

Exploiting Human Mistakes



Willy Sudiarto Raharjo

willysr@gmail.com

Auditorium Koinonia UKDW, May 2 2009



**All information, tools, methods presented
here are given for educational or security
awareness purposes**

The speaker take no responsibilities for any actions
conducted or damage caused by the use or misuse of
this information by the audience



What is the biggest IT
security threat ??

Human Error Article

Human error is the greatest IT security threat

26 NOVEMBER 2008 JJ Robinson



Staff remain the weak point when it comes to protecting an organisation's data, according to a new poll

Human error is the number one threat to a company's IT security, according to a poll of IT directors conducted by YouGov.

Despite the common public perception that the greatest risk to corporate data security comes from the external hacker breaking in and stealing sensitive data, 86% of IT directors regard the greatest threat as coming from their colleagues ignoring security policies (31%), making mistakes (37%), having insufficient training (13%) and committing industrial espionage (5%).

<http://www.information-age.com/home/information-age-today/816227/human-error-is-the-greatest-it-security-threat.html>

Human Error Article

Human Error at Center of Most IT Security Breaches



Menschliches Fehlverhalten: Hauptursache für IT-Sicherheitsverletzungen



Printer-friendly



E-mail this article to a friend



Your Comment

CompTIA Survey Finds; Number of Reported Incidents Grows, but Impact Mitigated by Better Training, Certification

Human error continues to be the primary cause of information technology (IT) security breaches, but better training and preparation are enabling organizations to limit their impact on operations, according to the second annual survey on IT security and the workforce released today by CompTIA, the Computing Technology Industry Association.

Even with higher awareness of IT security threats; more emphasis on security practices and procedures; and more spending on preventive measures, 84 percent of organizations on nearly 900 organizations who participated in this year's survey blamed human error either wholly or in part for their last major security breach. Last year, human error was cited as the cause of 63 percent of security breaches.

"The findings underscore the fact that security and human capital, more so than security and technology, should be given the highest priority by all organizations," said John Venator, president and chief executive officer, CompTIA. "Human knowledge and action are critical to making networks and IT infrastructure secure. And while awareness of the threat posed by IT security breaches has increased dramatically, many organizations have been slow to make the appropriate investments in time and budget to properly address these threats."

Nearly six in ten organizations (58 percent) said they have experienced at least one major IT security breach - defined as one that caused real harm, resulted in the loss of confidential information or interrupted business operations - in the last six months. That's up significantly from a year ago when 38 percent of organizations reported at least one major IT security breach.

http://www.securitymanager.net/magazine/article_448_human_error_it_security.html

Human Error Article

Human Error Tops the List of Security Threats

Majority of companies list "human error" as root cause of security failures, well ahead of operations and technology, new Deloitte survey says.

By Diann Daniel

 [Leave a comment \(1\)](#)

TUE, FEBRUARY 05, 2008 — **CIO** — When it comes to security, human threats score much higher than those posed by technology. So says a new survey by consulting firm Deloitte of more than 100 technology, media and telecommunications companies worldwide. Seventy-five percent of companies listed human error as the leading cause of security failures such as breakdowns and systems outages. Forty-eight percent also cited operations and technology lapses as key causes of security failures. Problems resulting from third parties such as contractors and business partners, meanwhile, received 28 percent of the votes as a root cause of security failures.

Misbehaving employees also figure prominently in IT fears: Ninety-one percent of respondents say the risk of employee misconduct related to information systems worries them.

Another security worry is many line-of-business executives' tendency to see information security as solely IT's problem, Deloitte says. Forty percent of surveyed companies give IT the primary responsibility for information security, and 45 percent say top management is informed about security issues only on an ad hoc basis. And although 62 percent say security is a key imperative at the board or executive level, that number is low, says Deloitte, since security should be top strategic priority for every TMT company.

To mitigate these security threats, Deloitte recommends that security goals be integrated into business strategies and plans. Measuring ROI on security efforts and providing thorough and ongoing security training to all levels of the organization are also key, Deloitte advises. Training can educate employees on how to deal with the latest security threats and can serve as a reminder to stay vigilant. For more lessons on security ROI, see **"How GE Uses Six Sigma to Drive Security ROI"** and **"Your Guide To Good-Enough Compliance."**

"The technology, media and entertainment and telecommunications industries are still in a reactive mode when it comes to their approach to security," said Rena Mears, Deloitte's global and U.S. privacy and data protection leader, in a press release. "A prerequisite for effective information security is the implementation of a proactive information security strategy that is closely linked to the company's overall business strategy, business requirements, and key business drivers."

http://www.cio.com/article/179802/Human_Error_Tops_the_List_of_Security_Threats

"This site may harm your computer" on every search result?!?!

