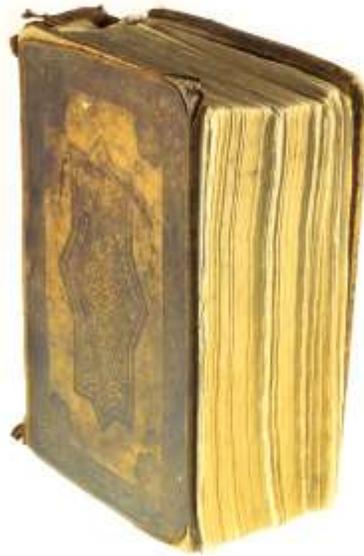




Sicherheit

im Internet und auf dem Heim-PC

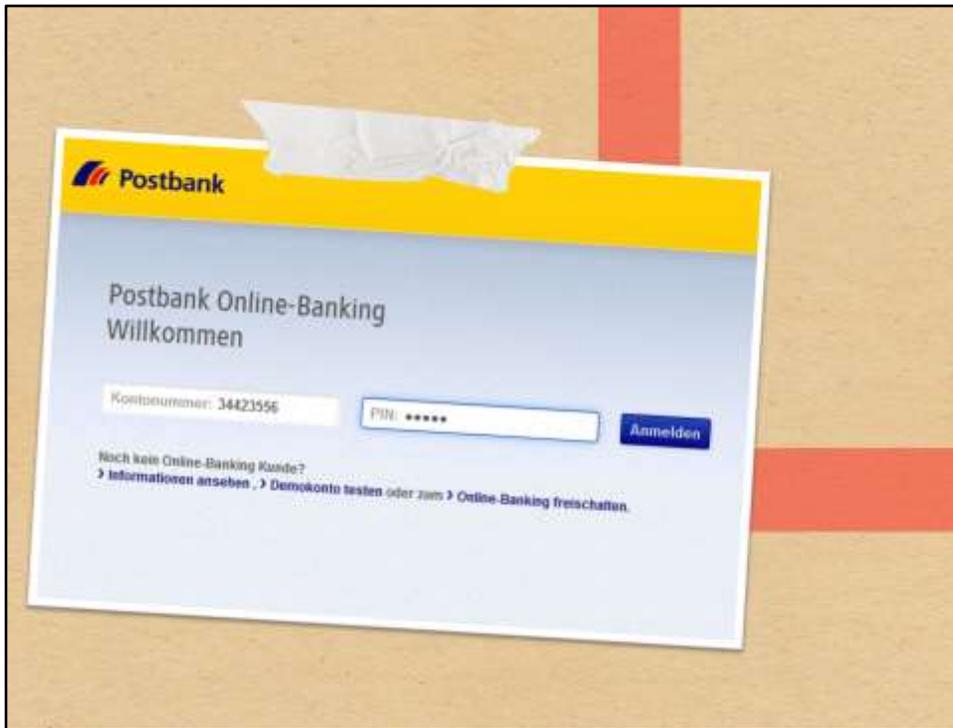
Es **war**
einmal...



Ich möchte zum Einstieg eine kleine Geschichte erzählen.



Sie handelt von Stefan, einem ahnungslosen Internet- und PC-Benutzer.



- Stefan Freitagabend allein am Laptop, Frau ist im Urlaub
- E-Mail von Bank mit Bitte, er möge Online-Banking kontrollieren mit PIN und TAN
- Klick auf den Link in der E-Mail
- Alles scheint in Ordnung
- Stefan geht schlafen



- Samstagmorgen Schreiben einer Anwaltskanzlei im Briefkasten
- angeblich MP3s von Bushido in Peer-to-Peer-Netzwerk zum Download angeboten
- 650,- EUR Anwaltsgebühren bezahlen ansonsten Rechtsstreit
- Stefan kennt weder Bushido noch P2P



- Stefan stellt PC ein und sucht im Internet nach Hilfe
- Link eines Forenteilnehmers angeklickt
- Bildschirm gesperrt, Warnung der GEMA
- PC war nicht mehr benutzbar
- Wochenende gelaufen, da kein Internet
- Frau hat Zweitlaptop mit, kommt erst Sonntagabend zurück



- Montagmorgen Stefan fährt mit U-Bahn zur Arbeit
- nimmt Laptop der Frau mit um in Pause nach Trojaner zu suchen
- Laptop wird ihm gestohlen
- sämtliche privaten Fotos seiner Familie drauf, nicht extern gesichert → Frau sauer!
- wenigstens Windows-Konto mit Passwort geschützt, Dieb hat also keine Daten



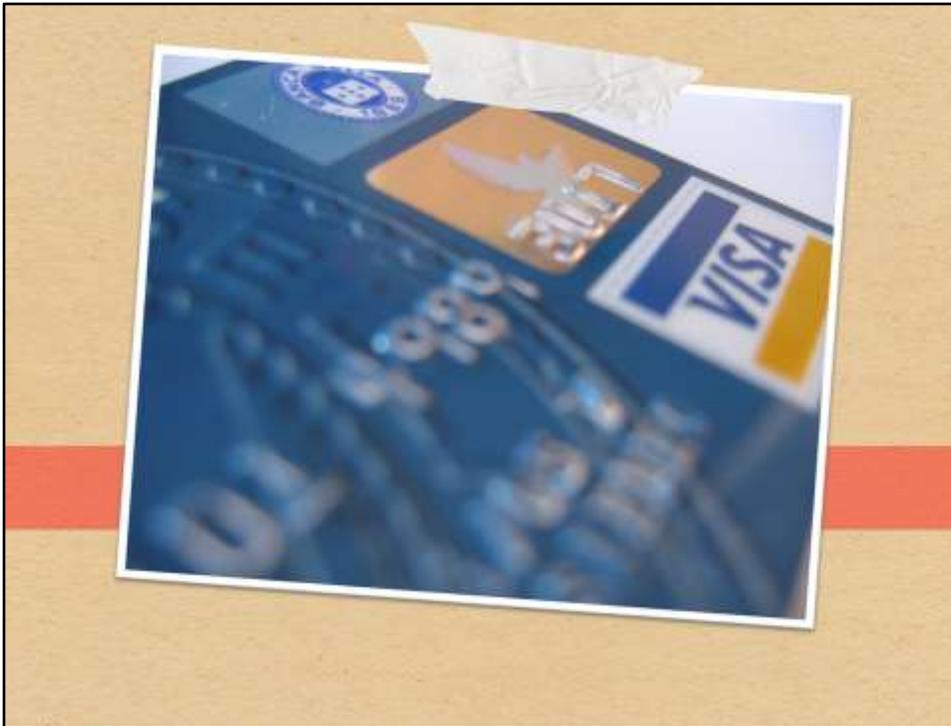
- Arbeitgeber untersagt private Internetnutzung
- in Mittagspause ins Internetcafe, wg. GEMA-Meldung
- Fake, aber spezielle Software nötig, um seinen PC zu befreien
- soll 20 EUR kosten, er bestellt

The screenshot shows the Postbank online banking interface. At the top, there is a navigation bar with 'Kontenübersicht', 'Umsätze', 'Auftragslisten', and 'Service'. A 'Nachrichtenkorb' icon is visible in the top right. The main content area displays a table of accounts and their balances, along with a transaction history for the selected account.

Konto	Kontotyp	Umsatz €	Saldo €
			0,00
Giro plus - EK	999900999		
BLZ: 25010020	08.02.2012	Überweisung	-5.328,71
Kartbank Einzelkonto	08.02.2012	Überweisung	-228,81
IBAN: DE31200100250000990000	09.02.2012	Guthaben	2.780,70
BIC: FBWDE33	08.02.2012	Überweisung	-21,50
↳ Kontodetails	08.02.2012	Scheckeinreichung...	-1.830,90
↳ Alle Umsätze			729,44
↳ Giro plus - GK	999900999		2.312,55
↳ Giro Tagesgeld - EK	999900999		2.712,46
↳ SparCard 2000 plus direkt - EK	229900999		13.081,27
↳ Anlage - EK	799900919		
Gesamtstand (in EUR)			24.018,77

Additional text at the bottom of the screenshot includes: '↳ alle Konten anzeigen' and '↳ Weitere Konten hinzufügen'.

- Stefan will 20 EUR überweisen
- Login bei Bank
- Konto leer
- Bank hat Mittagspause → warten



- GEMA nervt trotzdem
- anderes Konto, mit Kreditkarte
- Kreditkartendaten auf Website eingeben



- schnell nach Bestelleingang per Mail kontrollieren
- ab zur Bank
- Rückbuchung erfolgreich



- GEMA geklärt, aber Abmahnung wartet
- Anwalt kontaktiert, Abmahnung für 200 EUR abgewehrt



- am nächsten Samstag: Rechnungen der Kreditkartenfirma
- Käufe von Waren im Ausland
- Zweitkonto bereits im Minus



- Anwalt hat Wochenende, also Mail
- Zugang wird verwehrt
- falsches Passwort
- am Montagmorgen gleich zu EDV-Kollegen
- im Büro lächeln ihn alle seltsam an



- sein Sitznachbar schaut sich gerade Stefans Frau im Bikini bei Facebook an



Publikum fragen: Was hat Stefan alles falsch gemacht?
→ Handout im Blog



Stefan hat auf verschiedenen Ebenen Fehler gemacht: im Netzwerk, auf seinem PC/Betriebssystem und beim Browsen/Mailen.

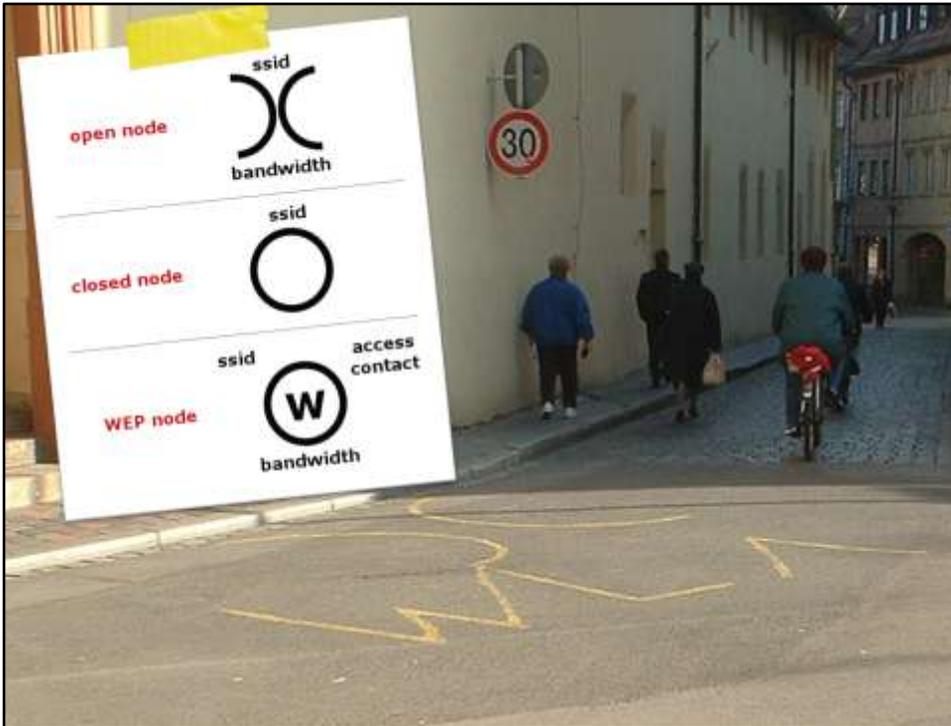


Schauen wir uns zunächst einmal die Netzwerkebene an.
Teilnehmer fragen: Wer hat ein WLAN zuhause?



WLAN

Sichere Passwörter
Firewall



Stefan hat keine Ahnung von P2P und dennoch eine Abmahnung bekommen. Wie kann das sein? → Er hat sein WLAN gar nicht oder nicht gut genug abgesichert, sodass es von Angreifern zum Surfen genutzt werden kann. In großen Städten gibt es das sog. Warchalking, bei dem offene oder leicht zugängliche WLANs mit Kreide gekennzeichnet werden.



Übersicht

Internet

Telefonie

Heimnetz

WLAN

Funknetz

Funkanal

Sicherheit

Gastzugang

WDS

DECT

System

Assistenten

Erstmalig, Update, Backup

Funknetz

Ihre FRITZ!Box kann ein WLAN-Funknetz bereitstellen. Der Name des Funknetzes ist frei wählbar. Sobald das Funknetz aktiviert ist, können sich WLAN-Geräte daran anmelden. Sie sehen die Liste der bekannten WLAN-Geräte und können diese bearbeiten und einschließen.

Funknetz

WLAN-Funknetz aktiv

Das WLAN-Funknetz Ihrer FRITZ!Box ist für andere WLAN-Geräte mit einem Namen, der sogenannten SSID, sichtbar.

Name des WLAN-Funknetzes (SSID)

Name des WLAN-Funknetzes sichtbar

AVM Stick & Surf aktivieren

MAC-Adresse dieser FRITZ!Box: 08.24.FE.A4.25.2F

Bekannte WLAN-Geräte

Die Liste zeigt die WLAN-Geräte, die zur Zeit mit der FRITZ!Box verbunden sind. Darüber hinaus zeigt die Liste WLAN-Geräte an, die der FRITZ!Box aus früheren Verbindungen oder Verbindungsversuchen bekannt sind.

