

Tips and Tricks to Surf and Do Business Securely on the Internet

C.K. Lung, CISSP, CISA

Consultant, Information Security

cklung@yahoo.com

416-906-0116

A decorative vertical bar in a light olive green color runs down the left side of the slide. A thin horizontal line in a dark purple color spans the width of the slide, intersecting the vertical bar. On the right side of this horizontal line, there is a small rectangular block in a light grey color.

Internet is fantastic, but there are risks!

Objective

You will be able to effectively protect yourself against on-line threats / attacks.

Agenda

- Common activities on Internet (iNet)
- Methods accessing iNet
- Threats in/on iNet
- How to be Safe on iNet?
- Q & A

Common activities on the iNet

- **E-Mail**
- **Web Surfing:**
 - News
 - Stock Quotes
 - Travel Information
 - Product Information
- **On-line transactions:**
 - Shopping
 - Paying Bills
 - Banking / Trading Stocks
 - Auctions
 - Charity Donations

Common activities on the iNet

- P2P File Sharing: e.g.,
 - eDonkey / Overnet
 - BitTorrent
 - Limewire
 - BearShare
 - Kazaa
- Blog (博客)
- Myspace
- YouTube

Common activities on the iNet

- Downloading: MP3, video, etc.
- Instant Messaging (MSN, Yahoo, Google Talk), ICQ, chat room
- Discussion Boards / Newsgroups
- Entertainment / Games – poker, casinos
- Job Search

Tools accessing iNet

- Desktop / Laptop computers:
 - Wired
 - Wireless
- Cellular phones, including Blackberry,
 - Wireless
- Personal Digital Assistants (PDA)
 - Wireless
- Automatic Banking Machines (ATM)*
- Public Accessible Computers (libraries, hotels, airports)

Bad things (Threats) on iNet

- Scams / Frauds (騙局, 陷阱)
- Identity Theft
- Malicious Code: (惡意代碼)
 - Adware
 - Spyware – keystroke logger, cookies, Trojan
 - Viruses/worms
 - Automatic Dialer
 - Rootkit
- Phishing / Pharming / vishing - VoIP
 - Collecting Personal Information (Identity Theft)

Bad things (Threats) on iNet

- **Attacks**
 - Hackers
 - Hijack
- **Pornography, Porn sites**
- **Violent / hateful content**
- **“Crooks”**
- **Unauthorized disclosure of personal information / Privacy Invasion**
- **Online predators**
- **Cyber bullying**

This talk's focus

“This talk is focused on “on-line business transactions” on iNet” and hardening your tool (computer).”

Assumption Abbey

Ava, Missouri 65608
417.683.5110

[Home](#)[About the Abbey](#)[Site Map](#)[Account Login](#)[Quick Order](#)[Contact Us](#)

Subtotal : \$0.00

Qty in Basket : 0

[View Basket](#)

Search

Description



GO

DEPARTMENTS

[Specials](#)[Fruitcake](#)[Donations](#)

ACCOUNT INFO

[View Basket](#)[Order Status](#)[Address Book](#)

BEST SELLERS

- 1) Shipped outside US
- 2) Cake shipped to U.S. zipcodes
- 3) Canadian addresses
- 4) Donation

SPECIALS

- Cake shipped to U.S. zipcodes
- Canadian addresses
- Shipped outside US

On-line business transactions

- Shopping
- Paying Bills (Hydro, credit card, ...)
- Banking / Trading Stocks
- Auctions
- Charity Donations

ATM Fraud

電子機票詐騙案 層出不窮

本報綜合報道

花了幾千元，到機場卻發現電腦記錄根本沒有訂票。近日，一些「詐騙分子」盯上了在中國剛剛實行不久的電子機票，他們上門收款，之後失蹤，旅客到機場才發現拿得是假票。

據《半島晨報》報道，目前中國已發生多起此類案例。大連機場一位負責人透露，10月24日，電子機票僅僅實行不到一周時間，北京首都機場就有3名乘客被騙。他們都是通過手機短信和訂票卡片上


多市晨報
A
版
18/11

On-line Transactions Risks

- Bogus sites
- Fraudulent merchants (crooks)
- Interception of financial and/or personal information
- The tool (web browser, the Operating System, the wired / wireless network)

How to be Safe?

