
Sicherheitsfaktor Mensch



Fraunhofer Institut
Sichere Informations-
Technologie

Sicherheitsfaktor Mensch

Ist der Benutzer eine vertrauenswürdige
Komponente?

Sven Türpe
Fraunhofer SIT

Rheinstraße 75
64295 Darmstadt

tuerpe@sit.fraunhofer.de
+49 (0)6 15 1/8 69 - 42 38



Fraunhofer Institut
Sichere Informations-
Technologie



Sicherheit? Nichts leichter als das!

x0%kL^By-Wo3n

ssh-keygen(1): „Good passphrases are 10-30 characters long, are not simple sentences or otherwise easily guessable (...), and contain a mix of upper and lowercase letters, numbers, and non-alphanumeric characters.“

„There is no way to recover a lost passphrase.“

CA-2000-04 Love Letter Worm

„Exercise caution with attachments in email. (...) Users should never open attachments from an untrusted origin, or that appear suspicious in any way.“

(CERT Advisory CA-2000-04)

Akzeptanz der digitalen Signatur

„Durch das Festschreiben bürokratischer, komplizierter Verfahren und überzogener technischer Anforderungen, (...) dazu beigetragen, dass die digitale Signatur für viele Bürger und Unternehmen in Deutschland schlicht unattraktiv ist. Der Gebrauch ist so umständlich und teuer, dass kaum ein Bürger oder Unternehmen in Deutschland die digitale Signatur haben will.“

(CDU/CSU-Fraktion im Bundestag)

Akzeptanz der digitalen Signatur (Forts.)

„For some time, C&E has been encouraging electronic VAT returns (...), but until recently required the use of an X509 client certificate to submit.

Presumably this has proved unpopular, since they are now permitting good old username/ password to be used.“

(Risks Digest Vol. 23, Issue 56)



Phishing

Quelle:
www.antiphishing.org

Dear PayPal valued member, 

Due to concerns, for the safety and integrity of the PayPal community we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive accounts, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account deletion. This notification expires on April 16th 2004.

Once you have updated your account records your PayPal will not be interrupted and will continue as normal.

Please note that you are prohibited to send or receive money until you confirm that you are the trueholder of this account.

Please follow the link below and renew your account information.

<https://www.paypal.com/cgi-bin/webscr?cmd=login-run>



PayPal Service Department

Was nun?



Sichtweisen

Usability Engineering:

Sicherheitstechnik ist zu kompliziert

Security Engineering:

Benutzer sind zu blöd

Ein unlösbarer Widerspruch?

Usability Engineering

- Aufgaben und Ziele des Benutzers
- Einfacher/schneller als ohne Computer
- Benutzer kennt sich im Gegenstandsbereich aus
- zum Beispiel:
 - Aufgabenangemessenheit
 - Erlernbarkeit, Selbstbeschreibung
 - Effizienz
 - Keine katastrophalen Fehler

Sicherheit aus Sicht der Mensch-Maschine-Interaktion

Sicherheitstechnik hat besondere Eigenschaften (Whitten & Tygar, 1999):

- Sicherheit ist Sekundärziel
- Sicherheit ist kompliziert
- Wenig und schlechtes Feedback
- Kein „Undo“
- Angreifer muss nur *eine* Lücke finden