Signalstärke	Name	IP-Adresse	MAC-Adresse	Datensatz	Eigenschaften		
📶	iPad-von-Gl	192.168.178.37	D8-A2:5E:33:94:E9		nicht verbunden	🔍	✖
📶	PC-FS-D1-11-31-03-40		F8-D1:11:31:03:40		nicht verbunden	🔍	✖
📶	Philips-BO	192.168.178.34	5C:33:8E:72:66:5C		nicht verbunden	🔍	✖
📶	Bertram(T)	192.168.178.27	94:37:F9:95:93:F4	25 MB/s	WPS, WMM	🔍	✖
📶	SonyEricsson	192.168.178.35	84:00:02:A5:F8:02		nicht verbunden	🔍	✖

Die angezeigten WLAN-Geräte dürfen untereinander kommunizieren.

Alle neuen WLAN-Geräte zulassen

WLAN-Zugang auf die bekannten WLAN-Geräte beschränken

WLAN-Gerät hinzufügen



- Unsichtbare SSID ist kein echter Schutz, aber hilft gegen Script Kiddies
- MAC kann gefälscht werden, aber dazu muss eine erlaubte MAC bekannt sein



- Übersicht
 - Internet
 - Telefonie
 - Heimnetz
 - WLAN
 - Funknetz
 - Funkkanal
 - Sicherheit**
 - Gastzugang
 - WDS
 - DECT
 - System
- Assistenten
Zurichten, Update, Testfone

Sicherheit

Verschlüsselung WPS - Schnellverbindung

Legen Sie hier fest, wie Ihr WLAN-Funknetz gegen unberechtigte Nutzung und gegen Abhören gesichert werden soll.

- WPA-Verschlüsselung (empfohlen, größte Sicherheit)
- WEP-Verschlüsselung (nicht empfohlen, unsicher)
- unverschlüsselt (nicht empfohlen, ungeschützt)

WPA-Verschlüsselung

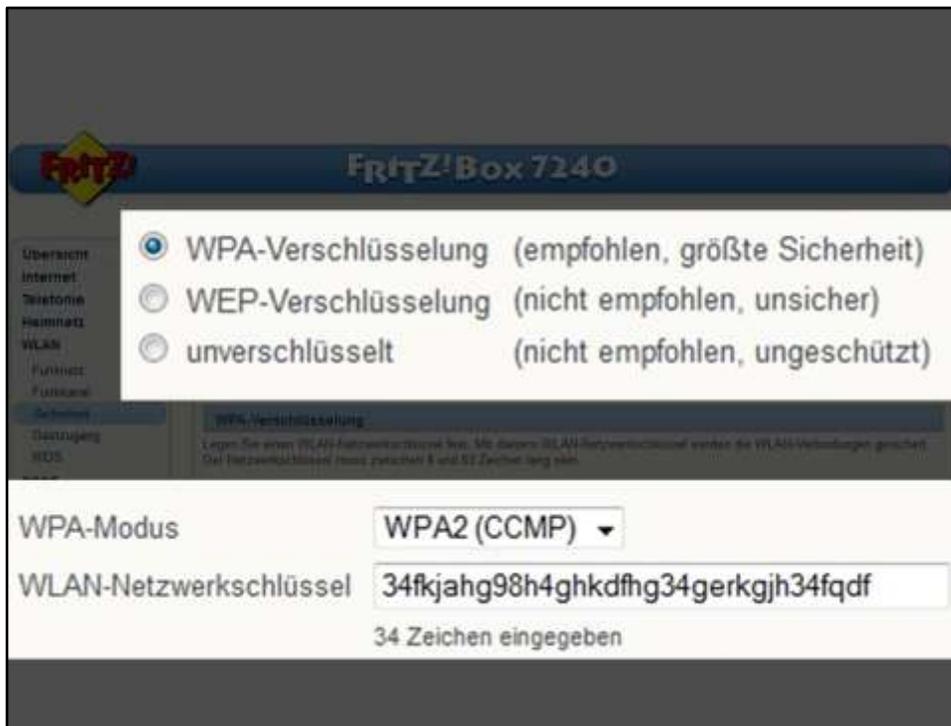
Legen Sie einen WLAN-Netzwerksschlüssel fest. Mit diesem WLAN-Netzwerksschlüssel werden die WLAN-Verbindungen gesichert. Der Netzwerksschlüssel muss zwischen 8 und 63 Zeichen lang sein.

WPA-Modus WPA2 (CCMP) ▾

WLAN-Netzwerksschlüssel 34kjahg98Mghkdthg34gerkjh34lqdf

34 Zeichen eingegeben

Übernehmen Abbrechen Hilfe



- WEP ist schon geknackt
- Auch WPA kann geknackt werden, wenn das Passwort schwach ist



WLAN
Sichere **Passwörter**
Firewall



Teilnehmer fragen: Wer kennt den Computer?

- Passwörter sind sicher, wenn es sehr lange dauert, sie mit heute verfügbarer Technik zu knacken
- Sichere Passwörter sind in allen anderen genannten Bereichen wichtig!

Brute Force

Mögliche **Kombinationen:**

[Anzahl Zeichen]^[Anzahl Stellen]

[a-z A-Z 0-9 !\$%&...] 10 Stellen

(26 + 26 + 10 + 20)¹⁰

$82^{10} = 13.744.803.133.596.058.624$

→ **44,6 Mio.** Jahre (10.000 Kom./s)

„Beliebteste“ Passwörter 2011

- password
- 123456
- 12345678
- qwerty
- abc123
- monkey
- 1234567
- letmein
- trustno1
- dragon
- baseball
- 111111
- iloveyou
- master
- sunshine
- ashley
- bailey
- passwOrd
- shadow
- 123123
- 654321
- superman
- qazwsx
- michael

- Wörterbuchattacken: Mittel für Angreifer, Laufzeit zu verringern
- Beliebteste Passwörter 2011 laut <http://splashdata.com/splashid/worst-passwords/index.htm>

Passwortsätze

komplexes Pw.: $82^{10} = 1,4 * 10^{19}$ Kombi.
vs. nur Buchstaben (52 Zeichen)

→ $\log(82^{10}) / \log(52) = 11,15 \rightarrow 12$ Stellen
 $52^{12} = 3,9 * 10^{20}$

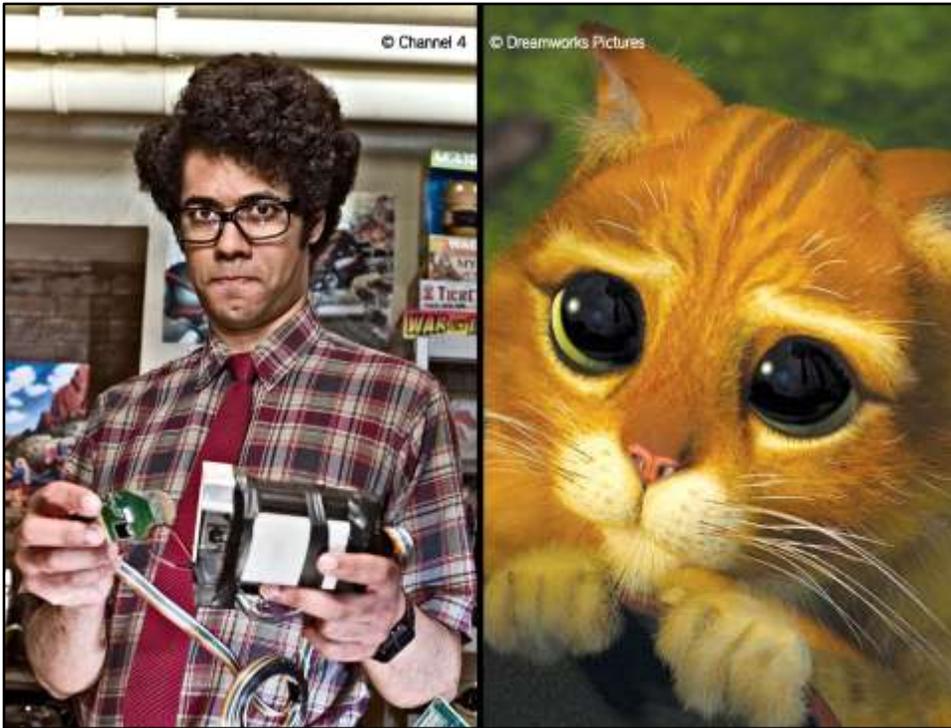
„diesisteingutesPasswort“

$52^{23} = 2,9 * 10^{39}$

<p>UNCOMMON (NON-GIBBERISH) BASE WORD</p> <p>ORDER UNKNOWN</p> <p>Tr0ub4dor&3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO SECURITY FOR THE TRIZ TRIZ SHI IS ONLY ONE OF A FEW COMMON SEPARATORS)</p>	<p>~28 BITS OF ENTROPY</p> <p>$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$</p> <p>(PUNISHABLE ATTACK ON A WORK REMOTE WEB SERVICE. YES, CRAWLING A STORED MIGHT BE FASTER, BUT IT'S NOT WHAT THE PEOPLE USE (SHOULD WEARY ABOUT))</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR, AND ONE OF THE O's WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p>  <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT!</p>  <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

<http://xkcd.com/936/>



„Social Engineering“ → Passwörter niemals herausgeben, auch nicht an den IT-Support

MOVIE HACKING...

IF I CAN JUST OVERCLOCK THE UNIX
DJANGO, I CAN BASIC THE DDOS
ROOT. DAMN. NO DICE. BUT WAIT... IF I
DISENCRYPT THEIR KILOBYTES WITH A
BACKDOOR HANDSHAKE
THEN... JACKPOT.







WLAN
Sichere Passwörter
Firewall



Die meisten privaten Netzwerke sehen so aus: Computer geht über Router ins Internet. Der Router lässt den ein- und ausgehenden Verkehr durch. Das ist ok, solange es nur gewünschten Netzwerkverkehr gibt.

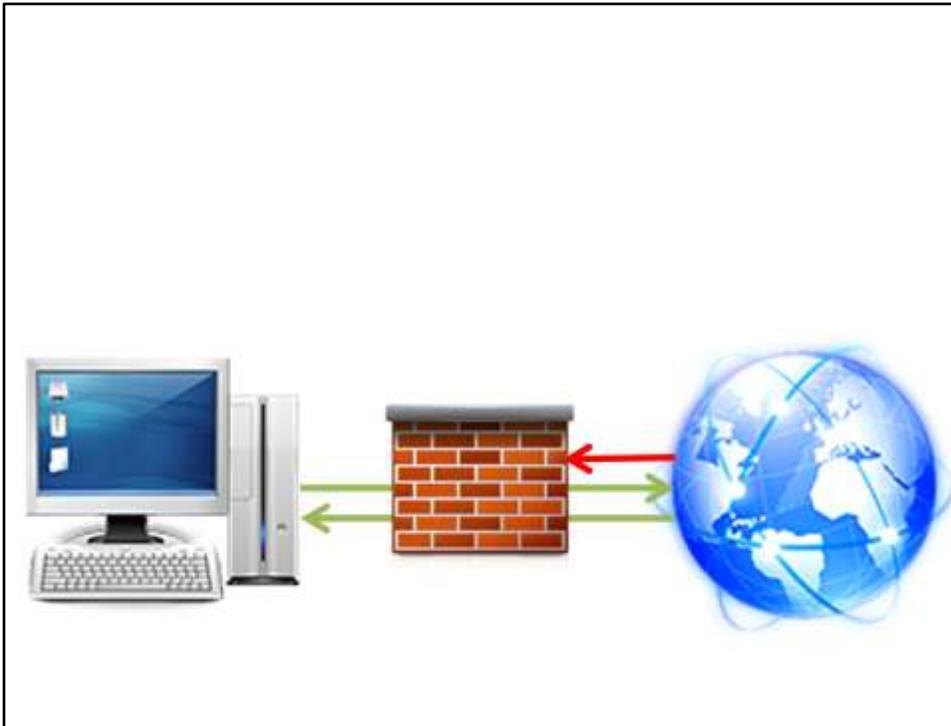
Teilnehmer fragen: Wer hat keinen Router zuhause, sondern nutzt direkt ein (DSL-)Modem?

