

## Thema: Safer Internet Day 2010

Zeichen Artikel: 11.039 (mit Leerzeichen)

### Safer Internet Day 2010 – Clever im Netz unterwegs

#### Gefahren zwischen SchuelerVZ und Billig-Flügen

*Das Internet ist auf den ersten Blick ein riesiges Freizeitparadies: Kinder und Jugendliche treffen dort Freunde in sozialen Netzwerken, Eltern gehen auf Einkaufstour und Senioren planen die nächste Reise. Doch hinter dieser schönen Fassade lauern für jede Gruppe ernste Gefahren – der Safer Internet Day rückt sie ins Licht der Öffentlichkeit.*

Nach einer Studie von Microsoft [1] werden Europäer ab Juni 2010 mehr Zeit im Internet als vor dem Fernseher verbringen. Mitte des Jahres stehen dann laut der Voraussage 2,5 Tage Internetnutzung im Monat (14,2 Stunden pro Woche) knapp zwei Tagen (11,5 Stunden pro Woche) TV-Konsum gegenüber. Dabei liegen die Europäer bei der Internet-Nutzung (rund 52 Prozent der Bevölkerung) nur im Mittelfeld. Nach Angaben der Internet World Stats [2] hat Nord-Amerika die Top-Platzierung mit 74,2 Prozent Internet-Nutzern inne, das andere Ende der Fahnenstange bildet dagegen Afrika mit lediglich 6,8 Prozent. Weltweit gesehen ist rund ein Viertel der Bevölkerung im Jahr 2010 online.

#### Von Facebook bis zum Wetterkanal

Doch was die Nutzer im Internet machen, hängt in erster Linie vom Alter ab. Aktuelle Nutzungsstatistiken, etwa in Deutschland [3] oder USA [4] zeigen, dass die jungen Internet-Nutzer der Altersgruppe von 12 bis 19 Jahren das Internet vor allem zur Kommunikation nutzen. Rund 50 Prozent der Online-Zeit verbringen Jugendliche in sozialen Netzwerken, sowie mit Messenger- oder Mail-Programmen.

Je älter die Internet-Nutzer werden, desto mehr Zeit verwenden sie für Informationsrecherche. Dagegen nimmt die aufgebrauchte Zeit für Unterhaltung und Spiele ab. Als Kommunikationsmittel steht bei den Erwachsenen E-Mail ganz oben auf der Liste. Rund zwei Drittel der erwachsenen Internet-Nutzer kauft auch im Internet ein und bucht Urlaubsreisen. Ein Drittel der Nutzer macht regelmäßig Online-Bankgeschäfte. Eine magische Grenze für die Beliebtheit von sozialen Netzwerken scheint der 30. Geburtstag zu sein [5]: Drei Viertel aller jüngeren Internet-Nutzer sind in sozialen Netzwerken unterwegs, über 30-Jährige nur zu einem Drittel.

Internet-Nutzer über 65 sind auf anderen Wegen im Internet unterwegs: E-Mail ist zwar auch hier der am meisten genutzte Dienst. Danach kommen aber fast ausschließlich Informations-Dienste, von der Reiseplanung über Wetterinformationen bis zu Nachrichten [6].

### **"Think before you post"**

Das Motto des Safer Internet Day 2010 heißt "Think before you post" also „Überlege erst bevor Du veröffentlichst“ und soll vor allem ein Leitsatz für die jüngere Generation sein, die viel Zeit in sozialen Netzwerken verbringt. Denn Fakt ist: Trotz Internet haben sich die grundsätzlichen Probleme und Bedürfnisse von Kindern und Jugendlichen nicht verändert. Vor allem persönliche Probleme sind für die Heranwachsenden wichtig; der Unterschied ist nur, dass diese nicht mehr im Tagebuch unter dem Kopfkissen landen oder im Freundeskreis thematisiert werden, sondern sich in Blogs oder als Kommentare in sozialen Netzwerken wiederfinden. Dass bei zu laxen Datenschutzeinstellungen Gott und die Welt mitlesen kann, ist vielen Jugendlichen dabei nicht bewusst – oder egal.

Wer sich mit Suchmaschinen auskennt, sammelt im Handumdrehen Informationen über eine Person, die früher schlichtweg nicht zur Verfügung standen. Sie haben einen Wunschzettel bei Amazon? Die Titel sagen vermutlich viel über Ihre Hobbys aus. Im Facebook-Profil stehen Geburtsdatum und Wohnort: So kann sich jeder via Google Maps einen Eindruck von der Wohngegend verschaffen. Mit dem gegoogelten Namen der Eltern lassen sich Passwort-Sicherheitsabfragen von Accounts knacken. Fazit: Das Internet erleichtert vor allem die Kombination verschiedener Info-Quellen, um ein komplettes Persönlichkeitsprofil zu erstellen.