- Know Thy Dealers
- Ensure Secure Connections / Transactions
- Keep Thy Passwords “secret”
- Payment Methods
- Keep Records
- Check Financial Statements
- Use Different E-mail Address
- Privacy
- Harden Thy Computer



KNOW THY DEALERS

REPUTABLE?

TRUSTWORTHY?

Know Thy Dealers

- Business' Name
- Mailing Address, **more than P.O. Box**
- Telephone
- Is the merchant local or international?
- Is it an authorized seller? or electronic agent?
- Descriptions or pictures of the product

Know Thy Dealers

- Authenticity of the product (counterfeit)
- Ask for a paper catalog / brochure
- Cost: Price, Shipping, Taxes
- Delivery time
- Warranty Information
- Manager's name

Know Thy Dealers

- Return Policy – damaged product, stocking fee, time limit, e.g. within 30 days
- Refund Policy
- Compliant Policy – mediation, arbitration
- Privacy Policy
- Background Check / Better Business Bureau (BBB) (www.bbb.org) / members of related organizations, e.g., Chamber of Commerce

Know Thy Dealers



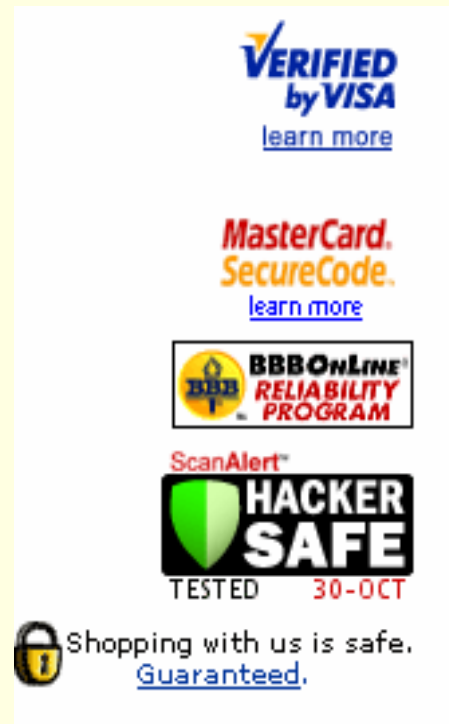
Make Privacy Your Choice



Know Thy Dealers



Know Thy Dealers



Know Thy Dealers

- How do you come to know the merchant?
 - Word of mouth?
 - Google?
 - Unsolicited e-mail, aka spam, scam?

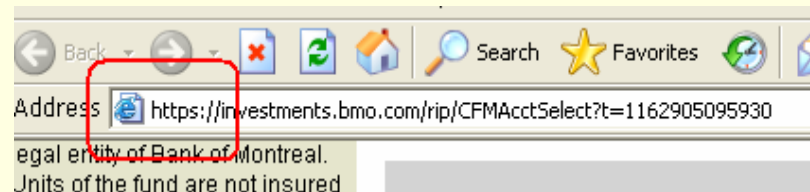
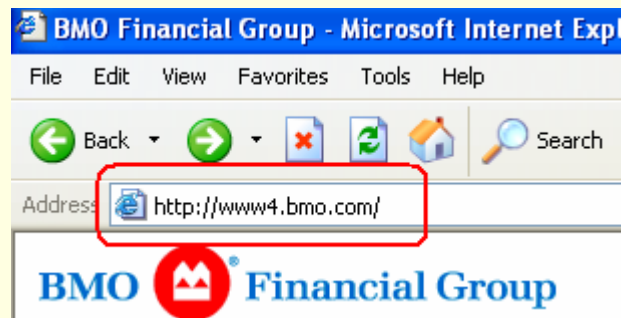