1/31/2009 09:02:00 AM

If you did a Google search between 6:30 a.m. PST and 7:25 a.m. PST this morning, you likely saw that the message "This site may harm your computer" accompanied each and every search result. This was clearly an error, and we are very sorry for the inconvenience caused to our users.

What happened? Very simply, human error. Google flags search results with the message "This site may harm your computer" if the site is known to install malicious software in the background or otherwise surreptitiously. We do this to protect our users against visiting sites that could harm their computers. We maintain a list of such sites through both manual and automated methods. We work with a non-profit called StopBadware.org to come up with criteria for maintaining this list, and to provide simple processes for webmasters to remove their site from the list.

We periodically update that list and released one such update to the site this morning. Unfortunately (and here's the human error), the URL of 'I' was mistakenly checked in as a value to the file and 'I' expands to all URLs. Fortunately, our on-call site reliability team found the problem quickly and reverted the file. Since we push these updates in a staggered and rolling fashion, the errors began appearing between 6:27 a.m. and 6:40 a.m. and began disappearing between 7:10 and 7:25 a.m., so the duration of the problem for any particular user was approximately 40 minutes.

<http://googleblog.blogspot.com/2009/01/this-site-may-harm-your-computer-on.html>

Human Mistakes

- Lack of knowledge
- Simple, but fatal mistakes
 - Easy, short password or even no password at all
 - Sharing computers
 - Careless
- Easy to exploit
 - Phishing emails
 - Fake login
 - Key logger

Phishing

- Phishing is an attempt to steal other person's **personal information**
- Mostly via **email (in HTML)**
- Masquerade as **well-known organization** or **companies which you do not even know**
- Can be in any form
 - Inactive accounts
 - Suspected doing illegal actions

http://www.consumerfraudreporting.org/phishing_examples.php

Phishing Examples

Dear Amazon® member,

We are contacting you to inform you that our Account Review Team identified some unusual activity in your account. In accordance with Amazon's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved. To secure your account and quickly restore full access, we may require some additional information from you for the following reason: We have been notified that a card associated with your account has been reported as lost or stolen, or that there were additional problems with your card.

This process is mandatory, and if not completed within the nearest time your account or credit card may be subject for temporary suspension. To securely confirm your Amazon information please click on the link bellow:

<http://citdsl.fix.netvision.net.il/login.html>

We encourage you to log in and perform the steps necessary to restore your account access as soon as possible. Allowing your account access to remain limited for an extended period of time may result in further limitations on the use of your account and possible account closure.

For more information about how to protect your account please visit Amazon Security Center. We apologize for any inconvenience this may cause, and we appreciate your assistance in helping us to maintain the integrity of the entire Amazon system.

Phishing Examples

Subject: eBay Account Verification

Date: Fri, 20 Jun 2003 07:38:39 -0700

From: "eBay" <accounts@ebay.com>

Reply-To: accounts@ebay.com

To:

Dear eBay member,

As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.

You are requested to visit our site by following the link given below

<http://arribba.cgi3.ebay.com/aw-cgi/ebayISAPI.dll?UpdateInformationConfirm&bpuser=1>

Please fill in the required information.

This is required for us to continue to offer you a safe and risk free environment to send and receive money online, and maintain the eBay Experience.

Thank you

Accounts Management As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and [User Agreement](#) if you have any questions.

Copyright © 1995-2003 eBay Inc. All Rights Reserved.

Designated trademarks and brands are the property of their respective owners.

Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).



Phishing Examples



HSBC Message Center

Welcome to "My Message" Service.


A New message of deposition has just been sent to your HSBC online Message Center and here is an alert to inform you that you have 1 new message from HSBC Bank Message Center.

HSBC customers may use this service to contact us with enquiries regarding your accounts or the products and services we offer. From time to time, we will also use 'My messages' to contact you. This may be in relation to existing products and services which you have with us or to keep you informed of enhancements to our products and services. Be sure to check 'My messages' regularly for any new messages. 'My messages' will only retain 10 messages so you may want to delete those you do not need. Click to view [My Message](#) to read your new messages now.

Bank Management
HSBC The World Global Bank
Code #231623483

Phishing Examples

HSBC United Kingdom You are viewing Personal Banking

HSBC  **The world's local bank** Personal | Business | Corporate

Personal Home | Current accounts | Savings | Investments | Credit Cards | Loans | Mortgages | Insurance | International Services | HSBC Premier | Sale

Internet Banking

Welcome
Input Internet Banking user ID
e.g. ID1234567890

[Log on ▶](#)

[▶ Forgotten ID?](#) [▶ Contact HSBC](#)
[▶ Help](#) [▶ Register](#)

New Customers

- ▶ Find out more about Internet Banking
- ▶ View interactive demo
- ▶ Find out about The Virtual Forest

Business Internet Banking

[Log on ▶](#)

IMPORTANT

Phishing is a scam where criminals seek to

Internet Banking

Personal [Log on ▶](#)

[Register ▶](#) [Security ▶](#) [Information ▶](#)

Interactive demo

To see how Internet Banking can help you manage your money online, take a look at our interactive online demo.

