

## Thema: Online-Shopping / Weltfrauentag

Zeichen Artikel: 13.290 (mit Leerzeichen)

### Shoppern ohne Reue

*"Retail Therapy" nennen die Engländer(innen) ausgedehnte Shopping-Touren zur Bekämpfung von Liebeskummer, Lebensschmerz und anderen akuten Frustzuständen. Auch wenn es immer noch am schönsten ist, die Objekte der Begierde selbst in den Händen zu halten, finden heute immer mehr Beutezüge virtuell statt. Bequem vor dem schicken Netbook oder Notebook neben sich eine Tasse Tee oder ein Glas Rotwein. So ein Einkaufsbummel kennt weder schlecht gelaunte Verkäuferinnen noch Gedränge in überfüllten Läden oder abgelaufene Parktickets. Ideale Voraussetzungen also, um sich so eine Shopping-Tour zum internationalen Frauentag am 8. März zu gönnen.*

Doch neben den unbestrittenen Vorteilen sorgt der schnelle Einkauf per Mausclick immer wieder für negative Schlagzeilen. Wer nicht sieht, was er kauft, muss sich auf die Angaben des Shops verlassen. Die können stimmen, eine Garantie dafür gibt es jedoch nicht. Und dass die Louis-Vuitton-Tasche außer einer marginalen Ähnlichkeit nichts mit dem Original zu tun hat, bemerken Sie erst nach der Lieferung. Dann ist das Geld bereits abgebucht. Die erste Sicherheitsmaßnahme sollte daher der gesunde Menschenverstand sein. Extrem niedrige Preise für teure Markenartikel klingen nicht nur zu gut um wahr zu sein, sie sind es in der Regel auch. Sehen Sie sich zunächst gründlich im Web-Shop um. Ist das Impressum vollständig, mit Geschäftsführer, Adresse und Steuernummer? Sind die allgemeinen Geschäftsbedingungen an prominenter Stelle hinterlegt? Wenn Sie sich unschlüssig sind, bringt oft die Suche nach dem Anbieternamen bei einem Bewertungsforum wie Ciao.de Klarheit darüber, ob es sich um eine empfehlenswerte Firma handelt.

Doch selbst wenn Sie bei einem seriösen Händler einkaufen, kann die Shopping-Tour danebengehen. Cyberkriminelle nutzen das Internet verstärkt für ihre Aktivitäten. Es geht um viel Geld - es werden jedes Jahr Millionenbeträge durch Online-Betrug ergaunert. Anfang Januar war die so genannte "Aurora"-Sicherheitslücke im Web-Browser Internet Explorer von Microsoft dafür verantwortlich, dass Cyberkriminelle Zehntausende von Computern ausspähen konnten. Die Angreifer verwenden immer raffiniertere Programme, die weitgehend automatisch arbeiten. Ob die Schadsoftware per E-Mail verschickt wird, auf einer geknackten Webseite lauert oder hinter dem Link einer Spam-Mail versteckt ist, spielt keine Rolle. Immer geht es darum, Zugriff auf den Computer zu erlangen und illegal Geld zu verdienen. Zum Beispiel in dem der Rechner als Basis für weitere Spam-Mails oder als Speicherplatz für Raubkopien vermietet wird. Oft werden auch die Zugangsdaten zu Web-Mail Diensten oder großen Online-Shops abgehört und verkauft. Im schlimmsten Fall versuchen die Cyberkriminellen, an die Zugangsdaten für das Bankkonto zu kommen und Geld auf ein eigenes Konto zu transferieren.

Der Schutz vor solchen und ähnlichen Attacken ist Sache einer Sicherheitssoftware. Aber während es früher genügte, den Computer vor Viren zu schützen, mussten sich die Schutzprogramme enorm wandeln. Die meisten Schadprogramme beherrschen heute zahlreiche Tricks, um sich zu tarnen und zu verstecken. Mittlerweile reagieren die digitalen Wächter bereits dann, wenn sie Programme finden, die sich verdächtig verhalten. Die Schutzsoftware überwacht auch den Web-Browser und erkennt zuverlässig, wenn Sie auf eine Phishing-Seite umgeleitet werden sollen.

