

Aktuelle Bedrohungen

DESY

Montag, 28. Mai 2012

Agenda

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

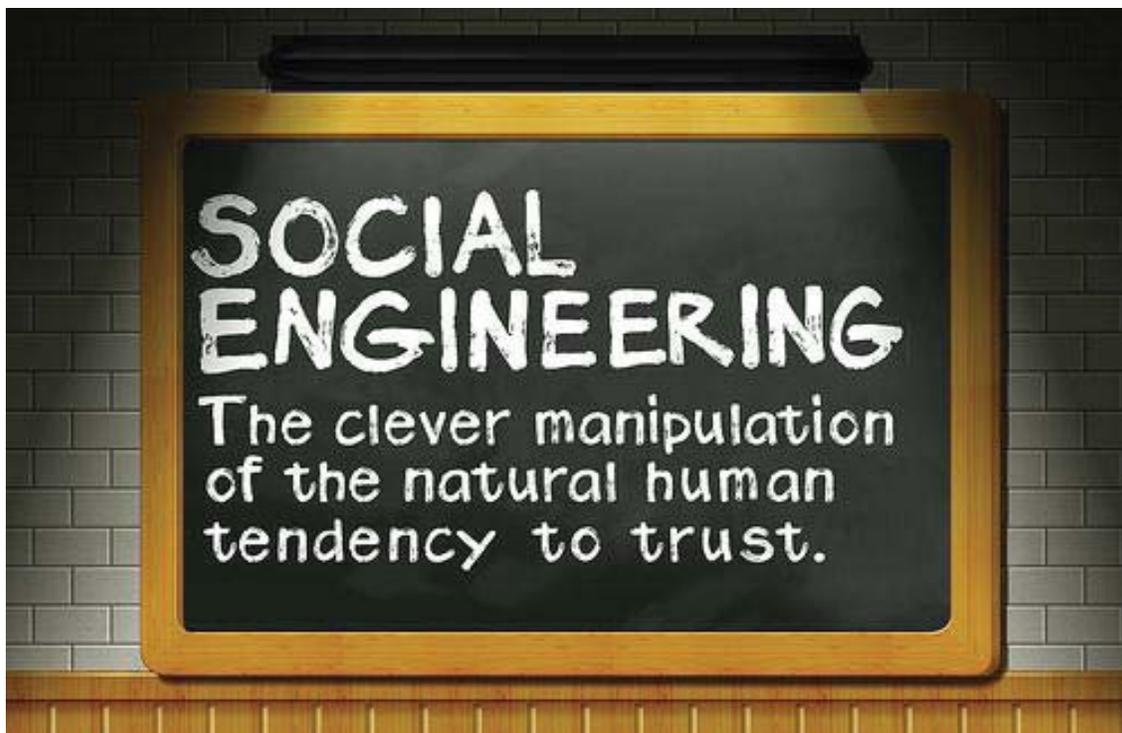
Social Engineering

SOCIAL MEDIA

28.05.2012

DESY - Aktuelle Bedrohungen

3



28.05.2012

DESY - Aktuelle Bedrohungen

4

Soziale Netzwerke



Facebook, Google+ und Co.

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



Collaboration

CLOUD COMPUTING

28.05.2012

DESY - Aktuelle Bedrohungen

9

Cloud Computing



28.05.2012

DESY - Aktuelle Bedrohungen

10

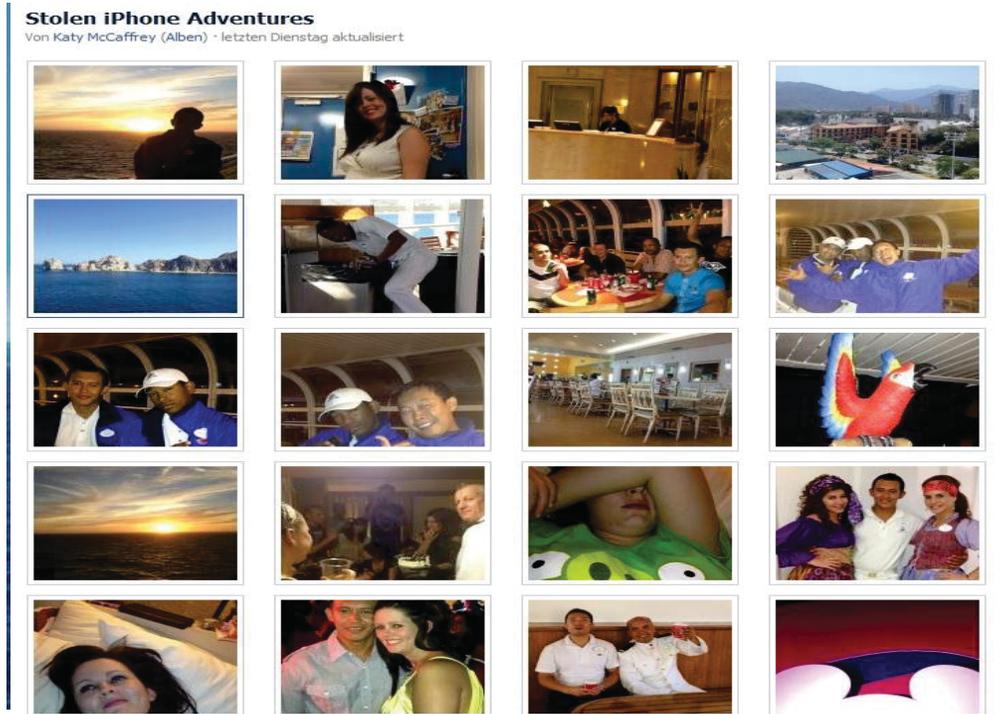
Dropbox, TeamDrive, SkyDrive und Co.

