Aktuelle Bedrohungen

DESY

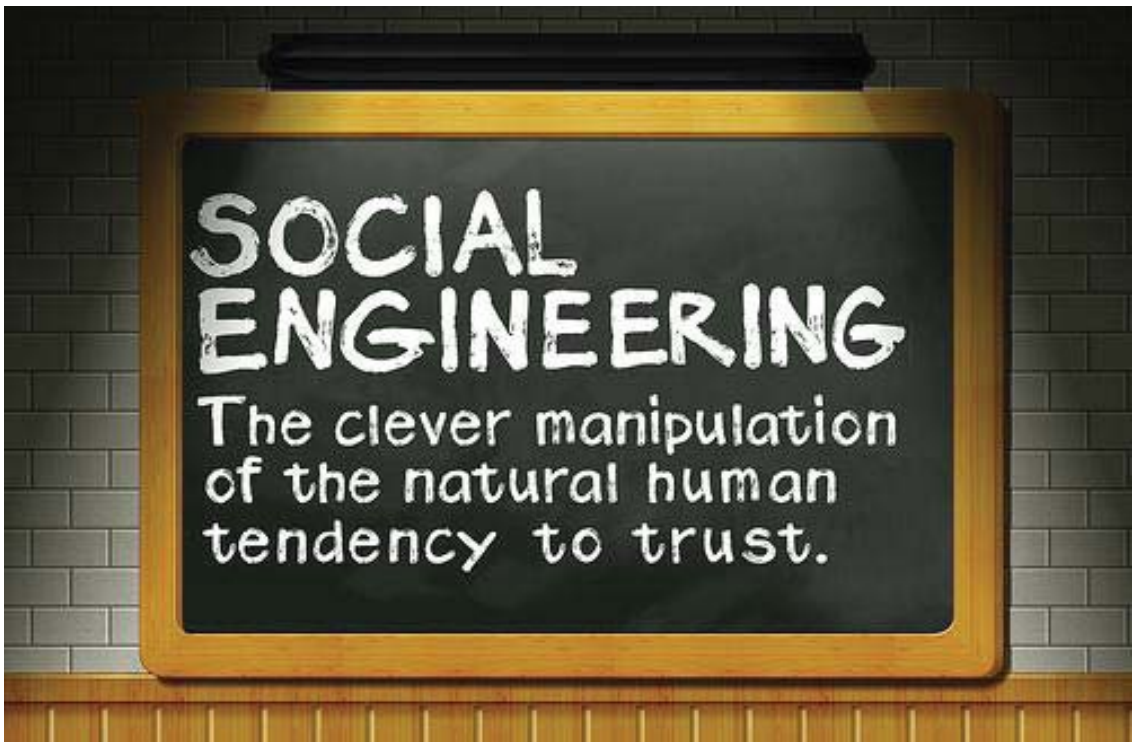
Montag, 28. Mai 2012

Agenda

- Social Media Social Engineering
- Cloud Computing
- Smart Phone Nutzung
- Hacker und Cracker
- Tipps

Social Engineering

SOCIAL MEDIA



www.social-engineer.org

Soziale Netzwerke

Facebook, Google+ und Co.

- Datenschutzeinstellungen
- Statusmitteilungen
- Profil
- Freunde / Kontakte
- www.reclaimprivacy.org

Collaboration

CLOUD COMPUTING

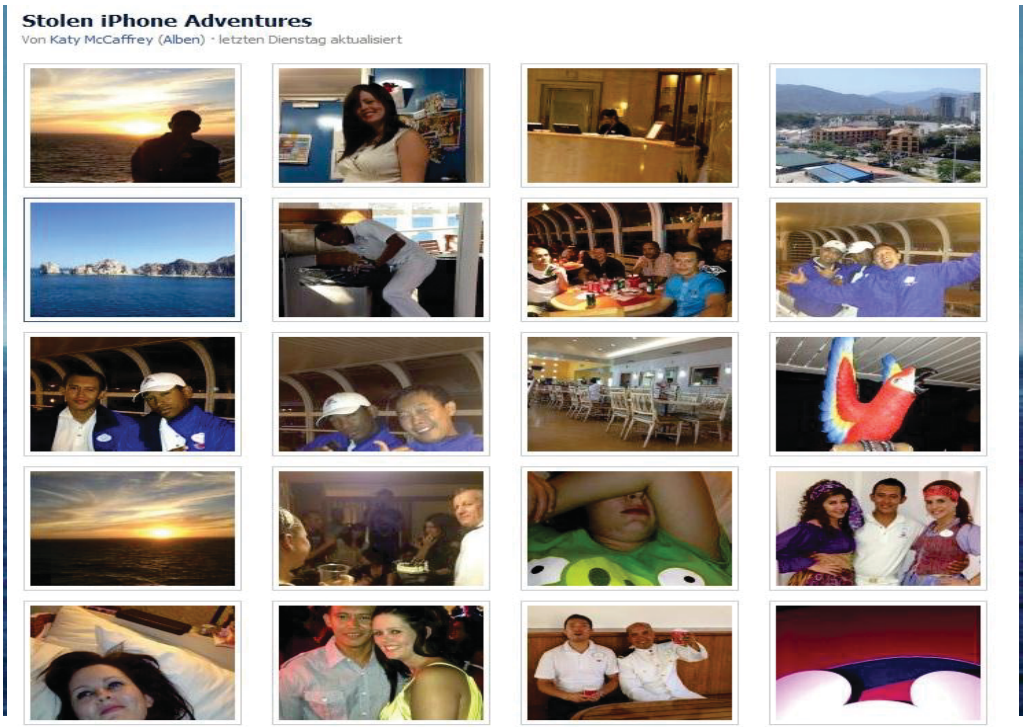
Cloud Computing

Dropbox, TeamDrive, SkyDrive und Co.