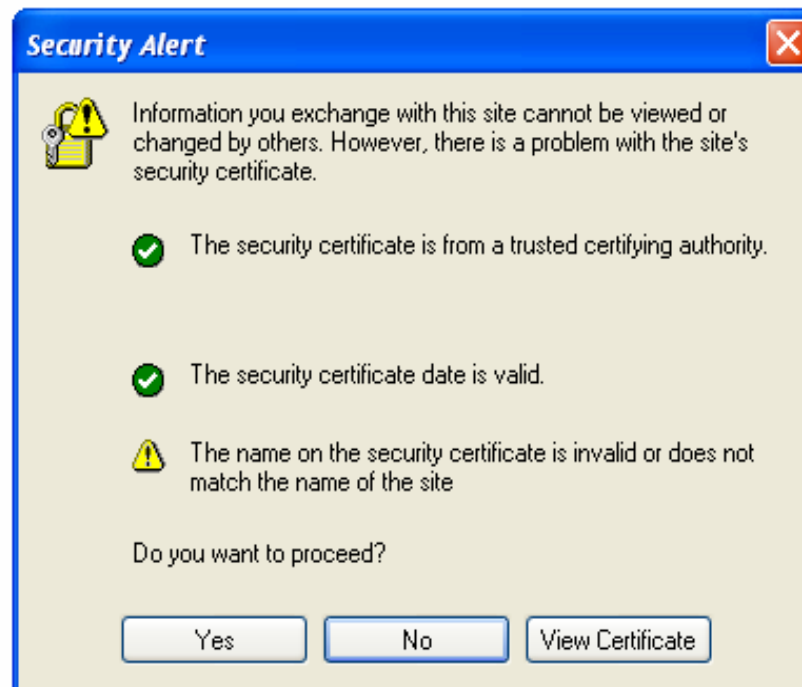
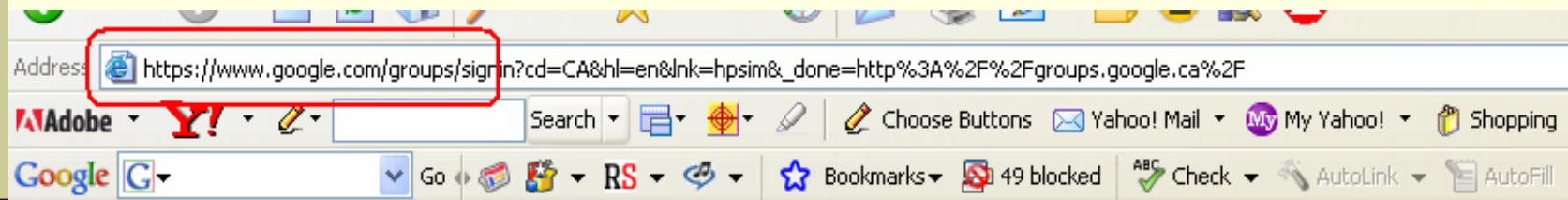
ENSURE TRANSACTIONS SECURE?

Ensure Transactions Secure

- The browser
 - http → https
 - Icon – lock

Ensure Transactions Secure





Ensure Transactions Secure

- Check for security icons before giving your personal identifiable information (PII) (vs personal information), e.g.,
 - SIN, driver's license, credit card numbers, vehicle registration plate number
- Always log out of a web site when you are through
- Disconnect from Internet if you are not using it.



**KEEP THY PASSWORD (S)
SECRET!**

Keep Thy Passwords Secret

- Uses of different password (s) for different function (s).
 - Login password
 - Authorization password
- Use combination of numbers, letters, and symbols, e.g., e@sy4u, 1T1sEc, ccUe
- Change the passwords often, 90 days, 180 days
- **Don't** share your password
- **Don't** enable the “save password” option if prompted to do so.



PAYMENT METHODS

Payment Methods

- Pay by Credit Cards, **No Debit Card**
 - Protected by the Fair Credit Billing Act (U.S.)
 - Right to dispute charges for goods or services that you never ordered, never received, or were mis-represented to you.
 - If a thief has used your credit, you are usually responsible for the first \$50.
- Paypal

KEEP RECORDS

Keep Records

- The order
- The confirmation number.
- The amount (\$\$) of the items, shipping and handling fees
- Warranties
- Delivery Dates

Check Financial Statements

- Bank Statements
- Credit Card Statements
- Investment Account Statements

Use Different E-mail Address

- Do not use your primary e-mail address in online submissions
- Devote one credit card, low credit limit, to online purchases
- Avoid using debit cards for online purchases



PRIVACY

Privacy

- Keep your personal, personal identifiable, account and financial information private
 - Personal information: e.g., age, gender, religion, marital status, phone number, date of birth
 - Personal identifiable information: e.g., social insurance number, driver's license, credit card numbers
- Look for a company's online privacy policy

HARDEN THY COMPUTER

Harden Thy Computer

- Apply **latest** patches, service packs
 - Operating systems
 - Web browsers
 - Applications
- Download **latest** virus / spyware pattern files
 - Virus/Worms
 - Spyware - Keystroke loggers, dialers.
- Enable Personal Firewalls
- Scan and remove virus, spyware, etc. **weekly**
- Enable Popup Blocker

POP-UP STOPPER brand ad blocker - FREE popup blocker from ...