Aber sie können auch selbst dafür sorgen, dass der virtuelle "Gönn-Dir-was"-Shoppingausflug ein reines Vergnügen bleibt: Achten Sie darauf, dass der Shop-Betreiber auf jeden Fall eine verschlüsselte Verbindung für die Transaktion anbietet, zumindest dann, wenn es ans bezahlen geht. Meist erkennt man Verschlüsselung an einem kleinen Schloss-Symbol oder der geänderten Farbe der Adressleiste. Diese Verschlüsselung ist sehr sicher und kann mit vertretbarem Aufwand nicht geknackt werden. Hier droht Ihnen tatsächlich keine Gefahr. Übrigens: auch die Polizei gibt auf ihrer Webseite „Online kaufen mit Verstand“ wertvolle Tipps für den sicheren Einkaufsbummel vor dem Bildschirm:

<https://www.kaufenmitverstand.de/home/home.php>. Englischsprachige Leser finden unter dem Link: <http://www.oft.gov.uk/html/shopping/index.html> ähnliche Informationen.

### **Meins, meins, meins!**

Es muss nicht immer Neuware sein, auch Schnäppchen von eBay können glücklich machen. Rechtzeitig zum Weltfrauentag am 8. März werden wieder unzählige Geschenke ersteigert werden, entweder von Ihrem aufmerksamen Partner oder von Ihnen selbst. Schließlich bietet sich so ein Tag ideal an, um sich etwas zu gönnen. Und die diversen Auktionsseiten im Internet haben alles, wirklich alles im Programm, was das Frauenherz höher schlagen lässt. Von der hochwertigen Kosmetika über Mode, Bücher, Sportartikel und Reisen - mit eBay und Co. bleibt kein Wunsch offen. Dass Sie nach dem Zuschlag nur Grund zur ungetrübten Freude haben, liegt jedem Beteiligten am Herzen, allen voran dem Auktionsbetreiber.

Ob eBay, QXL, eBid.net, Allegro.pl oder Sothebys - alle tun ihr möglichstes, um Auktionen so sicher wie möglich zu gestalten. Sie prüfen, zumindest teilweise, die Identität der Teilnehmer, überwachen Auktionen auf Fälschungen und greifen bei Beschwerden ein. Zudem hilft das Konzept der Bewertungen von Käufer und Verkäufer dabei, Vertrauen herzustellen. Allerdings sind Betrugsversuche nicht unüblich, immer wieder versuchen Anbieter anstelle des tatsächlichen Produkts nur die Verpackung oder ein Bild des Artikels zu verkaufen. Manchmal wird auch Bezahlung per Vorkasse gefordert und dann schlichtweg nichts geliefert. Der Verkäufer tröstet seinen Kunden zunächst, ist dann immer schlechter erreichbar und taucht schließlich ganz unter. Doch die große Mehrheit der Online-Auktion läuft völlig unproblematisch ab und die Garantieprogramme der Auktionsbetreiber federn die meisten Streitfälle ab.

Damit Sie solche Maßnahmen gar nicht erst in Anspruch nehmen müssen, gilt eine einfache Grundregel: schützen Sie Ihre persönlichen Daten! Fast alle Betrugsversuche bei Online-Auktionen basieren auf gefälschten Nutzerkonten oder gestohlenen Zahlungsmitteln. Nachdem die Auktionsanbieter Neumitglieder am liebsten durch einen Abgleich mit Schufa-Informationen oder einem Postident-Verfahren identifizieren, sind

Informationen, mit denen sich diese Checks umgehen lassen, für Kriminelle bares Geld wert. So sollten Sie misstrauisch werden, wenn Ihnen der Verkäufer nach der Auktion Kontodaten schickt, die sich von den in eBay eingetragenen Daten unterscheiden.