[View demo ▶](#)

Get Safe Online

To combat the threat of internet fraud and hacking, the Government and businesses like HSBC have combined to create Get Safe Online.

[Find out more ▶](#)

phishing scam reported at millersmiles.co.uk

Real Website



The world's local bank

[Site map](#) | [Contact us](#) | [HSBC Group](#)

Personal

Business

HSBC United Kingdom ▾

Search

Search ▶

HSBC Premier

HSBC Plus

Current accounts

Savings

Investments

Credit Cards

Loans

Mortgages

Insurance

International Services

Green

Internet Banking

Personal

Log on ▶

Register ▶

Security ▶

Information ▶

Internet Banking

Welcome

Input Internet Banking user ID
e.g. IB1234567890

Log on ▶

- ▶ [Forgotten ID?](#)
- ▶ [Contact HSBC](#)
- ▶ [Help](#)
- ▶ [Register](#)

New Customers

- ▶ [Find out more about Internet Banking](#)
- ▶ [View interactive demo](#)
- ▶ [Find out about The Virtual Forest](#)

Business
Internet Banking

Log on ▶



Vaccine Investment

Save more than money

- ▶ Make a fixed return, make a real difference

HSBC Plus

It all comes as standard

- ▶ Identity Theft Assistance
- ▶ Preferential rates
- ▶ Travel Insurance

Well Known Organization












SUMMARY REPORT GLOBAL PHISHING

View: [Brand Summary](#) | [Servers](#)

Output: [Print](#) | [XML](#) | [CSV](#)

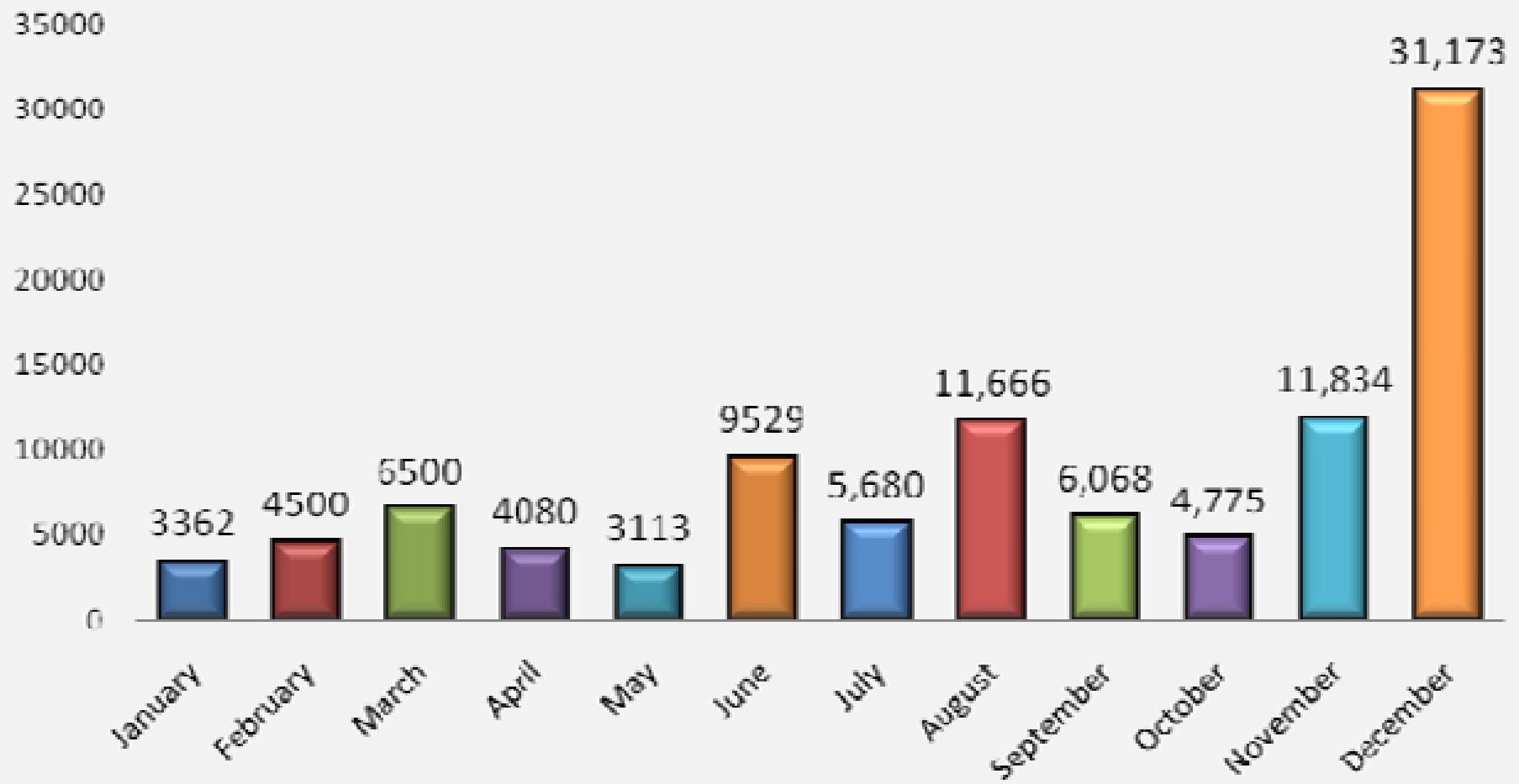
BRAND SUMMARY (past 24 hours)