Grundrauschen

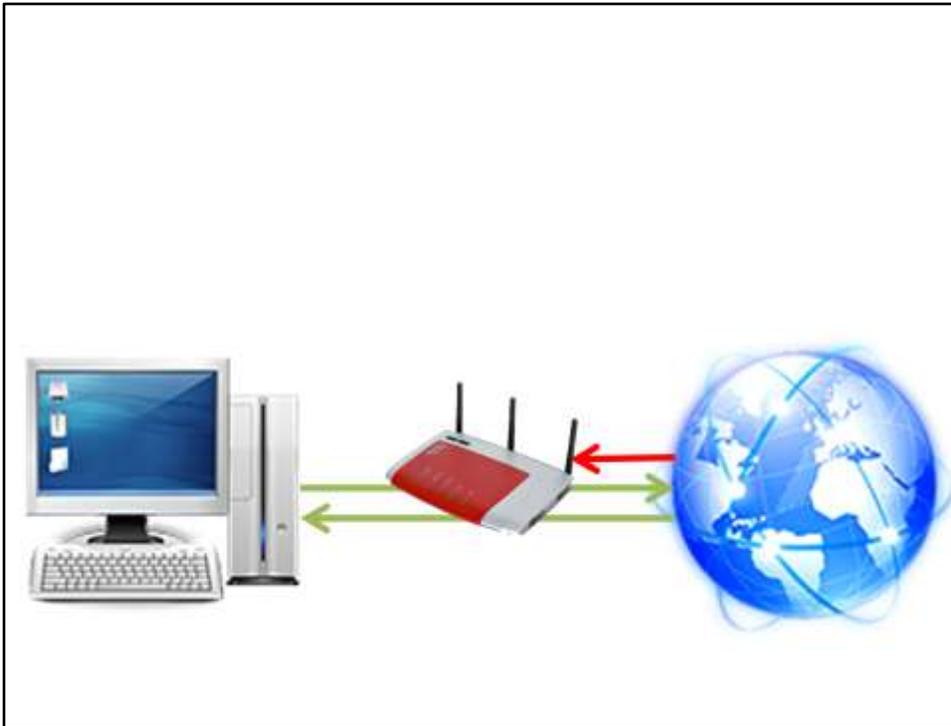


Doch was ist mit gefährlichem eingehenden Netzwerkverkehr? Dafür brauchen wir eine Firewall.

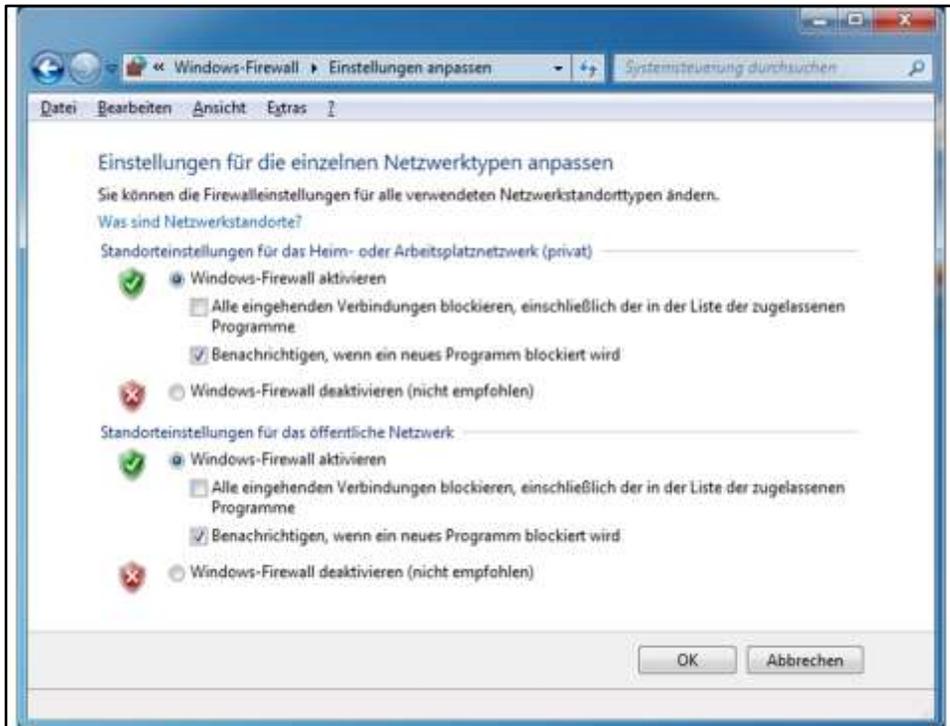
ISPs gehen von bis zu 50% Grundrauschen auf dem Netzwerk aus, von dem ein Großteil automatisierte Angriffe gegen IP-Adressbereiche sind (und natürlich Spam).

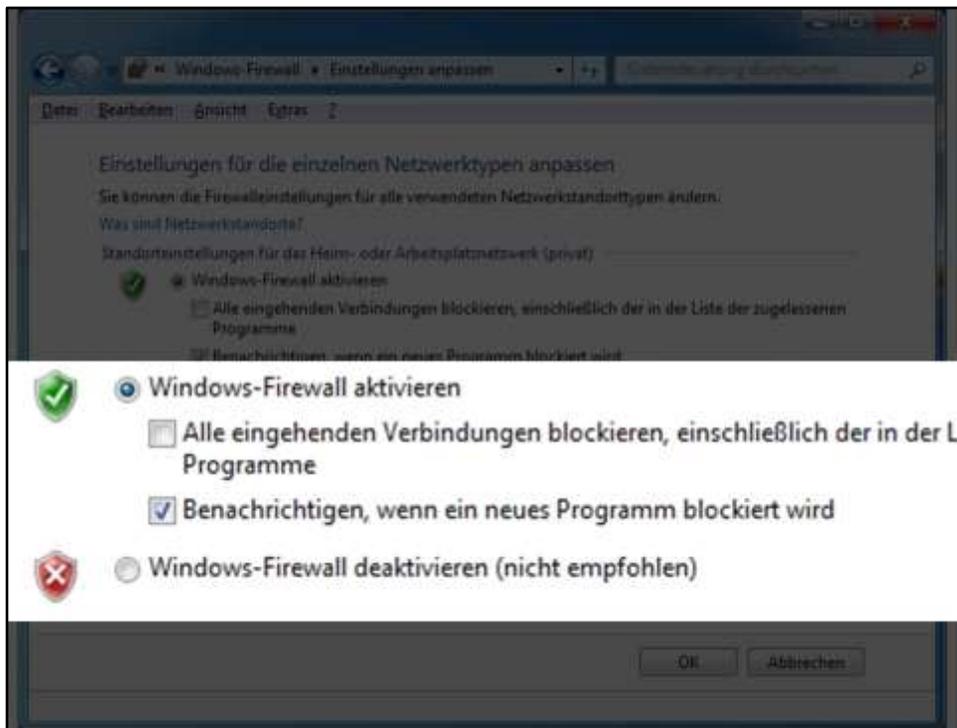


Eine Firewall blockiert unerwünschte Zugriffe von innen/außen, aber lässt gewünschte Verbindungen zu.



- Alle Router haben eine Firewall bereits eingebaut, sie muss nur aktiviert werden.
- Ansonsten reicht die Windows-Firewall
- Eigentlich nur nötig, wenn direkt im Internet und nicht hinter Router
- Vorsicht bei öffentlichen WLAN-Zugängen







Kommen wir nun zur Ebene des PCs/Betriebssystems.



Kommen wir nun zur Ebene des PCs/Betriebssystems.



- Virenschanner ist Geschmackssache
- einer reicht, nicht zwei gleichzeitig
- das Wichtigste sind die regelmäßigen Updates



Auf <http://www.testvirus.de> kann man die korrekte Funktionsweise seines Virenschanners testen.

AVIRA Deutsch Kontakt Über Avira Presse Beta-Test

Privatanwender Unternehmen Support Partner Free

Privatanwender Unternehmen Virenlabor Download Product Lifecycle VDF Update

Download Avira AntiVir Rescue System

Das Avira AntiVir Rescue System ist eine linux-basierte Applikation, die es erlaubt auf Rechner zuzugreifen, die nicht mehr gebootet werden können. Auf diese Weise ist es möglich, ein beschädigtes System zu reparieren, Daten zu retten oder eine Überprüfung des Systems auf Virenbefall durchzuführen. Das Rescue System kann nach dem Herunterladen per Doppelklick auf eine CD/DVD gebrannt werden. Dieses CD/DVD kann dann benutzt werden, um einen Rechner zu booten. Das Avira AntiVir Rescue System wird mehrmals täglich aktualisiert, so dass immer die aktuellsten Sicherheitsupdates zur Verfügung stehen.

Für das Avira Rescue System benötigen Sie einen PC/Notebook mit:
Arbeitsspeicher: mindestens 512 MB, 750 MB empfohlen
CD ROM Laufwerk oder einen freien USB Slot (Tastatur (blaus empfohlen)
Auflösung: mindestens 800x600 Pixel

Avira AntiVir Rescue System	Datum	Version	Typ	Größe
Avira AntiVir Rescue System	10.02.2012	20120010202720	iso	240,04 MB
Avira AntiVir Rescue System	10.02.2012	20120010202720	exe	341,73 MB

Startseite Impressum Datenschutz Rechtliche Hinweise RSSG TechBlog Newsletter

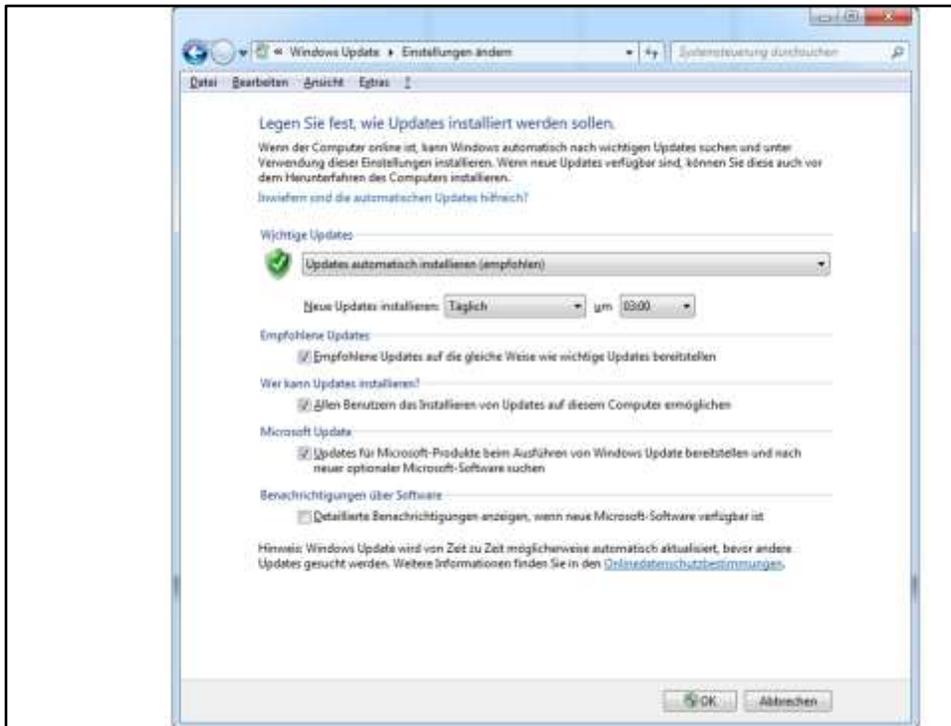
Privatanwender Unternehmen Support Partner Über Avira
 Avira Antivirus Premium Client/Server Small Business Privatanwender Partnersuche Auszeichnungen
 Avira Internet Security Avira Professional Security Managed Services Unternehmen Partner werden Karriere
 Avira Security Services Corporate Solutions Avira

Und als Vorbereitung auf den Ernstfall sollte man eine Live-CD mit Virenschanner bereithalten, wie zahlreiche Hersteller sie anbieten.

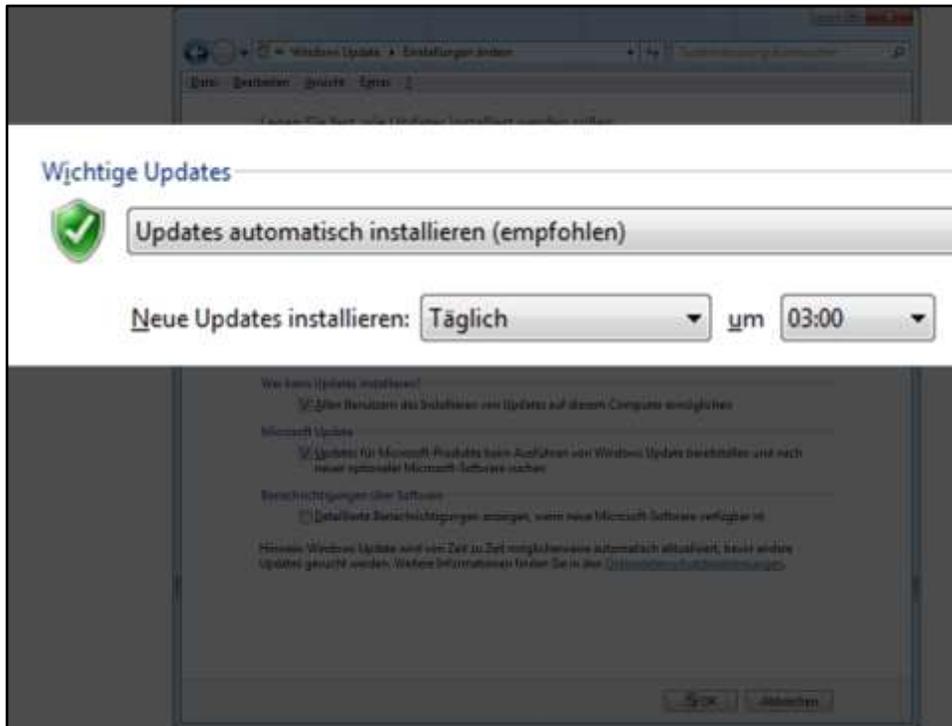
<http://www.avira.com/de/support-download-avira-antivir-rescue-system>



