Electronic Identity Theft and Basic Security

Prepared for DACS

By

Philip Chen

CCSP, NSA infosec Professional

10-2-2007

Pchen@hi-link.com

Agenda

- Introduction
- Examples
- Effective Security Defenses for Enterprises
- Effective Security Defenses for SOHO
- Basic Security measures
- Q&A

Introduction

- Hi-Link is a premier **solutions** provider.
- Certified Cisco Technology specialization.
- More than a decade of proven experience.
- Focus: Security, Wireless, IPT, Mission Critical LAN/WAN Infrastructure, Network Management.
- SMB,Governments, Enterprises, Healthcares, Financials and Education customers.
- CISSP, CCEA, CCSP, CCDP, CCNP, MCSE certifications.

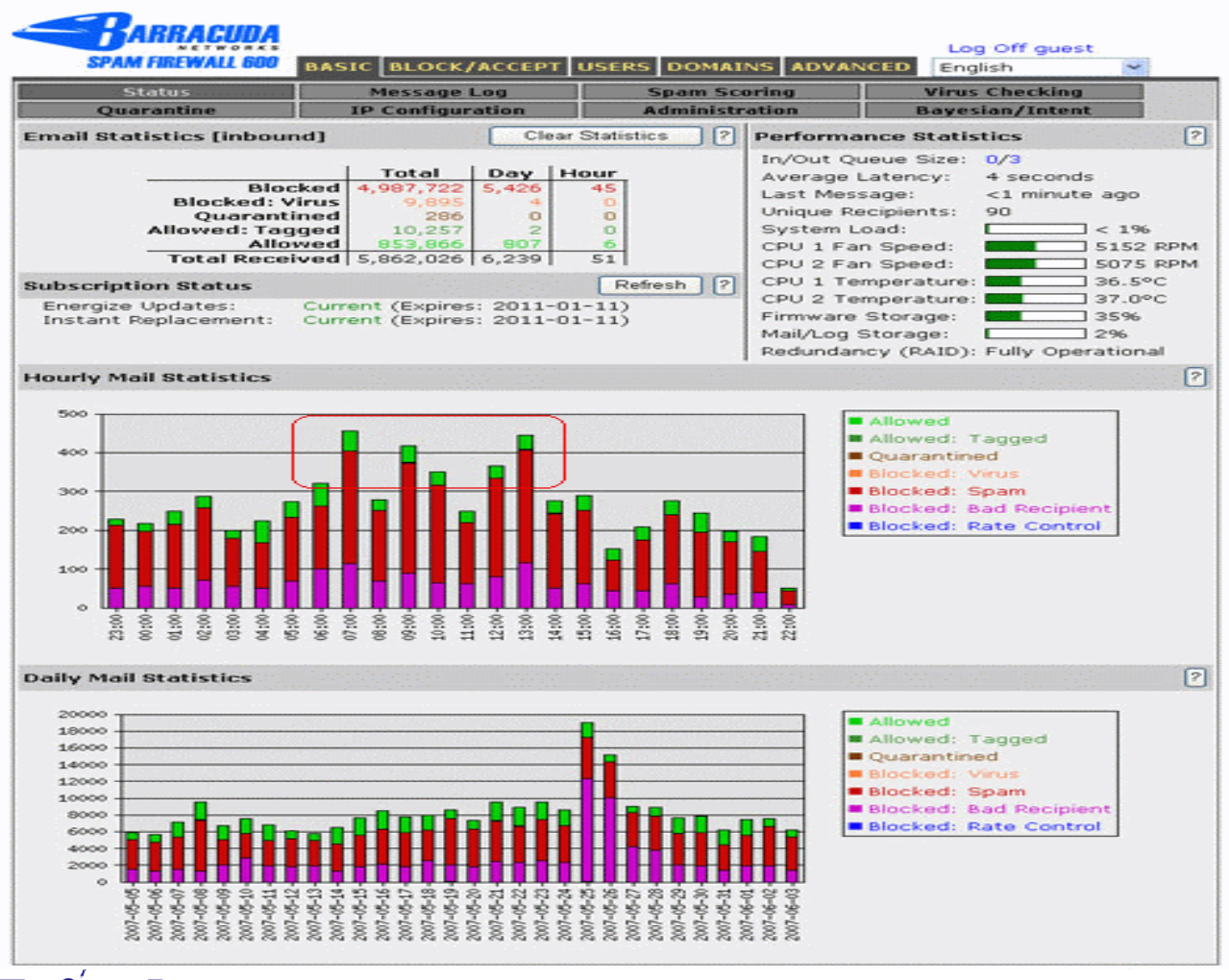
The New Crime Wave

Some federal cases within the last year suggest why identity theft has become one of the fastest-growing forms of white-collar crime:

- A man was indicted in Miami on identity theft-related charges relating to his alleged filing of false federal tax returns in the names of 614 Florida prisoners, seeking more than $3 million in fraudulent refunds.
- A woman was convicted in Seattle on various identity theft-related offenses involving at least $464,000 of fraud under false identities that the defendant and her co-conspirators had set up.
- A man was sentenced in Los Angeles to federal prison for managing an auto theft and identity theft ring, in which conspirators stole biographic and credit information from real people and used the data to buy luxury cars amounting to more than $200,000.

Source:http://www.usdoj.gov/criminal/fraud/

Garbage in, Garbage out



Sources of ID Theft

- Dumpster Diving

  Information collected from your garbage.

- Social Engineering

  Information divulged by you or someone or company who has your information.