- Verschlüsselung vor dem Hochladen
- Öffentlich oder nicht???

SMARTPHONES

Katy und Disney



Smartphone und Cloud Computing

Doppeltes Risiko???

Bring Your Own Device

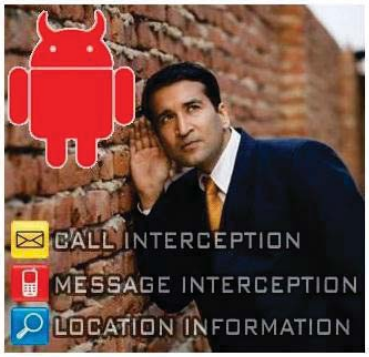
Android

Ist Android das neue Windows?

AUG 2

Neuer Android Virus nimmt offenbar Telefongespräche auf

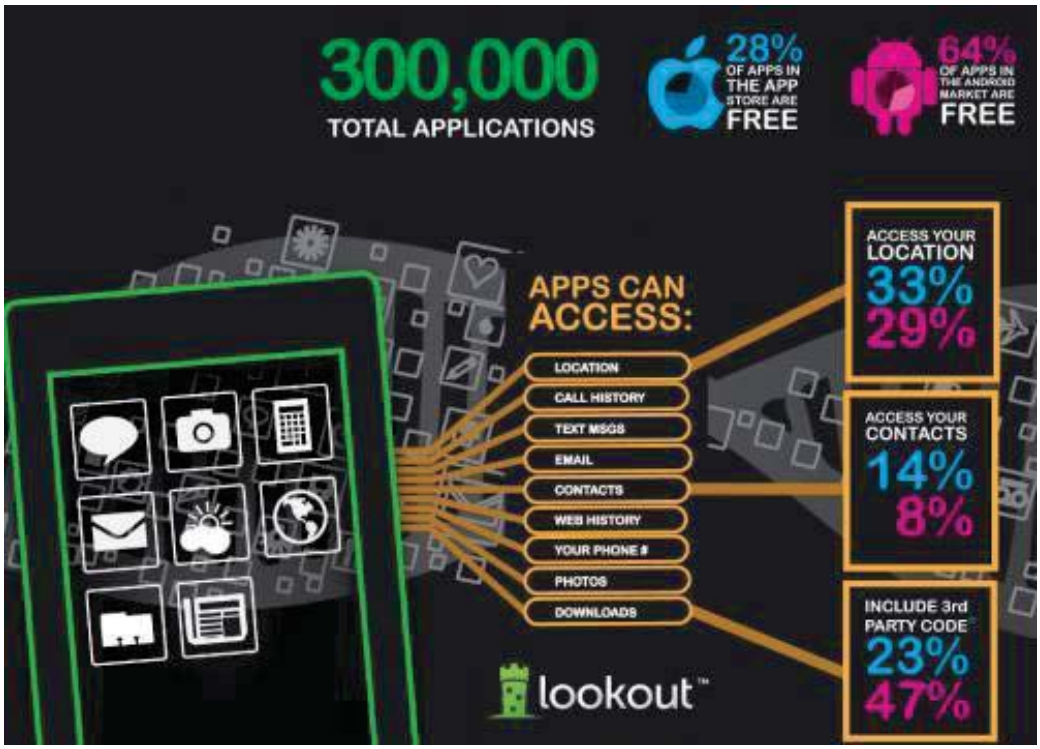
von Fabien Roehlinger am 02.08.2011 17:24:49 — 5.746 mal gelesen



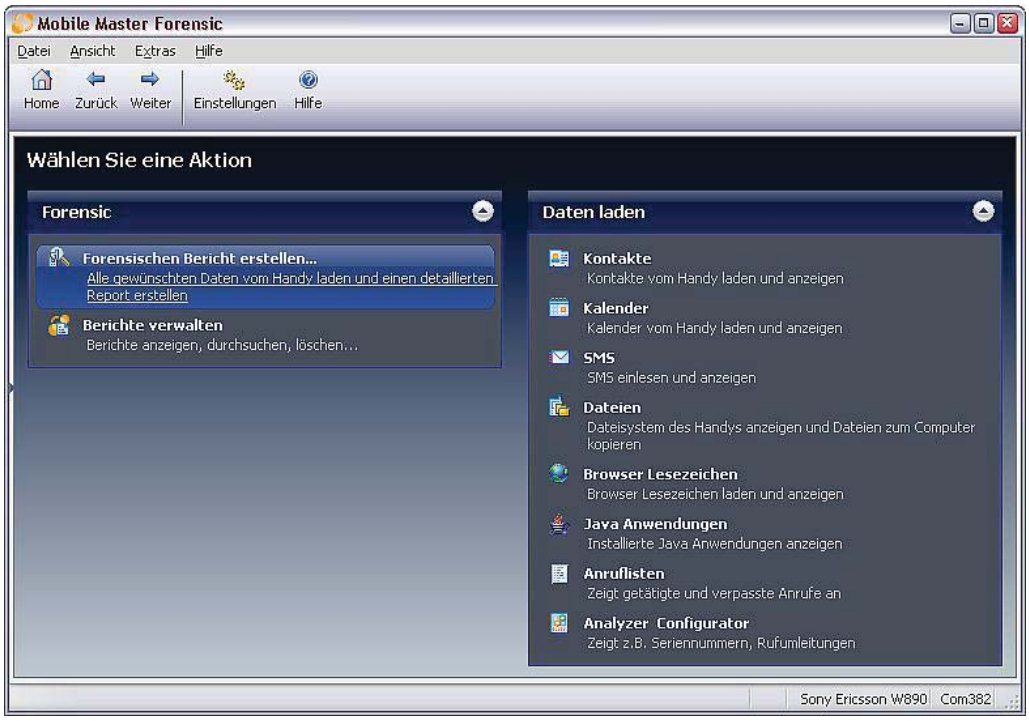
Noch ist August - und damit Sommer. Allerdings regnet es in diesem Jahr besonders häufig. Kein Wunder also, dass man sich sehr viel leichter einen Virus einfängt. Aber warum "erkälten" sich gerade Android Phones so einfach? Denn nach dem als "Angry Birds" getarnten Virus vor einigen Wochen, gibt es jetzt wieder einen neuen Schädling, der nicht nur den Datenschützern Schweiss auf die Stirn treiben dürfte.

