

ARTIKEL-
WEGWEISER

- Spam-Falle Produktbestellung: Medikamente, Uhren, Software Seite 71
- Spam-Falle Geldversprechen: Glücksspiele, Jobs, Gewinne Seite 74
- Spam-Falle Erotik: Kontaktangebote, Pornoseiten Seite 75
- So schützen Sie sich vor Spam Seite 76

[M] Foto: Photoshot; Montage: COMPUTERBILD



SPAMELA ANDERSON

Eine E-Mail von Pamela Anderson auf Ihrem PC? Schön wär's, aber in Wahrheit ist's nur Spam. Mit welchen Reizen die Werbemüll-Mafia sonst noch lockt und wie Sie sich gegen die Spam-Gefahr wehren, lesen Sie hier.

Der Montag ist schon schlimm genug, aber seit einiger Zeit hat er eine richtig fiese Strafe auf Lager: Wer morgens zu Hause sein E-Mail-Postfach öffnet, muss erst mühsam die wichtigen Mails vom Wochenende aus dem ganzen Werbemüll fischen und massenhaft Spam-Mails löschen. Und wer im Büro am PC arbeitet, darf das Spielchen kurz darauf wiederholen.

Doch die massenhaft versendeten Spam-Mails kosten nicht nur Zeit und Nerven. Im Postfach-Müll lauern auch viele Gefahren. COMPUTERBILD hat in einem Test ermittelt, was hinter den verschiedenen

Spam-Maschen steckt, und zeigt, was Nutzern droht, die auf Spam-E-Mails hereinfliegen.

Wie gefährlich ist Spam?

Von unverlangter Werbung für normale Produkte oder illegale Ware bis hin zu krimineller Abzocke weltweit organisierter Verbrecherbanden – Spam hat viele Gesichter:

■ **Werbung:** Zahlreiche Spam-E-Mails preisen verschreibungspflichtige Medikamente wie Potenzmittel, angebliche Luxus-Uhren, Software oder pornografische Internetseiten an.

■ **Geldwäsche und Betrug:** Gewinnmitteilungen, lukrative Jobangebote, Bonusversprechungen von Online-Casinos und Kontaktangebote von Frauen setzen auf gutgläubige E-Mail-Empfänger.

■ **Datenklau:** Ob bei der Bestellung angepriesener Ware, bei kostenpflichtigen Diensten oder vermeintlich persönlichen Nachrichten – Spam läuft meist darauf hi-

naus, dass der Nutzer sensible Daten wie Namen und Postanschrift, Ausweis- und Kreditkartennummer offenlegen soll. Was droht: betrügerischer Missbrauch persönlicher Daten.

■ **Schadprogramme:** Schon in zahlreichen Spam-E-Mails lauern Gefahren. Schadprogramme wie Viren oder Trojaner verbergen sich oft im E-Mail-Anhang und können Ihren Computer infizieren.

Wie Sie am besten mit Spam umgehen und wie Sie sich davor schützen können, steht auf Seite 76.

Sind Werbe-Newsletter auch Spam?

Ja, wenn Sie der Zusendung nicht ausdrücklich zugestimmt haben. Haben Sie aber im Internet einen Newsletter angefordert, handelt es sich um „erwünschte Werbung“. Beachten die Anbieter dabei die Datenschutzrichtlinien, sind Newsletter zulässig – wenn der Kunde sie jederzeit abstellen kann.

Wie erkenne ich Spam?

■ Ein unbekannter Absender mit ungewöhnlicher Zahlen- und Ziffernfolge in der E-Mail-Adresse.

■ Auf Englisch verfasste E-Mails, die unerwartet im Posteingang landen.

■ Ein Link*, eine kostenpflichtige Rufnummer (0900) oder ein Datei-anhang in E-Mails unbekannter Herkunft.

■ Rechtschreibfehler, die auf eine automatisierte Übersetzung von Texten ins Deutsche hinweisen. Oder bewusst eingebaute Fehler (etwa „V!agra“), mit denen Versender die Schutzfilter von E-Mail-Programmen überlisten wollen.

■ Verlockend, vertraulich oder bedrohlich klingende Betreffzeilen wie zum Beispiel „Sie haben gewonnen“, „Komm ins Geld-Paradies“, „Erinnerst du dich an mich?“, „Hallo mein Freund“ oder „Mahnung!“.

■ Vermeintliche Antworten – die Betreffzeile beginnt mit „Re:“ oder „AW:“ – von einem Absender, den Sie gar nicht kennen. [mas]

DARUM GEHT'S

- ▶ Spam per E-Mail – Fallstricke und Gefahren unerwünschter Nachrichten
- ▶ Was hinter Spam wirklich steckt – Betrüger und Kriminellen auf der Spur
- ▶ Wie Sie sich wirksam schützen können

Spam-Falle „Produktbestellung“

Viele der unerwünscht eintreffenden E-Mails werben für Produkte zu extrem günstigen Preisen.

In vielen Fällen wäre die Beschaffung solcher Waren für den Käufer auf regulärem Wege umständlich

oder gar peinlich. Klickt der Empfänger auf den in der Spam-E-Mail angegebenen Link*, landet er auf ei-

ner Internetseite, die einem regulären Online-Shop nachempfunden ist. Doch der Schein trügt ...