Virenschutz
Softwareupdates
Datensicherheit

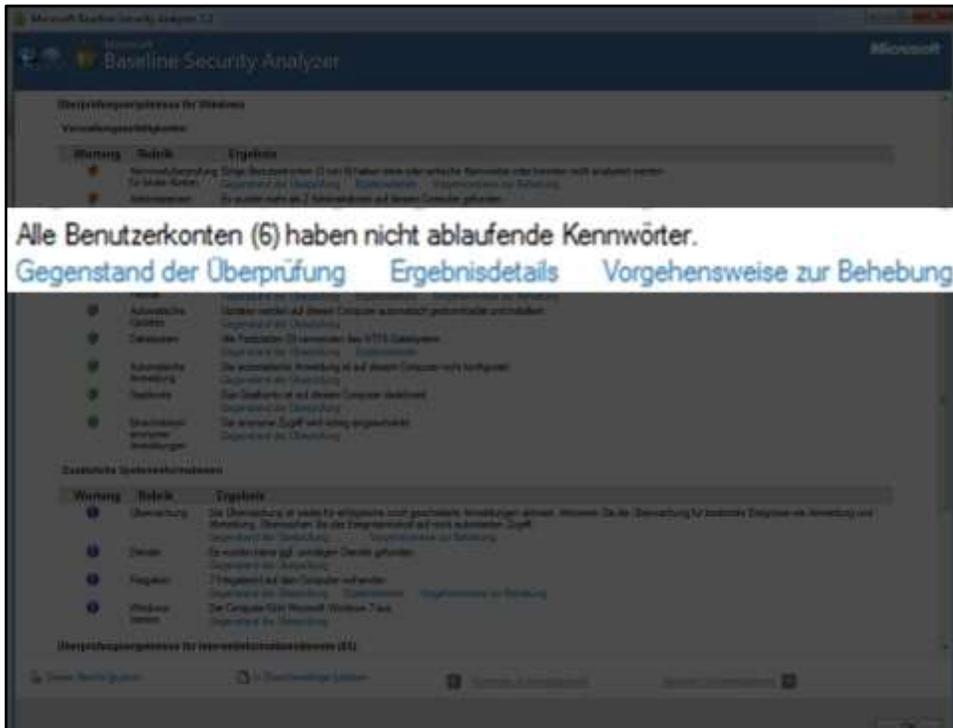


Die Windows Updates sollten konfiguriert sein. Windows ohne Updates am Netz → in wenigen Minuten mit Schädlingen befallen.





Der MBSA prüft einige grundlegenden Sicherheitseinstellungen...



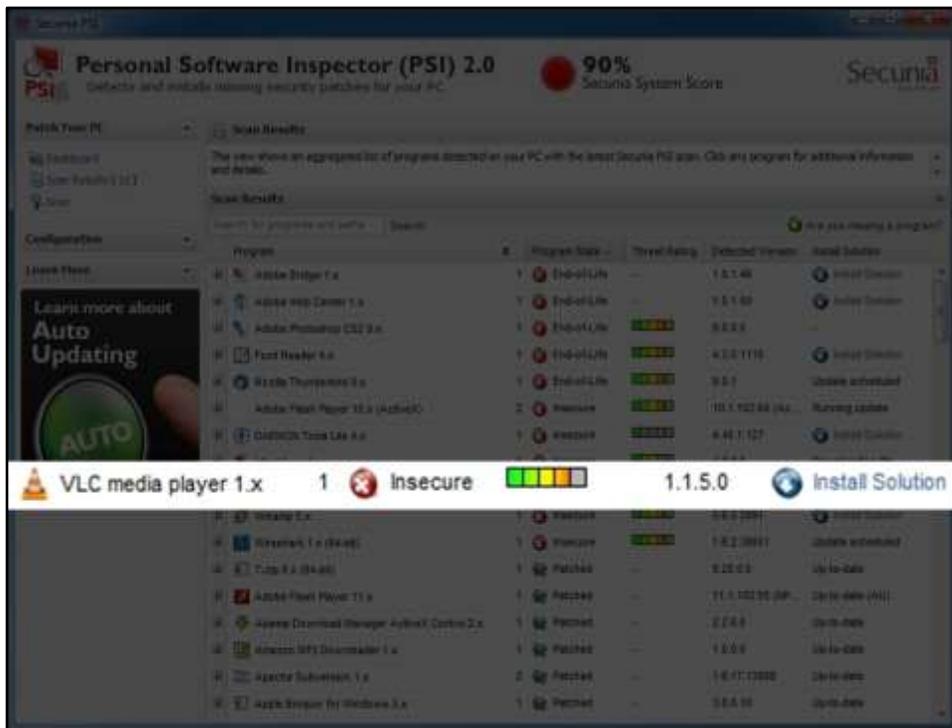
...und zeigt sie verständlich beschrieben an, damit sie behoben werden können.



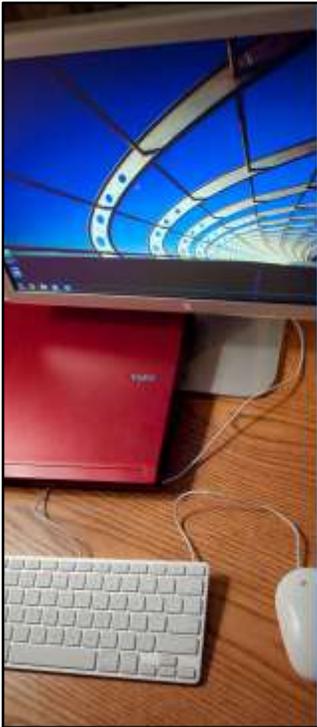
Ein großes Problem gerade in letzter Zeit waren Sicherheitslücken in Java → Updates aktivieren!



PSI scannt für alle anderen installierten Programme nach Updates...



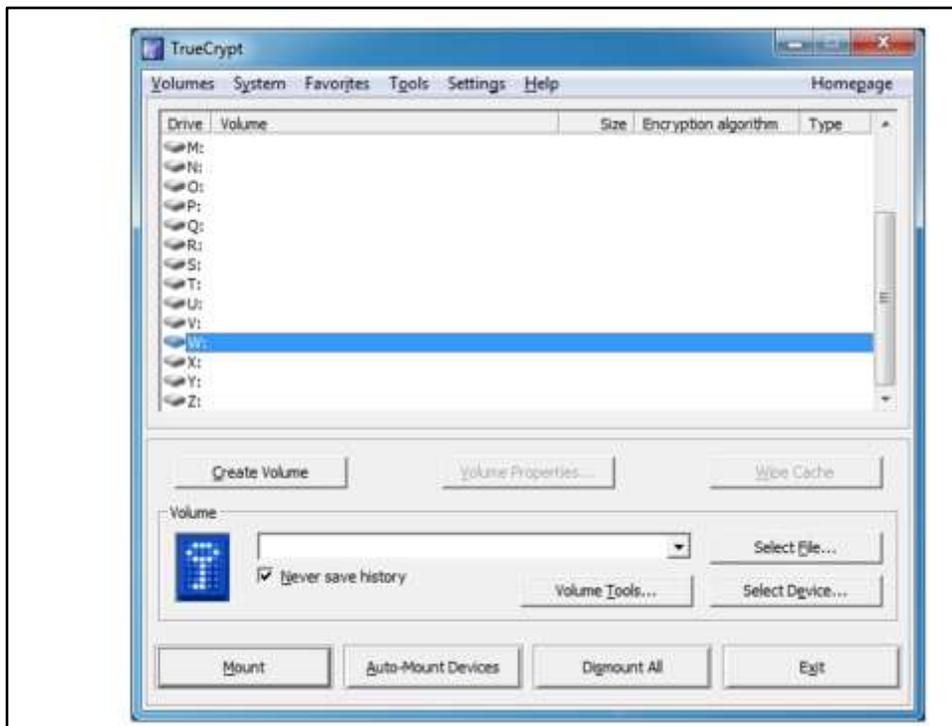
...und installiert sie auf Knopfdruck.



Virenschutz
Softwareupdates
Datensicherheit



- Windows-Kennwort hilft nicht bei Diebstahl der Hardware → Zugriff auf Hardware



- Nur Verschlüsselung der Daten hilft

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

BLAST! OUR
EVIL PLAN
IS FOILED!

NO GOOD! IT'S
4096-BIT RSA!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.



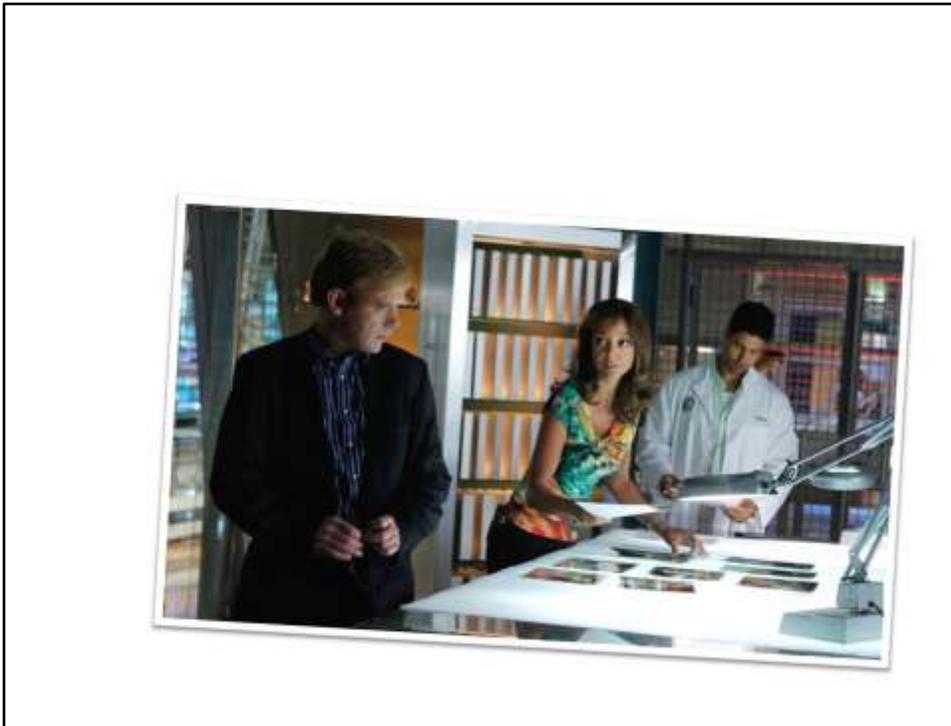
<http://xkcd.com/538/>



Festplatten halten ca. 5, DVDs ca. 10 Jahre



- Datenverlust vorbeugen durch Backup, z.B. mit SyncToy



- Vorsicht beim Verkauf alter Datenspeicher
- Einmal mit Nullen überschreiben reicht allerdings aus, um keine Daten wiederherstellen zu können



Kommen wir nun zur Ebene des Webbrowsers.



Kommen wir nun zur Ebene des Webbrowsers.



Teilnehmer fragen: Wer benutzt welchen Browser?

- Browser sind alle recht sicher
- Firefox hat viele AddOns
- Chrome hat Sandbox

The Internet Explorer 6 Countdown
Moving the world off Internet Explorer 6

Windows Internet Explorer
Download Now

10 years ago a browser was born
In 2002, we introduced Internet Explorer 6. Now that we're in 2012, in an era of modern web standards, it's time to say goodbye.

This website is dedicated to watching Internet Explorer 6 usage drop to less than 1% worldwide, so more web sites can choose to drop support for Internet Explorer 6, saving hours of work for web developers.

Here's what you can do...

Internet Explorer 6 usage around the world

7.7% of the world was using Internet Explorer 6, which was 10 percentage points less than the previous year.

2012 JAN

Breakdown of worldwide share by country/region

Global (all regions): Dec 31 2011 also: Internet Explorer 6 usage share by country (all 10)

Withdrawn to the champions circle: USA, Czech Republic, Portugal, Philippines, Myanmar and Monaco. Internet Explorer 6 usage had dropped below 1 percent in these countries, entering in a new era of modern web browsing.

JOIN THE CAUSE
Have a website? Encourage Internet Explorer 6 users to upgrade by displaying the countdown banner to Internet Explorer 6 users only. Get the word out on your site.

EDUCATE OTHERS
Friends don't let friends use Internet Explorer 6. And neither should acquaintances. Educate others about moving off of Internet Explorer 6. Why move off Internet Explorer 6?

TELL YOUR FRIENDS
Let others know that you're doing your part to get Internet Explorer 6 to 1%.

Microsoft | Contact Us | Terms of Use | Trademarks | Privacy Statement | © 2011 Microsoft

Live Us | Follow Us

Want to learn about Internet Explorer 9?

Wichtig ist ein aktueller (!) Browser



Browser warnen vor bekannten bössartigen Websites → man darf es nur nicht ignorieren.



- Browser-Updates immer sofort einspielen
- Auch wenn AddOns vielleicht nicht mehr laufen



Wer ganz sicher gehen will, installiert sich ein separates Windows in einer VM. Sollte die zerschossen werden, kann sie einfach zurückgesetzt werden.



ADD-ONS

ERWEITERUNGEN | PERSONAS | THEMES | SAMMLUNGEN | MEHR...