Pop-Up Stopper brand **PopUp Blocker** and Ad ~~blocker~~. ~~Pop Up Blocker~~ and Anti Spyware.

... **Download Pop-Up** Professional now and save and additional \$5.00 off ...

www.panicware.com/product_psfree.html - 20k - [Cached](#) - [Similar pages](#)

POP-UP STOPPER BRAND PopUp Blocker Ad Blocker - The Ultimate Pop ...

Pop-Up Blocker and Anti Spyware. Clean with SureClean. Anti-spam stop spam with ... **Pop-Up Stopper Free Edition: Basic ad-blocking for FREE | download now ...**

www.panicware.com/ - 14k - [Cached](#) - [Similar pages](#)

POP UP BLOCKER for Internet Explorer - FREE DOWNLOAD

POP UP BLOCKER - FREE DOWNLOAD - for Windows 98/ME/NT/2000/XP - Internet Privacy and Anti Spam Software Free Downloads.

www.synergeticsoft.com/ - 10k - [Cached](#) - [Similar pages](#)

Popup Blocker Free Download - stop pop up ads and adware removal

Use super **popup blocker** helps you to surf more comfortably by stop **popup** ads.

www.shareware4web.com/ - 15k - [Cached](#) - [Similar pages](#)

Google Toolbar

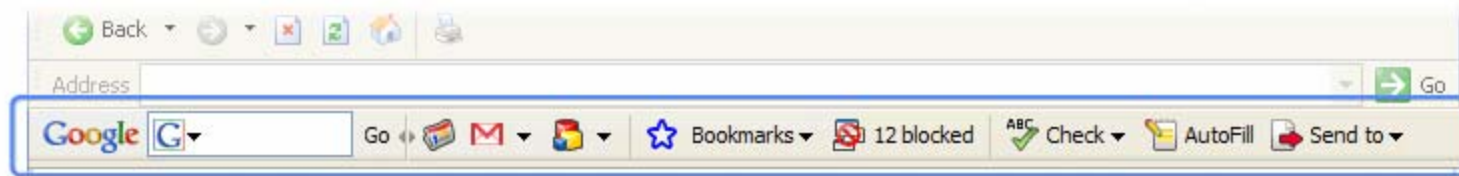
System requirements: • Windows Vista/2000/XP • Internet Explorer 6.0+ • Windows 98/ME users: **Download** previous version • Firefox version also available ...

toolbar.google.com/ - 11k - [Cached](#) - [Similar pages](#)



Select a language - [Help](#)

Take the power of Google with you anywhere on the Web



New! Google Toolbar

-  **Search smarter with instant suggestions** as you type in the search box
-  **Add buttons to the Toolbar** to search your favourite sites — [view button gallery](#)
-  **Bookmark frequently visited pages** and access them from anywhere
-  **Share web pages with friends** via blog, email, or SMS

More Features

- Block annoying pop-ups
- Fill out web forms with one click
- Translate pages into English instantly
- Correct spelling mistakes in your webmail

[Learn more](#)

Fast installation with Google Updater

Install Google Toolbar

System requirements:

- Windows Vista/XP
- Internet Explorer 6.0+
- Windows 98/ME users: [Download previous version](#)

[Firefox version](#) also available

Spyware

The top ten most prevalent spyware threats for the month of February 2007

http://www.marketwire.com/mw/release_html_b1?release_id=222319

Trojan-Downloader.Zlob.Media-C	2.44%
Trojan.FakeAlert	1.32%
Virtumonde	0.68%
Zango.CommonElements	0.40%
WinSpy	0.40%
Zango.SearchAssistant	0.39%
SpySheriff	0.39%
Command Service	0.38%
180solutions.SearchAssistant	0.33%
Trojan-Downloader.Gen	0.33%

Updates

7. March 2007

2007-03-07

Dialer

++ EngergyFactor0190

Keylogger

++ ActivityKeylogger + ActMon-Pro ++ Actual Keylogger

++ FamilyKeyloggerProDemo + Perfect Keylogger

Malware

+ Forbot + Smitfraud-C. (3) ++ SpyDawn ++ Win32.Delf.cc

++ Win32.Hupigon.edt

PUPS

+ CyberDefender

Spyware

+ 007 Spy Software ++ Marketscore.RelevantKnowledge (3)

