

Zwischen Rabatt und Risiko - Wie Konsument*innen beim Online-Shopping in die Fallen von Cyber-Kriminellen tappen

Wissenschaftler der DHBW Karlsruhe erklärt psychologische Hintergründe

Black Friday, Singles Day, Prime Day – für viele Konsument*innen gehören diese Online-Shopping-Events längst zur festen Jahresroutine. Doch während Millionen nach dem „**Big Deal**“ suchen, ist auch für eine andere Gruppe Hochsaison: **Cyber-Kriminelle**, die Momente der Unachtsamkeit und Konsumfreude gezielt ausnutzen.

Von **Fake-Shops** über **Phishing-Mails** bis hin zu **Identitätsdiebstahl**. Die Maschen werden immer ausgefeilter. Dabei ist das Problem nicht nur technischer, sondern vor allem psychologischer Natur. Denn wenn der **vermeintliche Rabatt** nur **wenige Minuten** gilt oder eine **Kontosperrung droht**, bleibt wenig Zeit für **kritisches Denken**. Genau das nutzen Angreifer aus.

Der psychologische Tunnelblick

„Unser Gehirn liebt schnelle Belohnungen bei der Schnäppchenjagd und einfache Lösungen zur Gefahrenabwehr. Beides macht uns in Sachen Cyber-Sicherheit besonders anfällig“, erklärt Jan Michael Rasimus, Leiter des Eye Tracking-Labors der Dualen Hochschule Baden-Württemberg (DHBW) Karlsruhe. Seit Jahren beschäftigt er sich im Bereich des Neuromarketings damit, wie Entscheidungen im digitalen Raum unter verschiedenen Bedingungen getroffen werden.

Schnelle Belohnungen bei der Schnäppchenjagd: „Wenn ein Angebot zu gut klingt, um wahr zu sein, setzt häufig das kritische Denken aus. Und genau in diesem Moment schlagen Betrüger zu“, warnt Rasimus. Besonders bei **groß angelegten Rabattaktionen** geraten Nutzer*innen leicht in eine Art **psychologischen Tunnelblick**: Sie **handeln impulsiv, vertrauen Angeboten schneller und übersehen wichtige Warnzeichen**.

Einfache Lösungen zur Gefahrenabwehr: Emotionale Trigger wie Zeitdruck oder Dringlichkeit setzen viele unter **Zugzwang**. Das wissen auch Cyber-Kriminelle. Gerade während großer Shopping-Events platzieren sie gezielt **Handlungsaufforderungen**: etwa zur **Eingabe von Passwörtern auf gefälschten Seiten**, zur **Verhinderung angeblicher Kontosperrungen** oder zur **vermeintlichen Rückerstattung** von Geldbeträgen. Ziel ist es, in **Stresssituationen sensible Daten zu erschleichen**, bevor der Verstand wieder einsetzt.

Die neue Welle der KI-Fakes

Doch **psychologischer Druck** ist längst nicht alles. Betrüger rüsten ihre Maschen inzwischen mit **Künstlicher Intelligenz (KI)** technisch auf: **Phishing-Mails** werden personalisiert und automatisch versendet, täuschend echte **Fake-Shops** binnen Minuten erstellt, und **Chatbots** geben sich in Echtzeit als vermeintlicher Kundenservice aus.

Zunehmend kommen auch **Bilder** und **Videos** bekannter **Influencer*innen** ohne deren Wissen zum Einsatz, um **betrügerische Angebote** zu **bewerben**. Noch gefährlicher sind sogenannte **Deepfakes**: Künstlich erzeugte Videos von Prominenten, die scheinbar glaubhaft unseriöse Produkte bewerben. Solche Fälschungen sind häufig kaum noch von echten Inhalten zu unterscheiden, wirken vertrauenswürdig und sind damit besonders perfide. Diese Entwicklung zeigt: Cyber-Kriminalität ist längst kein Werk einzelner mehr, sondern Teil einer **professionellen, global vernetzten Schattenindustrie**, die genau weiß, wie **Menschen in Ausnahmesituationen** reagieren.