Brand Name	Phished URLs	Percentage
PayPal	16865	 11.8%
eBay	9755	 6.8%
Abbey Bank	2710	 1.9%
Bank of America	1566	 1.1%
CitiCorp	1111	 0.8%
HSBC	1022	 0.7%
Halifax Bank	864	 0.6%
Lloyds of London	589	 0.4%
JP Morgan Chase	388	 0.3%
Wells Fargo	248	 0.2%
Other	107841	 75.4%

<http://atlas.arbor.net/summary/phishing>

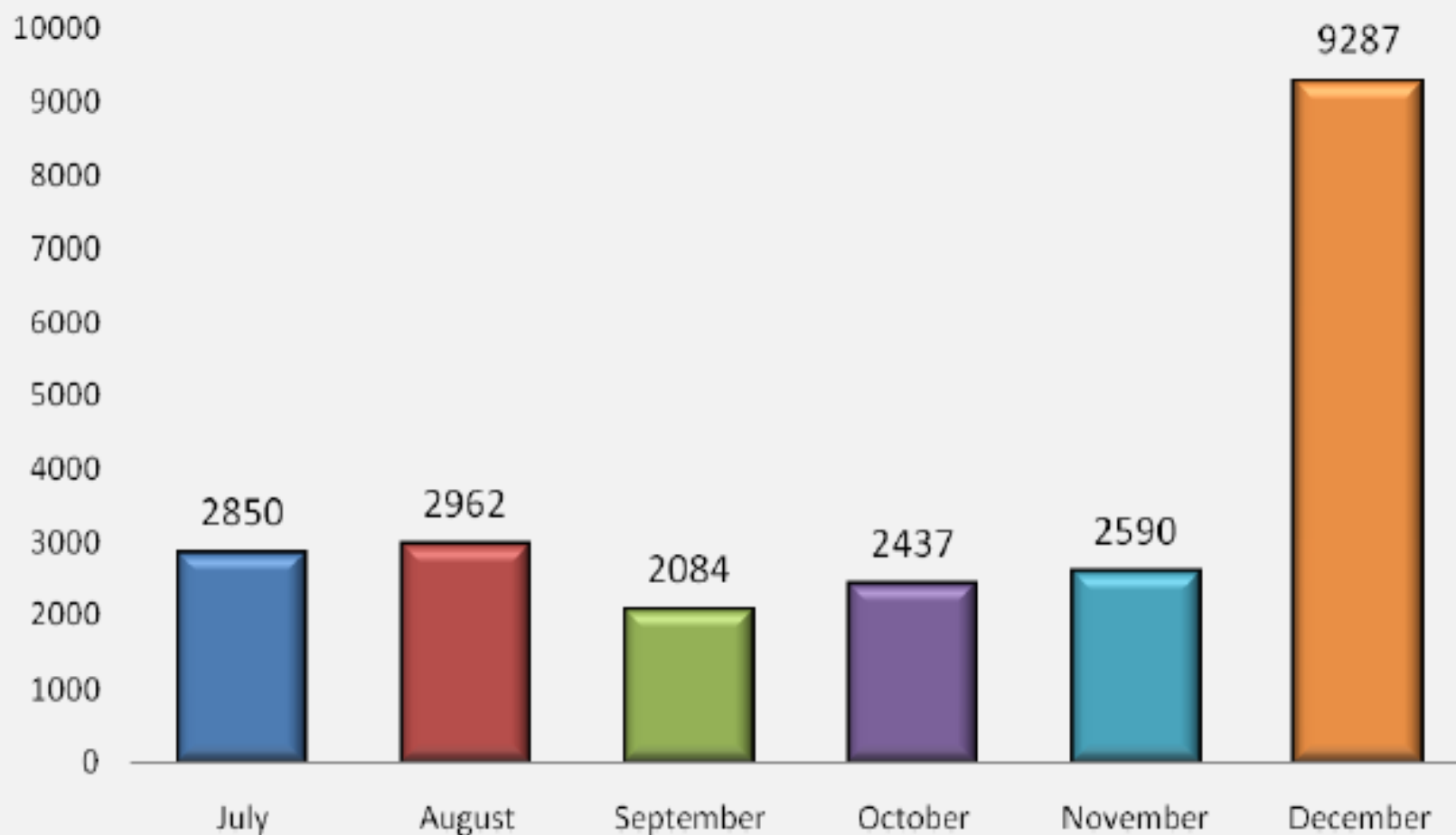
Password Stealing Malicious Code URLs



January – December 2008

<http://www.antiphishing.org/phishReportsArchive.html>

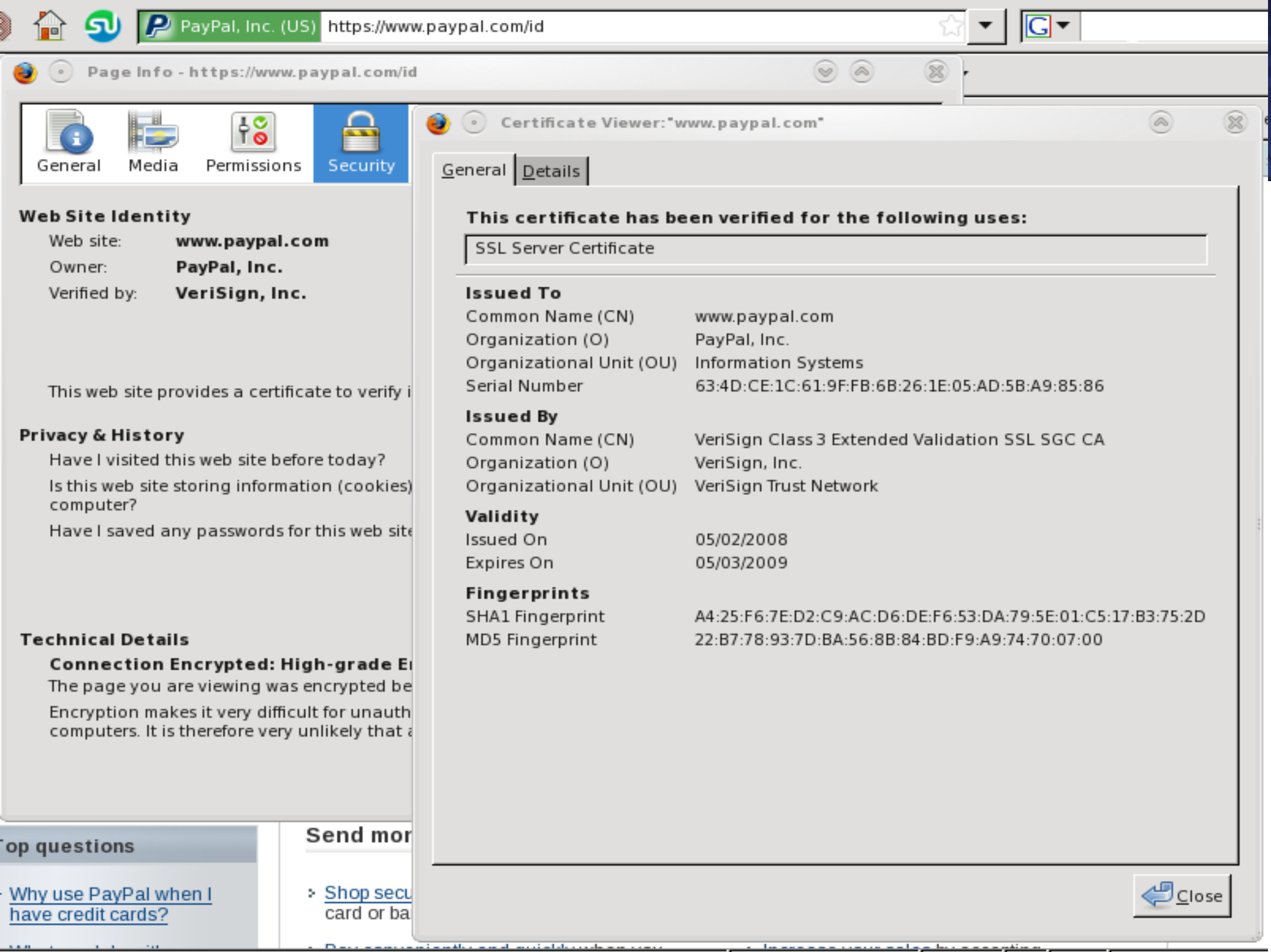
Rogue Anti-Malware Programs 2nd Half 2008