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



SMARTPHONES

Katy und Disney



28.05.2012

DESY - Aktuelle Bedrohungen

13

Smartphone und Cloud Computing

Doppeltes Risiko???

28.05.2012

DESY - Aktuelle Bedrohungen

14

Bring Your Own Device



28.05.2012

DESY - Aktuelle Bedrohungen

15

Android

Ist Android das neue Windows?

28.05.2012

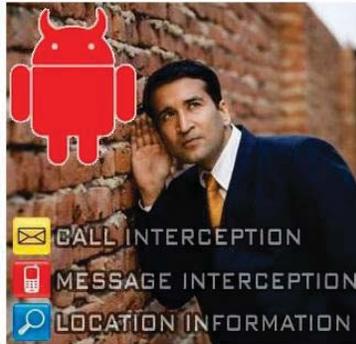
DESY - Aktuelle Bedrohungen

16

AUG
2

Neuer Android Virus nimmt offenbar Telefongespräche auf

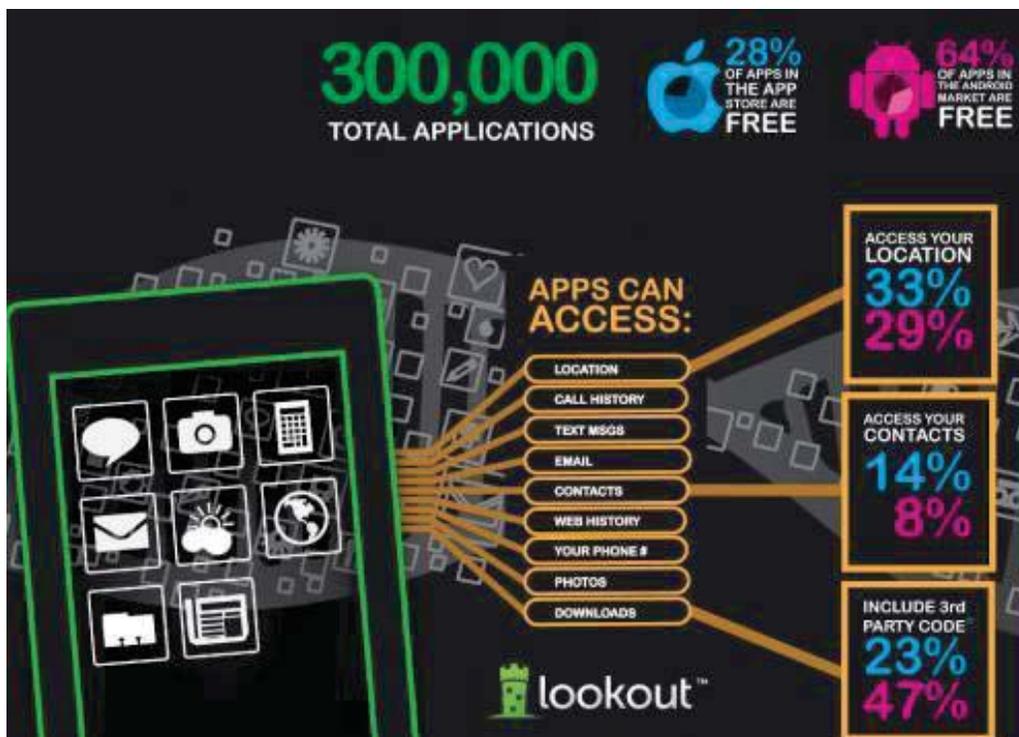
von Fabian Roehlinger am 02.08.2011 17:24:49 — 5.746 mal gelesen