Verschreibungspflichtige Medikamente

Viagra, Levitra & Co. – Werbe-E-Mails für diese Mittel stammen nie von den Pharmaherstellern. Denn: In Deutschland ist die Werbung für rezeptpflichtige Medikamente verboten. Der Anreiz für potenzielle Spam-Opfer liegt weniger im Preis. Verlockend ist

vor allem die angeblich problemlose Bestellung, ohne einen Arzt aufsuchen zu müssen. So preisen Spam-Mails zumeist Produkte an, die unbedachte Konsumenten nicht als Medikament, sondern eher als „Lifestyle-Mittel“ ansehen, wie zum Beispiel

■ potenzsteigernde Pillen,
■ Appetitzügler und
■ starke Schmerzmittel beispielsweise mit dem als „Gewaltdroge“ bekannten Wirkstoff Tilidin. Bei den Mitteln handelt es sich in der Regel um Nachahmer-Präparate. Die Absender werben mit dem

Markennamen und fälschen Aussehen und Verpackung. COMPUTERBILD ließ Pillenproben in zwei Fachlaboren analysieren. Das Ergebnis: Zwar wurde der Grenzwert für Schwermetalle eingehalten, aber der Wirkstoff wich gravierend vom Original ab (siehe links unten).

Von: Ethel Diggs [mailto:obituaryess@groups.msn.com]
An: @computerbild.de
Betreff: mehr Info

Ihrer Online Apotheke im Internet

- Aktuelle Angebote :

Vi. (Female) 100 mg x 60 Tab - 105.76 Euro
Vi. 10 Tab x 100 mg + Ci. 10 Tab x 20 mg - 56.93 Euro

In unserer Versandapotheke können Sie rezeptfreie Arzneimittel, Medikamente und Wellnessprodukte 10%-50% günstiger einkaufen als in der Apotheke vor Ort.

Vi. 30 Tab - 63.98 Euro - Sie sparen: 15.21 Euro
Ci. 30 Tab - 77.31 Euro - Sie sparen: 11.63 Euro

Bestellen Sie noch heute und vergessen Sie Ihre Enttäuschungen, anhaltende Versagensängste und wiederholte peinliche Situationen!

<http://firstseparate.com>

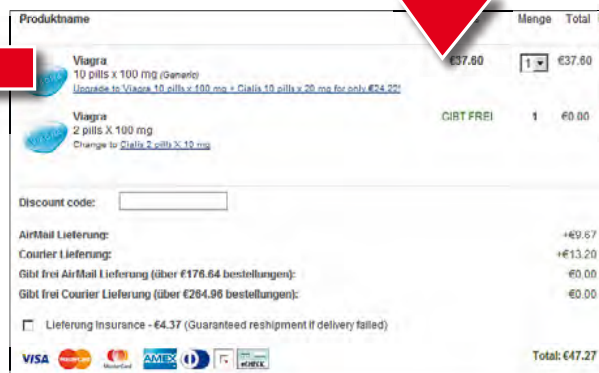
Von: Evangeli Brady [mailto:kerouacym2@saundersgroup.com]
An: @computerbild.de
Betreff: 100mg x 10 pills price

Viagra (Sildenafil) 100mg x 30 pills buy now <http://finehomehealth.com.es>

1 Einige E-Mails werben sehr direkt („Viagra ... buy now“). Andere verwenden Textbausteine seriöser Online-Apotheken („rezeptfreie Arzneimittel ... 10%-50% günstiger“), um Interessenten zu ködern.



2 Der Link* führt auf die Seite einer angeblich kanadischen Internetapotheke. Wie auf seriösen Seiten wird mit dem Bild eines Apothekers geworben, um Glaubwürdigkeit vorzugaukeln. In der deutschen Version der Seite fallen bizarre Fehler ins Auge – so heißt der Menüpunkt „Warenkorb“ hier „Ihre Karre“. Allgemeine Geschäftsbedingungen und Impressum fehlen, die Kontakttrufnummer führt nur zu einer Mailbox.



3 Hier schrillen die Alarmglocken: Nicht nur die „Bestseller“-Potenzmittel, sogar die Bestellung von Acompla möglich (Bild oben) – eine Schlankheitspille, die wegen ungeklärter Nebenwirkungen seit Herbst vergangenen Jahres nicht mehr verschrieben und verkauft werden darf. Im Bestellformular (links) sollen „Gratispillen“ den potenziellen Kunden zur Bestellung animieren. Zahlung ist nur per Kreditkarte möglich.

ZENTRALLABORATORIUM DEUTSCHER APOTHEKER e.V.			
Analysezertifikat			
Wirkstoffe: Sildenafil; Vardenafil			
Produkte: Viagra®; Levitra®			
Darreichungsform: Tabletten			
Dosierung: 100 mg; 20 mg			
ZL-Nr.: FE200900006-10			
Methode:			
Testnummer 1 (20 mg)	gemessene Konzentration	Wiederfindung (Bezug auf die deklarierte Konzentration von 20 mg)	
100 mg	19,7 mg	15,7 %	
Testnummer 2 (20 mg)	gemessene Konzentration	Wiederfindung (Bezug auf die deklarierte Konzentration von 20 mg)	
100 mg	21,98 mg	109,9 %	

4 Statt aus Kanada kommen die Pillen aus Indien oder China. Die Deklaration als Geschenk (englisch: „Gift“) soll den Zoll überlisten. Inhalt der Sendung: Zwei gefälschte Potenzmittel und ein chinesischer Beipackzettel. Die Pillen schickte COMPUTERBILD zur Analyse zum Zentrallaboratorium Deutscher Apotheker – mit erschreckendem Ergebnis ...