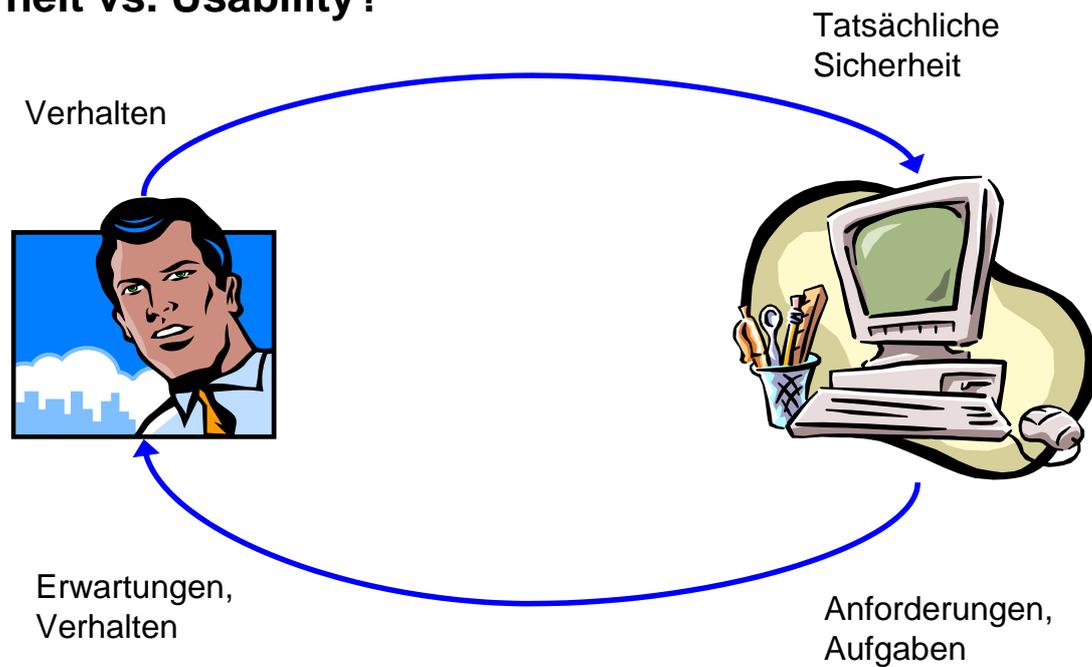
Security Engineering

- Bedrohung: intelligenter Angreifer
- System
- Komponenten
- Interaktion
- Vertrauensbeziehungen
- Sicherheitsmechanismen
 - Stärke, z.B. bei Kryptographie

Benutzer aus Sicht der Sicherheitstechnik

- Trusted Component ...
 - Ich bin `root`, ich darf das.
- ... aber nicht vertrauenswürdig, sondern
 - Fehleranfällig
 - Ahnungslos
 - Subversiv
- Schutz des *Systems* im Vordergrund
 - Angriffe auf Benutzer?
- Ist Sicherheit einfach zu kompliziert? Können wir User erziehen und schulen?

Sicherheit vs. Usability?



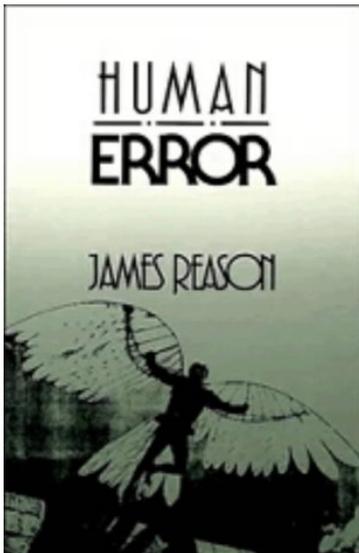
Human Factors

Missverständnis: Sicherheit einfacher machen.

- Fähigkeiten
- Wissen
- Verhalten
- Stress
- Wahrnehmung

→ Übereinstimmung zwischen Anforderungen an die User und ihrem tatsächlichen Verhalten.

James Reason: „Human Error“



- Rasmussen: Skill – Rule – Knowledge
- Generic Error Modeling System (GEMS)
 - Fehlerklassen analog Verhaltensebenen
 - Unterschiede z.B. in
 - Vorhersagbarkeit
 - Fokus der Aufmerksamkeit
 - Einfluss der Randbedingungen
 - Erkennungsmöglichkeit

Charles Perrow: „Normal Accidents“

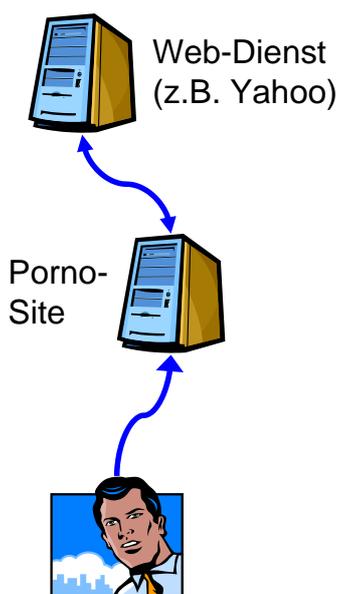


- Unfälle in technischen Systemen
 - z.B. Kernkraftwerk Harrisburg
- Was geht warum schief?
- „System Accident“
 - Komplexe Interaktion
 - Enge Kopplung
 - Mehrfachfehler
- Nur Sicherheit == Safety betrachtet

Stand der Technik:



Mein Lieblingshack



CAPTCHA:

Completely Automatic Public Turing test to tell Computers and Humans Apart

Verify Your Registration

* Enter the code shown:

[More info](#)

This helps Yahoo! prevent automated registrations.



