Black Friday: Kaufen Sie sicher ein

Ende November jeden Jahres locken Online-Shops mit grossen Preisreduktionen. Doch die Aktionen am sogenannten «Black Friday» oder in der «Black Week» locken nicht nur Kunden an, sondern auch Kriminelle. So schützen Sie sich.

Damit Sie im Internet möglichst sicher einkaufen, sollten Sie nachfolgende Empfehlungen beachten:

- Kaufen Sie nur bei bekannten und vertrauenswürdigen Online-Shops ein.
- Verwenden Sie auch bei Online-Shops sichere und einzigartige Passwörter (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/) .
- Seien Sie zurückhaltend bei Vorauszahlung. Bestellen Sie Ihre Ware, wenn immer möglich, auf Rechnung.
- Sorgen Sie dafür, dass Ihre Geräte mit unseren «5 Schritten für Ihre digitale Sicherheit (https://www.ebas.ch/5-schritte-fuer-ihre-digitale-sicherheit/) » gut geschützt sind.

Computer, Mobilgeräte, Fernseher oder Küchengeräte: Am Black Friday werden Detailhändler und Online-Shops von Schnäppchenjägern regelrecht überrannt. Viele Geschäfte machen den Umsatz des Jahres.

Wo viel Geld fliesst, sind auch Cyberkriminelle nicht weit entfernt. Falsche Shops und Phishing-Angriffe tauchen insbesondere gegen Jahresende gehäuft auf. Doch man kann sich schützen.

Fake Shops und falsche Schnäppchen

Beim Einkaufen im Internet wissen wir nie genau, mit wem wir es zu tun haben. Zahlreiche Tiefstpreisangebote locken Käuferinnen und Käufer.

Unseriöse Anbieter halten selten, was sie versprechen: Nach der Bestellung und Bezahlung ist das Warten auf die Lieferung meist vergebens. Manche dieser falschen Shops versuchen mit geschickten Ausreden, Sie davon abzubringen, die Überweisung zu stornieren oder Verdacht zu schöpfen: Angebliche Lieferengpässe, Schwierigkeiten mit dem Zoll oder fehlende Unterlagen.

Falsche Shops sind meist schwer zu erkennen. Teilweise sind sie gute Kopien existierender Shops. Fast immer wirken sie zunächst seriös. Einige typische Merkmale lassen jedoch Zweifel aufkommen.

Dubiose Internetadresse, Namen oder Logos

Viele Betrüger versuchen, bekannte Anbieter zu imitieren, indem sie die Internetadresse seriöser Shops unauffällig ändern, z.B. mit zusätzlichen oder ausgetauschten Buchstaben oder Zahlen wie zum Beispiel www.amaz0n.com (Ziffer «null» statt Buchstabe «o»). Achten Sie auch darauf, dass Internetadresse, Shop-Name, Logo und Post- bzw. Kontaktadresse übereinstimmen.

Zu günstige Preise

Oft sind angebliche Spezialangebote zu schön, um wahr zu sein. Vergleichen Sie den Preis eines Produkts daher mit denen anderen Online-Shops, zum Beispiel mithilfe von bekannten Preisvergleichsportalen wie www.toppreise.ch (http://www.toppreise.ch) . Ein brandneues iPhone etwa erhalten Sie wohl nirgends zum halben Preis.

Mangelhafte rechtliche Informationen

Shop-Websites müssen über ein Impressum mit Namen, Adresse und Telefonnummer sowie über Allgemeine Geschäftsbedingungen (AGBs) verfügen. Die darin enthaltenen Informationen sollten in korrektem Deutsch oder Englisch verfasst und plausibel sein. Fehlen diese Angaben oder machen sie einen unglaubwürdigen Eindruck, ist ein anderer Shop vorzuziehen.

Bewertungen und Gütesiegel

Bewertungen auf der Anbieter-Website selbst können gefälscht sein. Organisationen wie Trusted Shops (https://www.trustedshops.ch/) , der Schweizer Handelsverband (https://handelsverband.swiss/trustmark/swiss-online-garantie/) oder E-Commerce Europe (https://www.ecommerce-europe.eu/ecommerce-europe-trustmark/) zertifizieren dagegen seriöse Online-Shops und sammeln echte Bewertungen und Erfahrungsberichte von Endkunden. Sind letztere schlecht oder ist der Shop gar nicht gelistet, sollten Sie die Finger davonlassen.

Dubiose Zahlungsmethoden

Bei Anbietern, die nur Vorauszahlung oder Sofortüberweisung ermöglichen, ist Vorsicht geboten. Am sichersten ist die klassische Rechnung – oft wird diese aber auch von seriösen Shops nicht oder nur mit Zusatzgebühren angeboten. In den meisten Fällen ist die Zahlung per Kreditkarte die Standard- oder gar die einzige Option. In diesem Fall ist die Überprüfung des Shop-Betreibers vor dem Einkauf (siehe oben) besonders wichtig, um Ihre Kreditkartendaten vor Missbrauch zu schützen. Bei internationalen Webshops schützt PayPal zu einem gewissen Grad vor Betrug. Die Schweizer Variante Twint gilt ebenfalls als sicher, bietet jedoch bisher keinen vergleichbaren Käuferschutz.

Falls nach bereits erfolgter Zahlung Zweifel aufkommen, kontaktieren Sie unverzüglich Ihr Finanzinstitut, um eine Überweisung nach Möglichkeit rechtzeitig zu stoppen.

Phishing

Anstelle einen eigenen Fake Shop zu erstellen, begnügen sich viele Cyberkriminelle damit, eine Kopie eines realen, seriösen Anbieters wie z.B. Zalando, Galaxus oder Amazon zu erstellen. Das Vorgehen ist dabei dasselbe wie bei anderen Phishing-Angriffen (https://www.ebas.ch/phishing) : Der Endkunde erhält eine E-Mail, SMS oder Messenger-Nachricht vom vermeintlichen Shop, wonach er dringend eine Aktion durchführen müsse – zum Beispiel eine angebliche Bestellung oder Lieferung bestätigen oder seine Kontoangaben überprüfen, indem auf einen Link geklickt wird, welcher zur kopierten Website führt.

Das Ziel der Angreifer ist es, das Opfer auf die gefälschte Shop-Seite zu locken und dort seine eingegebenen Zugangsdaten oder Kreditkarteninformationen abzufangen, mit welchen die Betrüger anschliessend im echten Shop auf Kosten des Opfers einkaufen oder dessen Kreditkarte anderweitig belasten können.

Wie Sie sich vor Phishing-Attacken schützen, erfahren Sie hier (https://www.ebas.ch/phishing) .

Und schliesslich gilt beim Einkaufen im Internet die gleiche Empfehlung wie beim E-Banking: Ihr Gerät sollte mit den «5 Schritten für Ihre digitale Sicherheit (https://www.ebas.ch/5-schritte-fuer-ihre-digitale-sicherheit/) » geschützt sein, um Gefahren trotzen zu können.

Black Friday (englisch, «schwarzer Freitag») wird in den USA der Freitag nach Thanksgiving (englisch, «Danksagung») genannt und fällt auf den vierten Freitag im November. Er gilt als Beginn der Weihnachtseinkaufsaison. Viele Geschäfte animieren auch hierzulande mit Rabatten zum Einkaufen. Die Verkaufsveranstaltung wird teilweise zu ein-

er ganzen Woche ausgeweitet («Black Week» oder auch «Cyber Week»).