Noch einfacher wird ein Betrug, wenn die Angreifer an die Anmeldeinformationen der Auktionsteilnehmer kommen. Damit können Auktionen eröffnet und Artikel ersteigert werden. Die Betrüger stecken Geld oder Ware ein und das Opfer muss eBay und den anderen Geschädigten erst einmal nachweisen, dass die Account-Daten gestohlen wurden. Allein um einen solchen Fall auszuschließen, lohnt sich der Einsatz einer umfassenden Internet-Sicherheitslösung. Diese Programme überwachen den Computer und alle Verbindungen mit dem Internet. Denn die Kriminellen nutzen oft Schadsoftware wie Trojaner, die unbemerkt von Ihnen auf dem Computer installiert werden und dort Anmeldeinformationen ausspionieren. Ein so genannter Keylogger zeichnet jeden Tastenanschlag auf, egal ob es sich dabei um das Passwort für die Online-Banking Webseite oder um die Bewerbung für einen neuen Job geht. Sicherheitssoftware kann Angriffe mit Trojanern und Keyloggern erkennen, abblocken und Alarm schlagen.

Noch häufiger sind so genannte Phishing-Angriffe. Sie verwenden gefälschte E-Mails um die Opfer auf ebenfalls gefälschte Webseiten zu locken, wo die Anmeldeinformationen mitgeschnitten werden. So könnten Sie eine Mail im elektronischen Briefkasten finden, die angeblich von eBay selbst stammt. Dort wird auf eine absurd hohe Rechnung hingewiesen, die bald Ihrem Konto belastet wird. Klicken Sie auf den Link in der Mail, sieht das nun aufklappende Fenster wie der Startbildschirm bei eBay aus, in den Sie Ihren Benutzernamen und Ihr Passwort eingeben. Eine gute Sicherheitssoftware schützt doppelt vor dieser Art der Attacke. So erkennt das Programm bereits die E-Mail als Betrugsversuch und löscht sie automatisch. Klicken Sie trotzdem auf einen verdächtigen Link, warnt die Software vor einem möglichen Phishing-Angriff und blockt den Zugriff auf die Webseite.

Übrigens: eBay hat unter <http://pages.ebay.de/sicherheitsportal/> ein Sicherheitsportal mit vielen Tipps und Online-Schulungen eingerichtet. Hinweise, wie man Betrugsversuche erkennt und abwehrt, finden sich auch auf vielen anderen eBay Länderportalen wie hier in der englischen eBay Variante: <http://pages.ebay.co.uk/safetycentre/index.html>. Denn Übung macht den Meister, auch bei Wohlfühlangeboten für einen entspannten Weltfrauentag.

## Endlich Sonne sehen

Man braucht nicht unbedingt einen Grund um bei Minustemperaturen, Schneematsch und Dauergrau Sehnsucht nach Sonne zu verspüren. Aber wenn Sie noch mit der Entscheidung kämpfen - der Weltfrauentag am 8. März wird international gefeiert. Warum nicht an einem Strand in der Karibik, auf einem Gipfel über der Schneewolckendecke oder in einer spannenden Stadt im Süden? Ist die Entscheidung für den Kurztrip erst gefallen, stellt die Buchung keine Hürde mehr da. Reisen lassen sich heute problemlos im Internet buchen, virtuelle Reisebüros bedienen jeden Anspruch von Last Minute bis hin zum Luxustrip.

Doch während früher die größte Gefahr darin bestand, einem vermeintlichen Schnäppchenangebot auf den Leim zu gehen und zwei Woche in einer Bauruine mit

Kantinenfraß zu verbringen, müssen Sie sich heute vor Cybercrime in Acht nehmen. Oft wird das sogenannte Phishing genutzt, um an Anmeldedaten zu kommen. Beliebte sind angebliche Mails von großen Online-Reiseveranstaltern wie Opodo und Expedia mit unwiderstehlichen Sonderangeboten. Sie glauben, die vertraute Webseite des Reiseportals zu sehen, sind aber in Wirklichkeit auf der gefälschten Seite der Online-Gauner gelandet. Diese Phishing-Angriffe sind mittlerweile so ausgefeilt, dass sie selbst von erfahrenen Computernutzern nicht mehr erkannt werden. Gute Sicherheitssoftware schützt Sie und den PC vor solchen Attacken. Im Idealfall erkennt das Programm bereits die E-Mail mit dem Link als Betrugsversuch und löscht sie automatisch. Klicken Sie trotzdem auf eine verdächtige Web-Adresse, warnt die Software vor einem möglichen Phishing-Angriff und blockiert den Zugriff auf die Webseite.