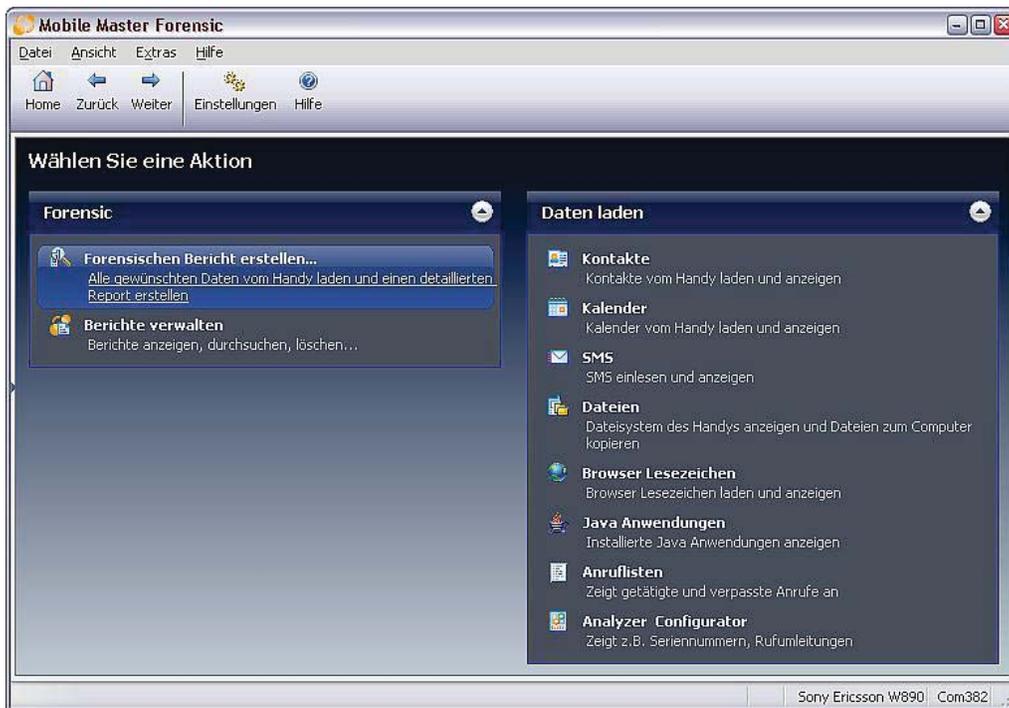
Noch ist August - und damit Sommer. Allerdings regnet es in diesem Jahr besonders häufig. Kein Wunder also, dass man sich sehr viel leichter einen Virus einfängt. Aber warum "erkälten" sich gerade Android Phones so einfach? Denn nach dem als "Angry Birds" getarnten Virus vor einigen Wochen, gibt es jetzt 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