Trojan

++ Absolute.Launcher ++ Colorado.ClipboardAdmin

++ CtyBank.Sound + Dropper.Mondo + Fake.IKEA-Bill

+ FakeWGA ++ HPT.RSV ++ KBui32.SMTP (5) ++ NetSky.Q (2)

++ Realsearch.Forte + Sallity.Badcro ++ SearchNineX

+ Smitfraud-C.EbayBill ++ Win32.Delf.zq + Win32.Rbot

++ Win32.VB.po ++ Win32.Zhelatin.ah (2) + Zlob.SiteTicket

+ Zlob.VideoAccessActiveXObject + Zlob.VideoKeyCodec

Worm

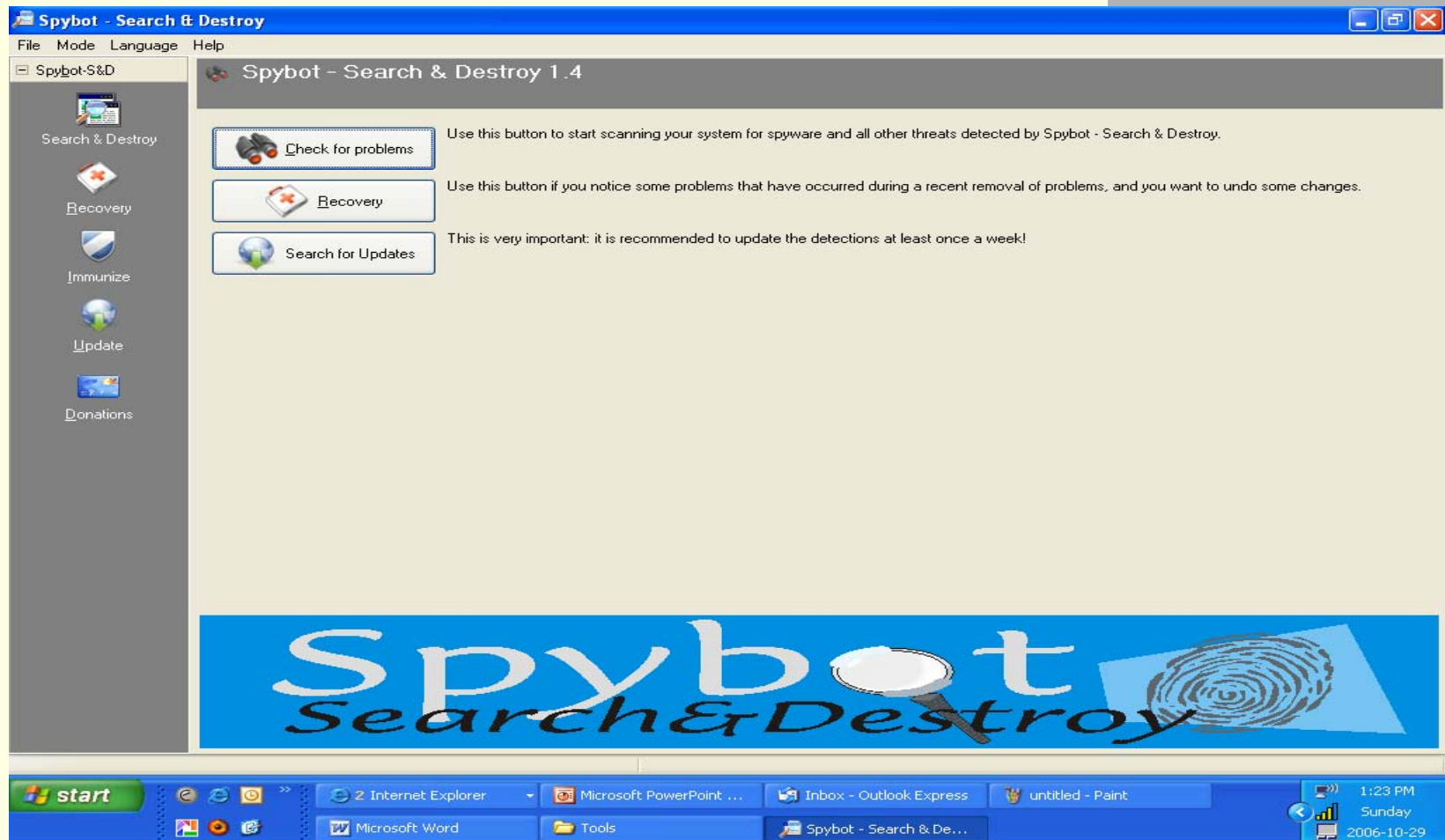
++ NetSky.R

Total: 365619 fingerprints in 62368 rules for 2733 products.