Forscher von CA Technologies sind einem Android Virus auf die Schliche gekommen, der die Telefonunterhaltungen seines Wirtes abhört und an einen Server schickt. Der Virus war allerdings nicht von echten Genies geschrieben, so dass es für die Forscher gar nicht so schwer war den Virus zu identifizieren. Alle Telefongespräche wurden nämlich auf der SD-Karte des befallenen Android Phones abgespeichert.

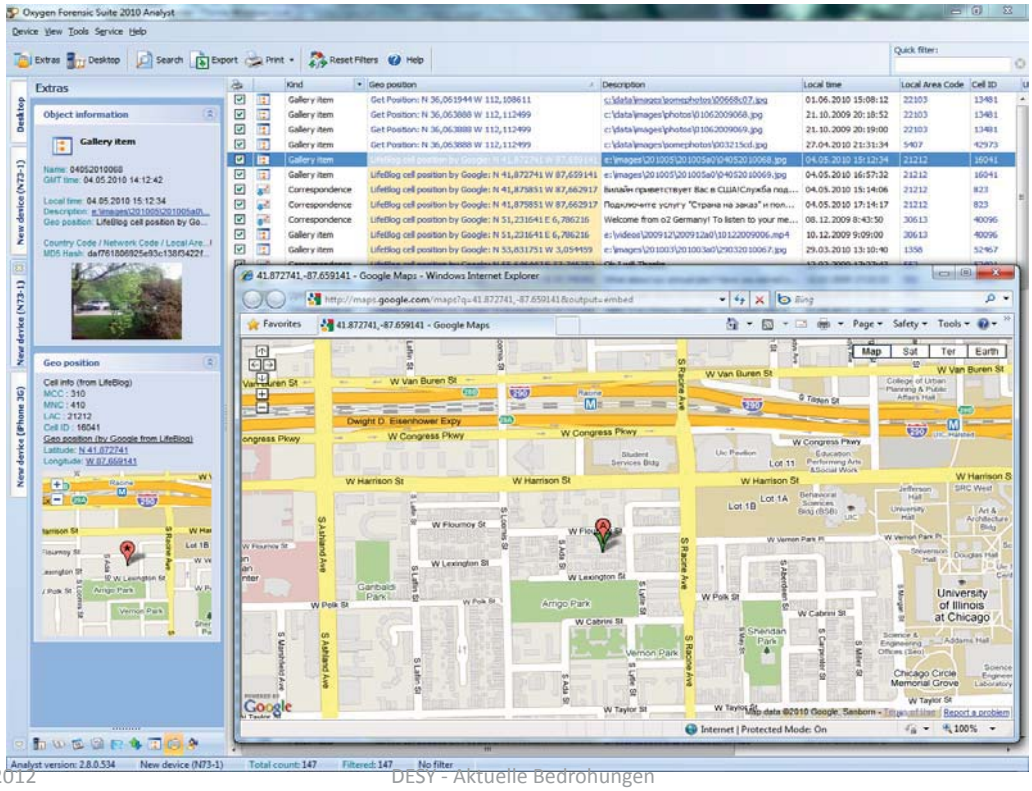
iOS vs Android



Mobile Master Forensic



Oxygene Forensic Suite



HACKER UND CRACKER

Monthly Malware Statistics: April 2012

April in figures

The following statistics were compiled in April using data collected from computers running Kaspersky Lab products:

- 280 million malicious programs were detected and neutralized;
- 134 million (48% of all threats) web-borne infections were prevented;
- More than 24 million malicious URLs were detected.