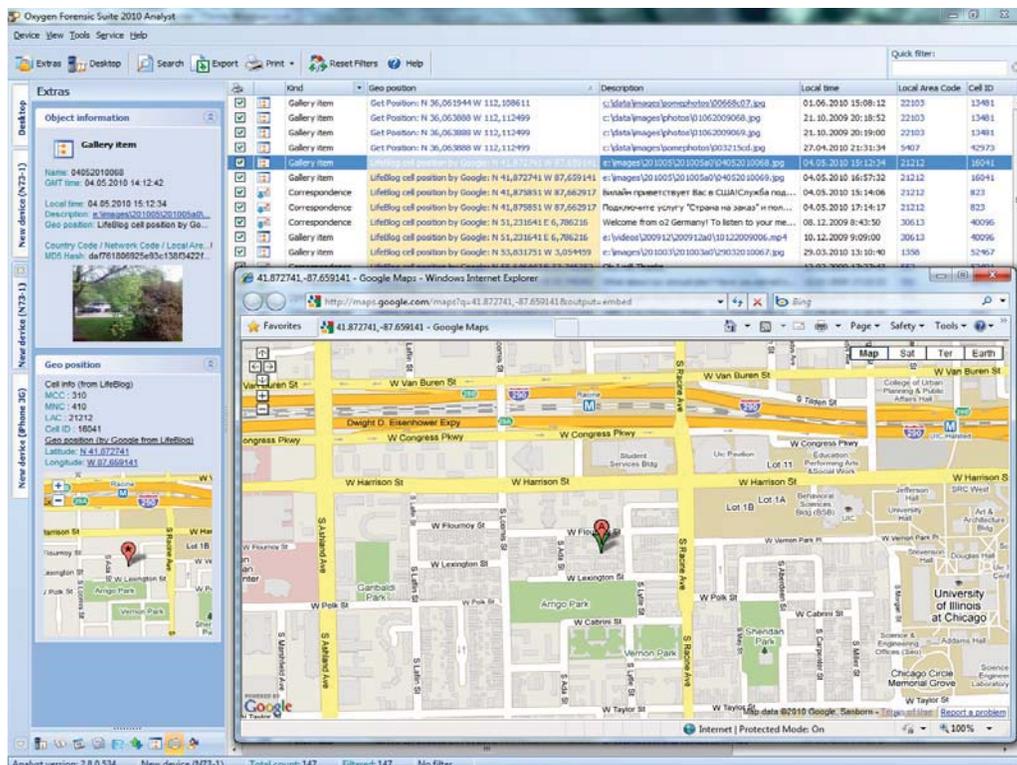


28.05.2012

DESY - Aktuelle Bedrohungen

19

Oxygene Forensic Suite



28.05.2012

DESY - Aktuelle Bedrohungen

20

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

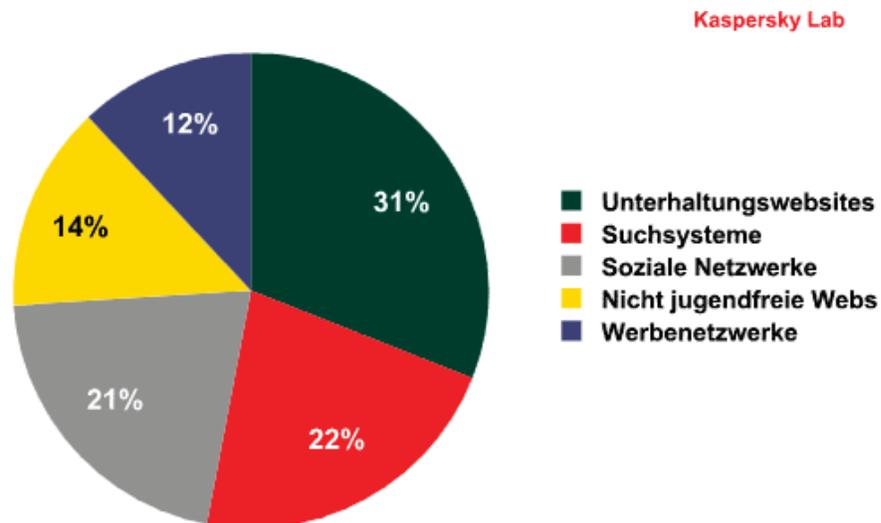
Gary McKinnon



...wie andere Jungs mit der elektrischen Eisenbahn spielen.



Wo schädliche Links platziert sind



Das Problem:

Suchergebnisse für **trojaner erstellen deutsch** (Ungefähr 179 Ergebnisse)

Filter

- orgaMAX Bürosoftware
- Dark Comet Tutorial: Trojaner erstellen + Trojaner entfernen
- trojaner erstellen leicht gemacht! darkcomet
- TuTorial Shark , Trojaner Erstellen
- Tutorial: Einen sehr schlimmen echten Virus erstellen (deutsch)
- Hacker Tutorials - Keylogger erstellen Tutorial Deutsch HD
- Fun Virus: Einen Falschen Trojaner erstellen Tu...

28.05.2012

DESY - Aktuelle Bedrohungen

27

Phishing Mail

eBay hat diese Mitteilung an gesendet.
Ihr Vor- und Nachname in dieser Mitteilung sind ein Hinweis darauf, dass die Nachricht tatsächlich von eBay stammt. [Mehr zum Thema](#).

Frage zum Artikel - Jetzt antworten

Diese Nachricht wurde von eBay im Namen eines eBay-Mitglieds über die Funktion "Meine Nachrichten" zugestellt. Rückantworten per E-Mail können nicht an das eBay-Mitglied weitergeleitet werden.

Frage von **neal9897**

neal9897 (118 ★)
Positive Bewertungen: 99,2%
Mitglied seit: 07.09.05
Ort: CA, Vereinigte Staaten von Amerika
Angemeldet bei: www.motors.ebay.com

Diese Nachricht wurde gesendet, nachdem das Angebot beendet wurde.

Hallo,

Ich bin an Ihren Produkt interessiert aber es ist ein Problem und Ich bin sehr verzweifelt weil ich ein ähnliches Produkt zum halben Preis gesehen habe. Bitte ansehen:

<http://218.108.235.43/gg.php>

Sollte der oben stehende Link nicht anklickbar sein oder nicht einwandfrei funktionieren, kopieren Sie alle Zeilen in die Adresszeile Ihres Browsers.

Vielen Dank für Ihren Verständnis

Antwort auf diese Frage senden

Jetzt antworten

Antworten in "Meine Nachrichten" enthalten nicht Ihre E-Mail-Adresse.