🏠 » Erweiterungen » NoScript



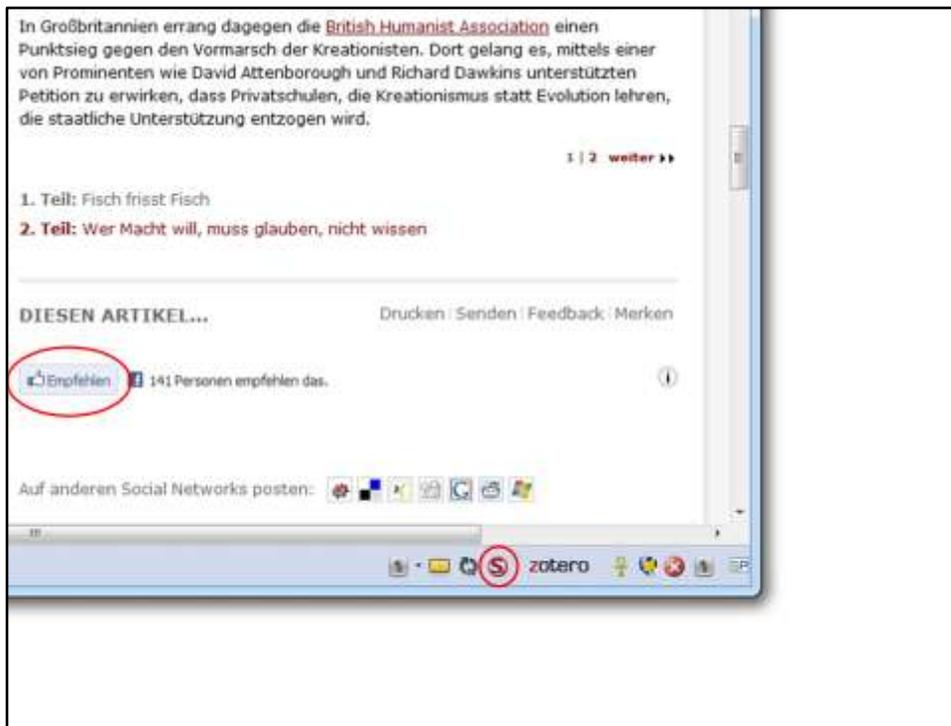
NoScript 2.3
von Giorgio Maone

Zusätzlicher Schutz für Ihren Browser!

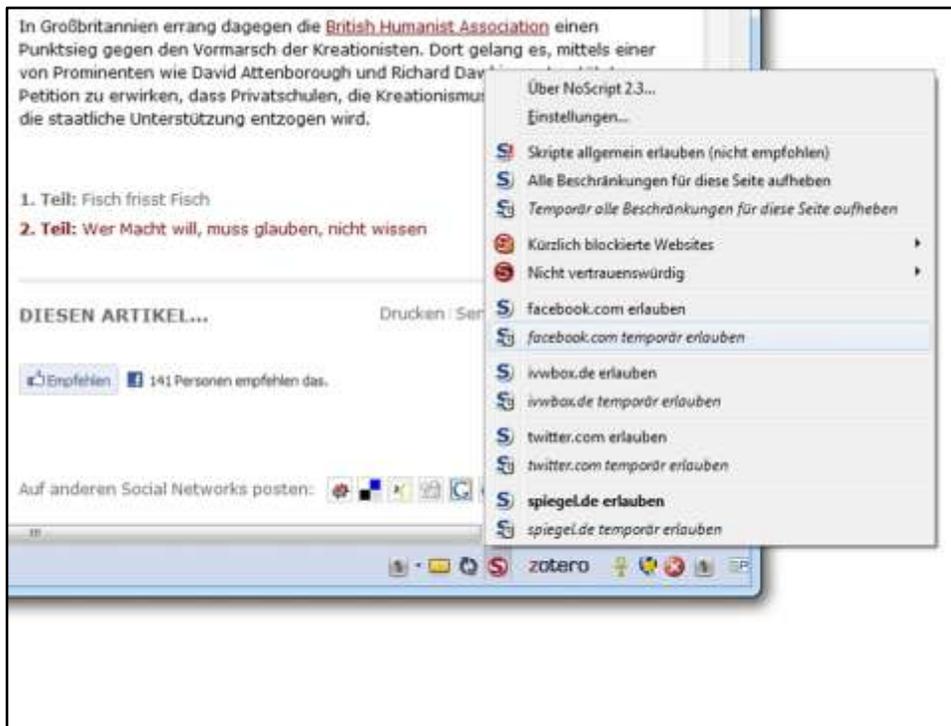
[+ Zu Firefox hinzufügen](#)

[Datenschutzerklärung](#)





- NoScript deaktiviert alle Scripts, z.B. die Facebook-Buttons



- Man kann dann gezielt die Scripts aktivieren, die man wirklich benötigt



Webbrowser

HTTPS

Sichere E-Mails

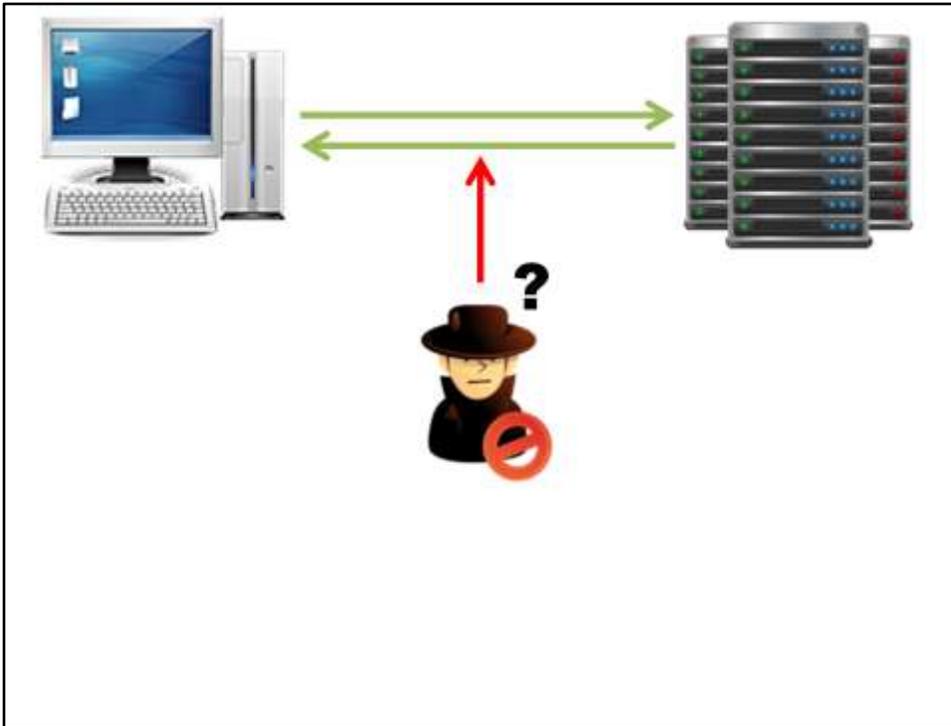
Dateidownloads

```
Follow TCP Stream
Stream Content
POST /PasswortTest/ HTTP/1.1
Host: public.macke.it
User-Agent: Mozilla/5.0 (windows NT 6.1; WOW64; rv:7.0.1) Gecko/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*
Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection: keep-alive
Referer: http://public.macke.it/PasswortTest/
Cookie: last_loginid=Stefan; last_domain=default
Content-Type: application/x-www-form-urlencoded
Content-Length: 63

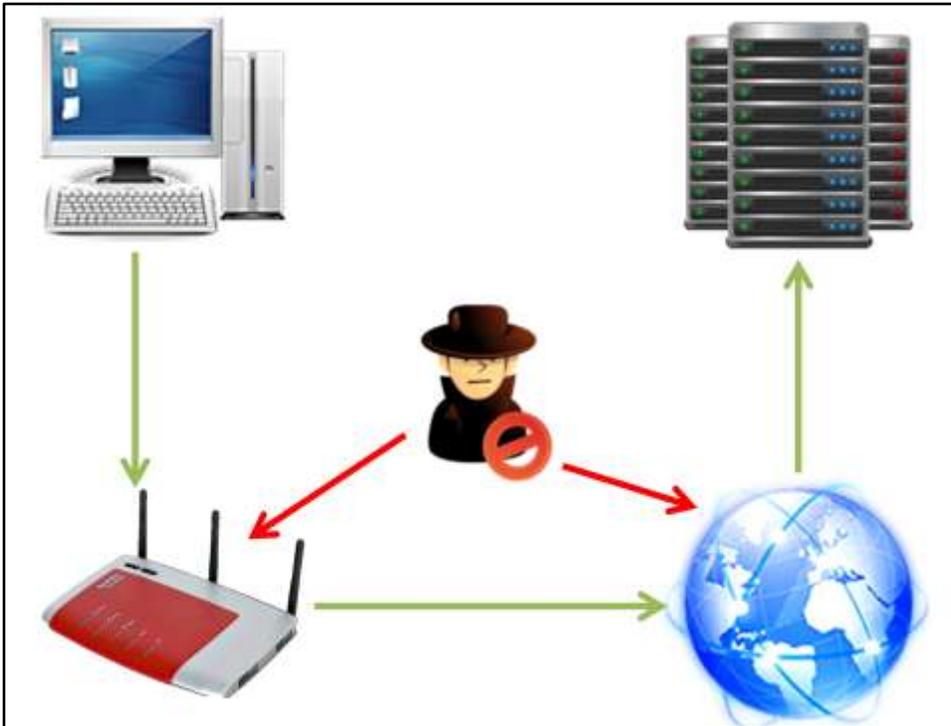
benutzername=Stefan&password=ganzgeheim&anmelden=Dat+en+absender
Date: Sun, 13 Nov 2011 15:52:14 GMT
Server: Apache/2.2.9 (Debian) DAV/2 SVN/1.4.5 PHP/5.2.6-1+lenny4
mod_python/3.3.1 Python/2.5.2 mod_ssl/2.2.9 OpenSSL/0.9.8g
X-Powered-By: PHP/5.2.6-1+lenny4
Content-Length: 697
Keep-Alive: timeout=15, max=93
Connection: Keep-Alive
Content-Type: text/html

<html>
<head>
<title>Passwort-Test</title>
</head>
```

Daten werden bei HTTP unverschlüsselt übertragen

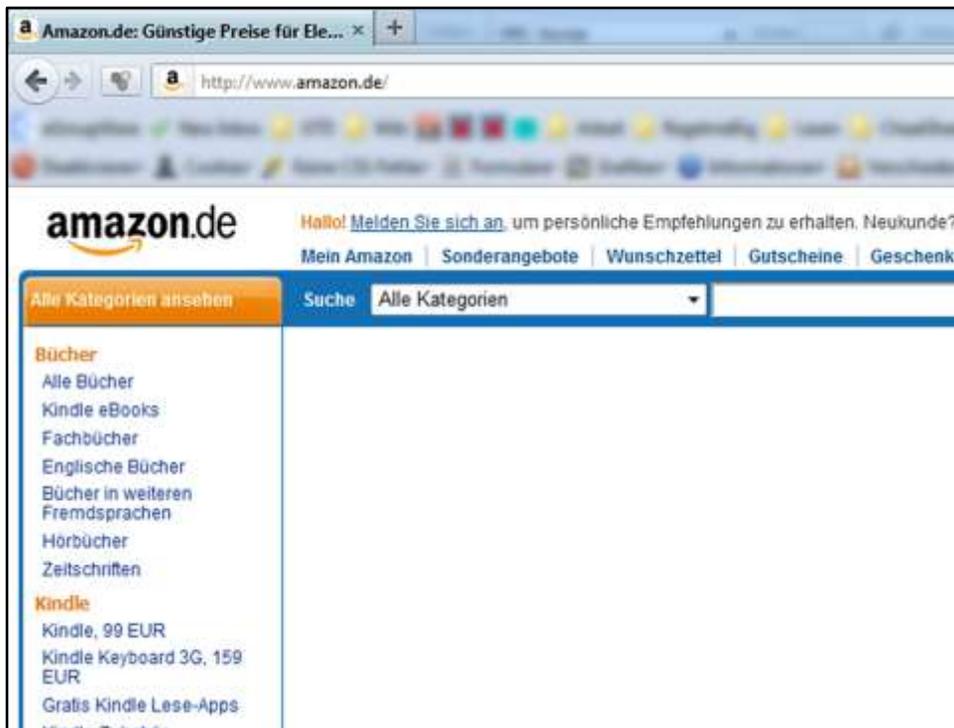


Das wäre kein Problem, wenn Client und Server direkt miteinander kommunizieren würden.



Doch das ist nicht so. Vielmehr gibt es eine Reihe an Zwischenstationen, die die Datenpakete passieren müssen.

An all diesen Zwischenstationen kann ein Angreifer die Daten problemlos auslesen. Die Daten müssen also zwischen Client und Server verschlüsselt werden.



Wie erkennt man nun, dass man verschlüsselt unterwegs ist? → Adresszeile des Browsers



Alle modernen Browser färben die Adresszeile ein, wenn die Verbindung verschlüsselt ist.



Mit einem Klick auf die Adresszeile bekommt man dann Informationen zum Zertifikat angezeigt.