Kaspersky,

http://www.securelist.com/en/analysis/204792228/Monthly_Malware_Statistics_April_2012

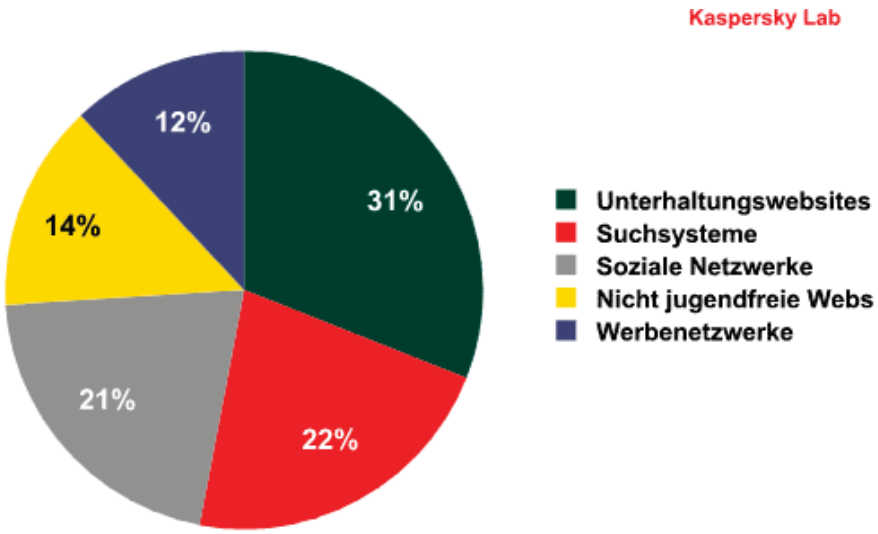
Hacker und Cracker

- Phishing
- Spear Phishing
- Super-targeted Malware
- Scareware
- Ransomware

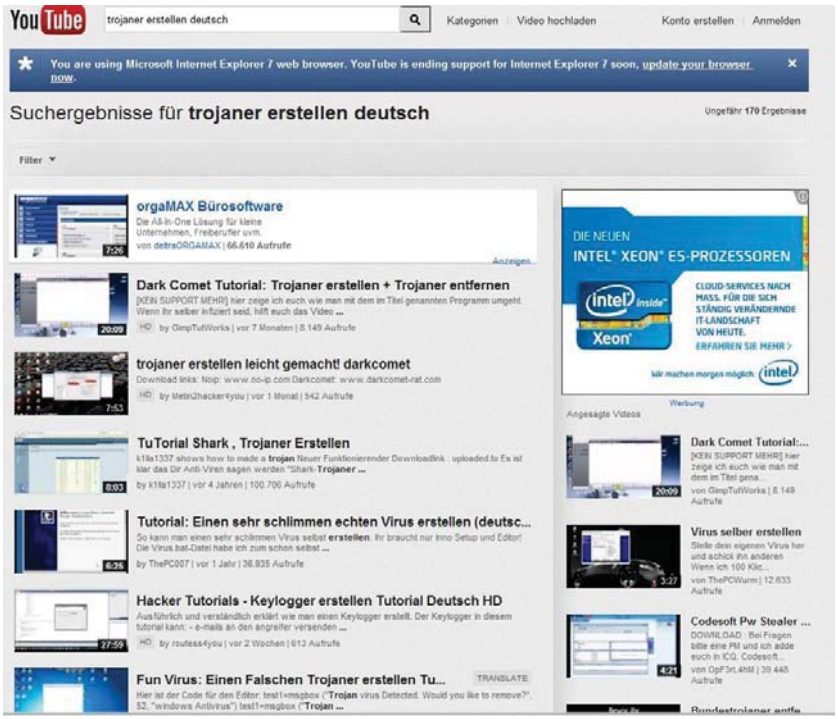
Gary McKinnon

…wie andere Jungs mit der elektrischen Eisenbahn spielen.