Sicherheitstipp

Schließen Sie Ihre Transaktionen immer über eBay ab. So handeln Sie sicher.

Bietet Ihnen der Verkäufer in dieser Mitteilung an, den Artikel direkt zu kaufen, obwohl Sie nicht der Höchstbietende sind oder den Artikel sofort gekauft haben? Dann lehnen Sie das Angebot ab und melden Sie uns dies bitte. Damit machen Sie eBay auch für andere Mitglieder noch sicherer. Solche Transaktionen außerhalb der eBay-Website sind nicht sicher und verstoßen gegen die eBay-Grundsätze. [Mehr zum Thema "Vertrauensvoll handeln"](#).

Details zum Artikel mit der Nummer:

Artikelbezeichnung:
URL für Artikel: <http://cgi.ebay.de/ws/EBaySAPIdi?viewitem&item>
Angebotsende: Mittwoch, 18. Jul. 2007 20:20:00 MESZ

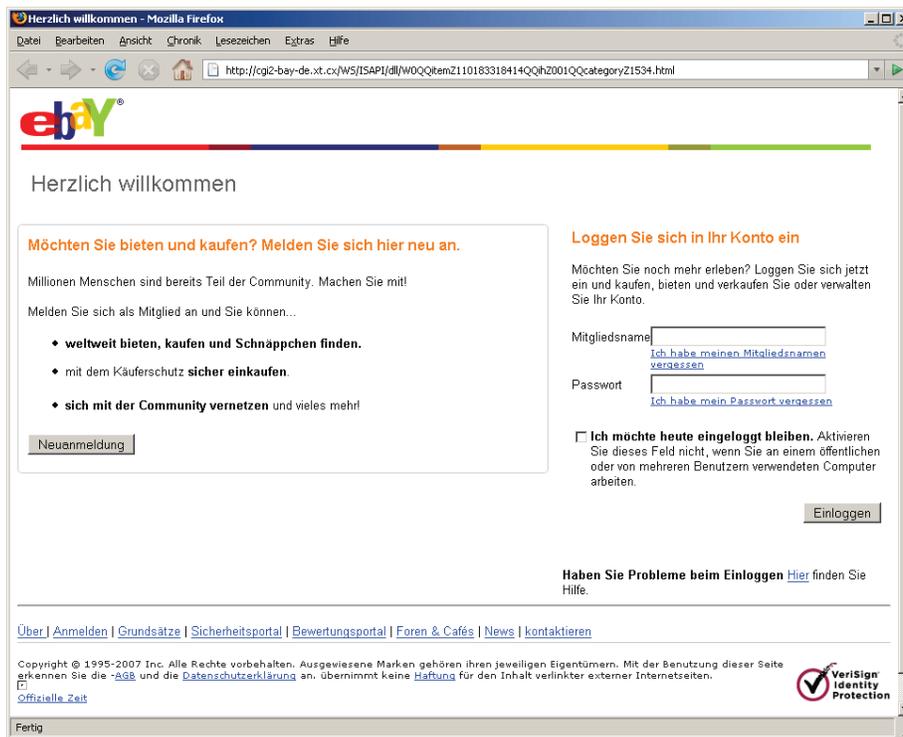
Ist diese E-Mail unerwünscht oder unangemessen? Wird damit gegen die [eBay-Grundsätze](#) verstoßen? Helfen Sie mit, die eBay-Gemeinschaft zu schützen, und [melden Sie diese E-Mail bitte](#).