Grün bedeutet, dass der Inhaber der Website intensiv geprüft wird (z.B. mit Telefonanruf und Prüfung der Adresse).



Unser Dienstleister, die ivv, entschlüsselt alle Verbindungen, um sie mitlesen zu können. Daher ändert sich auch die Farbe von grün in blau.



Dieser Verbindung wird nicht vertraut

Sie haben Firefox angewiesen, eine gesicherte Verbindung zu **www.ccc.de** aufzubauen, es kann aber nicht überprüft werden, ob die Verbindung sicher ist.

Wenn Sie normalerweise eine gesicherte Verbindung aufbauen, weist sich die Website mit einer vertrauenswürdigen Identifikation aus, um zu garantieren, dass Sie die richtige Website besuchen. Die Identifikation dieser Website dagegen kann nicht bestätigt werden.

Was sollte ich tun?

Falls Sie für gewöhnlich keine Probleme mit dieser Website haben, könnte dieser Fehler bedeuten, dass jemand die Website fälscht. Sie sollten in dem Fall nicht fortfahren.

[Diese Seite verlassen](#)

Technische Details

www.ccc.de verwendet ein ungültiges Sicherheitszertifikat.

Dem Zertifikat wird nicht vertraut, weil keine Zertifikatsausstellerkette angegeben wurde.

(Fehlercode: sec_error_unknown_issuer)

Ich kenne das Risiko

Zertifikatsfehler ab jetzt nicht mehr wegklicken, sondern genau lesen, was die Ursache ist!

- Abgelaufen?
- Unbekannter Aussteller?
- Falsche URL?



Leitet den Benutzer automatisch auf HTTPS um, wenn verfügbar.



Webbrowser
HTTPS
Sichere **E-Mails**
Dateidownloads

MYTH: COMPUTERS SUCK BECAUSE THEY
DON'T DO WHAT YOU SAY.

NO! I DON'T DOWNLOAD THAT FILE!
IT'S A VIRUS! NO! NOOO!



REALITY: COMPUTERS SUCK BECAUSE
THEY DO EXACTLY WHAT YOU SAY.



<http://www.smbc-comics.com/index.php?db=comics&id=1801>

Von: DHL <info@packstation.de>
An: [REDACTED]
Cc:
Betreff: Ihre neue Goldcard

Falls der Newsletter nicht richtig dargestellt wird, klicken Sie bitte hier.



Ihre neue Goldcard

07.07.2011 **PACKSTATION**

Sehr geehrter PACKSTATION Kunde,

vielen Dank für Ihre kürzliche Anmeldung zum PACKSTATION Service von DHL. Wie Sie vielleicht schon aus dem Newsletter erfahren haben, wurden sämtliche PACKSTATIONEN deutschlandweit aktualisiert. Nun ist eine Goldcard unabdingbar geworden.

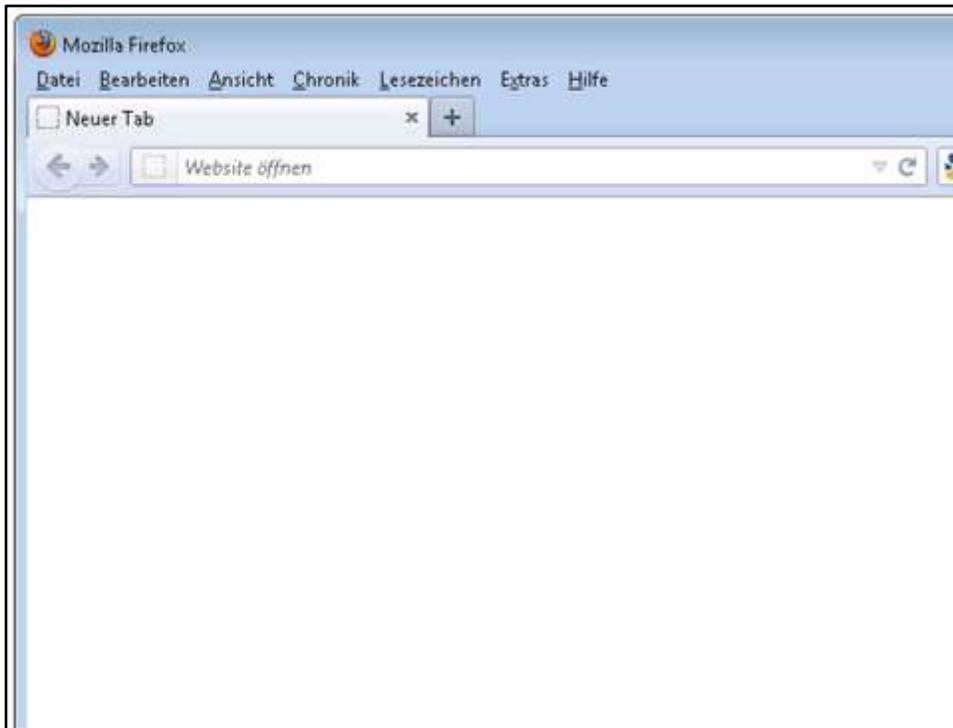
Fordern Sie jetzt Ihre neue Goldcard an, und profitieren Sie von vielen Neuerungen, wie z.B dem eingebauten RFI-Chip, mit dem sich verlorene oder gestohlene Kundenkarten orten lassen. So können Sie problemlos den PACKSTATION Service nutzen und sich gleichzeitig einige Überraschungen sichern - und das alles völlig kostenlos und unverbindlich.

[Jetzt kostenfrei anfordern!](#)

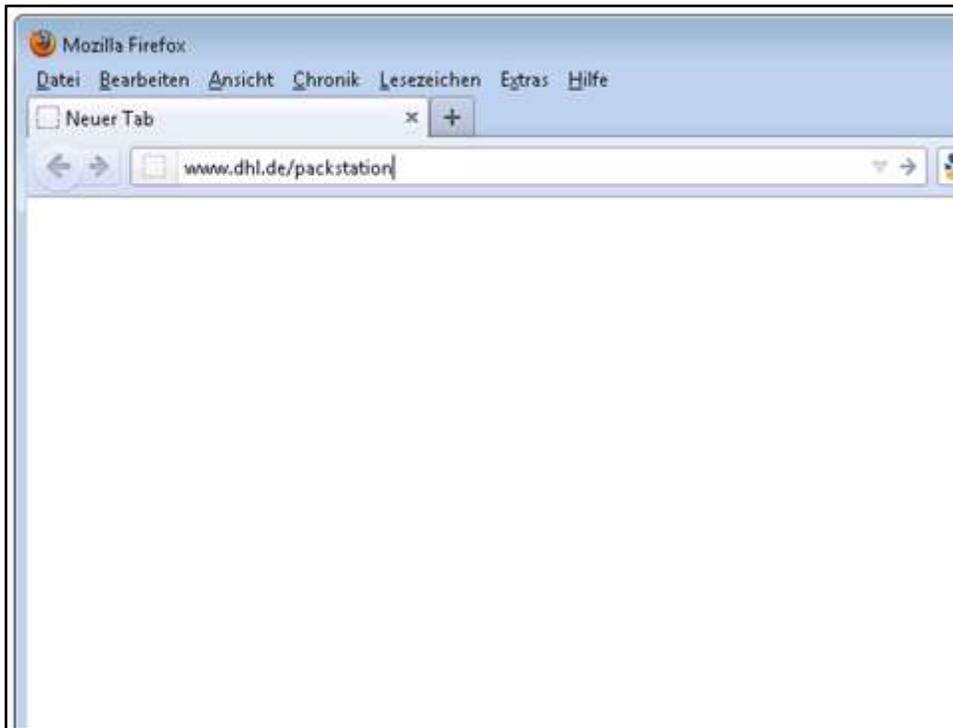
Und so einfach geht's:

- Vermerken Sie die Postnummer, Online-Passwort sowie Ihre PIN: Die

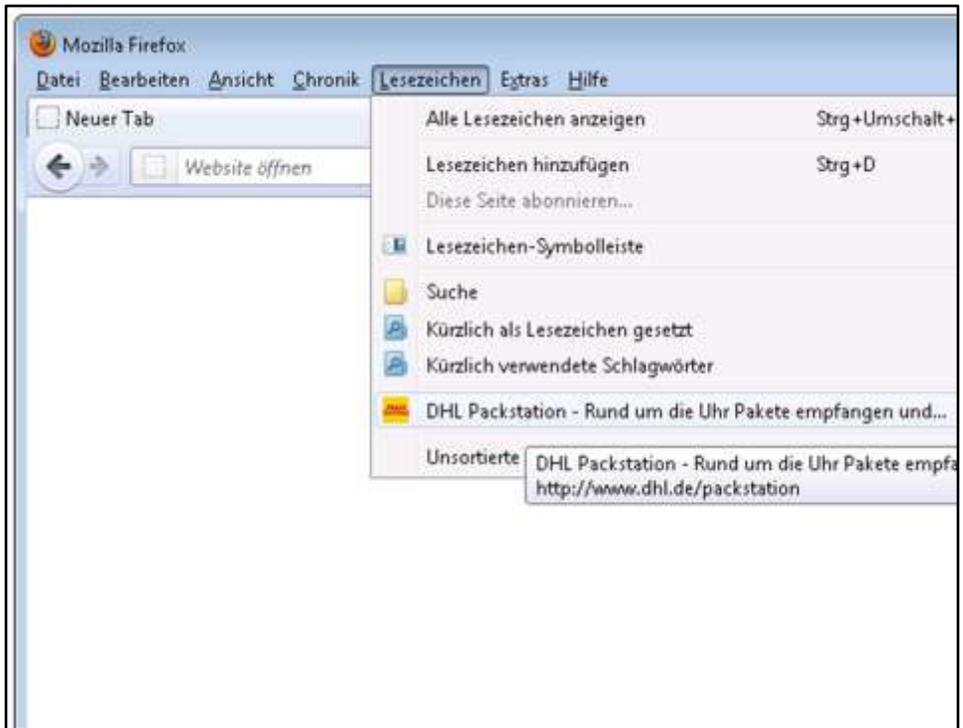
Teilnehmer raten lassen: Ist die Mail echt oder gefälscht?
nie Links aus Mails direkt öffnen...



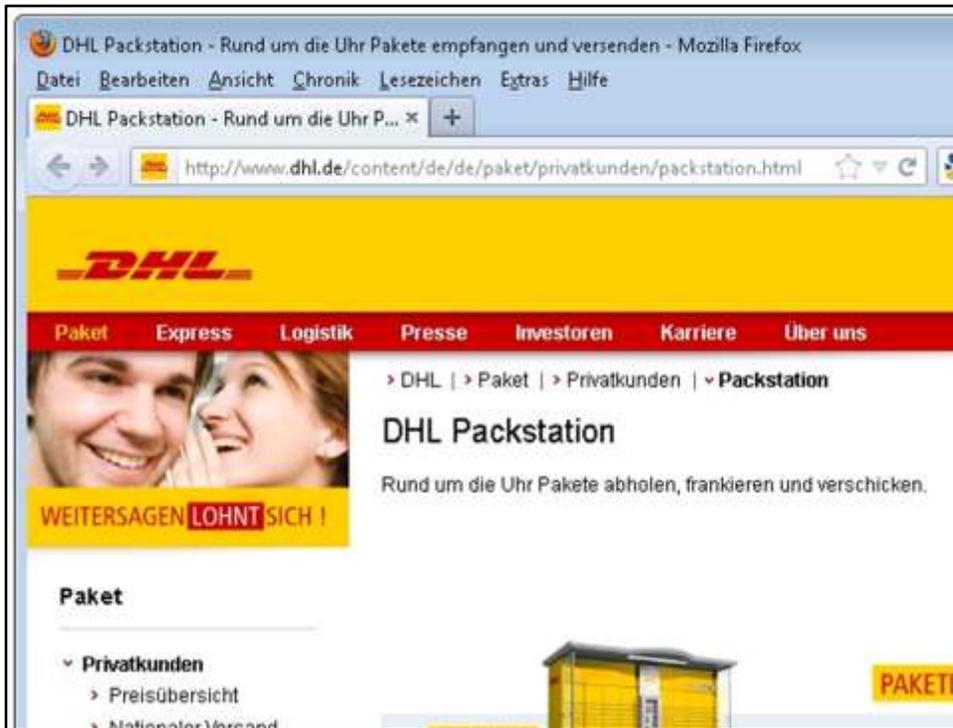
...sondern sie selbst im Browser eingeben