Ungewollte Lerneffekte

deutsch Microsoft Deutschland | Site Ma

Microsoft Office Online

Suchen: Downloads

Homepage
Unterstützung
Schulung
Vorlagen
ClipArt und Medien
Downloads
Office Marketplace
Microsoft Office System

Aktivitäten
Bereits installierte Office-
Updates anzeigen
Erhalten
Von anderen Office-
Benutzern
Erreichen Sie uns

Microsoft Office Update

Office Update Installation Engine wird geladen...

10% abgeschlossen

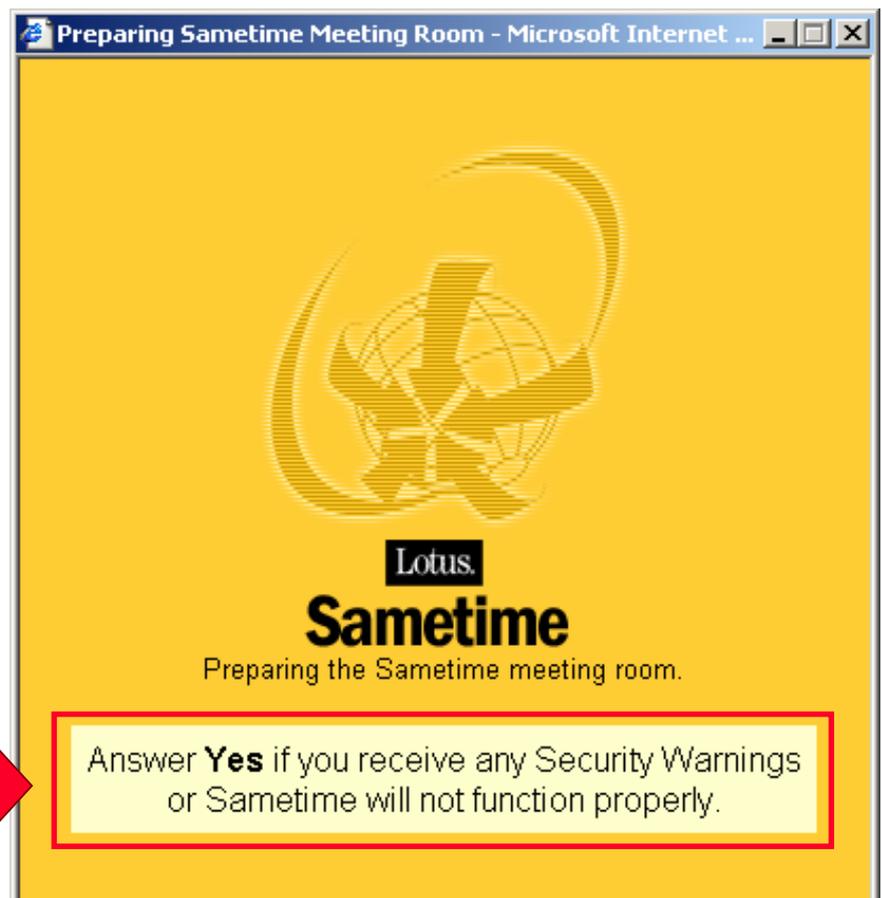
Dies kann bei einer Verbindung mit 56,6 Kbit/s bis zu 45 Sekunden dauern.

Klicken Sie auf **Ja**, wenn Sie in einem Dialogfeld gefragt werden, ob Sie **Office Update Installation Engine** von Microsoft installieren und ausführen möchten.



Ungewollte Lerneffekte

Preparing Sametime Meeting Room - Microsoft Internet ...



Lotus
Sametime
Preparing the Sametime meeting room.

Answer **Yes** if you receive any Security Warnings or Sametime will not function properly.

Was lernt uns das?



„Subversives“ Verhalten

Wissen Sie das Passwort noch?

x0%kL^By-Wo3n

Benutzerreaktionen:

- Aufschreiben
- Variation eines Standardpassworts
- ...