28.05.2012

DESY - Aktuelle Bedrohungen

28

„Ebay-Site“

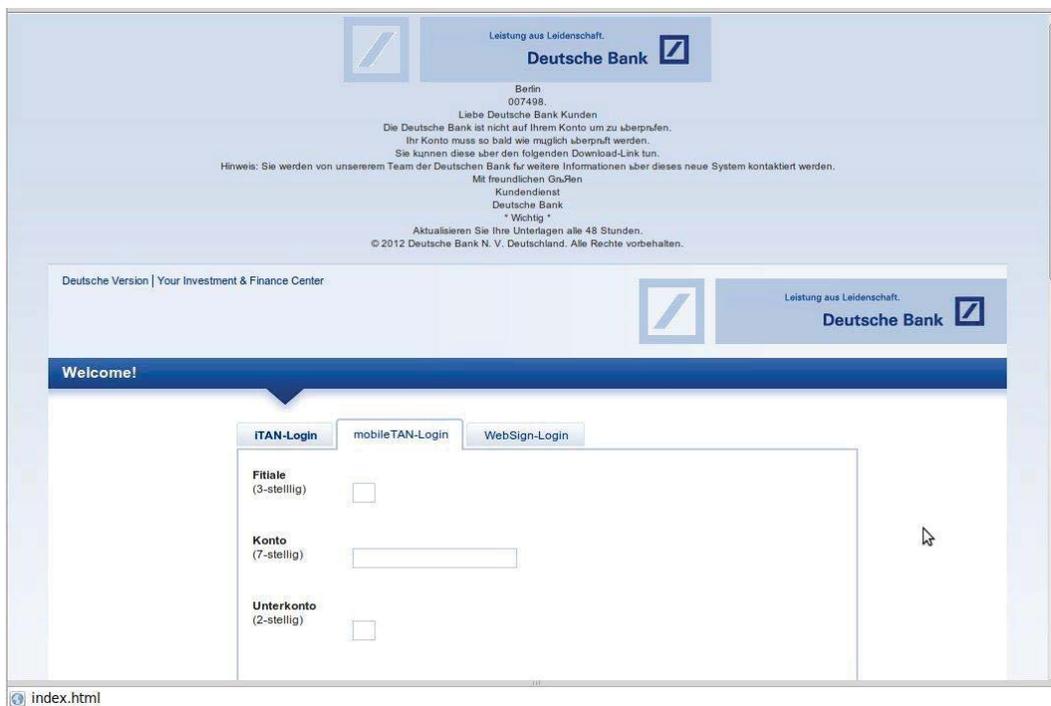


28.05.2012

DESY - Aktuelle Bedrohungen

29

Phishing Website



28.05.2012

DESY - Aktuelle Bedrohungen

30

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 auszuspäionieren. 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!

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

© SonicWALL Phishing-IQ-Test: Copyright 2006 SonicWALL Inc. Alle Marken sind Eigentum der jeweiligen Inhaber.

Scareware

System Antivirus 2008: WARNING

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

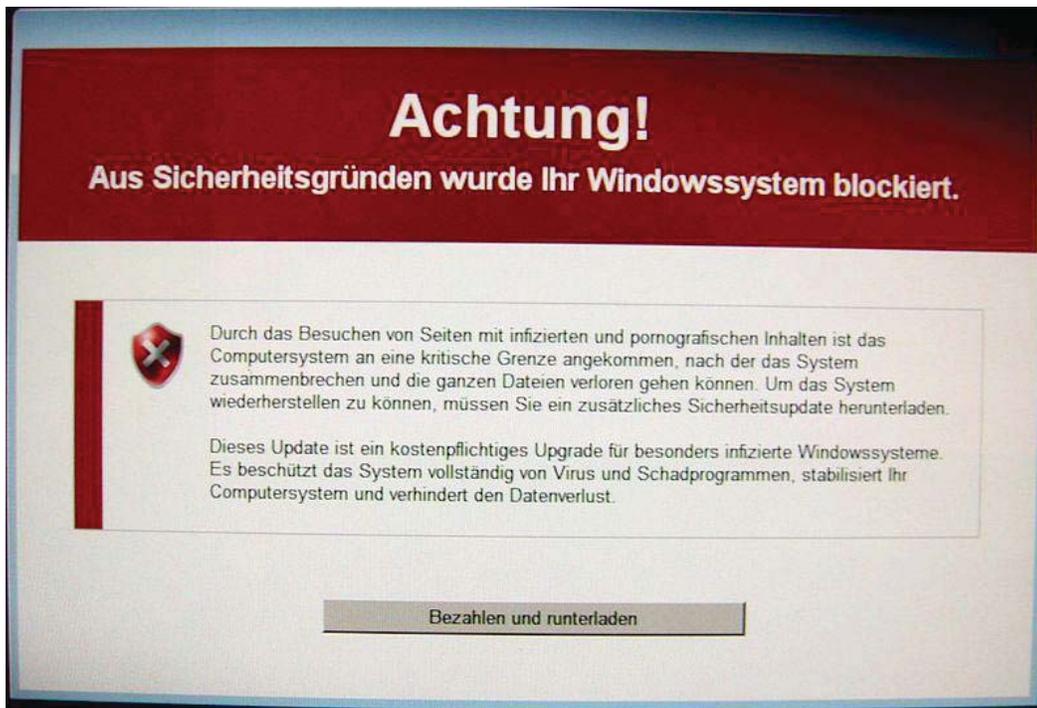
These harmful programs may cause:

- 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.