Immer wieder gern genommen ist eine E-Mail mit Schadsoftware im Anhang. Angeblich hat man eine horrend teure Reisebuchung vorgenommen, die angebliche Rechnung installiert aber nach dem Anklicken einen Trojaner auf dem Computer. Solche Trojaner spähen Passwörter, Kreditkartendaten und TAN-Nummern aus. Hat sich solch ein Trojaner erst einmal eingenistet, bekommen Sie ihn nur mit Mühe wieder los, manchmal hilft nur eine Neuinstallation des Betriebssystems. Am besten sperren Sie solche digitalen Schädlinge gleich aus, auch hier ist eine aktuelle und umfassende Sicherheitssoftware der beste Schutz. Mittlerweile finden die digitalen Wächter Schädlinge bereits, wenn sie sich verdächtig verhalten. „Behaviour Monitoring“ – Verhaltensüberwachung - nennen die Hersteller diese Fähigkeit.

Wichtig ist auch, dass das digitale Reisebüro auf jeden Fall eine verschlüsselte Verbindung für die Transaktion anbietet, spätestens dann, wenn es an das Bezahlen geht. Oft weisen die Betreiber an der virtuellen Kasse explizit darauf hin, man kann die Verschlüsselung aber auch an einem kleinen Schloss-Symbol oder der geänderten Farbe der Adressleiste des Web-Browsers erkennen. Diese Verschlüsselung ist sehr sicher und kann mit vertretbarem Aufwand nicht geknackt werden. Hier droht Ihnen tatsächlich keine Gefahr.

Endlich geht es los, Sie fiebern am Flughafen dem Boarding entgegen um das gräuliche Wetter in hinter sich zu lassen. Da könnten Sie doch noch eine schnelle Abschiedsmail an die armen Kollegen im Büro schicken, schließlich ist das schicke Netbook auch im Handgepäck. Doch denken Sie daran: Wer zu Hause online geht, tut das in der Regel über einen Router. Der hält mit seiner eingebauten Firewall als vorgeschaltete Hürde viele Gefahren aus dem Internet ab. Per WLAN-Hotspot am Flughafen online zu sein, heißt direkt mit dem Internet zu kommunizieren, ganz ohne zwischen geschaltete Barriere. Schon seit vielen Jahren prüfen automatisierte Programme wahllos IP-Adressen nach Schwachstellen ab, es dauert weniger als eine Minute, bis so ein Tool einen neu ins Internet eingeloggt PC findet. Ist eine der gesuchten Schwachstellen auf Ihrem Smartphone noch nicht durch einen entsprechenden Patch entschärft, kann ein Angreifer innerhalb von Sekunden von Ihnen unbemerkt Crimeware installieren.

Aktuelle Sicherheitssoftware stellt sich schützend vor Ihre digitale Kommunikation, ob in München, Kapstadt oder Bangkok. Je mehr Sie mit Ihrem elektronischen Begleiter fernab des Privatnetzwerks tun wollen, desto mehr sollte das Schutzprogramm können. Viren erkennen und stoppen ist die Mindestanforderung, doch reiner Virus-Schutz wirkt nicht gegen Schwachstellen im Betriebssystem oder einen aktiven Lauschangriff auf die

Kommunikation. Achten Sie daher auch auf eine intelligente Firewall, die eingehende Verbindungen erkennt und auf ihre Absichten untersucht.

**Redaktionskontakt:**

essential media GmbH  
Florian Schafroth  
Florian.Schafroth@essentialmedia.de  
Tel.: +49-89-7472-62-43  
Fax: +49-89-7472-62-843  
Augustenstraße 24  
80333 München

Kaspersky Labs GmbH  
Christian Wirsig  
christian.wirsig@kaspersky.de  
Tel.: +49-841-98-189-241  
Fax: +49-841-98-189-100  
Steinheilstraße 13  
85053 Ingolstadt

© 2009 Kaspersky Lab. The information contained herein is subject to change without notice. The only warranties for Kaspersky Lab products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Kaspersky Lab shall not be liable for technical or editorial errors or omissions contained herein.