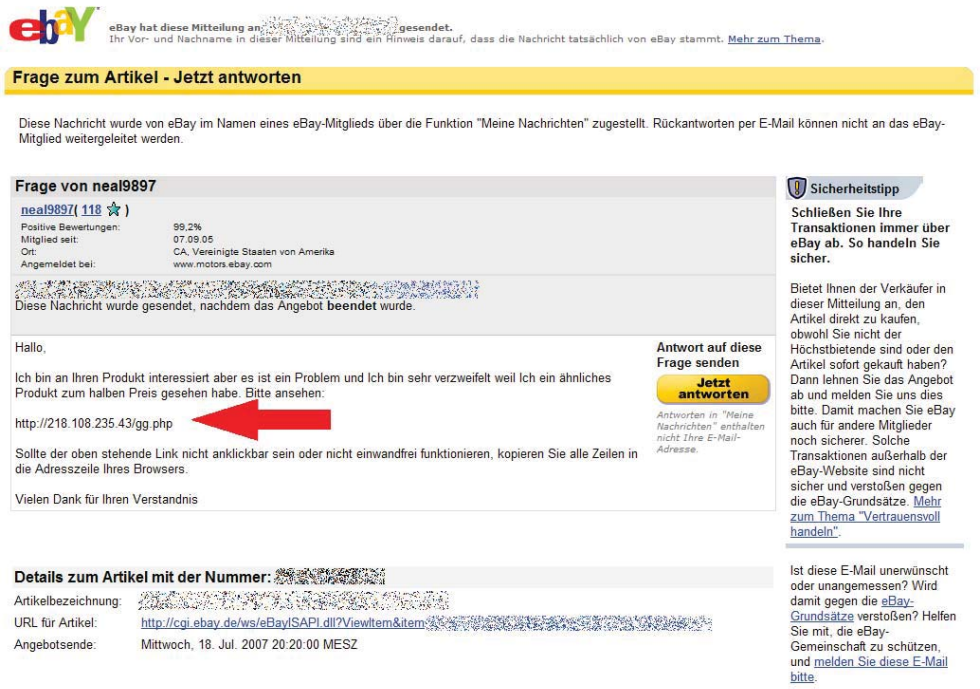
Wo schädliche Links platziert sind



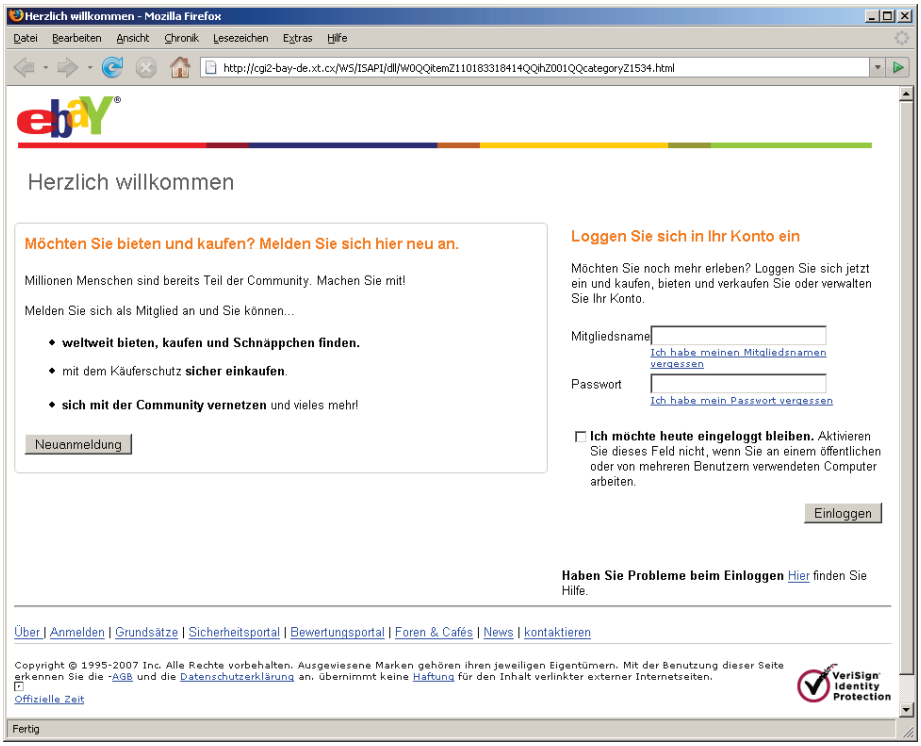
Das Problem:



Phishing Mail

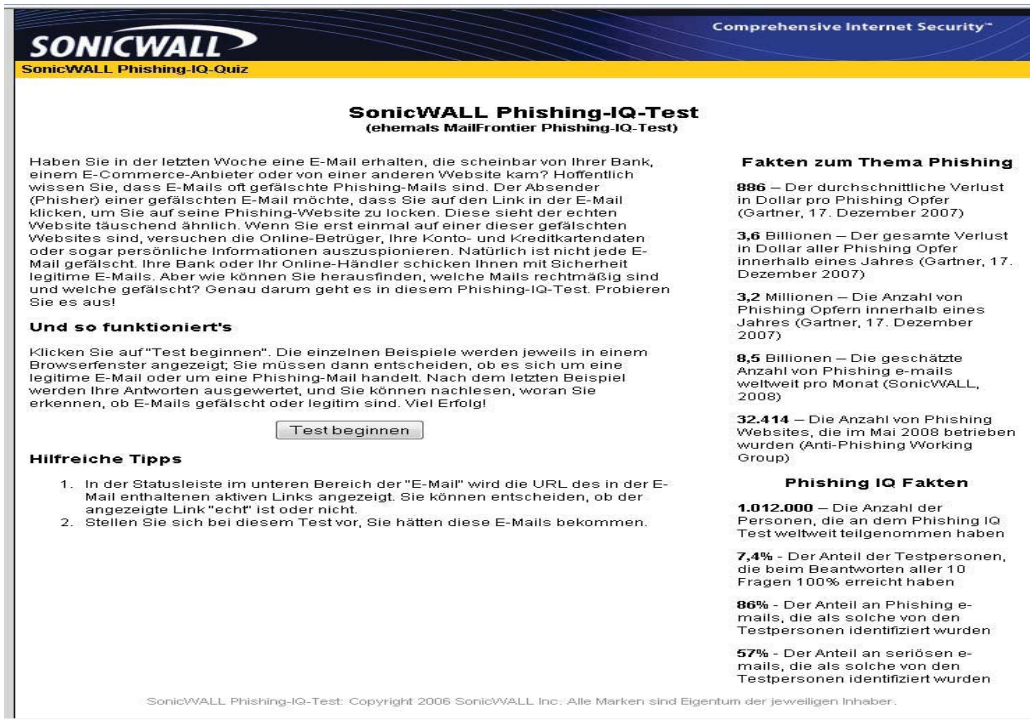


„Ebay-Site“



Phishing Website

http://www.sonicwall.com/phishing_de/



SONICWALL
Comprehensive Internet Security™
SonicWALL Phishing-IQ-Quiz

SonicWALL Phishing-IQ-Test
(ehemals MailFrontier Phishing-IQ-Test)

Haben Sie in der letzten Woche eine E-Mail erhalten, die scheinbar von Ihrer Bank, einem E-Commerce-Anbieter oder von einer anderen Website kam? Hoffentlich wissen Sie, dass E-Mails oft gefälschte Phishing-Mails sind. Der Absender (Phisher) einer gefälschten E-Mail möchte, dass Sie auf den Link in der E-Mail klicken, um Sie auf seine Phishing-Website zu locken. Diese sieht der echten Website täuschend ähnlich. Wenn Sie erst einmal auf einer dieser gefälschten Websites sind, versuchen die Online-Betrüger, Ihre Konto- und Kreditkartendaten oder sogar persönliche Informationen auszuspionieren. Natürlich ist nicht jede E-Mail gefälscht. Ihre Bank oder Ihr Online-Händler schicken Ihnen mit Sicherheit legitime E-Mails. Aber wie können Sie herausfinden, welche Mails rechtmäßig sind und welche gefälscht? Genau darum geht es in diesem Phishing-IQ-Test. Probieren Sie es aus!