Register now and clean your PC Threats will **NOT** be removed

Ransomware



28.05.2012

DESY - Aktuelle Bedrohungen

33



28.05.2012

DESY - Aktuelle Bedrohungen

34

Kaspersky Labs
TECHNISCHER SUPPORT

Dieser Artikel auf:

Startseite / Bekämpfung von bösartigen Programmen / Viren und Lösungen

Suche: Artikel ID #: Suche

Tipps zur Suche

Kaspersky WindowsUnlocker - Anwendung für die Bekämpfung von Ransomware

Dieser Abschnitt enthält Informationen über die Methoden der Bekämpfung von bösartigen Programmen, die mithilfe von Produkten von **Kaspersky Lab** nicht neutralisiert werden können. Um ein solches Programm zu neutralisieren/löschen, müssen Sie das Systemverzeichnis modifizieren oder ein zusätzliches Tool benutzen. Haben Sie die erforderliche Information in diesem Abschnitt nicht gefunden, so senden Sie bitte eine Anfrage an den Technischen Support Service von **Kaspersky Lab** [über das Kontakt-Formular](#).

Kaspersky WindowsUnlocker - Anwendung für die Bekämpfung von Ransomware

Artikel ID: 6989 | Andere Sprachen: | 5 539 | 12.04.2012 12:21 | Druckversion

Wenn bei der Benutzung Ihres PCs Meldungen erscheinen, die Sie auffordern, eine SMS an eine bestimmte Telefonnummer zu senden, ist Ihr Computer sehr wahrscheinlich mit sogenannter Ransomware (Erpressungsprogramm) verseucht. Schädliche Software dieser Art zielt darauf ab, den Zugang zu Ihrem Computer oder auf bestimmte Funktionen zu verbieten und Lösegeld zu erpressen, um die Funktion des Computers wiederherzustellen.

Um Ransomware zu entfernen, haben die Spezialisten von **Kaspersky Lab** ein spezielles Hilfsprogramm namens **Kaspersky WindowsUnlocker** entwickelt. Dieses Programm kann ausgeführt werden, wenn Sie Ihren Computer von der **Kaspersky Notfall-CD 10** starten und funktioniert im grafischen sowie im Textmodus von **Kaspersky Notfall-CD**.

In diesem Artikel finden Sie eine detaillierte Beschreibung für die Benutzung von **Kaspersky WindowsUnlocker**:

1. [Funktionen von Kaspersky WindowsUnlocker](#)
2. [Wie startet man den Computer per CD mit Kaspersky WindowsUnlocker](#)
3. [Wie startet man Kaspersky WindowsUnlocker und desinfiziert den Computer](#)
4. [Computerüberprüfung mit der Kaspersky Rescue Disk](#)
5. [Berichte von Kaspersky WindowsUnlocker](#)

28.05.2012

DESY - Aktuelle Bedrohungen

35

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.....