Bedenken sollte man auch, dass es oft unmöglich ist, verbreitete Fotos oder Kommentare aus sozialen Netzwerken wieder vollständig zu löschen. Selbst wenn man ein selbst eingestelltes Foto entfernen kann, hat es vielleicht schon jemand anders kopiert oder eine Suchmaschine verweist noch im Cache darauf. Eine weitere Gefahr: Ist der virtuelle Freund bei Facebook wirklich der, der er vorgibt zu sein? Schwer zu sagen, denn bei den beliebten sozialen Netzwerken lässt sich nicht so ohne weiteres feststellen, wer wirklich hinter einem Profil steckt. Einerseits besteht so die Gefahr, dass man ausspioniert wird, andererseits bereiten Cyber-Kriminelle über Links gezielt Angriffe auf Computer vor.

Antiviren-Spezialist Kaspersky Lab geht davon aus, dass Crimeware, die soziale Netzwerke ausnutzt, zu den am stärksten zunehmenden Bedrohungen 2010 gehören wird. Am Safer Internet Day gibt es zahlreiche Veranstaltungen, die die Gefahren von sozialen Netzwerken zum Thema haben, etwa zu "Persönlichen

Daten von Jugendlichen im Web 2.0" oder "Datenschutz ist Bildungsaufgabe" [7].

### **Shoppen birgt Gefahren**

Auch wer – wie die meisten Erwachsenen - nicht seine komplette Freizeit im Internet verbringt, wird mit immer mehr Gefahren und ausgefeilteren Angriffsszenarien konfrontiert. Übrigens ist das einer der Haupttrends beim Thema Computer-Sicherheit 2010: Viren-Analysten prognostizieren für 2010 sehr viel raffiniertere Schadsoftware, die auch Gelegenheits-Internet-Nutzer in Bedrängnis bringen kann. Zum Beispiel registrieren die Virenschützer von Kaspersky Labs rund 30.000 neue Internet-Bedrohungen pro Tag (!). Vorbei ist auch die Zeit, in der man im Internet noch recht sicher war, wenn man sich nicht auf dubiosen Seiten rumtrieb.

Schon beim Einkaufen im Internet droht Gefahr. Extrem niedrige Preise für teure Markenartikel klingen nicht nur zu gut um wahr zu sein, sie sind es in der Regel auch nicht. Auch via E-Mail wird immer noch fleißig abgezockt: Dabei wird einfach Schadsoftware selbst oder ein Link auf eine infizierte Webseite verschickt. Wird der Computer nicht von einem aktuellen Antiviren-Programm geschützt, installiert sich das Schadprogramm mit einem Klick im Hintergrund und späht beispielsweise Passwörter, Kreditkartendaten und TAN-Nummern aus.

Oft werden Schadprogramme auch dafür genutzt, um den Computer auf andere Webseiten umzuleiten. Sie glauben, die vertraute Webseite des Online-Shopping-Anbieters auf dem Bildschirm zu sehen, sind aber in Wirklichkeit auf der gefälschten Seite des Online-Gauners gelandet. Diese "Phishing"-Angriffe sind mittlerweile so ausgefeilt, dass sie selbst von erfahrenen Computernutzern oft nicht mehr erkannt werden. Gibt man auf der falschen Internetseite seine Zugangsdaten ein, erscheint eine Fehlermeldung mit der Bitte um Geduld, es handle sich um ein technisches Problem. Doch Benutzername und Passwort wurden in Wahrheit längst zum Angreifer gesendet, der damit auf Ihre Kosten einkauft oder Banktransaktionen vornimmt.

### **Silver Surfer im Visier**

Im Internet kann jeder seine Traumreise individuell planen und buchen – hohe Rabatte gegenüber dem Pauschalangebot vom Reisebüro sind drin. Aber der digitale Weltenbummler packt besser ein paar Sicherheitsmaßnahmen in den Koffer, sonst endet die Traumreise, bevor sie richtig angefangen hat. Allein in den USA haben Computernutzer über einen Zeitraum von zwei Jahren Schäden von knapp 8,5 Milliarden Dollar erlitten [8]. Die Angreifer verwenden immer raffiniertere Programme, die weitgehend automatisch arbeiten und auf unterschiedliche Weise vorgehen. Der bekannteste Weg ist das Verschicken von Schadsoftware per E-Mail. Beliebte sind angebliche Mails von großen Online-

Reiseveranstaltern wie Opodo und Expedia, im Anhang befindet sich eine gefälschte Rechnung, die nach dem Anklicken einen Trojaner auf dem Computer installiert, wenn dieser nicht von einem aktuellen Antiviren-Programm geschützt wird. Trojaner spähren zum Beispiel Passwörter, Kreditkartendaten und TAN-Nummern aus. Hat sich solch ein Trojaner erst einmal eingenistet, bekommen Sie ihn nur mit Mühe wieder los. Die meisten Schadprogramme beherrschen nämlich zahlreiche Tricks, um sich vor der Entdeckung zu schützen. Dazu kommt, dass Sie in der Regel nichts von Ihrem ungebetenen Gast merken. Im Gegenteil, der Trojaner vermeidet alles, was auf ihn aufmerksam machen würde.