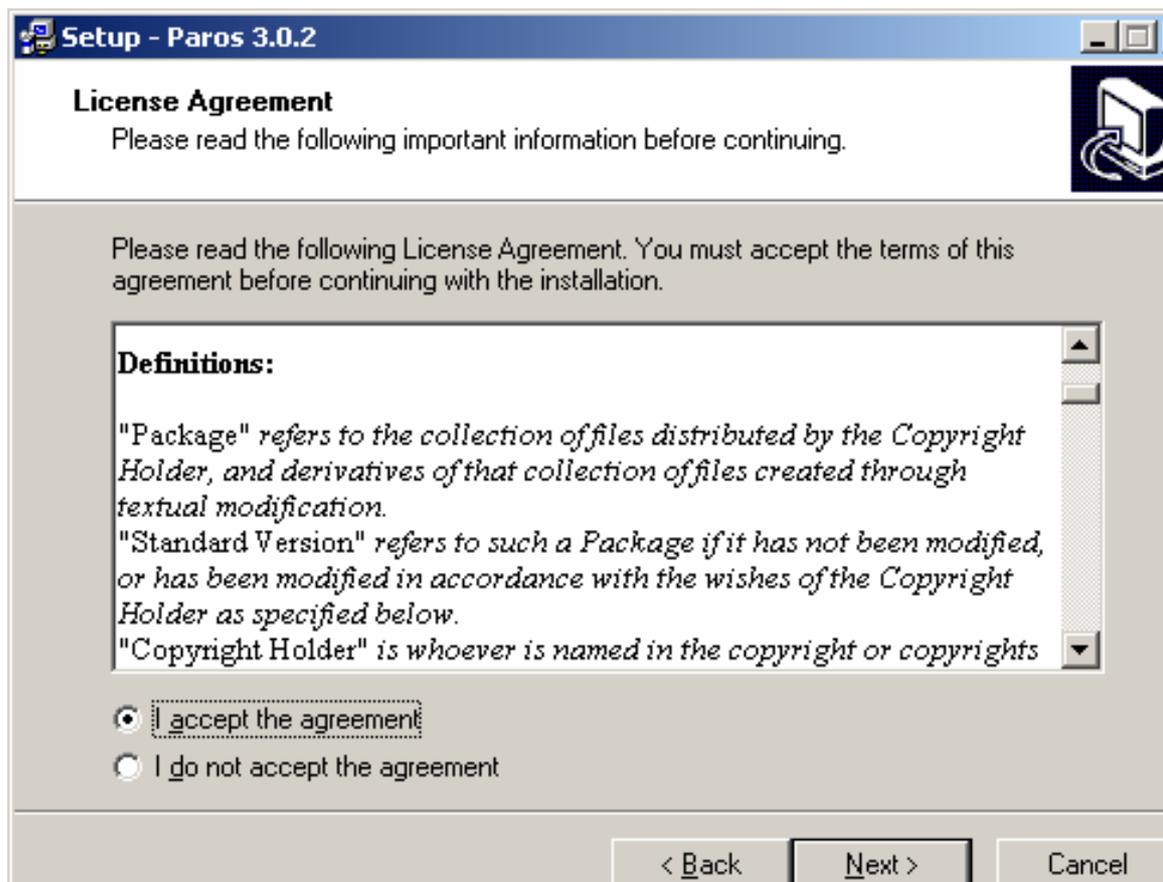
Adams & Sasse: Users are not the enemy

„Subversives“ Verhalten

- Problem: Laptop borgen. Deadline: in 2 Stunden.
- Gastzugang?
 - Wie geht das?
 - Account “Gast” gesperrt
 - Wo steckt der Admin?
- Ergebnis: Gastzugang mit schlechtem Passwort
 - Problem gelöst
- Es hätte schlimmer kommen können



