

EgisTec / Sicheres Weihnachts-Shopping

10 Tipps für mehr Sicherheit beim Geschenke einkaufen im Internet

Jetzt geht es los: das große Weihnachtshopping. Doch ebenso, wie Weihnachtsmärkte Taschendiebe anziehen, zieht der Internet-Advent auch Online-Gauner an, die im Web ihre Fallen aufspannen. EgisTec gibt zehn Tipps, wie Geschenkesuchende unbeschwert durch Shops surfen und auch sonst sicher am PC arbeiten können.

Taipei, Taiwan / München, 8. Dezember 2009

Taschendiebe gibt es auf Weihnachtsmärkten, seitdem es Weihnachtsmärkte gibt. Und seitdem es das Internet gibt, gibt es eben auch Internet-Kriminelle. „Im Internet einzukaufen ist trotzdem nicht gefährlicher als in der Einkaufspassage.“, weiß **Steve Ro**, CEO von EgisTec. „Doch analog zum gefälschten Bankautomaten, der Kontodaten stiehlt, gibt es im Web gefälschte Webseiten, die Zugangsdaten abgreifen. Man darf also durch die virtuelle Warenwelt keineswegs sorgloser spazieren, als man es auch durch die Wirklichkeit täte.“ Das Sicherheitsunternehmen EgisTec schlägt zehn Verhaltensregeln vor, die das Online-Leben sicherer machen.

1. PC-Sicherheit erhöhen

Stellen Sie sicher, dass Ihr Rechner prinzipiell „sicher“ ist. Laden Sie dazu die neuesten Aktualisierungen für das Betriebssystem herunter. Deaktivieren Sie *nicht* die automatische Update-Funktion. Verwenden Sie außerdem stets die jüngste Version Ihres Webbrowsers. Erwerben Sie eine Sicherheitssoftware mit einem Virens Scanner, der einen Echtzeitschutz im Hintergrund verwendet. Aktualisieren Sie auch den Virens Scanner vor dem Einkaufen.

2. Nicht jeden virtuellen Laden betreten

Einen „Shop“ im Internet zu eröffnen ist einfach und billig – auch für Gauner und Abzocker. Informieren Sie sich daher vor dem Anmelden in einem Webshop, ob dieser vertrauenswürdig ist. Achten Sie auf Anbietertransparenz: Gehen Identität und Anschrift des Anbieters (möglichst in Deutschland) sowie seine Bedingungen für Garantie, Gewährleistung, Widerruf und Rückgabe eindeutig aus dem Impressum hervor? Sind die AGBs leicht auffindbar und verständlich? Sind alle Preise klar und unmissverständlich angegeben? Existieren Medienberichte über diesen Shop? Dies, und ob andere Nutzer im Web schon mal in diesem Shop gekauft haben, lässt sich mit einer Suchmaschine ermitteln. Meist lässt sich sagen: Je länger ein Shop im Geschäft ist, desto vertrauenswürdiger ist er.

3. Möglichst auf Rechnung zahlen, Kreditkarten meiden

Viele Shops bieten die Möglichkeit, per Rechnung, Bankeinzug oder Kreditkarte zu bezahlen. Es steht völlig außer Zweifel, dass die meisten Shop-Betreiber sich auch Mühe geben, die Daten ihrer Kunden zu schützen. Und doch werden immer wieder Fälle bekannt, in denen Datensätze von Kunden im Web auftauchen oder in Hacker-Foren gehandelt werden. Abhilfe schafft nur, diese Daten gar nicht erst ins Internet zu bringen. Daher sollten Sie jede Möglichkeit nutzen, vor allem auf Rechnung zu zahlen. Wenn das nicht geht, dann Bankeinzug. Auf Kreditkarte und Vorkasse sollten Sie nur im Notfall zurückgreifen.

4. Sichere SSL-Datenübertragung wählen

Alle Daten, die im Web vom Besucher zur Website fließen, müssen auf dem Weg dazwischen unsichtbare Zwischenstationen überqueren – jede von Ihnen kann theoretisch mitlesen. Daher ist es wichtig, vertrauliche Daten wie Kontodaten und Kreditkartennummer nur über verschlüsselte Wege zu übertragen. Versenden Sie daher niemals Ihre Kontodaten und Kreditkartennummer per E-Mail. Achten Sie bei der Eingabe dieser Daten auf den Formularseiten eines Shops darauf, dass der Browser die Webadresse mit **https://** beginnend zeigt, denn das zusätzliche „s“ steht für eine verschlüsselte („secure“) Datenverbindung. Zusätzlich zeigt der Browser ein **geschlossenes Vorhängeschloss-Symbol**. Bietet ein Shop keine sichere Datenübertragung bei der Eingabe Ihrer Kontodaten samt Zahlungsarten, dann ist ein anderer Shop unter Umständen ratsamer.

5. Sichere Passwörter verwenden

Die meisten Shops versorgen Sie letztlich mit einem Zugang, der aus einem Benutzernamen (oder E-Mail-Adresse) und einem Passwort besteht. Vorsicht: Wer diese Daten hat, kann in Ihrem Namen einkaufen! Achten Sie daher darauf, stets ein sicheres Passwort zu wählen. Ein sicheres Passwort ist **mindestens zehn Zeichen lang** und besteht aus kleinen und großen Buchstaben und einigen Ziffern, also zum Beispiel „PRLsna2410“. Meiden Sie komplette Wörter („sesam“), Bestandteile Ihres Namens, Kosenamen für Partner und Haustiere oder ähnliche Begriffe - denn sie lassen sich erraten und daher leicht knacken.