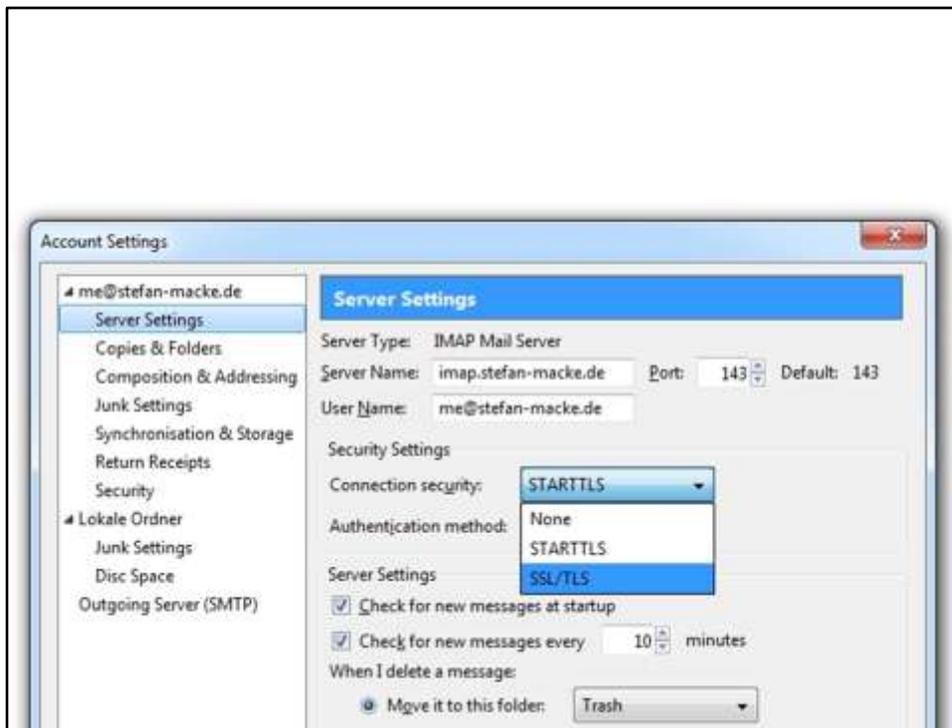
...sondern sie selbst im Browser eingeben



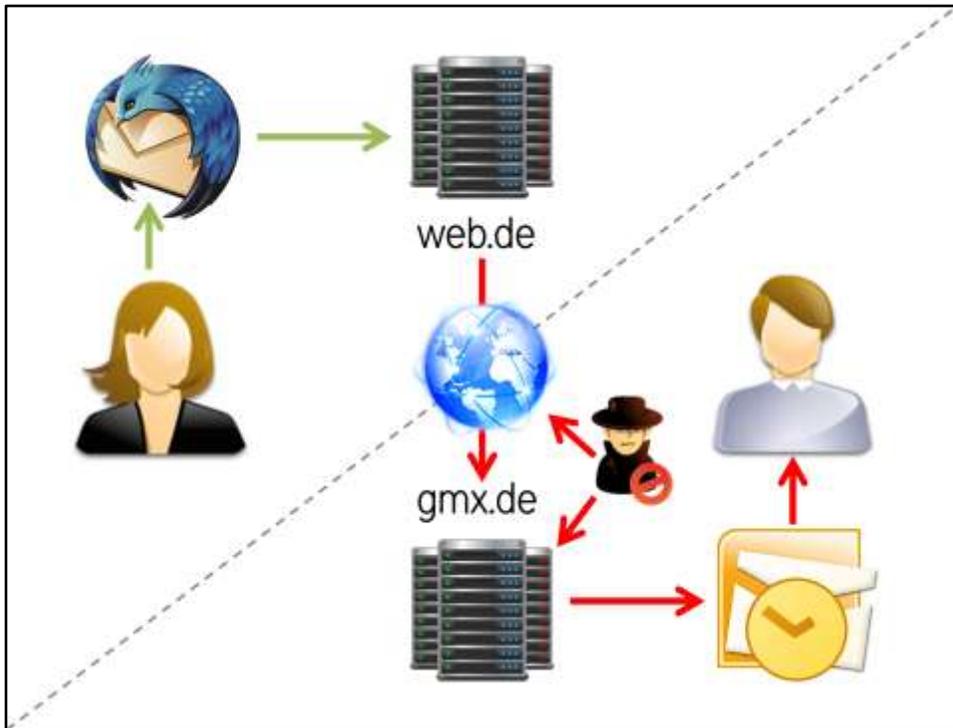
...sondern sie selbst im Browser eingeben



...sondern sie selbst im Browser eingeben



- Was für das WWW gilt, gilt genauso für E-Mails: alles wird unverschlüsselt übertragen.
- Nur verbindet man sich üblicherweise nur mit einem einzigen Server.



- SMTPS verschlüsselt nur die Daten zwischen Mailclient und eigenem Mailserver
- Nicht zwischen den Mailservern über das Internet

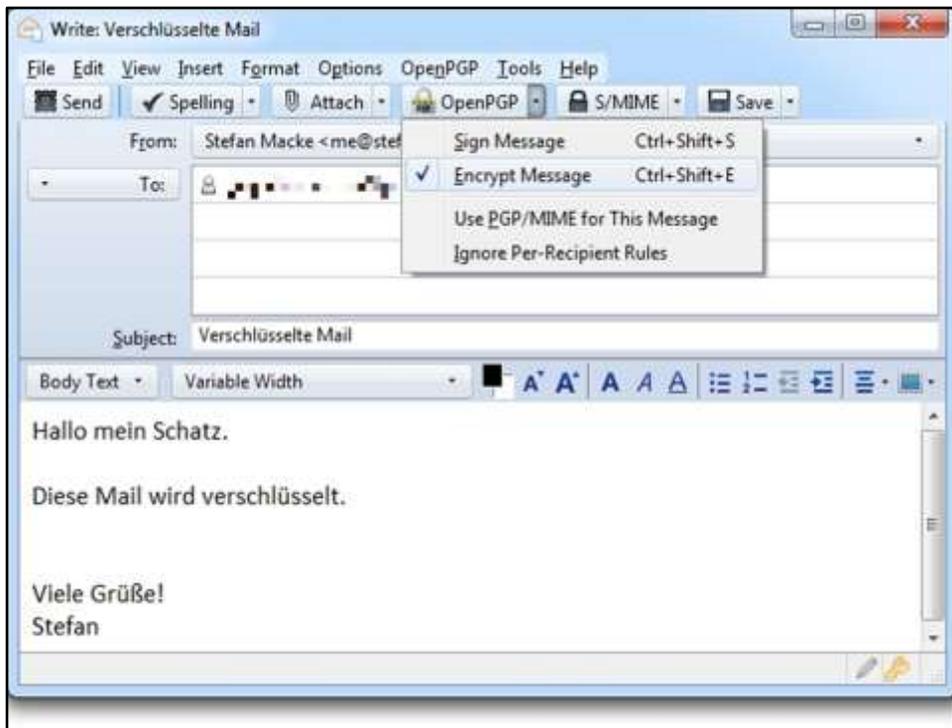
S/MIME

- entspricht Verfahren von HTTPS (CA)
- kostenpflichtige Zertifikate nötig

PGP

- basiert auf gegenseitigem Vertrauen
- kostenfrei nutzbar

Um die Mailinhalte zu verschlüsseln kann PGP oder S/MIME verwendet werden.



Beispiel: Enigmail



Webbrowser

HTTPS

Sichere E-Mails

Dateidownloads

English | Deutsch

GPG4WIN Über Gpg4win Dokumentation Gemeinschaft Support Spenden

Home » Download

Download Gpg4win 2.1.0

Änderungshistorie · Integrität prüfen

Download

Freie Software zum freien Download

(Aufgrund von Problemen mit dem dem Hostingprovider Strato.de, haben wir vorübergehend alle Links auf den Mirror in Irland abgeändert)

Gpg4win 2.1.0

Die Vollversion (inklusive des deutschen Gpg4win-Kompendiums) von Gpg4win 2.1.0 kann hier herunter geladen werden:

Gpg4win 2.1.0
6904x, 35 MB/Byte | Veröffentlicht: 2011-03-15

- **OpenPGP-Signatur** (für gpg4win-2.1.0.exe)
- **SHA1-Prüfsumme** (für gpg4win-2.1.0.exe):
`7419213cb42241d6877d30d24e814b81a1fe7f6d gpg4win-2.1.0.exe`
- **Änderungshistorie**
- **Quelltexte und andere Gpg4win-2.1.0 Varianten**:
 - Vollversion aber ohne Kleopatra und Gpg4win-Kompendium:

Gpg4win 2.1.0 enthält:

GnuPG 2.0.27
 Kleopatra 2.1.0 (2011-02-04)
 GPA 0.9.1-svn1024
 GpgOL 1.1.2
 GpgEX 0.9.7
 Claws Mail 3.7.8cv47
 Kompendium (de) 3.0.0
 Kompendium (en) 3.0.0-beta1

Woher weiß man, dass heruntergeladene Dateien nicht manipuliert wurden?

- Trojaner drin?
- Hintertürchen bei Verschlüsselung?

[GPG4WIN](#)
[Über Gpg4win](#)
[Dokumentation](#)
[Gemeinschaft](#)
[Support](#)
[Spenden](#)

[Home](#) > [Downloads](#)

Download

Free Software zum freien Download
 (Auffgrund von Problemen mit dem Hostingprovider Strato.de, haben wir vorübergehend alle Links auf den Mirror in Mainz abgeändert)

Gpg4win 2.1.0

Die Vollversion (inklusive des deutschen Gpg4win-Kompendiums) von Gpg4win 2.1.0 kann hier kostenlos geladen werden:

[Gpg4win 2.1.0](#)

Gpg4win 2.1.0 enthält:

- gnupg 2.1.0-17
- Kleinsysteme 2.1.0 (1030-02-04)
- GPA 0.9.1-001104
- GpgOL 1.1.2
- GpgEX 0.9.7
- Claws Mail 3.7.0-00007

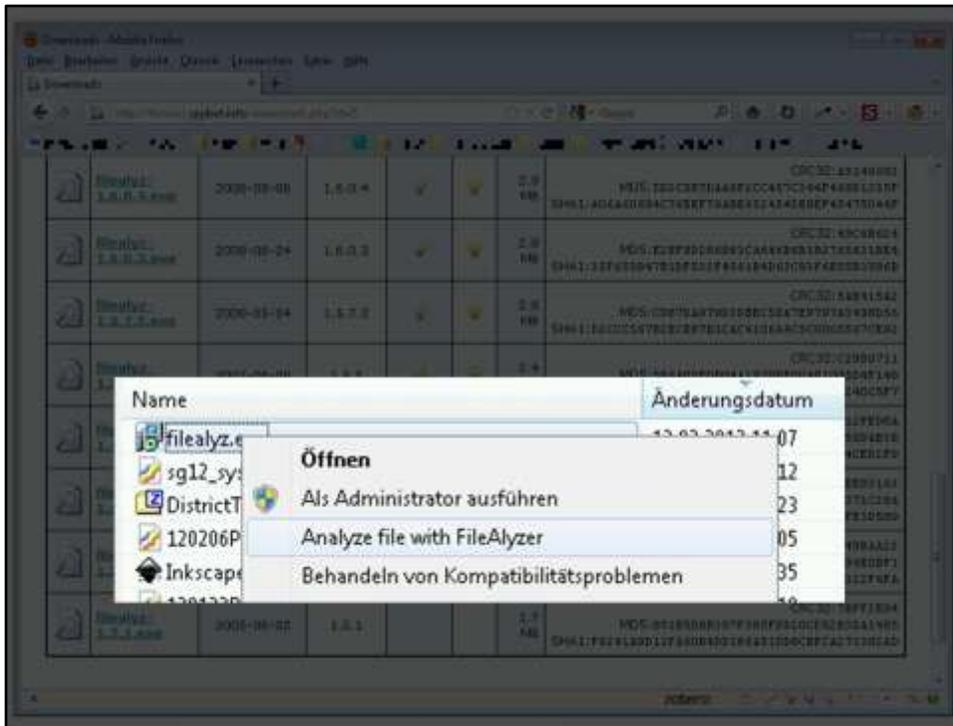
SHA1-Prüfsumme (für gpg4win-2.1.0.exe):
 f619313cb42241d6837d20d24a814b81a1fe7f6d gpg4win-2.1.0.exe