Informierte Entscheidung



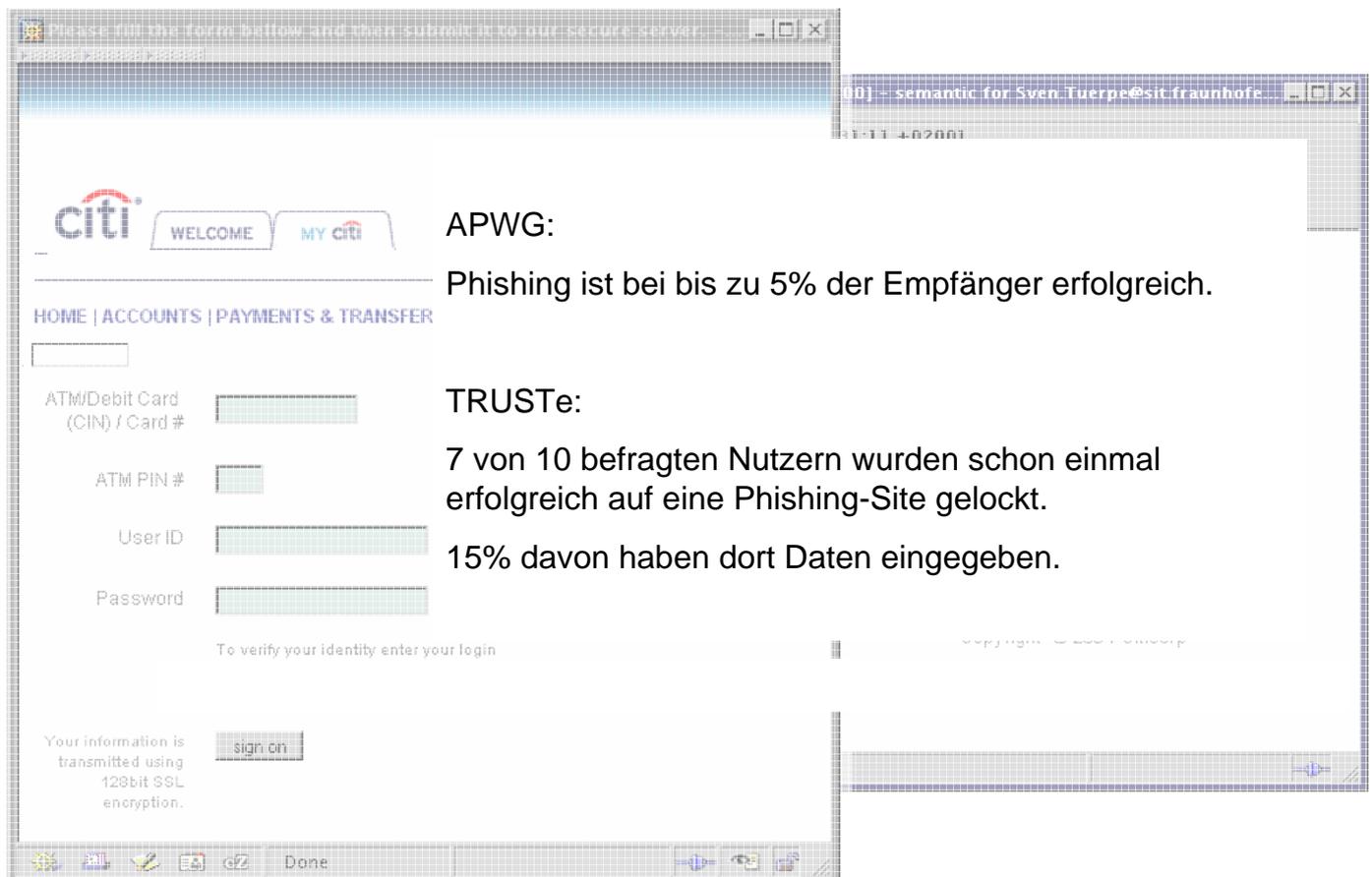
Informierte Entscheidung

Friedman, Howe & Felten:
Informed Consent in the Mozilla-Browser

- Cookie-Verwaltung als Sidebar im Browser
 - Farbcodierung für Herkunft
 - Unmittelbare Eingriffsmöglichkeit
- Vorgänge werden sichtbar und verständlich gemacht
- Kein Zwang, keine Störung



Phishing: Betrug mit gefälschten E-Mails und Webseiten

A screenshot of a web browser displaying a phishing website that mimics the Citi.com login page. The page includes the Citi logo, a 'WELCOME MY CITI' banner, and navigation links for 'HOME | ACCOUNTS | PAYMENTS & TRANSFER'. Below these are input fields for 'ATM/Debit Card (CIN) / Card #', 'ATM PIN #', 'User ID', and 'Password'. A 'sign on' button is visible at the bottom. A security notice states 'Your information is transmitted using 128bit SSL encryption.' The browser's address bar shows a URL that appears to be a legitimate Citi page, but the overall layout and content are designed to trick users into entering their credentials.

APWG:
Phishing ist bei bis zu 5% der Empfänger erfolgreich.

TRUSTe:
7 von 10 befragten Nutzern wurden schon einmal erfolgreich auf eine Phishing-Site gelockt.
15% davon haben dort Daten eingegeben.