5 Der Wirkstoff in den Pillen wich in einem Fall um 10, im anderen gar um 84 Prozent von den Original-Medikamenten ab!



6 Schockierende Zustände: Unter haarsträubenden Bedingungen wie etwa in dieser von der Polizei ausgehobenen chinesischen „Giftküche“ werden die in Spam-E-Mails beworbenen Medikamente hergestellt.

Vorsicht, Falle!

- Wer verschreibungspflichtige Medikamente ohne Rezept bestellt und in Deutschland einführt, begeht eine Ordnungswidrigkeit – unterliegt das Mittel dem Betäubungsmittelgesetz, sogar eine Straftat.
- Der Zoll kann die Ware beschlagnahmen. Das per Kreditkarte im Voraus überwiesene Geld ist futsch.
- Das Gesundheitsrisiko bei Einnahme der Pillen ist unkalkulierbar.
- Missbrauch der preisgegebenen Kreditkartendaten ist möglich.

Luxus-Uhren, -Handtaschen und andere Markenware

Rolex, Omega, Prada, Sony – edle Luxuswaren und hochwertige Elektronikartikel werden massenhaft per Spam beworben. Die Preise erscheinen irrwitzig niedrig: ein Indiz dafür, dass es

sich nicht um Originalprodukte handelt. Wer sich auf eine der „Shop“-Seiten locken lässt, findet dort denn auch in der Regel den Hinweis „Replica“. Dieser Begriff bedeutet letztlich nichts anderes

als „Produktfälschung“. Wer sich blauäugig dennoch ein Original erhofft, hat den Schaden: Eine Reklamation solcher Ware – selbst wenn sie den Zoll passiert – ist faktisch unmöglich. Auch ein Umtauschrecht steht dem Kunden in diesen Fällen nicht zu. Zudem sind die meisten dieser „Shops“ nur wenige Tage im Internet erreichbar, denn die Fälscher führen sie regelmäßig unter neuer Internetadresse weiter. Die Masche bleibt gleich, nur der E-Mail-Text bekommt den jeweils aktuellen Link*.



Vorsicht, Falle!

- **Rechtlich:** Käufer begehen eine Schutzrechtsverletzung; kostenpflichtige Abmahnung durch betroffene Firmen wie Rolex oder Prada möglich
- Der Zoll darf Ware beschlagnahmen
- Weder Möglichkeit noch gesetzlicher Anspruch auf Reklamation/Umtausch
- Möglicher Missbrauch der beim Kauf angegebenen, meist unverschlüsselt übertragenen Kreditkartendaten
- Überhöhte Preise für minderwertige Produkte beziehungsweise Fälschungen

Von: Geschenke für neues Jahr [mailto:lorons@weiss@domen.com]
An: [mailto:lorons@weiss@domen.com]
Betreff: Uhren, Taschen, Schmuck – alles, was Sie wollten

Die letztendliche Auswahl der neuen Version 2008 Luxus-Uhren ab sofort verfügbar.

Warum zahlen Hunderttausende für den ursprünglichen, wenn Sie können wählen einen Spiegel Kopie für ein Bruchteil des Preises?
Für nur \$ 49 ~ \$ 249, können Sie ein **IDENTISCH UHR auf das Original** Ihre Freunde, Geschäftspartner und Kollegen Partner werden nie in der Lage zu sagen, der Unterschied.

Rolex, Pateks, Breitlings, Cartiers – alle zur Verfügung stehenden in ein erstklassigen Online-Shop.

Shop heute, speichern Zehntausende, und fordern Sie Ihre Traum Uhr heute

1 In abstrusem Deutsch offeriert die E-Mail „Uhren, Taschen, Schmuck – alles was Sie wollten“. „Identisch Uhr auf das Original“ bedeutet ganz einfach: Fälschung!

2 Der COMPUTERBILD-Tester folgte dem Link und landete in einem vermeintlichen Online-Shop namens Prestige – mit dem kleinen Hinweis „Replicas“. Laien können die Uhren nicht von der Originalware unterscheiden. Doch statt wie hier rund 200 US-Dollar kostet etwa eine echte Rolex Daytona im Handel über 15 000 Euro. COMPUTERBILD bestellte dieses „Schnäppchen“, doch die Uhr traf nie ein. Immerhin: Unrechtmäßige Abbuchungen vom Konto gab's nicht – noch nicht ...



3 Die Fälscher könnten nun von der Kreditkarte hohe Beträge abbuchen. Dann bliebe nur die Möglichkeit, die Abbuchungen beim Kreditkartenunternehmen anzufechten.



4 Uhren-Experte Klaus Prüfer von der Firma Christ urteilte schon in einem vorherigen Test für COMPUTERBILD (Ausgabe 5/2007): Es handelt sich um billige Imitate. Der Wert: „maximal 100 Euro“.