Und so funktioniert's

Klicken Sie auf "Test beginnen". Die einzelnen Beispiele werden jeweils in einem Browserfenster angezeigt; Sie müssen dann entscheiden, ob es sich um eine legitime E-Mail oder um eine Phishing-Mail handelt. Nach dem letzten Beispiel werden Ihre Antworten ausgewertet, und Sie können nachlesen, woran Sie erkennen, ob E-Mails gefälscht oder legitim sind. Viel Erfolg!

Test beginnen

Hilfreiche Tipps

1. In der Statusleiste im unteren Bereich der "E-Mail" wird die URL des in der E-Mail enthaltenen aktiven Links angezeigt. Sie können entscheiden, ob der angezeigte Link "echt" ist oder nicht.
2. Stellen Sie sich bei diesem Test vor, Sie hätten diese E-Mails bekommen.

Fakten zum Thema Phishing

886 – Der durchschnittliche Verlust in Dollar pro Phishing Opfer (Gartner, 17. Dezember 2007)

3,6 Billionen – Der gesamte Verlust in Dollar aller Phishing Opfer innerhalb eines Jahres (Gartner, 17. Dezember 2007)

3,2 Millionen – Die Anzahl von Phishing Opfern innerhalb eines Jahres (Gartner, 17. Dezember 2007)

8,5 Billionen – Die geschätzte Anzahl von Phishing e-mails weltweit pro Monat (SonicWALL, 2008)

32.414 – Die Anzahl von Phishing Websites, die im Mai 2008 betrieben wurden (Anti-Phishing Working Group)

Phishing IQ Fakten

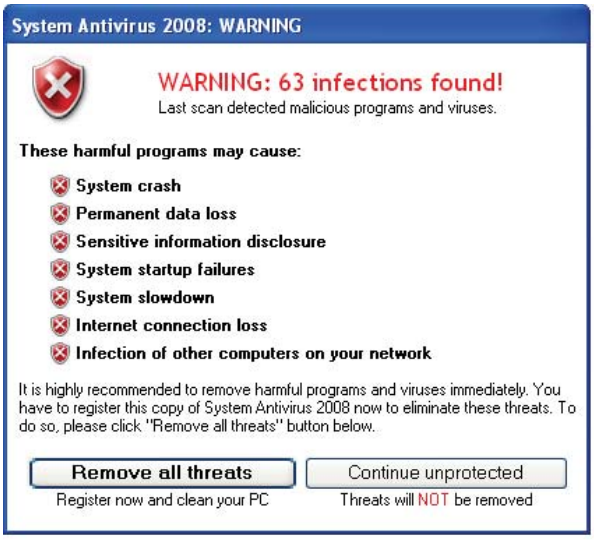
1.012.000 – Die Anzahl der Personen, die an dem Phishing IQ Test weltweit teilgenommen haben

7,4% - Der Anteil der Testpersonen, die beim Beantworten aller 10 Fragen 100% erreicht haben

86% - Der Anteil an Phishing e-mails, die als solche von den Testpersonen identifiziert wurden

57% - Der Anteil an seriösen e-mails, die als solche von den Testpersonen identifiziert wurden

Scareware



System Antivirus 2008: WARNING

WARNING: 63 infections found!
Last scan detected malicious programs and viruses.

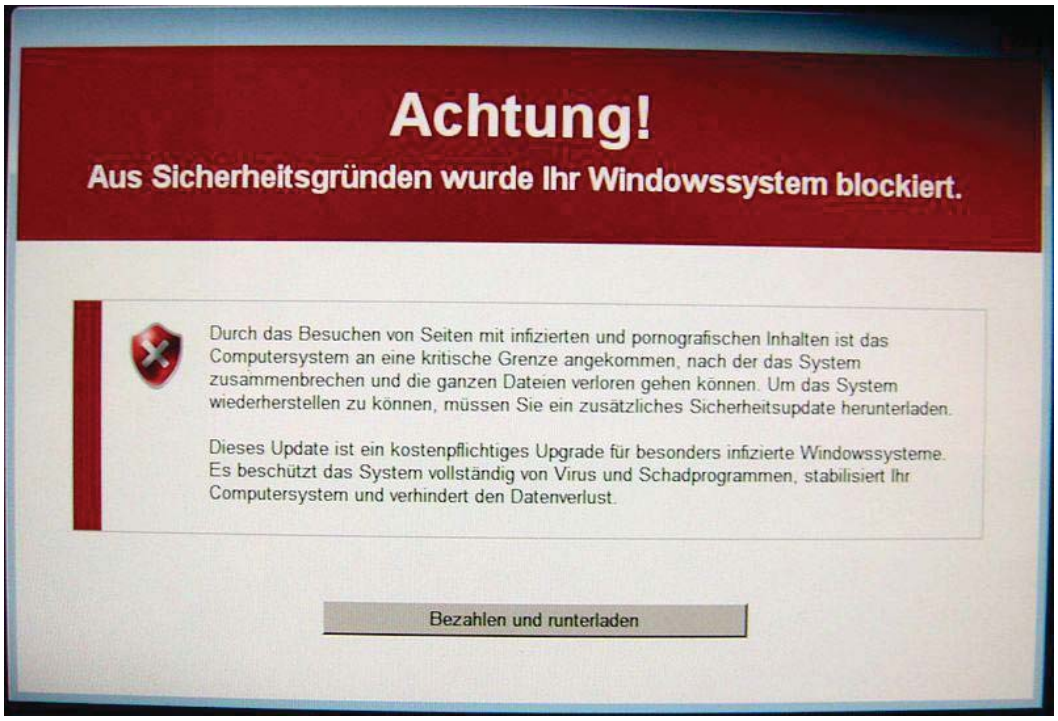
These harmful programs may cause:

- System crash
- Permanent data loss
- Sensitive information disclosure
- System startup failures
- System slowdown
- Internet connection loss
- Infection of other computers on your network

It is highly recommended to remove harmful programs and viruses immediately. You have to register this copy of System Antivirus 2008 now to eliminate these threats. To do so, please click "Remove all threats" button below.

Remove all threats — Register now and clean your PC
Continue unprotected — Threats will NOT be removed

Ransomware


Achtung!
Aus Sicherheitsgründen wurde Ihr Windowssystem blockiert.
Durch das Besuchen von Seiten mit infizierten und pornografischen Inhalten ist das Computersystem an eine kritische Grenze angekommen, nach der das System zusammenbrechen und die ganzen Dateien verloren gehen können. Um das System wiederherstellen zu können, müssen Sie ein zusätzliches Sicherheitsupdate herunterladen.
Dieses Update ist ein kostenpflichtiges Upgrade für besonders infizierte Windowssysteme. Es beschützt das System vollständig von Virus und Schadprogrammen, stabilisiert Ihr Computersystem und verhindert den Datenverlust.
Bezahlen und runterladen


Wählen Sie Ihre bevorzugte Zahla
(Paypal-Logo)
Nicht möglich da PC stark virenverseucht!
(Sofortüberweisung-Logo)
Nicht möglich da PC stark virenverseucht!
(Visa-/Mastercard-/AmEx-Logos)
Nicht möglich da PC stark virenverseucht!
(Paysafe-Logo)
Möglich!
(Ukash-Logo)
Möglich!
Damit Ihr Computersystem schnellstens verbessert wird, geben Sie bitte weiter unten einen Code für 50,-Euro Ukash oder Paysafe ein. Diese können Sie an fast jeder Tankstelle oder einen Kiosk in Ihrer Nähe kaufen. Diese Codes gibts auch überall da, wo Sie Handyaufladekarte erwerben können. Sofort nach der Eingabe und der Gültigkeitsprüfung wird Ihr Computer komplett aktualisiert und gesichert - alle Trojaner und Viren werden gelöscht.
Paysafe PIN-Code:
Zahlen

http://support.kaspersky.com/de/viruses/solutions?qid=208641247

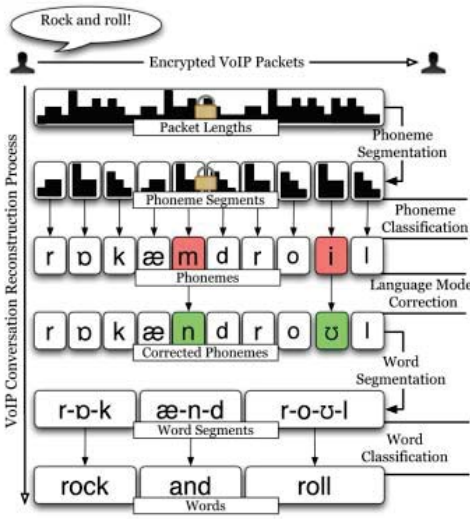
Allerdings:

Hallo zusammen,

ich habe auch seit dem 11.05.2012 mit der neuen Form des Trojaners zu kämpfen. Der Befall in einer kleinen Firma erfolgte am 09.05.2012 um 08.34 Uhr, wohl durch das Öffnen der gezippten “Abrechnung.exe”. Habe alle 6 bekannten Tools ausprobiert, habe noch die Originaldateien zur Schlüsselgenerierung vorliegen…. aber bislang hilft gar nichts in meinem Fall. Gibt es schon neue Erkenntnisse? Bislang hat ScareUncrypt bei mir die meiste Aussicht auf Erfolg versprochen…….

