Checkliste «Sicher online einkaufen» (November 2013)

Grundsätzliches

Seriöse Webshop-Betreiber

- Das Aussehen einer Webseite und gute Kundenbewertungen sind keine guten Prüfkriterien für die Seriosität eines Webshop-Betreibers. Achten Sie statt dessen auf folgendes:
  - Hat die Webseite eine vollständige Adresse mit Strassennamen, Nummer und Ortschaft, die auf www.search.ch oder www.directories.ch auffindbar ist?
  - Stimmt die Telefonnummer, unter der man die Betreiber erreichen kann, mit den Angaben auf www.search.ch oder www.directories.ch überein?
  - Was wird in Foren und Blogs über die Betreiber berichtet? Machen Sie dazu eine Google-Suche mit dem Namen des Webshop-Betreibers.
  - Bei Firmensitzen im Ausland und seltsamen Firmenformen in Steueroasen sollten sie kritisch sein!

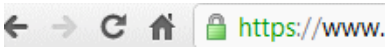
Passwörter

- Namen, Geburtstage oder ähnliches von Familienangehörigen und Freunden sind denkbar ungeeignete Passwörter!
- Datenschützer empfehlen: Mindestens 10 Zeichen; Einsatz von Gross- und Kleinbuchstaben; Mix aus Zahlen, Buchstaben und Sonderzeichen; Zeichen doppelt verwenden.

Zahlungen

Sichere Zahlungsverbindungen im Browser

- Achten Sie darauf, dass Sie Kreditkarten- oder Bankdaten nur eingeben, wenn die URL auch eine «HTTPS»-gesicherte Verbindung anzeigt. Nur dann sind Ihre Daten vor Fremdzugriffen geschützt! So sehen sichere Verbindungen aus:



Zahlungen über PayPal und Kreditkarten

- Beide Verfahren haben den Vorteil, dass schnell und einfach Geld überwiesen werden kann. Ausserdem können Sie im Missbrauchsfall die Zahlungen zurückziehen. Bei PayPal müssen Sie darauf achten, dass niemand Ihr Passwort kennt. Bei Kreditkarten ist darauf zu achten, dass Sie Ihre Karte nie jemandem überlassen, da im Regelfall Ihr Name, die Nummer und der Sicherheitscode für einen Online-Einkauf ausreichen. Grundsätzlich gilt: Abrechnung immer sofort überprüfen und wenn nötig Einspruch erheben.

Überweisung mit Geldtransferservices (Western Union, Moneygram o.ä.)

- Wenn Sie bei einem Online-Einkauf zu einer Zahlung via Geldtransferservice aufgefordert werden, ist grundsätzlich Skepsis angebracht. In vielen Betrugsfällen werden Überweisungen über Geldtransferservices gefordert, da man sie anonym nutzen und Geld nicht mehr zurückgefordert werden kann.

Superschnäppchen

- Sehr günstige Angebote werden mitunter auch als Lockvogel eingesetzt. Beachten Sie aber, dass nicht selten ein Super-Sonderangebot online zum Verkauf angeboten wird und nach erfolgter Anzahlung dieses so genannten Schnäppchen nie geliefert wurde. Wenn etwas «zu schön ist, um wahr zu sein!» dann ist es meist auch nicht wahr. Niemand hat etwas zu verschenken!

Ihre Rechte beim Onlinekauf

Allgemeine Geschäftsbedingungen (AGB)

- Die AGB eines Webshops bilden die Vertragsgrundlage, die Sie mit dem Händler eingehen. Mit dem Kauf akzeptieren Sie diese, auch wenn darin Sachverhalte anders als im Schweizer Recht geregelt sind. In der Schweiz besteht grundsätzlich Vertragsfreiheit, allerdings haben AGBs Vorrang vor dem Obligationenrecht (OR), sofern diese nicht sittenwidrig sind.

Rücktrittsrecht vom Kauf

- Ein gesetzlich geregeltes Rücktrittsrecht von Online-Einkäufen gibt es nicht. Das Rücktrittsrecht (bis 7 Tage nach Kauf) gilt nur bei Haustürgeschäften! Genaueres zum Rücktrittsrecht beim Online-Einkauf finden Sie in den AGBs des jeweiligen Webshop-Betreibers.

Risiken beim Onlinekauf

Fremde Computer

- Tätigen Sie keine Online-Geschäfte über fremde Computer (z.B. in Internetcafés)! Solche Computer können mit Keyloggern verseucht sein, die Ihre Tasten-Eingaben mitprotokollieren und sie an Betrüger übermitteln. Falls es einmal nicht anders geht, verwenden Sie die Bildschirmtastatur, diese kann nicht protokolliert werden.

Phishing

- Betrüger versuchen, Ihre Zugangsdaten über Phishing-Methoden zu stehlen. Dabei erhalten Sie gefälschte E-Mails, die anscheinend von Ihrer Kreditkartenfirma, Ihrer Bank oder Ihrem Auktionshaus verschickt wurden. Darin werden Sie aufgefordert, Ihre Daten zu bestätigen oder anzugeben. Solche E-Mails immer löschen! Seriöse Firmen fragen Sie nie per E-Mail nach persönlichen Daten!

Social Engineering

- Social Engineering bezeichnet u.a. das Ausspionieren von Passwörtern im persönlichen Kontakt. Betrüger können Ihre Kontoinformationen nutzen, um sich z.B. in Ihr eBay Konto einzuloggen und in Ihrem Namen einzukaufen. Achten Sie auf sichere Passwörter und geben Sie diese niemals an Dritte weiter!

Produktfälschungen

- Hier warnen wir insbesondere vor gefälschten Medikamenten, die über Auktionen oder dubiose, zum Teil via Spam beworbene, Webseiten angeboten werden. Bei der Produktion von gefälschten Medikamenten werden oft unwirksame oder sogar schädliche Wirkstoffe verwendet!

Zusätzliche, spezifische Sicherheitshinweise

Für sicheres Einkaufen bei Online-Auktionen, siehe unsere Checkliste «Sicherer unterwegs bei eBay»

- Prüfen Sie die Bewertung des Verkäufers und achten Sie darauf, dass nicht immer die gleichen Leute den Anbieter positiv bewerten bzw. er bei diesen positive Berichte schreibt.

Auto / Motorradkauf

- Hier nahmen die Betrugsversuche in den letzten Jahren zu. Informieren Sie sich auf unserer Anti-Betrugswebseite.

Vermeintliche «Gratis»-Angebote und -Abonnemente; Abofallen

- Diese Betrugsart gibt es vorwiegend im deutschsprachigen Raum. Dabei entpuppt sich ein als Gratis-Angebot (kostenloses Downloadarchiv) ausgeschriebenes Webangebot als sehr teurer «zahlungspflichtiger» Service. Als Schweizer oder Schweizerin haben Sie in einem solchen Fall die Möglichkeit, sich auf «Irrtum» zu berufen. (OR Art. 24)

Weitere Informationen zum Thema «Sicher online einkaufen» finden Sie auf der Webseite unserer Anti-Betrugskampagne: www.den-trick-kenne-ich.ch