Computer-Software

Programme, die ein Shop 70 bis 90 Prozent unter dem Marktpreis anbietet, können gar nicht aus einer legalen Quelle stammen. Dennoch preisen Spam-E-Mails

die Programme zum Download als „100% legal“ an. Allerdings sollte schon dieser Hinweis stutzig machen – ebenso wie ein Blick auf die Internetadresse des Anbieters: Viele der angeblich professionellen Internetshops nut-

zen für Ihren Auftritt kostenlos erhältlichen Internet-Speicherplatz – zum Beispiel beim Google-Service Blogger (www.blogger.com). Wer hier Software kauft, muss von einer Raubkopie ausgehen. Zudem besteht die Gefahr, dass der Kunde mit dem Programm auch einen Virus oder andere Schädlinge auf seinen Computer holt.



Vorsicht, Falle!

- **Rechtlich:** Für den Käufer kostenpflichtige Abmahnung bis hin zur Schadenersatzforderung durch den Softwarehersteller möglich
- Software kann fehlerhaft oder mit einem Schadprogramm infiziert sein
- Möglicher Missbrauch der beim Kauf angegebenen Kreditkartendaten
- Ungültige Registrierungscode der Programme – Kundenservice durch Originalhersteller ist ausgeschlossen
- Reklamation faktisch unmöglich

Von: Parker Whitlock [mailto:morse@topglobalbusiness.com]
An: mamin@computerbild.de
Betreff: Downloadable OEM latest full version MS Office 2007

Microsoft Office 2007 Ultimate
Retail Price: \$679.95
Our Price: \$199.95
You save: \$480

<http://cyqqkymxwkeynyundskqwh.blogspot.com>

1 Beim Büropaket Microsoft Office 2007 Ultimate 480 US-Dollar sparen? Stutzig macht schon die unprofessionelle Internetadresse in der E-Mail: Bei Blogspot gibt's eigentlich keine Software zum Herunterladen, sondern Internet-Tagebücher („Blogs“).



2 Der COMPUTERBILD-Tester folgte dem Link und gelangte zu einer auf den ersten Blick unverdächtig erscheinenden Download-Seite im Internet. Doch Pflichtangaben des Shops, wie Impressum oder Geschäftsbedingungen, waren nicht zu finden.



83,90 Dollar sollte das Microsoft-Office-2007-Paket kosten. Bei der Zahlung per Kreditkarte brach die Verbindung plötzlich ab – zum Glück.



3 COMPUTERBILD deckte auf, dass hinter der nicht fälschbaren IP-Adresse des E-Mail-Absenders ein Valery Rigalo, Moskau, steckt. Das Angebot, vor dem bereits Internet-Spamlisten („Blacklists“) warnen, wurde in Südkorea ins Netz gestellt.

Spam-Falle „Geldversprechen“

Geldgeschenke? Gewinne? Prima, immer her damit! Und wer träumt nicht von einem hochbezahlten Job,

der nur geringen Einsatz erfordert? „Viel Cash in mickriger Zeit“ – mit solchen E-Mail-Betreffzeilen locken

die Spammer. Dahinter lauert Betrug! Eine andere Masche: „Bettelbriefe“ – vermeintlich notleidende

Personen („russische Studentin“) wollen Leichtgläubigen Geld aus der Tasche ziehen.

Glücksspiele im Online-Casino

Glücksspiele mit Geldeinsatz sind hierzulande bis auf wenige Ausnahmen verboten – auch wenn Sie im Internet stattfinden. Der Grund: das staatliche Glücks-

spielmonopol. Das Verbot betrifft:

- Sportwetten,
- Casinospiele wie beispielsweise Roulette oder Poker und
- Lotterien.

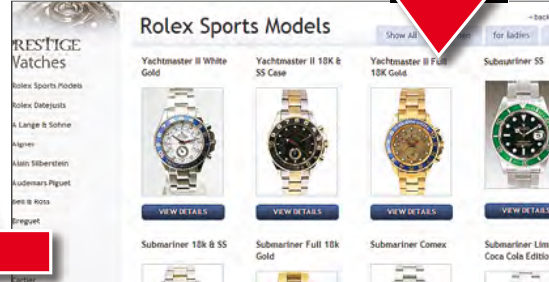
Dennoch animieren Spam-E-Mails mit Bonusversprechungen zum Glücksspiel. Das ist nicht nur verboten, dahinter steckt oft auch Betrug! Trotz des Verbots fallen

manche Spielernaturen darauf herein. Immer in der blauäugigen Annahme: Im anonymen Internet erwischt mich niemand. Installiert das Opfer die Casino-Software, muss es sich anschließend registrieren – und zahlen! Denn: Den Bonus bekommt der Zocker nur, wenn er sein Spielerkonto zuvor mit

1 Royal Club Casino verspricht Neukunden einen 555-Euro-Bonus. Link anklicken, anmelden und kassieren – so einfach soll's gehen.



2 Infos zum Veranstalter oder zu den Nutzungsbedingungen: Fehl-anzeige! Ganz gleich, auf welchen Bereich der Internetseite geklickt wird – automatisch startet der Download der „Casino-Spielsoftware“.



Die Sicherheitswarnung bietet die letzte Chance, das Herunterladen abubrechen.



3 Die Prüfung im COMPUTERBILD-Labor enthüllt: Im Casino-Programm verbirgt sich ein Trojaner*. Wer die Software startet, infiziert seinen PC. Einzige Schutzmaßnahme: das Programm sofort löschen und den Test abbrechen. Neben dem Trojaner drohen im Internet-Casino jedoch weitere Gefahren (siehe Kasten oben).

Vorsicht, Falle!