Problem: Tatsächliches vs. formal korrektes Nutzerverhalten

- Formal korrekt:
 - Sicherheitszertifikat prüfen

- Tatsächlich:
 - Aussehen
 - Gewohnheit
 - Erwartungen
 - Nur Abweichungen fallen auf

Es gibt kaum technische Gegenmittel

„Die erste grundlegende Sicherungsinstanz ist der bloße Anschein. Sofern Sie große Abweichungen zu den erwarteten Informationen sehen, könnte hier eine Manipulation im Hintergrund stehen“

http://www.1822direkt.com/onlinebanking/sicherheit_pintan.html

→ Was tun Anbieter, um ihre Kunden bei der Erkennung zu unterstützen?

Studie: Was tun Banken, um ihre Online-Banking-Kunden bei der Phishing-Abwehr zu unterstützen?

- Vergleichstest: Websites von 12 Banken
 - Allgemein zugängliche Informationen
 - Heuristische Bewertung:
 - Technik
 - Homebanking-Software
 - Kundeninformation
 - Annahme: idealer Nutzer
 - Punkte für erfüllte Kriterien
-

Kategorie Technik

- Konsistenz der URLs
 - URL sichtbar?
 - SSL vor dem Login?
 - Zertifikat auf die Bank ausgestellt?
 - Doppelt gewichtet: maximal 8 Punkte
-



Web Site Identity Verified

The web site ww2.homebanking-sachsen.de s page you are viewing. The identity of this web VeriSign Trust Network, a certificate authority

View

View the security certificate th identity.

Connection Encrypted: High-grade Encr

The page you are viewing was encrypted bef Internet.

Encryption makes it very difficult for unauthor traveling between computers. It is therefore this page as it traveled across the network.

Certificate Viewer: "ww2.homebanking-sachsen.de"

General Details

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN) ww2.homebanking-sachsen.de
Organization (O) FinanzIT GmbH
Organizational Unit (OU) Terms of use at www.verisign.com/rpa (c)00
Serial Number 73:F7:65:53:70:11:A8:D3:0F:A4:F1:AE:03:AF:44:2D

Issued By

Common Name (CN) <Not Part Of Certificate>
Organization (O) VeriSign Trust Network
Organizational Unit (OU) VeriSign, Inc.

Validity

Issued On 17.05.2004
Expires On 18.05.2005

Fingerprints

SHA1 Fingerprint 17:31:D9:DC:37:32:9E:73:54:09:34:83:9F:84:D5:79:B1:D3:E7:1A
MD5 Fingerprint D1:17:8B:89:45:D7:FC:AF:81:B1:D3:1E:47:83:F1:8A

Help

Close

zur Demo | Hilfe

Anmeldung

Konto

VR-NetKey

Kontonummer:

PIN:

Anmelden

Hilfe

[JavaScript Application]



Die rechte Maustaste ist für diese Anwendung deaktiviert.

OK

Kategorie Homebanking-Software

- Alternative zum Web
- Wird HBCI unterstützt?
- PIN/TAN?
- Informationen zu Software, Konfiguration etc.?
- 3 Punkte

Kategorie Kundeninformation

- Informationen über Phishing?
- Kontaktmöglichkeit für Sicherheitsfragen?
- Konkrete Parameter für die Zertifikatsprüfung?
- Formulare: Frage nach E-Mail-Adresse?
- 4 Punkte

Wichtiger Sicherheitshinweis!

ING-DiBa. Die neue Generation Bank - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.diba.de/

Google Alerts Tahiti.Oracle.Com Livelink - Anmelden PDBDATA FIS

Banking | Kontakt | Infos per Post | Sitemap | FAQ | Suche

ING DiBa

Über die ING-DiBa + Direktbanking | Konto+Service | Anlegen + Sparen | Kredite + Finanzierung | Wertpapier + Brokerage | Vorsorge + Versicherung

Zugang zu Ihrem Konto oder Depot
→ Login Internetbanking + Brokerage

Zum ersten Mal hier?
■ So finden Sie was Sie suchen
■ Vorteile für ING-DiBa Kunden

Services
■ Ihr Bedarf – unser Angebot
■ Nützliche Finanztools
■ Investor-Center
■ Fonds-Center
■ Formular-Center
■ Vorsorge-Check
■ Finanztips-Newsletter
■ Im Notfall – Karte sperren

