen Anbietern immer der Weg der Rechtshilfe vorgeschrieben. Zwischenstaatlich bestehen über Eurojust Möglichkeiten des direkten Informationsaustausches nach vorheriger Vereinbarung.

Erst prüfen, dann kaufen

Seit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) ist die Abfrage nach dem Eigentümer einer IP-Adresse (DENIC-Auskunft) für Internetnutzer nicht mehr möglich. Dennoch empfiehlt das LKA Niedersachsen, einen sogenannten „Whois“-Dienst (z. B. domaintools.com) zu nutzen, um Grunddaten

über den Domaininhaber in Erfahrung zu bringen. Darüber hinaus kann die „Wayback Machine“ möglicherweise anzeigen, wie eine Webseite in der Vergangenheit aussah. „Zeigt das Ergebnis einen komplett anderen Inhalt im Vergleich zu heute, sollte man vorsichtig sein“, warnt Henschel. Suchmaschinen können ebenfalls genutzt werden, um genaueres über den Shop zu erfahren. Handelt es sich um einen Fakeshop, stößt man schnell auf andere Bewertungen von Geschädigten. Google Maps oder Streetview helfen bei einer genaueren Betrachtung der Örtlichkeit: Existiert die im Impressum angegeben Anschrift? Sieht das Gebäude nach einer Vertriebsadresse oder einem Ladengeschäft aus? Über eine Google-Rückwärtssuche für Bilder kann man auch nach Produktfotos aus einem vermeintlichen Fakeshop suchen lassen. Weitere Tipps fürs Online-Shopping:

- Kaufen Sie nur in Ihnen bekannten Shops. Sind Sie sich unsicher, nehmen Sie Kontakt zum Betreiber auf. Seien Sie misstrauisch, wenn der Kontakt nur über E-Mail erfolgen kann.
- Schauen Sie auf der Seite des Originalherstellers nach, ob dieser explizit vor Fakeshops bzw. angeblichen Outletshops der Marke warnt.
- Überprüfen Sie ggf. vorhandene Gütesiegel und führen Sie eine Gegenprobe beim Siegelaussteller durch.
- Nutzen Sie nur Bezahldienste, die Ihnen vertraut sind, oder den Kauf auf Rechnung. Vermeiden Sie Käufe und Überweisungen außerhalb von Geschäftszeiten Ihrer Bank (z. B. Freitagabend), um im Notfall einen Ansprechpartner bei Ihrer Bank zu erreichen.
- Folgen Sie keinen Links aus Spammails auf möglicherweise gefälschte Seiten.

KF (28.06.2019)

Folgende Artikel könnten Sie auch interessieren:

- Die neue Abteilung Cybercrime im BKA
- Mehr Sicherheit beim Online-Banking
- Gefährlicher als Phishing?
- Vorsicht vor Deep Fakes
- Mobile Fraud: Vorsicht vor gefälschten Apps
- Bankgeschäfte und Einkaufen im Netz

Alle Artikel dieser Kategorie

Weitere Infos zum Thema Internet und Mobil

Eltern sollten Inhalte genau prüfen

Riskante Spiele-Apps

Spiele-Apps für das Smartphone wie „Angry Birds“, „Candy Crush“ oder...[mehr erfahren]

Die Täter sehen alles

Digitales Stalking

Eine unangenehme Vorstellung: Jemand verschafft sich heimlich Zugriff...[mehr erfahren]

Was ist bei der Nutzung von sprachgesteuerten Lautsprechern zu beachten?

Wanzen im Wohnzimmer

„Smart Home“ – Mit diesem Trend halten viele mit dem Internet...[mehr erfahren]

„Verfolgen statt nur Löschen“ unterstützt NRW-Medien

Hetze im Netz ist strafbar

Im Zuge der so genannten Flüchtlingskrise wurde das Internet in den...[mehr erfahren]

Medienkompetenz für Eltern

Spiele muss man spielen, um sie zu verstehen

Jürgen Sleegers arbeitet am Institut „Spielraum“ der Fachhochschule...[mehr erfahren]

Cookie Einstellungen

☐Statistiken
☐Essentiell

Wir nutzen Cookies auf unserer Website, die in unserer Datenschutzerklärung beschrieben sind. Wir verwenden anonyme Statistiken, um unsere Website zu verbessern. Bitte unterstützen Sie unsere wichtige Präventionsarbeit und akzeptieren Sie alle Cookies. Vielen Dank!

Nur essentielle Cookies akzeptierenAlle akzeptieren