- Rechtlich: Straftatbestand wegen Teilnahme an verbotenem Glücksspiel (nach aktueller Rechtslage)
- Hohe Gefahr von Schadprogrammen
- Einzahlungen aufs Spielkonto per Kreditkarte – Datenmissbrauch möglich
- Auszahlung von Boni unmöglich; Gefahr des Diebstahls eingezahlter oder gewonnener Beträge
- Bei Betrug keine Rechtsmittel möglich, da Teilnahme an verbotnem Glücksspiel

Jobangebote

Geringer Aufwand, Heimarbeit, dicke Provisionen – wer auf E-Mails hereinfällt, die solche Jobs und Nebentätigkeiten anpreisen,

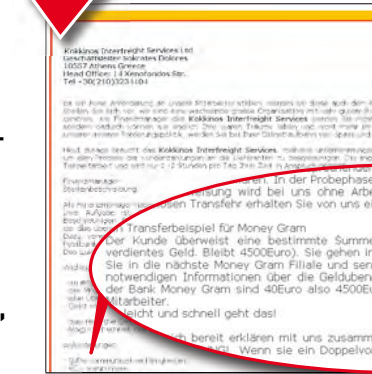
begibt sich in Teufels Küche. Denn: Betrüger sind hier auf der Suche nach Geldwäschern. Die Arbeitsstellen werden als „Finanzagent“,

„finance manager“ oder „transfer controller“ beworben. So funktioniert's: Für die Einzahlung angeblicher Kundengelder soll der Interessent sein Girokonto einer Auslandsfirma zur Verfügung stellen.

10 Prozent der Summe darf der „Finanzagent“ als Provision gleich behalten. Doch hinter der Firma stecken kriminelle Banden: Die Ganoven haben mit gefälschten Internetseiten PIN- und TAN-Nummern ahnungsloser Bankkunden ausgespäht – sogenanntes „Phishing“. Um das Geld von diesen Konten abzuräumen und damit abzutauchen, brauchen sie einen Mittelsmann – den nichtsahnenden „Finanzagenten“! Dem überweisen die Diebe von dem gekaperten Konto hohe Geldbeträge. Der „Finanzagent“ soll dieses Geld abheben und per Geld-



1 Wer auf das Jobangebot antwortet, erhält eine weitere E-Mail – hier angeblich von der Firma Kokkinos. Auch die Internetadresse ist angegeben: Der COMPUTERBILD-Tester prüfte die Adresse: Das griechische Logistik-Unternehmen Kokkinos existiert tatsächlich. Jobinfos?



2 Wie in der Spam-Mail erklärt, sollten nähere Infos unter einer völlig anderen Internetadresse stehen. COMPUTERBILD folgte dem Link und gelangte auf eine in fehler-

Vorsicht, Falle!

- Rechtlich: Wer sich als „Finanzagent“ betätigt, begeht den Straftatbestand des Computerbetrugs und der Geldwäsche. Zudem droht zivilrechtliche Haftung: Der „Finanzagent“ muss das weitergeleitete Geld an den Geschädigten zurückzahlen
- Missbrauch der preisgegebenen persönlichen Daten möglich

haftem Deutsch verfasste Seite. Hier wird's konkret: Man könne als Finanzmanager anfangen. Die Arbeitsbeschreibung (links) erklärt, wie die Betrugs-masche abläuft! Über eine Prüfung der Internet-adresse (whois.domaintools.com) deckte COM-PUTERBILD auf: Von wegen griechische Logis-tik-Firma! Ins Netz gestellt wurde die Seite von einem Mann namens Liu Xiaobing aus Beijing, China.

Gewinnmitteilungen und Geldgeschenke

Sie haben in einer Lotterie gewonnen, deren Namen Ihnen gänzlich unbekannt ist? Finger weg! Die per E-Mail eingetrof-

fenen, meist englischen Gewinnbenachrichtigungen nennen häufig auch renommierte Firmen wie Nokia oder Microsoft als Lotterieveranstalter. Doch statt mit einem Gewinnspiel haben Sie es mit einer Variante des „Vorschuss-Betrugs“ zu tun. Diese Masche – auch unter dem

are simple. To start with, we have nine million, three hundred and seventy thousand dollars. There will be three of us involved in this. We shall each get 30% of the proceeds. If the transaction is proper, we will forward to you a complete bio-data of the original owner of the account, Mr. Alonzo. The



Vorsicht, Falle!

- **Rechtlich: Betrugsoffer können Strafanzeige stellen.** Wegen der gefälschten Identität der Betrüger gibt's aber keine Aussicht auf Erfolg
- **Mögliche Virengefahr durch „Gewinnstätigkeiten“ als Datei-Anhang**
- **Persönliche Daten bis hin zur Hausadresse werden Betrügnern frei Haus geliefert – hohe Missbrauchsfahrer**

Gleiche Masche: Ein „Verstorbener“ hinterlässt ein großes Erbe, und Sie können sich einen großen Batzen sichern – reich werden aber nur die Betrüger.