ING-DiBa Informationen
■ Produkte und Konditionen

Höchstleistung!
+25 € Tankgutschein
Extra-Konto

Jetzt günstig Wünsche erfüllen!
Ratenkredit
6,49%

100 Tage jeweils einen Mini gewinnen!
ING-DiBa Gewinnspiel

Top-Angebote
Beste Bank
Platz 1 in der Gesamtwertung
Ausgabe 5/2004
FINANZEN
→ Alle Top-Angebote auf einen Blick

ING-DiBa Nachrichten
→ **Wichtiger Sicherheitshinweis!**
→ Noch kein Extra-Konto? Sonderaktion: "Volks-Sparkonto" mit 25 Euro Tankgutschein!
→ Fonds des Monats: Flexibilität für bessere Performance
→ Direkt-Depot der ING-DiBa von Fachzeitschrift empfohlen!
→ DiBa wird ING-DiBa: Ein Grund zu feiern!

Done

Neugierig

Online-Banking: Antragsformular

Meine persönlichen Angaben (Kontoinhaber):

* Anrede:

* Vorname:

* Zuname:

* Straße, Haus-Nr.:

* PLZ:

* Wohnort:

* Geburtsdatum: (TT.MM.JJJJ)

* Geburtsort:

* Staatsangehörigkeit:

Telefon:

Fax:

* E-Mail:

Konto-Nr.:

Hiermit beantrage ich die Freischaltung der nachfolgenden Konten/Depots für folgende Verfahren:

- Online-Banking mit PIN TAN
- Online-Banking mit HBCI

Phishing-Studie: Ergebnisse

1 x „sehr gut“

0 x „gut“

5 x „befriedigend“

5 x „ausreichend“

1 x „mangelhaft“

Technische Mängel bei 6 Banken (50%)

<http://www.sit.fraunhofer.de/german/hps1/phishing.pdf>



Nicht nur User

OWASP Top Ten:

- Unvalidated Input
 - Broken Access Control
 - Broken Authentication and Session Management
 - Cross Site Scripting (XSS) Flaws
 - Buffer Overflows
 - Injection Flaws
 - Improper Error Handling
 - Insecure Storage
 - Denial of Service
 - Insecure Configuration Management
-



Sicherheit und Barrierefreiheit

- Zugang für Nutzer mit Einschränkungen
 - z.B. Blinde
 - z.B. Alte
- Für eGovernment vorgeschrieben
- Behörden *lieben* die digitale Signatur
- Funktioniert das zusammen?

Sicherheit und Barrierefreiheit

- Hürden bei Beantragung und Zertifikatsabfragen
- Medienbrüche bei Erstauthentisierung
- Kartenleser für Blinde schwer zu nutzen
 - Hilfsmittel funktionieren nur für Standard-UI (Tastatur, Bildschirm)
- Accessibility-APIs nicht unterstützt
- Biometrie?
 - Erleichterung vs. vorgegebene Merkmale
- Fraunhofer SIT: Prototyp barrierefreie Signatur

Barrierenfrei?

CAPTCHA:

Completely Automatic Public Turing test to tell Computers and Humans Apart

Verify Your Registration

* Enter the code shown: [More info](#)

This helps Yahoo! prevent automated registrations.



Fazit

- Benutzer funktionieren nicht
- Technik muss damit zurechtkommen
 - Nur das verlangen, was Benutzer leisten können
 - Restrisiko
- Fahrlässigkeit, Schuld, Haftung?
- Sicherheit nicht auf Verhinderung beschränken
 - Reaktion auf Vorfälle
 - Regelungen für den Schadensfall

Pläne

- Schwieriges Thema
- Forschung:
 - Erste Ansätze
 - Kleine Community
- Im Alltag: Viele Probleme, kaum Lösungen

- NoE im 6. Forschungsrahmenprogramm?



Ende

Fraunhofer SIT

Sven Türpe

Rheinstraße 75
D-64295 Darmstadt

Telefon: +49-6151-869-4238
Telefax: +49-6151-869-224

Email: tuerpe@sit.fraunhofer.de
www: <http://www.sit.fraunhofer.de>

Kontakt

Fraunhofer Institut für Sichere Informationstechnologie
Sichere Prozesse und Infrastrukturen

Sven Türpe

Rheinstraße 75
D-64295 Darmstadt

Telefon: +49-6151-869-4238

Telefax: +49-6151-869-224

mail: tuerpe@sit.fraunhofer.de

www: <http://www.sit.fraunhofer.de>