Skype

University of North Carolina

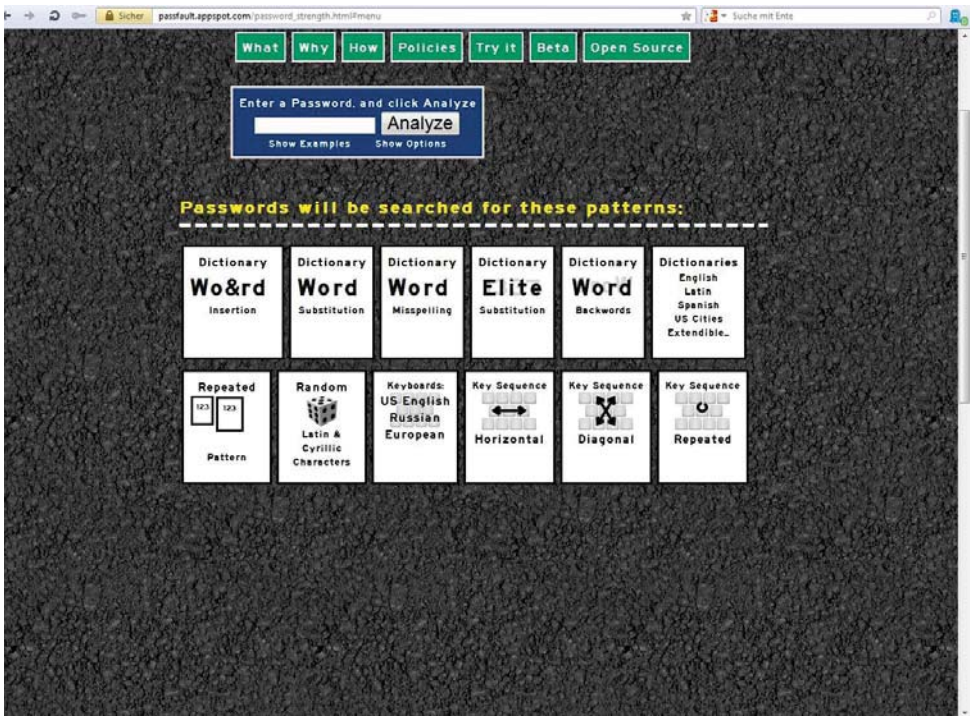


DARPA – Maschinelle Übersetzung

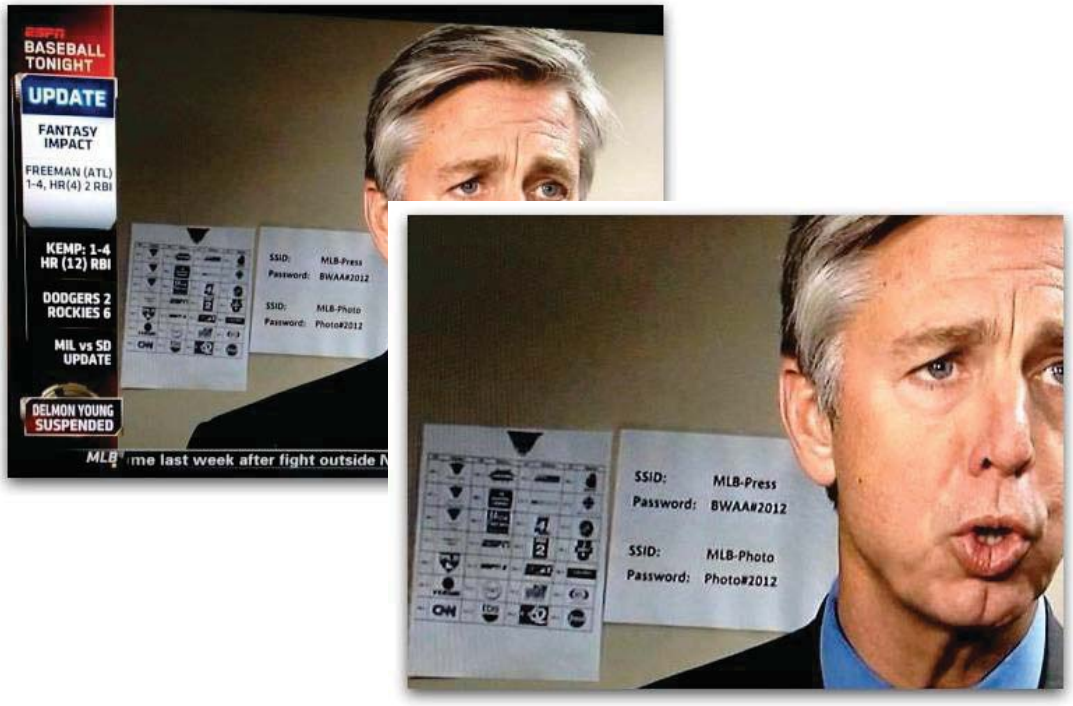
Tipps

- www.duckduckgo.com
- Browserauswahl
- E-Mail-Konten
- Do Not Track
- www.youhavedownloaded.com/
- www.reclaimprivacy.org
- Ghostery-Ad-On
- P@ssw0rt ist kein Passwort!
- https://shouldichangemypassword.com/
- https://passfault.appspot.com/password_strength.html#menu

Sicheres Passwort??

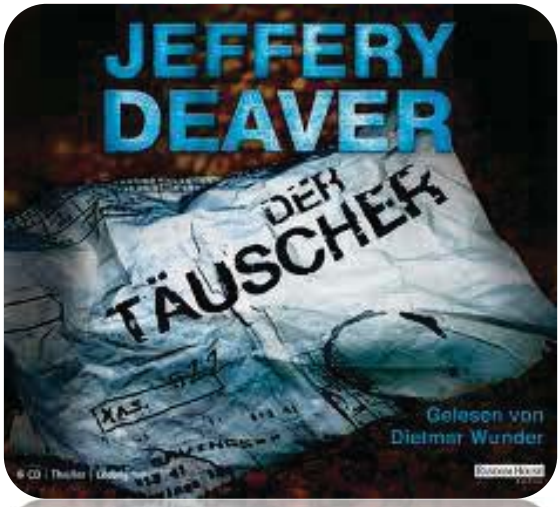


So nicht!



Der Tipp:

Buchtipp:



Fragen / Kontakt

Jens Olaf Krügermann
Datenschutz / Datensicherheit

kpp-group GmbH
Zimmerstr. 23 / 24
10969 Berlin

Fon: 030 – 206 7372-280
jens.kruegermann@kpp-group.de
www.kpp-group.de