Der Schutz vor solchen und ähnlichen Attacken ist Sache einer Sicherheitssoftware. Mittlerweile finden die digitalen Wächter die Schädlinge bereits, wenn sie sich verdächtig verhalten. "Behaviour Analysis" – Verhaltensanalyse – nennen Experten diese Fähigkeit. Die Sicherheitsprogramme überwachen auch den Web-Browser und erkennen zuverlässig, wenn Sie auf eine Phishing-Seite umgeleitet werden sollen.

Das ist auch bitter nötig, denn bezahlt wird im Internet in der Regel per Kreditkarte oder über eine Lastschrift. Kontodaten oder Kartenummer preiszugeben stellt immer ein gewisses Risiko dar. Darum sollten Nutzer unbedingt darauf achten, dass das digitale Reisebüro auf jeden Fall eine verschlüsselte Verbindung für die Transaktion anbietet. Oft weisen die Betreiber an der virtuellen Kasse 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.

Wenn Sie diese Tipps beherzigen, sind Sie clever – und sicher – im Netz unterwegs:

1. Installieren Sie eine aktuelle Sicherheits-Software und beziehen Sie regelmäßig Signatur-Updates.
2. Beziehen Sie regelmäßig Updates für Ihr Betriebssystem (z.B. Windows) und alle genutzten Programme.
3. Sichern Sie regelmäßig Ihre persönlichen Daten auf CD, DVD oder einem externen Speichermedium.
4. Beantworten Sie nicht jede E-Mail, wenn Sie den Absender nicht kennen.
5. Klicken Sie auf keine E-Mail-Anhänge, wenn Sie den Absender nicht kennen.
6. Klicken Sie niemals auf in E-Mails oder Instant Messages enthaltene Links.
7. Geben Sie, wenn Sie auf eine E-Mail antworten, keine persönlichen Informationen preis, auch wenn die E-Mail offiziell aussieht.

8. Betreiben Sie Online-Shopping und -Banking nur auf sicheren Seiten. Wenn Sie in ihrem Browser vor der URL-Adresse ein Schloss-Symbol sehen, ist die Seite gesichert.
9. Benutzen Sie für jede Webseite oder Onlinedienste unterschiedliche Passwörter. Verwenden Sie Passwörter, die mehr als 5 Zeichen enthalten und aus Ziffern, Zahlen, Sonderzeichen und sowohl aus Groß- und Kleinbuchstaben bestehen. Verwenden Sie keine ähnlichen und keine leicht zu erratenden Passwörter (z.B. Namen der Mutter oder des Haustiers). Teilen Sie niemandem Ihre Passwörter mit.
10. Reden Sie mit Ihrem Kind über dessen Interneterfahrungen und installieren Sie eine Sicherheits-Software, mit der Sie über eine Kindersicherung fragwürdige Inhalte für Ihre Kinder sperren und die Online-Zeit beschränken können.

#### Quellen:

[1]

[http://download.microsoft.com/documents/uk/finland/press/europe\\_logs\\_on.pdf](http://download.microsoft.com/documents/uk/finland/press/europe_logs_on.pdf)

[2] <http://internetworldstats.com/stats.htm>

[3] [www.mpfs.de/fileadmin/JIM-pdf09/JIM-Studie2009.pdf](http://www.mpfs.de/fileadmin/JIM-pdf09/JIM-Studie2009.pdf)

[4] [www.scribd.com/doc/16753035/Nielsen-Study-How-Teens-Use-Media-June-2009-Read-in-Full-Screen-Mode](http://www.scribd.com/doc/16753035/Nielsen-Study-How-Teens-Use-Media-June-2009-Read-in-Full-Screen-Mode)

[5] <http://arstechnica.com/web/news/2009/02/study-twitter-users-are-mobile-urban-and-engaged-online.ars>

[6] [http://blog.nielsen.com/nielsenwire/online\\_mobile/six-million-more-seniors-using-the-web-than-five-years-ago](http://blog.nielsen.com/nielsenwire/online_mobile/six-million-more-seniors-using-the-web-than-five-years-ago)

[7] <https://www.klicksafe.de/ueber-klicksafe/safer-internet-day/sid-10/veranstaltungen/veranstaltungen-am-safer-internet-day-2010.html>

Der Artikel und Zitate daraus dürfen unter Nennung des Unternehmens Kaspersky Lab sowie des Autors frei veröffentlicht werden.

**Kaspersky Lab** ist Europas größtes Unternehmen für Antivirus-Technologie und reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crimeware, Hacker, Phishing-Attacken und Spam. Das Unternehmen gehört zu den weltweit vier erfolgreichsten Herstellern von Sicherheits-Lösungen für den Endpoint (IDC 2008). Die Produkte von Kaspersky Lab haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und kurzen Reaktionszeiten einen Namen gemacht. Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen.

Weitere Details zum Unternehmen sind unter <http://kaspersky.de> zu finden. Kurzinformationen von Kaspersky Lab erhalten Sie zudem über [http://twitter.com/Kaspersky\\_DACH](http://twitter.com/Kaspersky_DACH). Aktuelles zu Viren, Spyware und Spam sowie Informationen zu anderen IT-Sicherheitsproblemen und Trends sind unter [www.viruslist.de](http://www.viruslist.de) abrufbar.

**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.