Begriff „Nigeria-Connection“ ge-
läufig – kursiert schon seit etli-
chen Jahren, findet aber noch im-
mer Opfer: Hat ein vermeintlicher
Gewinner angebissen und auf die
Nachricht reagiert, erhält er ei-
ne Statusmeldung über den
Gewinn. Weitere E-Mails
folgen – auch mit der Auf-
forderung, persönliche Da-
ten mitzuteilen. Dann end-
lich die ersehnte E-Mail-
Nachricht: Der Gewinn sei

nun abrufbar. Der Haken: Es werden vorab Steuern, Notar- oder Bearbeitungsgebühren in oft vierstelliger Höhe fällig, die der „Gewinner“ auf ein ausländisches Konto überweisen muss. Wer darauf hereinfällt, ist sein Geld los. Die Betrüger tauchen mit der leicht verdienten Beute ab, Nachfragen per E-Mail oder Telefon laufen ins Leere. Gewonnen hat das Opfer nur an Erfahrung.

From: Microsoft Corporations <nuknhervey@inl.cz>
Subject: Microsoft Prize Notification!!!
To: undisclosed-recipients

Microsoft Corporations:
Customer Service
Your Reference No: WAHL-108796
Your Batch No: 20089SEPTE

From: Microsoft Corporation
Subject: Microsoft Prize Notif
To: undisclosed-recipients

OFFICIAL WINNING NOTIFICATION
We are pleased to inform you of your selection as one of our Sweepstakes promotion organizers.
Foundation for the promotion of the small business award of 2008, in Europe. Winners in your email address have been selected as winning emails in the 2nd category and therefore will receive a cash award of 150,000.00 (Four Hundred and Fifty Thousand Euros) and a Dell Laptop.

To begin your claim, do file for the release of your winning by contacting our Foreign Service Manager:

Dr. Pedro Marios Ruben,
Tel: +31 634 032 995
Internet fax: +1-001-532-9044
Email: dr_pedro_ruben@sintomaticos.com



Wie gefordert meldete der COMPUTERBILD-Tester per E-Mail seinen Gewinnanspruch an. Kurz darauf bestätigte „Dr. Ruben“ von „Microsoft“ den Gewinn: „450 000 Euro and a Dell laptop“. Vor der Ausschüttung sei aber noch eine Prüfung nötig („verification procedure“). Verlangt wurden persönliche Daten und sogar eine Ausweiskopie. Vorsicht: Die sensiblen Daten lassen sich für spätere Betrügereien verwenden.

EX:
 ADDRESS:
 POST CODE:
 CITY:
 STATE:
 COUNTRY:
 MOBILE-TELEPHONE:
 FAX NUMBER:
 SCAN OR FAX COPY
 OF YOUR PASSPORT
 OR DRIVING LICENSE
 OWNER EMAIL ADDRESS:

■ Spam-Falle „Erotik“

Das Geschäft rund um Lust und Liebe läuft gerade im Internet wie geschmiert. Spam-Versender

überschwemmen E-Mail-Postfächer mit Kontaktangeboten und unmissverständlicher Werbung für porno-

grafische Internetseiten. Wer gedankenlos auf solche Lockangebote hereinfällt und der vermeintlichen

Anonymität im Internet vertraut, läuft schnell Gefahr, abgezockt zu werden.

Kontaktangebote von Frauen

Die Betreffzeilen der E-Mails klingen vertraut: „Hallo mein Freund“, „Lieber Freund“ oder kurz und knapp „Hi“. Es stellt sich eine – zumeist russische – Frau

vor, die „neue Freunde sucht“. Hat der Interessent angebissen, bekommt er im Tagesrhythmus Fotos und Herz-Schmerz-Geschichten aufgetischt. Dabei handelt es

sich um „Bride-Scam“, die elektronische Variante des Heiratschwindels. Es gibt zwei Maschen:

- Direkte Abzocke: Nach langem Schriftwechsel gibt die „Frau“ plötzlich vor, in einer Notlage zu stecken, und bittet um Geld – zum Beispiel für einen Krankenhausaufenthalt. Wenn das naive Opfer überweist, ist das Geld futsch.

■ **Geldwäsche:** Nach etlichen E-Mails kündigt die „Frau“ ihren Besuch an. Das Geld für die Reise würde ein Freund überweisen. Das Opfer müsse ihr dies weiterleiten – ins Ausland, per Bargeldtrans-

 **Vorsicht, Falle!**

- **Rechtlich:** Im Fall der zweiten „Bride-Scam“-Variante machen sich Nutzer strafbar. Die Konsequenzen: siehe Kasten „Jobangebote“
- **Finanzieller Schaden**
- **Preisgabe persönlicher Daten, Fotos**
– Missbrauch für Betrügereien möglich
- **Gefahr von Viren in Datei-Anhängen**

fer. Ähnlich einem „Finanzmanager“ (siehe Kasten „Jobangebote“) läuft man so Gefahr, sich wegen Geldwäsche strafbar zu machen!

1 Im Postfach des COMPUTER-BILD-Testers landet die E-Mail der kontaktsuchenden „Lauren“, 29 Jahre, Russin, wohnhaft in den USA, Absenderadresse aus Singapur(!). Als „Johannes“, 72 Jahre, „kein Opa-Typ“, startet der Tester den Briefwechsel ...

Betreff: Ich hoffe ihre antwort bekommen
Von: "Walter Harder" <w_h_q@yahoo.com.sg>
An: lauren.buelow78@gmail.com
Datum: 27.11.08 11:08:35
Anlagen: Lauren.jpg

Hallo, mein name Lauren

Mir 29 Jahre. Ich lebe in Schwille NC, USA. Ich die suchte der neuen freunde.
Wenn du mit mir abgeschlossen werden willst schicke mir den Brief.

