

**5,5
MILLIARDEN €**

Umsatz machte der Onlinehandel in Österreich im Vorjahr, ein Anteil von neun Prozent am Einzelhandel.



**39
PROZENT**

der österreichischen Internetnutzer sind wegen des Onlineshoppings im Netz, Tendenz steigend.

Schöne Bescherung

Falsche Webshops locken jetzt in die Falle. So gehen Sie beim Weihnachtseinkauf im Internet auf Nummer sicher.

Von Robert Prazak

Das Angebot klingt allzu verlockend: Nicht einmal 400 Euro soll ein nagelneues iPhone 6 kosten. Was für ein tolles Weihnachtsgeschenk! Doch das Smartphone wird trotz sofortiger Überweisung nicht rechtzeitig eintreffen, ja es wird überhaupt niemals geliefert. Der Internetshop war nämlich ein potemkinsches Dorf, dessen einziger Zweck darin bestand, gutgläubige Onlinekäufer auszunutzen wie die sprichwörtliche Weihnachtsgans. „Vor allem vor Weihnachten steigt die Gefahr, auf Fake-Webshops hereinzufallen“, sagt Sonja Schwarz, Projektleiterin der Watchlist Internet, einer Informationsplattform von Sozialministerium, Arbeiterkammer und Internet Foundation Austria, auf der aktuelle Betrugswarnungen zu finden sind.

Tatsächlich sind falsche Shoppingportale eine vergleichsweise einfache und günstige Möglichkeit für Betrüger, an Geld zu kommen. Sie bauen auf Gier und Gutgläubigkeit der Konsumenten – und auf das rasant wachsende Onlinegeschäft, das in fünf Jahren schon ein Viertel des Einzelhandels ausmachen wird (derzeit: rund neun Prozent).

GÜTESIEGEL Gut oder böse?

Mit dem österreichischen E-Commerce-Gütezeichen (Bild unten) können seriöse Anbieter identifiziert werden. Bisher haben sich 289 Unternehmen das Siegel geholt, das von Wirtschaftsministerium, Arbeiterkammer und Wirtschaftskammer unterstützt wird. Überregionale Onlinehändler vertrauen eher auf ihre Bekanntheit. Im Übrigen sind Zertifikate, die Webshops abbilden, für sich alleine kein ausreichender Hinweis. Nur wenn man nach Anklicken des Symbols auf die jeweilige Gütesiegel-Organisation gelangt, ist das ein gutes Zeichen.



Pro Tag sind österreichische Internetnutzer im Schnitt mehr als eineinhalb Stunden im Netz unterwegs – da ist die Gefahr groß, auf einen der unzähligen Fake-Shops hereinzufallen. Deren Tricks werden immer ausgeklügelter: Gütesiegel, PayPal-Hinweise, perfektes Design, gute Produktfotos – oft wirken die Seiten äußerst seriös. „Die Betrüger kopieren reale Shops und sind schwer zu entlarven“,

sagt Sonja Schwarz. Doch wie erkennt man Fake-Angebote? Die wichtigsten Tipps für sicheres Onlineshopping:

Preise vergleichen: Absurd niedrige Preise sollten Käufer stutzig machen, speziell bei aktuellen Elektronikwaren. Am besten auf Vergleichsplattformen wie etwa geizhals.at überprüfen, ob das Angebot überhaupt realistisch sein kann.

Impressum und AGB: Diese sind wichtige Hinweise, ob der Webshop seriös ist – wo keine zu finden sind, heißt es: Finger weg! Aber Achtung: Oft kopieren die Betrüger die Informationen echter Shops. Angegebene reale Adressen können mit Hilfe von Google Maps kontrolliert werden: Wenn sich die angebliche Firmenzentrale auf einem Feld befindet, sollte das zu denken geben. Hotmail- und GMX-Mailadressen sind verdächtig.

Bezahlmöglichkeiten kontrollieren: Wird Vorkasse als einzige Bezahlmöglichkeit angeboten, sollte das hellhörig machen. Allerdings bieten Gauner-Shops zunehmend vordergründig sichere Bezahlmethoden wie Kreditkarte oder PayPal an. „Das Geld ist dann oft verloren“, warnt Schwarz. Dann heißt es, auf eine Kulanzlösung seitens der Payment-Abwickler zu hoffen.

Nicht von Marken blenden lassen: Mit bekannten Modemarken locken Betrüger gutgläubige Onlineshopper in die Falle. Dazu integrieren sie Marken wie Michael Kors oder Ray-Ban in die Webadresse. Beim echten Unternehmen checken, ob besagter Webshop offizieller Handelspartner ist.

Länderkürzel sagen nichts aus: Ein .at-Kürzel für Österreich heißt nicht, dass der Webshop sicher ist. Webadressen können überall angemeldet werden. |

Aktuelle Übersicht über Fake-Webshops bietet www.watchlist-internet.at, derzeit wird unter anderem vor den Fake-Shops wieneu.eu, lager-verkauf.net und greeninnov-tech.com gewarnt.