Schutz beginnt mit Bewusstsein

Auch wenn Cyberangriffe durch KI zunehmend raffinierter werden, bleibt der Mensch das größte Sicherheitsrisiko. Neben grundlegenden Verhaltenstipps, etwa zu besonderen Shopping-Events, sollte der **Fokus der Gefahrenabwehr** stets auf einem **bewussten** und **reflektierten Handeln** liegen. Gefragt sind vor allem kritisches Denken und die Fähigkeit, auch in hektischen Situationen einen kühlen Kopf zu bewahren.

Acht grundlegende Verhaltenstipps bei Shopping-Events

1. **Preise realistisch vergleichen**: Wenn Produkte (z. B. aktuelle Markenartikel) extrem günstig angeboten werden ist Vorsicht geboten. Preise, die zu gut klingen, um wahr zu sein, sind oft genau das.
2. **Anbieter überprüfen**: Ein vollständiges Impressum, erreichbarer Kundenservice und transparente Unternehmensdaten sind Grundvoraussetzungen für seriöse Online-Shops.
3. **Keine Käufe über Links aus Mails oder sozialen Medien**: Immer direkt über den Browser oder die offizielle App zum Shop navigieren, nie über zugesandte Links klicken.
4. **Sichere Zahlungsmethoden nutzen**: Finger weg von Vorkasse per Überweisung. Besser sind Zahlungsmethoden mit Käuferschutz (z. B. Kreditkarte, PayPal oder Rechnungskauf über Klarna).
5. **Gütesiegel prüfen, aber nicht blind vertrauen**: Trusted Shops, EHI oder TÜV-Siegel können ein Hinweis auf Seriosität sein. Aber: Fälschungen sind leicht gemacht. Siegel immer direkt auf der Website der Aussteller überprüfen.
6. **SSL-Zertifikate richtig einordnen**: Ein Schloss-Symbol im Browser zeigt nur, dass die Verbindung verschlüsselt ist. Nicht, dass der Shop an sich vertrauenswürdig ist.
7. **Verdächtige Seiten prüfen**: Shop-Namen einfach bei Google suchen (z. B. mit „[Shop-Name] + Erfahrungen“ oder „[Shop-Name] + Fake“). Auch Warnlisten der Verbraucherzentralen und Tools wie ChatGPT können helfen.
8. **Technischen Basisschutz ernst nehmen**: Systeme regelmäßig aktualisieren, starke Passwörter verwenden und, wo möglich, Zwei-Faktor-Authentifizierung aktivieren. Viele Angriffe zielen auf unzureichend gesicherte Konten oder veraltete Software.

Fazit

Cyber-Kriminalität rund um große Verkaufsaktionen ist längst **kein Randphänomen** mehr. Sie ist professionell organisiert und zielt zu 90 % auf die **„Schwachstelle Mensch“** ab. Emotionale Reize wie Zeitdruck, Rabatte oder Dringlichkeit versetzen Konsument*innen in einen **impulsiven Entscheidungsmodus**, in dem **kritisches Denken** häufig **aussetzt**. Der ideale Moment für Betrüger.

Künstliche Intelligenz macht Täuschungen zwar immer professioneller, doch so bedrohlich die technische Entwicklung auch ist: Der **wirksamste Schutz** bleibt das **eigene Bewusstsein**. Wer die **psychologischen Tricks** erkennt, kann mit **Vorsicht** und **Reflexion** gegensteuern. Besonders in heißen Phasen der Schnäppchenjagd, sind es meist Routine und Besonnenheit, die vor bösen Überraschungen schützen. Und das lässt sich durchaus trainieren.

Mit der Bitte um Veröffentlichung.

Jan Michael Rasimus steht gerne für ein Interview zur Verfügung.

<p>Susanne Diring Presse- und Öffentlichkeitsarbeit Tel.: 0721 / 9735-718 E-Mail: susanne.diring@dhw-karlsruhe.de</p>	<p>Jan-Michael Rasimus Leitung Eye Tracking-Labor Tel.: 0721 / 9735-865 E-Mail: janmichael.Rasimus@dhw-karlsruhe.de</p>
---	---