Meine email: lauren.buelow78@gmail.com

Ich werde deinen brief warten :) :) :)
Lauren

p.s Du kannst mir deutsch oder die englische Sprache auch schreiben.

Betreff: Hallo Johannes
Von: patricianelpo@gmail.com
An: schundmails@online.ms
Datum: 16.01.09 16:59:51
Anlagen: Michoma.jpg, DRen0825.jpg, InaMaui.jpg

guten Abend Johannes,
Wie geht es Ihnen? Patricia meins namens.
Ich deinen e-Mail zu finden, und, sich zu entscheiden, dir zu schreiben.
Ich bin 28 Jahre. Ich lebe in Spanien, Stadt Madrid. Ich reise viel. Ich
Ich bin Frau, ich schau, um einige neue Menschen und Freunde für die be-
Ich hoffe, Du nicht gegen unser Bekanntschaft.
Auch, wenn wir die freie und bequeme Zeit, so können wir Video-Chat haben, an der Zukunft finden.
Ich hoffe, das du mir antwortest, du erzählst grosser über dich und du zu schicken deine Fotos.
Ich zu schicken dir meine Fotos, die ein Paar Tage rückwärts gemacht waren, in meinem Haus auch.
Auch kann ich noch über mich sagen, ich bin einfach, lustig, und auf das Treffen mit dem richtigen Mann ernst gestimmt.
Und dann zu sehen, dass es sich davon ergibt.
Ich werde zu warten e-Mail in Hoffnung bald, Ihren Brief zu erhalten.

2 Drei Wochen und 18 E-Mails von „Lauren“ (mit 44 Fotos!) später: Sie hat ihren Tanzlehrerjob gekündigt, ist nach Russland zurückgekehrt und hat den Entschluss gefasst: „Johannes, ich will mit dir mein Leben teilen“. Dieser solle seine Privatadresse mitteilen, Johannes konterte mit derselben Bitte. Abrupt bricht der Kontakt ab.

LEBENSFRAGEN!!!

Schnell antworten. Ich bitte dich verliere die Zeit nicht
den Eltern über meinen Beschluss schon gesagt.
Unabhängig. Ich nicht das kleine Mädchen.
Die VOLLE HAUSLICHE Adresse, DEN VOLLEN Namen
noch einmal allen geben.

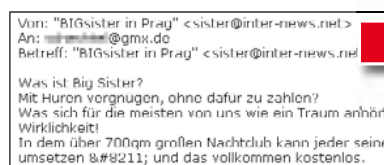
3 Wenige Tage später: „Patricia“, 28 Jahre, Polin, wohnhaft in Spanien, möchte Bekanntschaft schließen. Betreffzeile: „Hallo Johannes“. Doch nur „Lauren“ konnte Namen und E-Mail-Adresse kennen. Fazit: Die Kontakt-Mails stammen aus einer Quelle!

Pornografische Angebote

Auf einschlägigen Seiten erwartet die Voyeure nicht jugendfreies Material: Pornofilmchen zum Betrachten per Mausklick, Bildergalerien für Erwachsene und Übertragungen von Internet-

kameras („Webcams“), vor denen sich allenfalls leicht bekleidete Damen räkeln. Doch die Nutzer dieser Angebote werden heftig – oft per Abo – abkassiert. Viele dieser Seiten sind auch von Schad-

programmen „verseucht“. Und: Kreditkartenzahlung öffnet dem Datenmissbrauch Tür und Tor.



1 **Kostenlosen Sex mit Damen des horizontalen Gewerbes verspricht die E-Mail. Wie's geht, stehe im Internet. Der Tester folgte dem Link*.**



2 Auf der beworbenen Internetseite erfuhr man(n): Nutzer können – gegen Bares – pornografische Filme aus einem Bordell betrachten.



3 Abzocke: Das angebliche „2-Tages-Testabo“ schließt man gleich auf unbestimmte Zeit ab. Der Tester nahm Abstand ...




■ So schützen Sie sich vor Spam

Spam gelangt automatisch an Millionen Empfänger und birgt außer riskanter Werbung und Betrugsversuchen eine weitere Gefahr: Viren und andere Schadprogramme bedrohen Ihren Computer. Betrug per Spam und die Einschleusung eines Schädlings gehen häufig sogar Hand in Hand: Ein Link* lockt Spam-Leser auf Internetseiten, von denen aus Schädlinge den PC angreifen.

Spam-Versender („Spammer“) nutzen spezielle Suchmaschinen („Harvester“), um E-Mail-Adressen im Internet aufzuspüren und mit Werbebotschaften zu bombardieren. Selbst bei Newsletter-Anmeldungen droht Spam: Illegale Adresshändler beschaffen sich über unsichere Daten und verkaufen die Adressen an Spammer. So können Sie sich schützen:

■ Löschen Sie offensichtliche Spam-Mails ungelesen.

■ Betrachten Sie Ihre E-Mails im sicheren „Nur-Text-Modus“. Bei Microsoft Outlook geht's so:

Starten Sie das Programm, klicken Sie zuerst auf **Extras**, und wählen Sie dann **Optionen...** per Mausklick aus. Klicken Sie auf den Menüreiter **Einstellungen** und anschließend auf **E-Mail-Optionen...** Setzen Sie hier 

☐ Standardnachrichten im Nur-Text-Format lesen

ein Häkchen, und bestätigen Sie mit zwei Klicks auf .