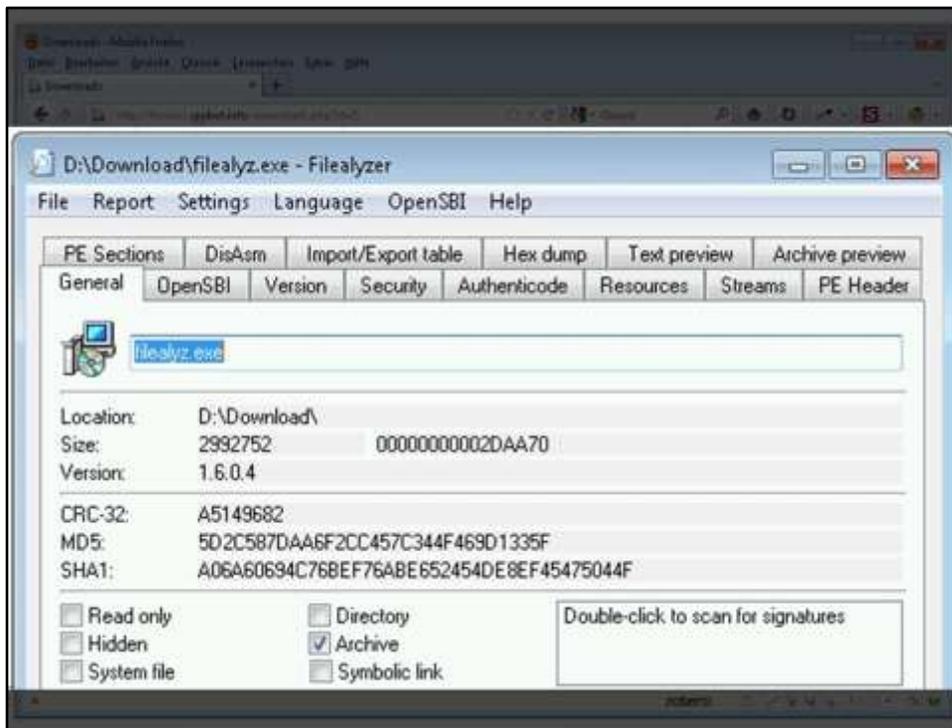
- [Anforderungen](#)
- [Quellcode und andere Gpg4win-2.1.0-Varianten](#)
 - [Mitbringen oder über Kleinsysteme und Gpg4win-Kompendium](#)



	filealyz-1.6.0.4.exe	2008-08-06	1.6.0.4			2.9 MB	CRC32: A5149682 MD5: 532C9D7DA8A8F2CC457C344F46901335F SHA1: AD6A6D694C748EF76A8E6524549E8EF45475D44F
	filealyz-1.6.0.3.exe	2008-06-24	1.6.0.3			2.8 MB	CRC32: 49C8B624 MD5: E23F9D266963CA646B81B1765631BE4 SHA1: 33F455847B1D7332F4541B4D43C93F6E8E83556B
	filealyz-1.5.7.2.exe	2008-05-04	1.5.7.2			2.8 MB	CRC32: 5A841582 MD5: C867DA979D3DBEC5A7E9797A3498D56 SHA1: D2CC567B2ECC87B1C4C4106A4C3C0D65547CE92
	filealyz-1.5.5.exe	2007-05-08	1.5.5			2.4 MB	CRC32: C2900711 MD5: 5B6A85F0B0411979F0DAD1095D4F16B SHA1: EF48EB0A1D9CF09EA7779116E75E48BF240C5F7
	filealyz-1.4.1.exe	2005-12-15	1.4.1			1.8 MB	CRC32: 812FE08A MD5: E4C748AA8EFD2CDAB048B3D555DAB3B SHA1: 50E8E3BE4E3E01E1434F0E967752C314CED2F9
	filealyz-1.4.0.exe	2005-12-13	1.4.0			1.8 MB	CRC32: 8EE93169 MD5: 15F18ECE177976F4AF46E2FE6371C28A SHA1: AEE3BC7206553E64F34EBFDD8A75C3627FE3D589
	filealyz-1.2.2.exe	2005-07-00	1.2.2			1.7 MB	CRC32: 1498AA22 MD5: 802ADC89CA23E8BF7D4E9F0A294E08F1 SHA1: 6B522D8E6984FEE46111D4805E7C0F0D332F4FA
	filealyz-1.2.1.exe	2005-05-02	1.2.1			1.7 MB	CRC32: 78FF2E84 MD5: 85185D88397F385F820C0D52E3D41685 SHA1: F6241A9D13FA60B4D9186A51D8E8FCA273392AD

Ein Tool zum Überprüfen der Hashes von Downloads ist FileAlyzer.





File Name	Release Date	Version	Download	Checksums	Size	Checksums
 filealyz-1.0.0-4.exe	2008-08-06	1.0.0.4			2.9 MB	CRC32: A5149682 MD5: 5D2C587DAA6F2CC457C344F469D1335F SHA1: A06A60694C768EF76ABE6524549E8EF45475044F
 filealyz-1.0.0-3.exe	2008-08-24	1.0.0.3			2.9 MB	CRC32: 89C98024 MD5: E28F80D68895C8A8E88182783811854 SHA1: 32F835847810F822F8541840007617420281096D
 filealyz-1.0.0-2.exe	2008-08-24	1.0.0.2			2.8 MB	CRC32: 58341544 MD5: 0870A8790108E138A72F79783430055 SHA1: 18102554781028781C4C4108A8C30800079082
 filealyz-1.0.0-1.exe	2007-08-28	1.0.0			2.4 MB	CRC32: C2980711 MD5: 58C4DFF0804A17D9F03A81030047146 SHA1: E740280A120CF80E47FF9114E70E408F240C5F7
 filealyz-1.0.0-0.exe	2005-12-10	1.0.0			1.8 MB	CRC32: 842F8D6A MD5: F9C79822889307D6A0498105004818 SHA1: 0280C18E4E1E8E1E1424F8E80782C314C8E8F9
<p>CRC-32: A5149682</p> <p>MD5: 5D2C587DAA6F2CC457C344F469D1335F</p> <p>SHA1: A06A60694C768EF76ABE652454DE8EF45475044F</p>						
 filealyz-1.0.0-0.exe	2005-08-02	1.0.0			1.7 MB	CRC32: 78FF7834 MD5: 80185068187F38F9310C82803A1485 SHA1: F92F130D17F8408450186431000C8F7A271302AD

Zeiten
ändern sich...



Ich möchte zum Abschluss noch einmal die kleine Geschichte vom Anfang erzählen, aber an die heutige Zeit angepasst.



Stefan ist nun kein ahnungsloser Internet- und PC-Benutzer mehr, denn er hat einiges über Sicherheit gelernt.



Anstatt die Links in seinen Mails direkt anzuklicken, lädt er die Seite manuell im Browser und schaut nach dem Rechten.



Angreifer auf sein WLAN können ihm nichts mehr anhaben...



...denn er hat seinen Router mit WPA2 und einem sicheren Kennwort abgesichert.



Und selbst wenn er sich auf zwielichtigen Seiten rumtreibt, warnt ihn sein Virens Scanner rechtzeitig vor Schadsoftware.



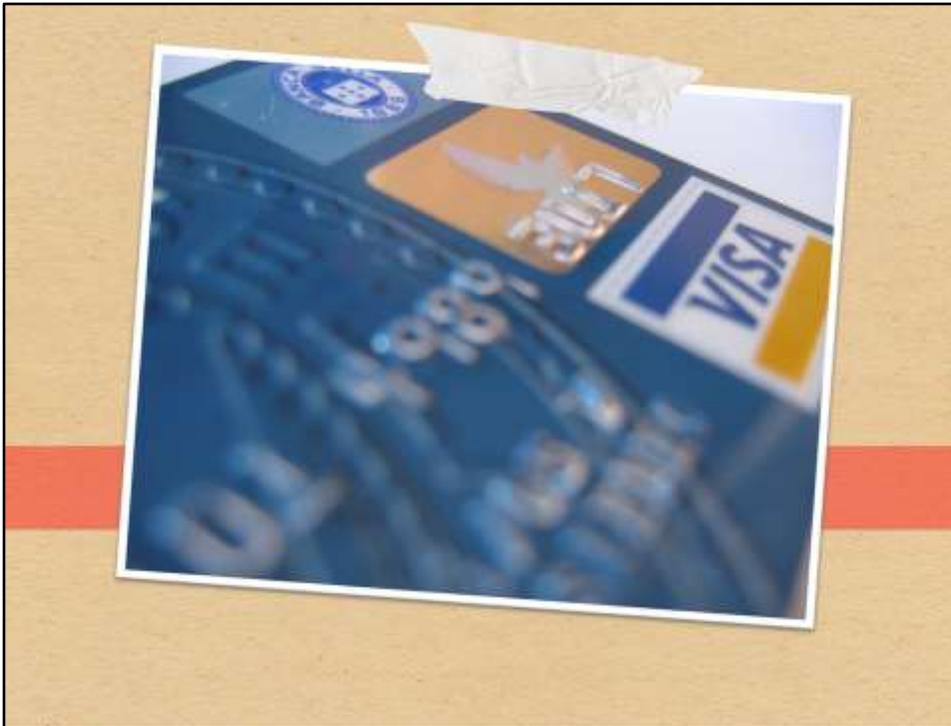
Stefan hat alle Daten auf externen Medien und seinen tragbaren Geräten mit TrueCrypt verschlüsselt, sodass Diebe nichts mit ihnen anfangen können.



Wenn Stefan im Internetcafé oder sonstigen öffentlichen Netzwerken unterwegs ist...



...achtet er darauf, nur verschlüsselte Verbindungen zu benutzen.



Egal ob Online-Bezahlvorgänge...



...oder der Webmail-Zugang, immer achtet Stefan auf die blaue/grüne Adresszeile.



Seinen Anwalt muss Stefan jetzt nur noch selten anrufen.



Anstatt seltsamer Rechnungen...



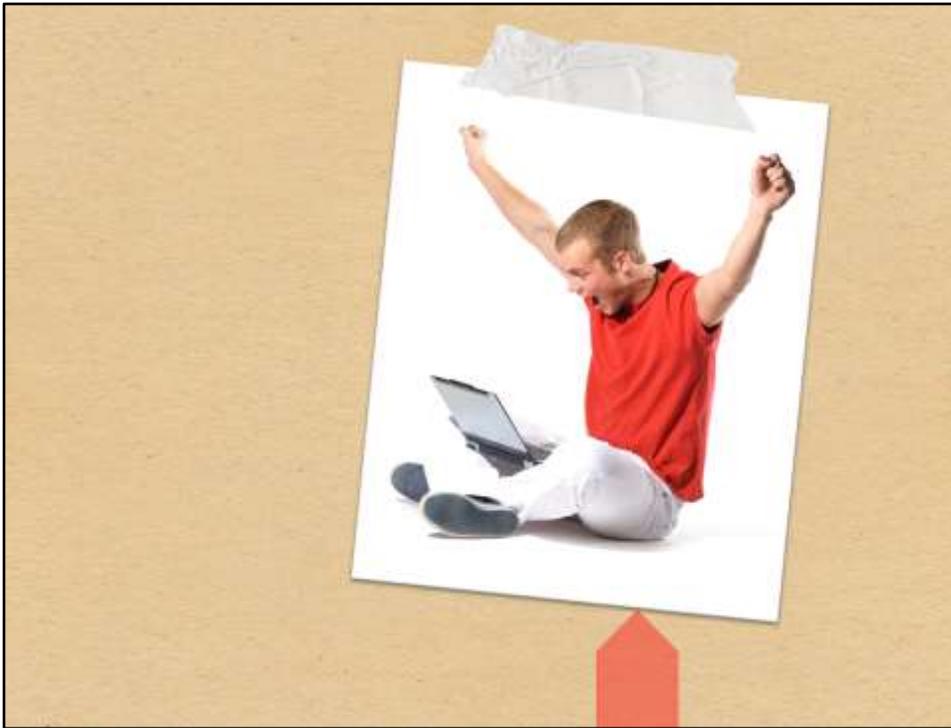
...bekommt Stefan jetzt nur noch Postkarten von Freunden, denen er Tipps zum Thema Sicherheit im Internet gegeben hat.



Und wenn die GMX-Meldung kommt, hat er sich tatsächlich vertippt.



Und Stefans Urlaubsfotos bleiben nun auch privat.



Stefan ist rundum zufrieden und lebt fröhlich und sicher bis an sein Lebensende.

Fazit





Die Tipps sind zwar einfach, aber bedeuten auch Einschränkungen: Hier ein Klick, dort ein Schritt mehr...



Sicherheit ist ein ganzheitliches Konzept. Einzelne Maßnahmen reichen nicht aus.



Mit den paar einfachen Tipps kann sich nun jeder sicher im Internet bewegen! ;-)





David Ritter

www.sxc.hu/photo/603585



Andrzej Pobiedzinski

www.sxc.hu/photo/1318896



Glen Jeffreys

www.sxc.hu/photo/228778



Thad Zajdowicz

www.sxc.hu/photo/623446



Ante Vekic

www.sxc.hu/photo/1237883



Alex Fiore

www.sxc.hu/photo/197626



s_falkow

www.flickr.com/photos/safari_vacation/6257284524



Sarah Gilbert

www.flickr.com/photos/cafemama/718939603/



c.alberto

www.flickr.com/photos/cacobeto/3212630910/



Simon Cataudo

www.sxc.hu/photo/116120



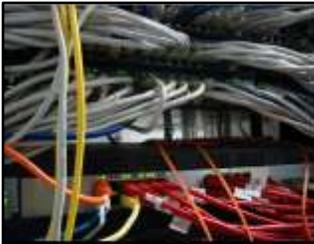
Philippe Ramakers

www.sxc.hu/photo/250528



Shawn McCullough

www.flickr.com/photos/shawnmichael/4302375313/



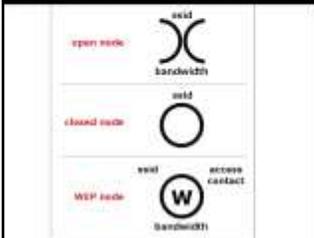
Gary Scott

www.sxc.hu/photo/746494



Maha

www.flickr.com/photos/maha-online/62811764/



Isaac Mao

<http://www.flickr.com/photos/isaacmao/191604830/>



Sebastiaan ter Burg

www.flickr.com/photos/ter-burg/5520210028/



Alchemist

de.wikipedia.org/wiki/Datei:Hard_disk_head_crash.jpg



Antonio Jimenez Alonso

www.sxc.hu/photo/779951



Metro Centric

www.flickr.com/photos/16782093@N03/3642988815/



Guglielmo Losio

www.sxc.hu/photo/1356926



Johanna Friedman

www.sxc.hu/photo/403571/



Sicherheit

im Internet und auf dem Heim-PC