Fake Anti-Malware

Steps to Avoid Phishing

- Never open untrusted emails
- Never click suspicious link
- Check and validate URL
- Always check site's certificate (if any)
- Use text-mode when reading emails



General



Media



Permissions



Security

Web Site Identity

Web site: **www.paypal.com**

Owner: **PayPal, Inc.**

Verified by: **VeriSign, Inc.**

This web site provides a certificate to verify its identity.

Privacy & History

Have I visited this web site before today?

Is this web site storing information (cookies) on my computer?

Have I saved any passwords for this web site?

Technical Details

Connection Encrypted: High-grade Encryption

The page you are viewing was encrypted before being sent to your computer.

Encryption makes it very difficult for unauthorized computers to intercept the data. It is therefore very unlikely that a third party can read the information you are sending or receiving.



Certificate Viewer: "www.paypal.com"

General

Details

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	www.paypal.com
Organization (O)	PayPal, Inc.
Organizational Unit (OU)	Information Systems
Serial Number	63:4D:CE:1C:61:9F:FB:6B:26:1E:05:AD:5B:A9:85:86

Issued By

Common Name (CN)	VeriSign Class 3 Extended Validation SSL SGC CA
Organization (O)	VeriSign, Inc.
Organizational Unit (OU)	VeriSign Trust Network

Validity

Issued On	05/02/2008
Expires On	05/03/2009

Fingerprints

SHA1 Fingerprint	A4:25:F6:7E:D2:C9:AC:D6:DE:F6:53:DA:79:5E:01:C5:17:B3:75:2D
MD5 Fingerprint	22:B7:78:93:7D:BA:56:8B:84:BD:F9:A9:74:70:07:00

Close

Fake BCA

klikBCA Individual - Mozilla Firefox


File Edit View History Bookmarks Tools Help

http://somnuk.ac.th/main/.ibank.klikbca.com/

Stumble! I like it! Send to Channels: All Favorite

Disable Cookies CSS Forms Images Information Miscellaneous Outline

klikBCA Individual klikBCA Individual

**INDIVIDUAL**[\[HOME\]](#)

USER ID dan PIN Internet Banking dapat diperoleh pada saat Anda melakukan Registrasi Internet melalui ATM BCA. Untuk informasi lebih lanjut hubungi Halo BCA (021) 52999888.

HOW TO GET STARTED:
To start using BCA Internet Banking, You must first register through any BCA ATM. For further information, please contact Halo BCA (021) 52999888.

[\[PRIVACY POLICY \]](#)

Silakan memasukkan USER ID Anda
Please enter Your USER ID

Silakan memasukkan PIN Internet Banking Anda
Please enter Your Internet Banking PIN

LOGIN


Catatan :


- Anda harus menggunakan **'KeyBCA'** setiap kali Anda melakukan transaksi finansial.
- Situs ini hanya dapat ditampilkan dengan menggunakan Internet Explorer ver. 6.0 keatas.

Notes :

- You have to use **'KeyBCA'** to do financial transaction.
- This site can be viewed only with Internet Explorer ver. 6.0 and above.

Klik BCA is secured with SSL 128 bit encryption.



Copyright © 2000  All Rights Reserved

Real BCA

klikBCA Individual - Mozilla Firefox


File Edit View History Bookmarks Tools Help

https://ibank.klikbca.com/

Stumble! | I like it! | Send to | Channels: | All | Favorite

Disable | Cookies | CSS | Forms | Images | Information | Miscellaneous | Outline

klikBCA Individual - Aktivat... | klikBCA Individual

**INDIVIDUAL**[\[HOME\]](#)

USER ID dan PIN Internet Banking dapat diperoleh pada saat Anda melakukan Registrasi Internet melalui ATM BCA. Untuk informasi lebih lanjut hubungi Halo BCA (021) 52999888.

HOW TO GET STARTED:
To start using BCA Internet Banking, You must first register through any BCA ATM. For further information, please contact Halo BCA (021) 52999888.