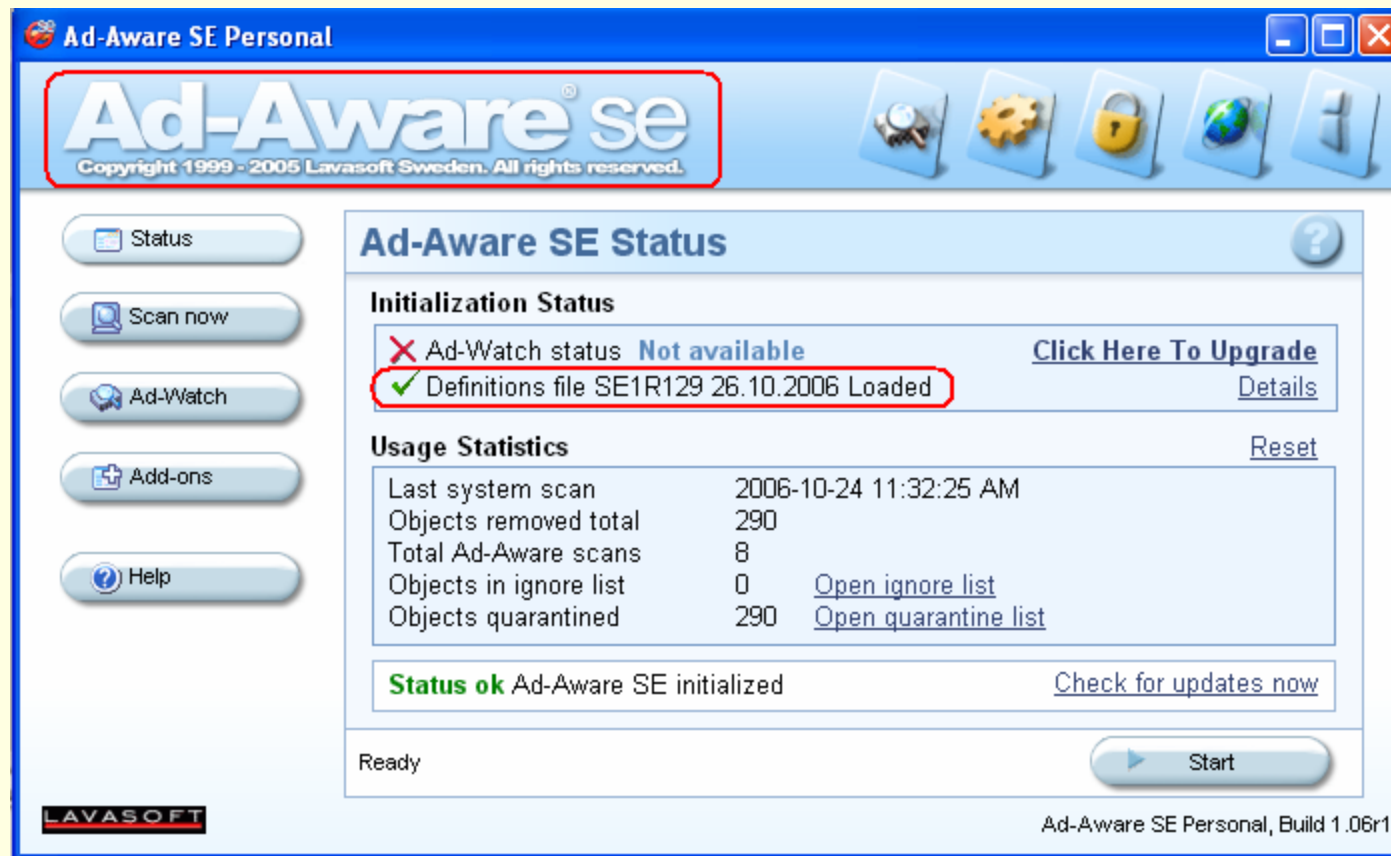


SOME FREE ANTI-SPYWARE PROGRAMS

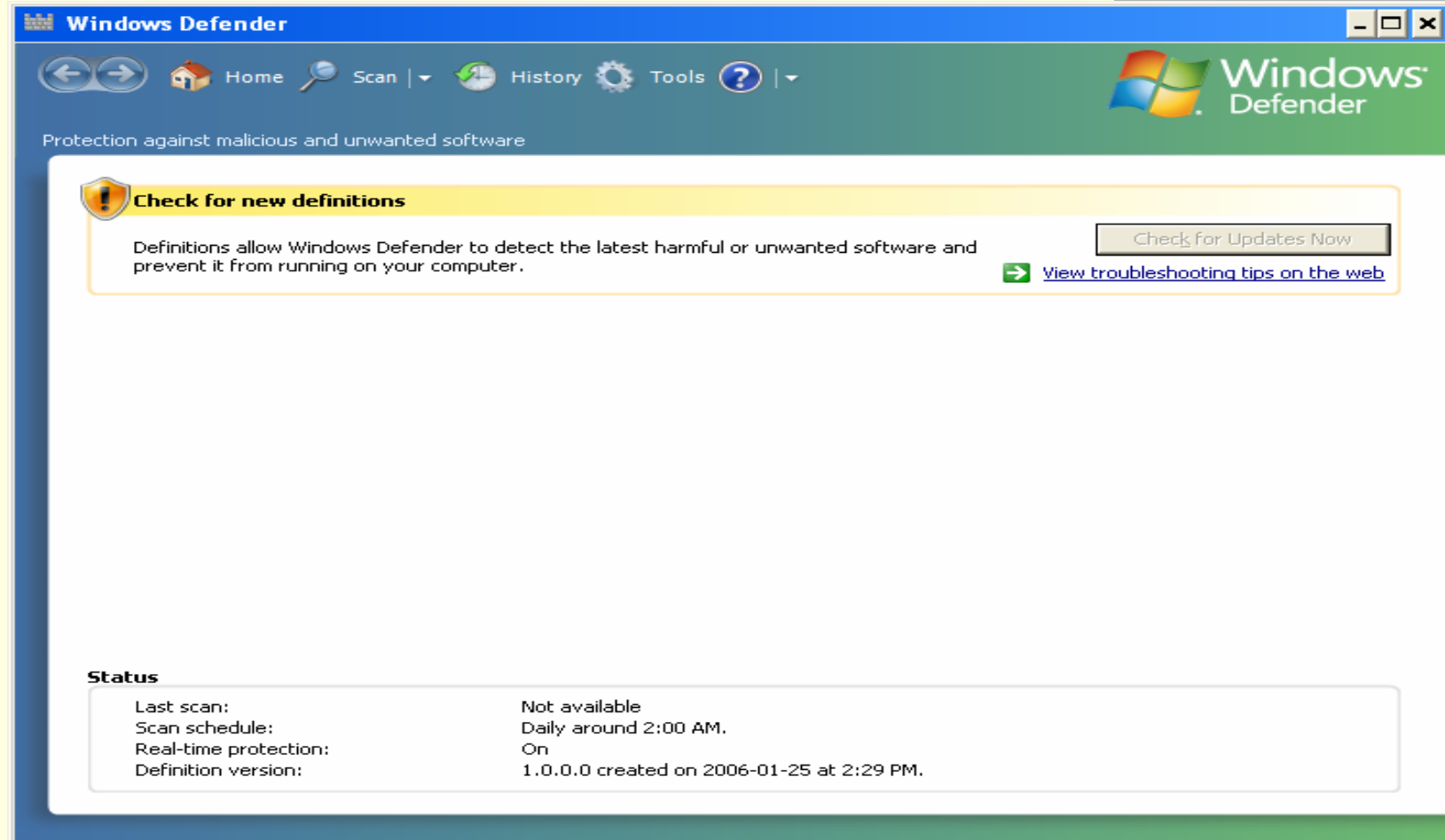
Anti-spyware Programs

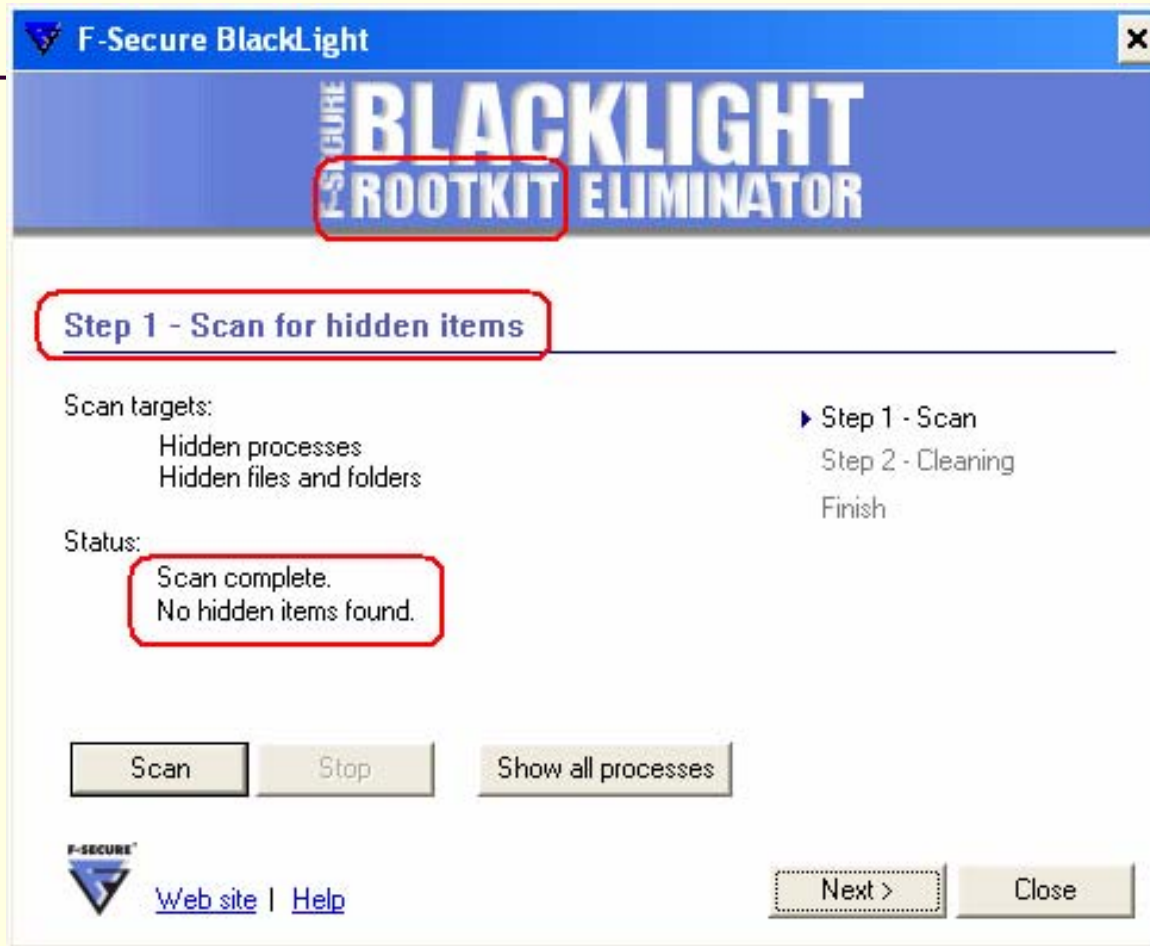


Anti-spyware Programs



Microsoft Windows Defender





Some References

- Privacy Commissioner's Fact Sheet on identity theft

www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp

- RCMP computer crime information

www.rcmp-grc.gc.ca/scams/ccprev_e.htm

- RCMP anti-phone-fraud service

www.phonebusters.com

Some References

- RCMP Scams Frauds

http://www.rcmp-grc.gc.ca/scams/index_e.htm

- Public Safety Portal

http://www.safecanada.ca/esafety/user_e.asp

What To Do If You Become A Victim in **Canada**

Phonebusters by RCMP and OPP

<http://www.phonebusters.com/english/index.htm>

Toll Free: 1-888-495-8501

Fax: (705) 494-4755

Toll Free Fax: 1-888-654-9426

Email: info@phonebusters.com

The Competition Bureau of Canada

1-800-348-5358

Website: www.cb-bc.gc.ca

Email: compbureau@cb-bc.gc.ca

RCMP

- To report an economic crime on-line using RECOL, please visit www.recol.ca

Contact Information

C. K. Lung

cklung@yahoo.com

Q & A Session