■ Klicken Sie nicht auf einen Link und öffnen Sie keinen Anhang in einer E-Mail unbekannter Herkunft.

■ Antworten Sie nicht auf verdächtige E-Mails – auch nicht, wenn dort

ein Hinweis zur Abbestellung solcher Nachrichten steht. Ansonsten wissen Spammer, dass die Adresse aktiv ist. Folge: noch mehr Spam!

■ Verwenden Sie die automatische Abwesenheitsnachricht („Autoreply“) Ihres E-Mail-Programms nur in dringenden Fällen. Geben Sie im Text keine weiteren Adressen an.

■ E-Mail-Programme, beispielsweise Microsoft Outlook oder Windows Live Mail, haben wie die meisten Internet-E-Mail-Dienste (zum Beispiel Web.de oder YahooMail einen eingebauten Spam-Filter. Unerwünschte Post wird automatisch in einen Ordner verschoben oder gelöscht. Allerdings schwankt die Wirksamkeit. Denn: Spammer nutzen ständig gefälschte oder geklaute Absenderadressen oder chiffrieren Texte, um die Filter auszutricksen.

■ Geben Sie Ihre private E-Mail-Adresse möglichst nicht im Internet preis, etwa bei Gewinnspielen, Registrierungen, in Gästebüchern oder für Grußkarten („E-Cards“). Richten Sie stattdessen für einmalige Anmeldungen eine sogenannte „Wegwerfadresse“ ein, etwa bei Spamgourmet ➔ ①. Eingehende E-Mails werden an Ihr normales Postfach weitergeleitet. Vorteil: Die Adresse erlischt nach einer festgelegten E-Mail-Anzahl automatisch.



■ Auch bei den meisten Internet-E-Mail-Diensten können Sie zusätzliche Wegwerf- oder Alias-Adressen einrichten. Das ist nützlich, wenn Sie regelmäßig Newsletter bekommen, die Sie abonniert haben. So

GMX bot im Test kostenloser E-Mail-Postfächer (COMPUTERBILD 15/2008) den besten Spamfilter. So können Sie zum Beispiel Sperrlisten für erwünschte und unerwünschte Absender-Adressen verwalten. Die persönlichen Filtereinstellungen finden Sie hier:


geht's mit Yahoo-Mail ➔ ②, dem COMPUTERBILD-Testsieger der Gratis-E-Mail-Postfächer (Ausgabe 15/2008):

1 Melden Sie sich mit Ihrem Benutzernamen und Passwort an, und klicken Sie ganz rechts auf [Optionen](#).

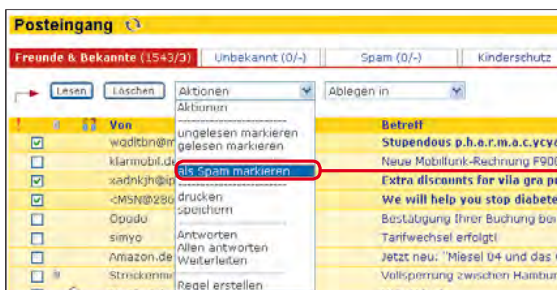
2 Per Mausklick wählen Sie die Option **Wegwerf-Adressen**.
Starten Sie die Einrichtung der Wegwerfadresse per Mausklick auf **Jetzt beginnen!**

3 Geben Sie hier   einen beliebigen Begriff oder Namen ein, zum Beispiel , und klicken Sie auf .


4 Bestätigen Sie Ihren gewählten Namen mit erneutem Mausklick auf **Weiter**.

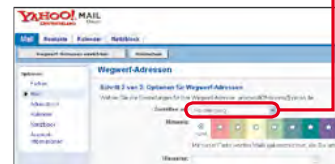
5 In einem Eingabefeld müssen Sie nun den beliebig wählbaren zweiten Teil Ihrer Wegwerfadresse festlegen zum Beispiel 

6 Nun können Sie noch Einstellungen vornehmen, wie die an Ihre Werbefradresse geschickten Nachrichten behandelt werden sollen. Bestimmen können Sie beispielsweise:



„Lernfähige“ Spam-Filter: Wenn Sie unerwünschte E-Mails im Posteingang – hier bei **Web.de** – als Spam kennzeichnen , werden künftige E-Mails des Absenders aussortiert.

in welchem Ihrer E-Mail-Ordner diese Nachrichten automatisch landen sollen:  _____



7 Schließen Sie den Vorgang per Klick auf **Wegwerf-Adressen einrichten** ab. Um weitere Adressen einzurichten oder eine bestehende Wegwerfadresse zu löschen, klicken Sie erneut auf **Optionen** und auf **Wegwerf-Adressen**.

Internet: ➔ ① www.spamgourmet.com
➔ ② de.vahoo.com

Computer TIPP

ANTIVIRUS-PAKET MIT SPAM-SCHUTZ

Eine gute Antivirus-Software ist Pflichtprogramm für jeden PC. Auf Heft-CD/-DVD gibt's gratis das Komplettpaket Kaspersky Security Suite CBE. Es schützt vor Schadprogrammen und bietet einen Spam-Filter. Verwenden Sie die Kaspersky Security Suite CBE zusammen mit dem integrierten Filter Ihres E-Mail-Programms, sind Sie also gleich doppelt vor unerwünschten Nachrichten geschützt.