[\[PRIVACY POLICY \]](#)

Silakan memasukkan USER ID Anda
Please enter Your USER ID

Silakan memasukkan PIN Internet Banking Anda
Please enter Your Internet Banking PIN

LOGIN


Catatan :


- Anda harus menggunakan 'KeyBCA' setiap kali Anda melakukan transaksi finansial.
- Situs ini hanya dapat ditampilkan dengan menggunakan Internet Explorer ver. 6.0 keatas.

Notes :

- You have to use 'KeyBCA' to do financial transaction.
- This site can be viewed only with Internet Explorer ver. 6.0 and above.

Klik BCA is secured with SSL 128 bit encryption.



Copyright © 2000  All Rights Reserved

Registration???

**INDIVIDUAL**[\[HOME\]](#)

USER ID dan PIN Internet Banking dapat diperoleh pada saat Anda melakukan Registrasi Internet melalui ATM BCA. Untuk informasi lebih lanjut hubungi Halo BCA (021) 52999888.

HOW TO GET STARTED:
To start using BCA Internet Banking, You must first register through any BCA ATM. For further information, please contact Halo BCA (021) 52999888.

[\[PRIVACY POLICY \]](#)

Silakan memasukkan Nama Anda
Please enter Your Name

Silakan memasukkan Alamat Lengkap Anda
Please enter Your Full Address

Silakan memasukkan Nomor ATM Anda
Please enter Your ATM Card Number

Silakan memasukkan Kadaluarsa Kartu Anda
Please enter Your Card Expired

Silakan memasukkan CVV Kartu Anda
Please enter Your Card CVV

* 3 Digit Terakhir Di Bagian Belakang Kartu

Silakan memasukkan Alamat Email Anda
Please enter Your Email Address

Silakan memasukkan KeyBCA Anda
Please enter Your KeyBCA

Catatan :

- Anda harus menggunakan 'KeyBCA' setiap kali Anda melakukan transaksi finansial.
- Situs ini hanya dapat ditampilkan dengan menggunakan Internet Explorer

Klik BCA is secured with SSL 128 bit encryption.



Key Logger

- **Software program** or **hardware device** that are capable of recording keystrokes
- Well hidden on systems
- Send information to other people/machine

Software Key Logger

Actual Spy

Start monitoring Stop monitoring Hide Clear all logs Registration Help Exit

PC Activity

Keystrokes (39) Screenshots (9) Applications (154) Clipboard (4) Printer (1) Files and Directories (21)

Time	Window Caption	Application Path	Username
2/9/2005 12:14:27 PM	actualspy.doc - Microsoft Word	C:\Program Files\Microsoft Offi...	Andrey
2/9/2005 12:14:21 PM	Microsoft Word	C:\Program Files\Microsoft Offi...	Andrey
2/9/2005 12:39:38 AM	Desktop	C:\WINDOWS\explorer.exe	Andrey
2/9/2005 12:39:17 AM	The Bat!	C:\Program Files\The Bat!\the...	Andrey
2/8/2005 11:25:05 PM	Microsoft Internet Explorer	C:\Program Files\Internet Expl...	Andrey
2/8/2005 6:44:14 PM	The Bat!	C:\Program Files\The Bat!\the...	Andrey
2/8/2005 5:02:02 PM	Statistics for www.actualspy.c...	C:\Program Files\Internet Expl...	Andrey
2/8/2005 4:58:01 PM	The Bat!	C:\Program Files\The Bat!\the...	Andrey
2/8/2005 4:57:46 PM	The Bat!	C:\Program Files\The Bat!\the...	Andrey

Time: 2/9/2005 12:14:27 PM
Window Caption: actualspy.doc - Microsoft Word
Application path: C:\Program Files\Microsoft Office\Office10\WINWORD.EXE
Username: Andrey

Keystrokes:
[Shift]Actual[Space][Shift]Spy
[Enter]

☐ Show characters only

Refresh Delete Delete all Search ☐ Match case

Status: stopped Total records: 253 Text logs size: 37.24 KB Screenshots size: 1.40 MB

