

# Sicheres Surfen

## Wie schütze ich meine Daten (im Internet und auch anderswo)?



# HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

By RANDY JEFFRIES / Weekly World News

**WASHINGTON** — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent "break-ins" that paralyzed the Amazon.com, Buy.com and eBay websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yabenson told Weekly World News.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 87-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.

"As dangerous as this technology is right now, it's going to get much scarier," Yabenson said.

"Soon it will be sold to terrorists, cults and fanatical religious-fringe groups.

"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

"That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be found out."

**... & blow your family to smithereens!**

**KABOOM!** It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

**Sickos can wreak death and destruction from thousands of miles away!**

Arnold Yabenson.

Quelle: <http://weeklyworldnews.com/> 2000

## **Sicherheit**

### **Was ist das und wozu brauche ich das?**

#### **Sicherheit beim Surfen**

Niemand darf ohne meine Erlaubnis oder ohne mein Wissen etwas auf meinem Rechner installieren oder platzieren.

Tipp: Konfigurieren Sie Ihren Browser so, dass alle so genannten aktiven Inhalte verboten sind.

#### **Sicherheit beim E-Mail schreiben**

Niemand darf ohne meine Erlaubnis oder ohne mein Wissen etwas auf meinem Rechner installieren oder platzieren. Niemand darf meine E-Mails lesen außer dem Empfänger.

Tipp: Verbieten Sie E-Mails in HTML oder lassen Sie sich E-Mails nur im Textformat anzeigen.

Öffnen Sie keine unverlangten Attachments von (unbekannten) Absendern (das gilt auch für Word!)

Verschlüsseln Sie Ihre E-Mails, wenn Sie die Nachricht offline in einen Briefumschlag stecken würden.

## Sicherheit des Rechners

Unbefugte Personen dürfen die Daten auf meinem Rechner selbst dann nicht sehen können, wenn der Rechner verlorengegangen ist / beschlagnahmt wurde.

Tipps:

Schützen Sie den Rechner und das BIOS mit einem starken Passwort.

Arbeiten und surfen Sie nicht mit dem Admin-Account des Rechners.

Tipp: Benutzen sie Truecrypt!

Durchsuchungen von Redaktionen und Beschlagname von Rechnern:

<http://meedia.de/fernsehen/razzia-bei-akte-redaktion-war-rechtswidrig/2011/09/07.html>

<http://www.graswurzel.net/news/durchsuchung.shtml>

<http://www.bverfg.de/pressemitteilungen/bvg07-021.html>

[http://de.wikipedia.org/wiki/Bruno\\_Schirra](http://de.wikipedia.org/wiki/Bruno_Schirra)

<http://www.taz.de/!64771/>

<http://www.taz.de/!70055/>

<http://www.labournet.de/ueberuns/beschlagnahme/index.html>

<http://visual-rebellion.com/hausdurchsuchung-bei-berliner-nachwuchsjournalisten/>

<https://netzpolitik.org/2011/stuttgart-webcams-beschlagnahmt/>

<http://iknews.de/2010/04/28/usa-hausdurchsuchung-und-beschlagnahme-bei-blogger/>

<http://www.initiative-tageszeitung.de/lexika/ol-persserecht/olp-artikel.html?LeitfadenID=70>

## Argumente für Sicherheit

Informanten können Ihnen ihre Daten aufvertrauen.

Sie müssen, sollen und können jederzeit Internet-Zensur umgehen.

Sie brauchen kein Geld und keine Zeit für "Virenschutzprogramme", "personal firewalls" und anderen Regenzauber mehr verschwenden.

Sie brauchen sich nicht mehr um Phishing und andere Gefahren zu kümmern.

Ihre persönlichen Daten können nicht mehr an andere verkauft werden.

Mitlesen Ihrer E-Mails und Nutzerprofile Ihres Kommunikationsverhaltens (Vorratsdatenspeicherung)?  
Verboten.

## Argumente gegen Sicherheit

Jetzt dauert alles zwei Sekunden länger.

Das haben wir aber noch nie so gemacht.

Das habe ich aber immer anders gemacht.

Faulheit ist eine Triebfeder der Evolution.

Ich habe nichts zu verbergen. Ich habe eine Webcam im Schlafzimmer.

Menschliches Verhalten lässt sich nur sehr schwer ändern.  
Fragen Sie den nächstbesten Pfarrer oder Philosophen.