6. Mehrere Passwörter verwenden

Hat ein Hacker ein Konto geknackt, ist er im Besitz eines Passwortes. Wenn ein Einkäufer in jedem Shop dieselben Zugangsdaten verwendet, kann sich ein Hacker theoretisch auch in den anderen Shops Zugang verschaffen. Abhilfe schafft, in jedem Shop ein eigenes, sicheres Passwort zu verwenden und kein Passwort in zwei Shops gleichzeitig zu benutzen.

7. Daten sicher verschlüsseln

Viele Anwender speichern ihre Kontodaten auf dem PC oder Notebook, um diese leichter per Cut & Paste eingeben zu können. Auch die Zugangsdaten werden oft direkt auf dem PC gespeichert. Gelangt das Gerät in falsche Hände, befinden sich die vertraulichen Zugangsdaten dann in den Händen Dritter. **EgisTec hilft hier mit einem cleveren Produkt: EgisTec MyWinLocker 3** verschlüsselt das gesamte Windows oder einzelne Daten mit Hilfe des AES-Verfahrens. Speichert der Benutzer seine Kontodaten und Passwörter im sogenannten **Yo-Safe**, einem virtuellen Datenträger, sind diese Daten für Hacker, Spione und Notebook-Diebe unzugänglich. Lässt der Benutzer MyWinLocker 3 das komplette Windows verschlüsseln, sind sogar die im Browser gespeicherten Zugangsdaten geschützt.

8. Datensparsamkeit wahren

Gehen Sie sparsam mit Ihren Daten um. Einfach gesagt: Was Sie ins Internet hineinschreiben, das lässt sich dort schwer wieder löschen. Ein Shop braucht ganz sicher Ihren Namen, Ihre postalische Adresse für den Versand und Ihre E-Mail-Adresse für eine Kaufbestätigung – mehr persönliche Daten braucht der Shop jedoch nicht. Übrigens: Der Gesetzgeber schreibt in Deutschland auch einem Shop vor, dass er nur solche Daten erheben darf, die für die geschäftliche Transaktion wirklich notwendig sind.

9. Daten vernichten

Geizen Sie auch mit Daten auf Ihrem PC: Wer sich zum Beispiel vom Weihnachtsgeld einen neuen Rechner kauft oder den vorhandenen aufrüstet, verscherbelt oft seinen alten Rechner oder die benutzte Festplatte über entsprechende Gebrauchtbörsen. Mit normalen Methoden „unsicher gelöscht“ Dateien mit Zugangsdaten und Kontodaten können so in die Hände von Unbefugten fallen, die Gelöschtes mit Hacker-Tools wieder sichtbar machen können. **Abhilfe schafft EgisTec Shredder**: Dieses Tool zur hochsicheren Zerstörung sensibler Daten vernichtet Files so, dass sie sich selbst mit teuren Spezial-Tools nicht mehr auslesen lassen. Bei Abhandenkommen des mobilen Rechners schützt **EgisTec Trust Delete** vor Datenklau: Diese Fernlösch-Software erlaubt es dem Besitzer eines Notebooks, vertrauliche Daten auch dann auf einem mobilen PC zu löschen, wenn der gestohlen wurde – eben aus der Ferne.

10. Vorsicht vor Phishing

Niemals wird ein „Mitarbeiter“ eines seriösen Shops bei Ihnen anrufen oder per Mail aus fadenscheinigen, meist „dringenden technischen“ Gründen Ihr Passwort erfragen wollen. Besondere Vorsicht ist auch angesagt, wenn Mails Sie aus nebulösen Gründen mit Links zu Shops locken, und Sie direkt nach dem Anklicken des Links auf einer Anmeldeseite landen: Es kann sich dabei um eine **Phishing-Attacke** handeln, bei der man versucht, Sie mit Hilfe einer täuschend echt aussehenden, aber gefälschten Shop-Webseite dazu zu verführen, Ihre

Kontodaten preiszugeben. Abhilfe: Beginnen Sie Ihren Einkauf stets auf der Hauptseite des Shops, dessen Web-Adresse Sie selbst in die Browserzeile eingeben.

Mehr Sicherheit mit EgisTec-Produkten

Die günstigen Sicherheitsprodukte von EgisTec ergänzen vorhandene Sicherheitsfunktionen von Microsoft Windows, laufen auf allen Windows-Versionen (Windows 7 32/64-bit, Windows Vista 32/64-bit, Windows XP 32-bit) und sind als zeitlich befristete Testversionen auf www.egistec.com als Download erhältlich.

Über EgisTec – Egis Technology Inc.

Egis Technology Inc. ist ein führender Anbieter für Datenschutz, biometrische Software und Fingerabdruck-Sensoren. Die schlüsselfertigen EgisTec-Lösungen werden im Bundle in über 30 Millionen PCs und Mobilgeräten weltweit in über 28 Sprachen vertrieben. Das Unternehmen hat seinen Hauptsitz in Taipei, Taiwan, und eine Niederlassung in Hangzhou, China.

Mehr Informationen erhalten Sie im Internet auf www.egistec.com oder direkt bei:

Kontakt Presseanfragen:	Kontakt Unternehmen:
Anette Keiser	Fay Tseng, Manager Marketing Depart.
FIRST SCOUT IN	EgisTec Hauptverwaltungen
Telefon: +49 (0) 89 2090 0135	Telefon: +886 2 2658-9768
E-Mail: keiser@firstscoutin.com	E-Mail: fay.tseng@egistec.com
Klenzestr. 51 80469 München	7F, No. 257, Sec. 2, TiDing Blvd., Neihu District, Taipei 114, Taiwan