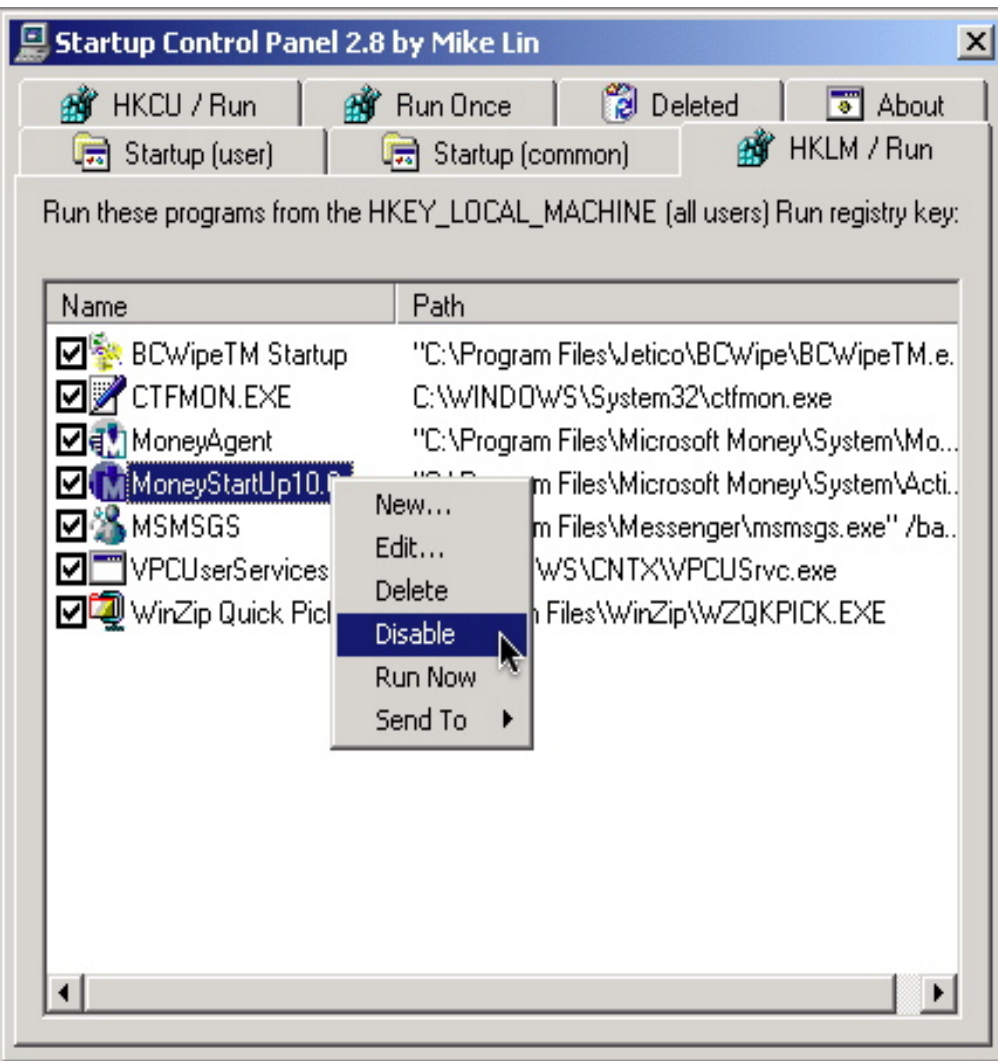
Hardware Key Logger



How to detect Keylogger

- Check every unusual process
- Check for unusual Internet connection
- Check application that runs automatically at start-up
- Use antivirus or keylogger detector
 - But don't depend too much
 - Keyloggers are as quick as virus/worms
- Look at files which is getting bigger and bigger (these might be logs of keystrokes)

Startup Control Panel + Startup Monitor



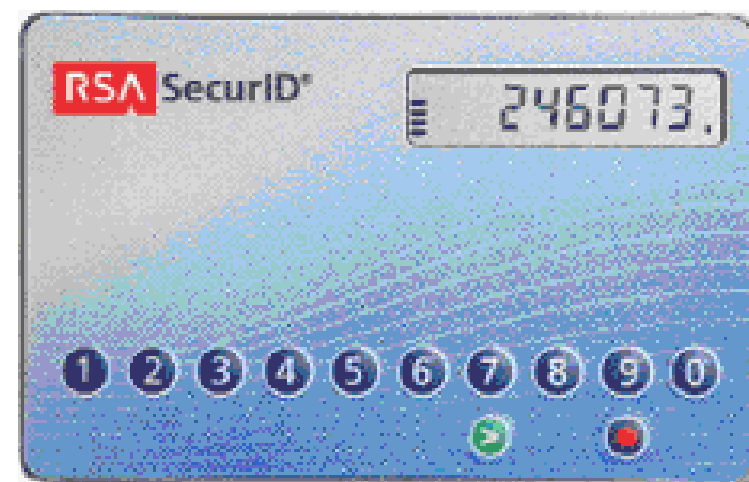
<http://mlin.net>

Working at public area

- Use virtual keyboards



- Look for unusual devices
- Use one-time password



References

- <http://www.technicalinfo.net/papers/Phishing.html>
- <http://www.antiphishing.org/resources.html>
- <http://www.millersmiles.co.uk/>
- <http://www.adoko.com/keyloggers.html>
- <http://www.viruslist.com/en/analysis?pubid=204791931>



Thank you