## **Nützliche Links:**

German Privacy Foundation – Digitales Aikido

[http://www.privacyfoundation.de/projekte/digitales\\_aikido/](http://www.privacyfoundation.de/projekte/digitales_aikido/)

## **Surfen:**

<http://www.heise.de/security/dienste/Browsercheck-2107.html>

Bundesamt für Sicherheit in der Informationstechnik – aktive Inhalte

[https://www.bsi.bund.de/ContentBSI/Themen/Internet\\_Sicherheit/Gefahren/AktiveInhalte/definitionen/definition\\_gefahren.html3](https://www.bsi.bund.de/ContentBSI/Themen/Internet_Sicherheit/Gefahren/AktiveInhalte/definitionen/definition_gefahren.html3)

Sammlung datenschützender Firefox Erweiterungen

[http://www.privacyfoundation.de/service/firefox\\_erweiterungen/](http://www.privacyfoundation.de/service/firefox_erweiterungen/)

Proxtube <https://addons.mozilla.org/en-US/firefox/addon/proxtube/>

Anonym Surfen:

<https://www.torproject.org/>

<http://www.anonym-surfen.de/>

## **Mailen:**

Installieren Sie das Verschlüsselungsprogramm GnuPG für Windows:

<http://www.gpg4win.org/>

Benutzen Sie zum Verschlüsseln ein Add-On, zu Beispiel Enigmail für des E-Mail-Programm Thunderbird.

<http://enigmail.mozdev.org/home/index.php.html>

Gefahren von Word-Attachments:

<http://www.computerbytesman.com/privacy/blair.htm>

Datensicherheit auf Ihrem Rechner:

Schützen Sie nicht nur den Rechner, sondern auch das BIOS

(<http://de.wikipedia.org/wiki/BIOS>) mit einem starken Passwort!

Keepass (Programm zum bequemen Verwalten von Passwörtern):

<http://keepass.info/>

(Apple-Computer vgl. Google: password manager, Linux/Ubuntu: Revelation)

<http://www.truecrypt.org/>

## Miscellaneous

Wie Abhören von E-Mails in Deutschland funktioniert:

[https://www.bsi.bund.de/DE/Themen/weitereThemen/SINA/Systembeschreibung/systembeschreibung\\_node.html](https://www.bsi.bund.de/DE/Themen/weitereThemen/SINA/Systembeschreibung/systembeschreibung_node.html)

Wie man Handy-Gespräche leicht abhören kann:

[http://www.iwi.uni-hannover.de/lv/ucc\\_ws04\\_05/riemer/literatur/imsi-catcher.htm](http://www.iwi.uni-hannover.de/lv/ucc_ws04_05/riemer/literatur/imsi-catcher.htm)

Browser SRWare Iron für Soziale Netzwerke, ebay, Twitter usw.

[http://www.srware.net/en/software\\_srware\\_iron.php](http://www.srware.net/en/software_srware_iron.php)

Beispiele für Gefahren (Auswahl)

History Stealing

<http://www.heise.de/newsticker/meldung/History-Stealing-fuer-die-Anzeigenkunden-1147598.html>

<http://www.heise.de/newsticker/meldung/History-Stealing-2-0-Ich-weiss-wo-du-wohnst-1005016.html>

Identifizierung von Browsern

hsten Kriterien versucht, einen möglichst eindeutigen "Fingerabdruck" des Browsers z

Missbrauch mit Cookies

<http://www.heise.de/newsticker/meldung/LinkedIn-schlampt-mit-Zugangs-Cookies-1247813.html>

Links in HTML-Mails: <http://www.heise.de/newsticker/meldung/BSI-warnt-vor-neuem-ZeuS-Trojaner-1271483.html>

Anatomy of a Spam Viagra Purchase

<http://www.technologyreview.com/blog/editors/26785/>

Mehrzweck-Wurm kapert Facebook-Konten

<http://www.spiegel.de/netzwelt/web/0,1518,807521,00.html>

Netzensur per SSL-Tunnel aushebeln

<http://www.heise.de/netze/artikel/Netzensur-per-SSL-Tunnel-aushebeln-1412967.html>

Burkhard Schröder [burks@burks.de](mailto:burks@burks.de)

licensed under a [Creative Commons Attribution-NonCommercial 3.0 Germany License](http://creativecommons.org/licenses/by-nc/3.0/de/) <http://creativecommons.org/licenses/by-nc/3.0/de/>