28.05.2012

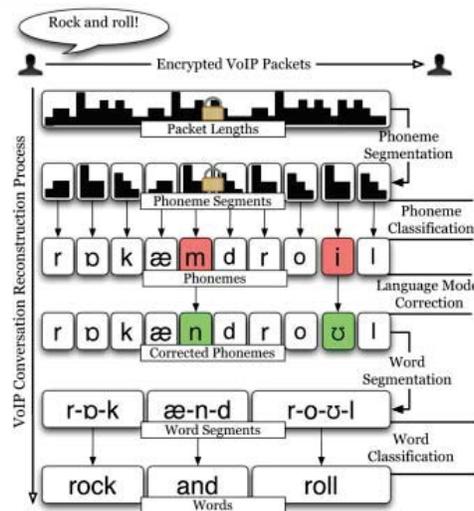
DESY - Aktuelle Bedrohungen

36

Skype



University of North Carolina

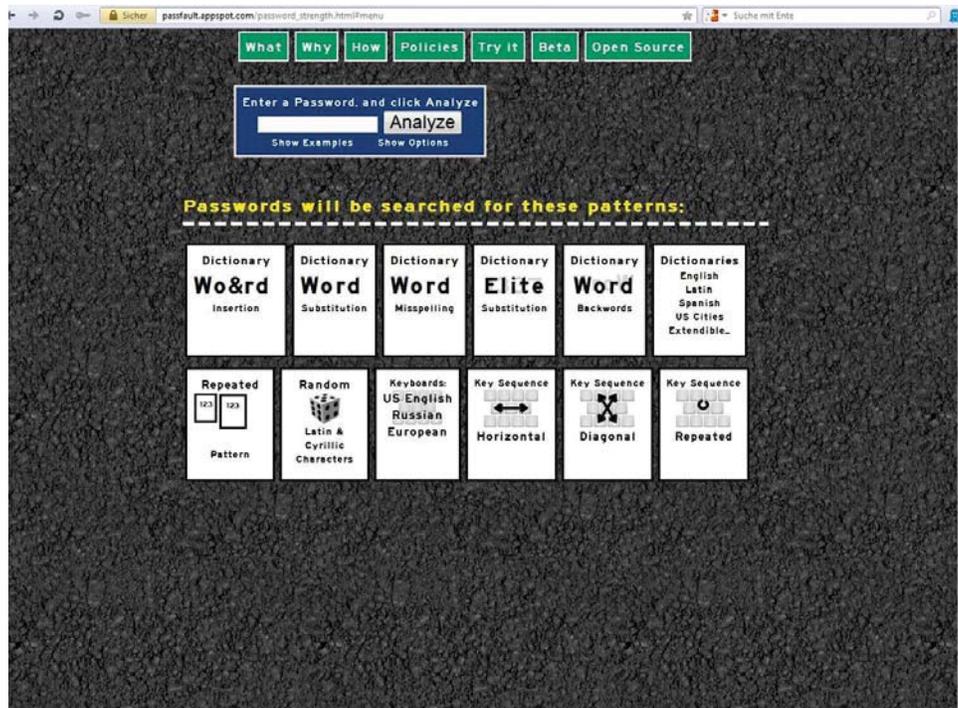




Tipps

- 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??

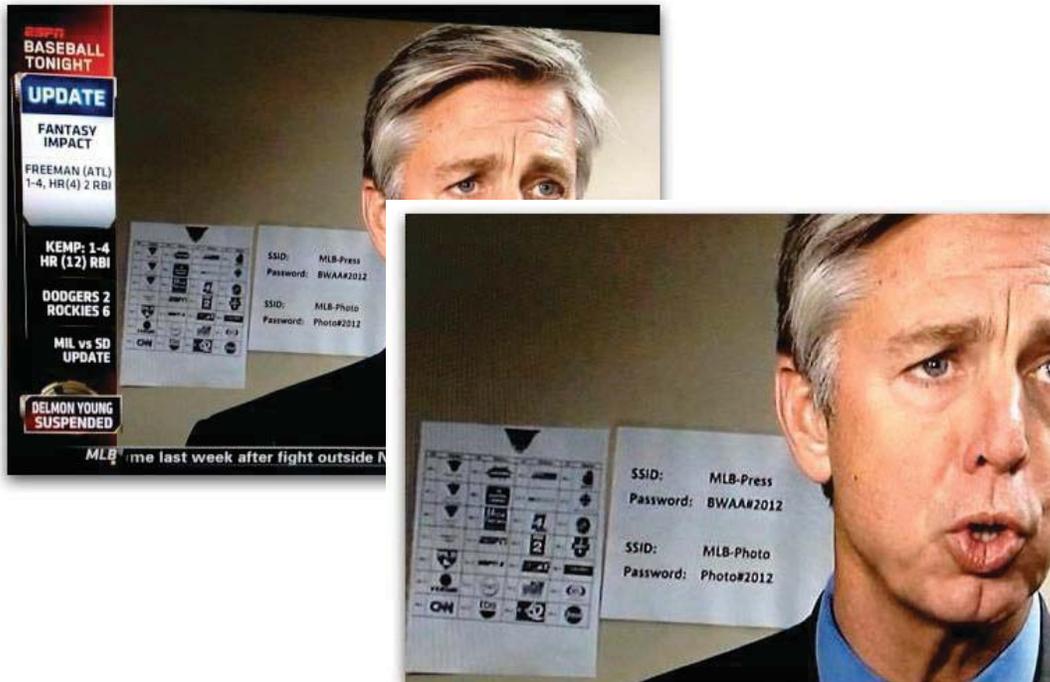


28.05.2012

DESY - Aktuelle Bedrohungen

41

So nicht!



28.05.2012

DESY - Aktuelle Bedrohungen

42

Der Tipp:

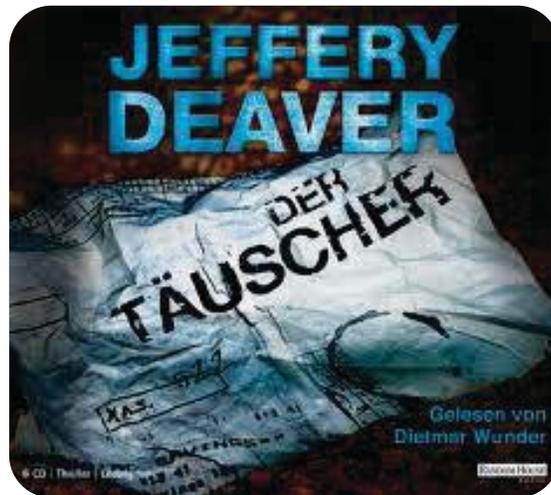


28.05.2012

DESY - Aktuelle Bedrohungen

43

Buchtipp:



28.05.2012

DESY - Aktuelle Bedrohungen

44

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