- Change Address Form

  Filling out falsified change of address form in your local post office to divert your billing and other sensitive information to an alternate address.

Sources for ID Theft (Cont.)

- **Phishing**

  ID theft using embedded Malware, viruses and pop- up messages in an email or a web page which tricks you into believing that it is something harmless.

- Property Theft

  ID theft from information obtained from stolen laptops, Desktops, harddrives, USB drives, and your wallets.

- **Security Breach**

  ID theft by comprising your computer in the form of network attacks.

What is Phishing

It is the act of tricking you into divulging sensitive private information such as social security number and bank accounts. It is usually done by using viruses, malwares, pop-up messages embedded in a SPAM email or a falsified web link.

Phishing

URL Obfuscation, clicking on the following do not direct you to the official page of ***http://www.mybank.com***

- http://www.mybank.com.ch/
- *http://mybank.com:ebanking@210.134.161.35/login.htm*
- http://mybank.com/ebanking?URL=http://evilsite.com/phishing/fakepage.htm
- http://mybank.com/ebanking?page=1&response=evilsite.com%21evilcode.js&go=2

Phishing (Cont.)

- URL Obfuscation, You may by asked to click on a URL like this in an email:

http%3A%2F%2F3515261219%2Fphishing%C0%AEfakepage%2Ehtm

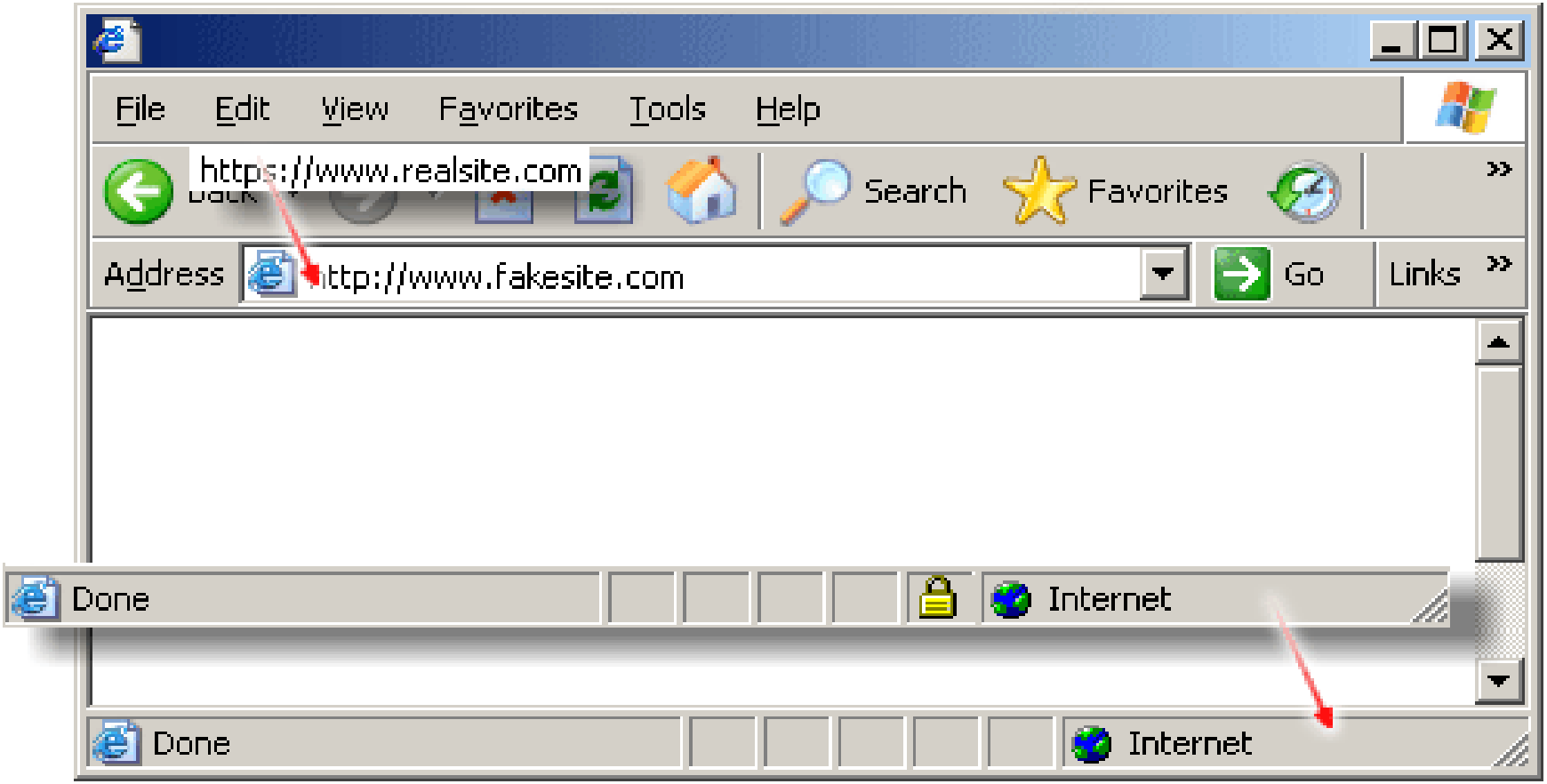
This URL is encoded in Unicode to disguise its evil identity. The real website is really:

http://evilsite.com/phishing/fakepage.htm

- Key logger: a piece of hardware or software installed on a computer to silently record your key strokes and replay them back to the perpetrator later

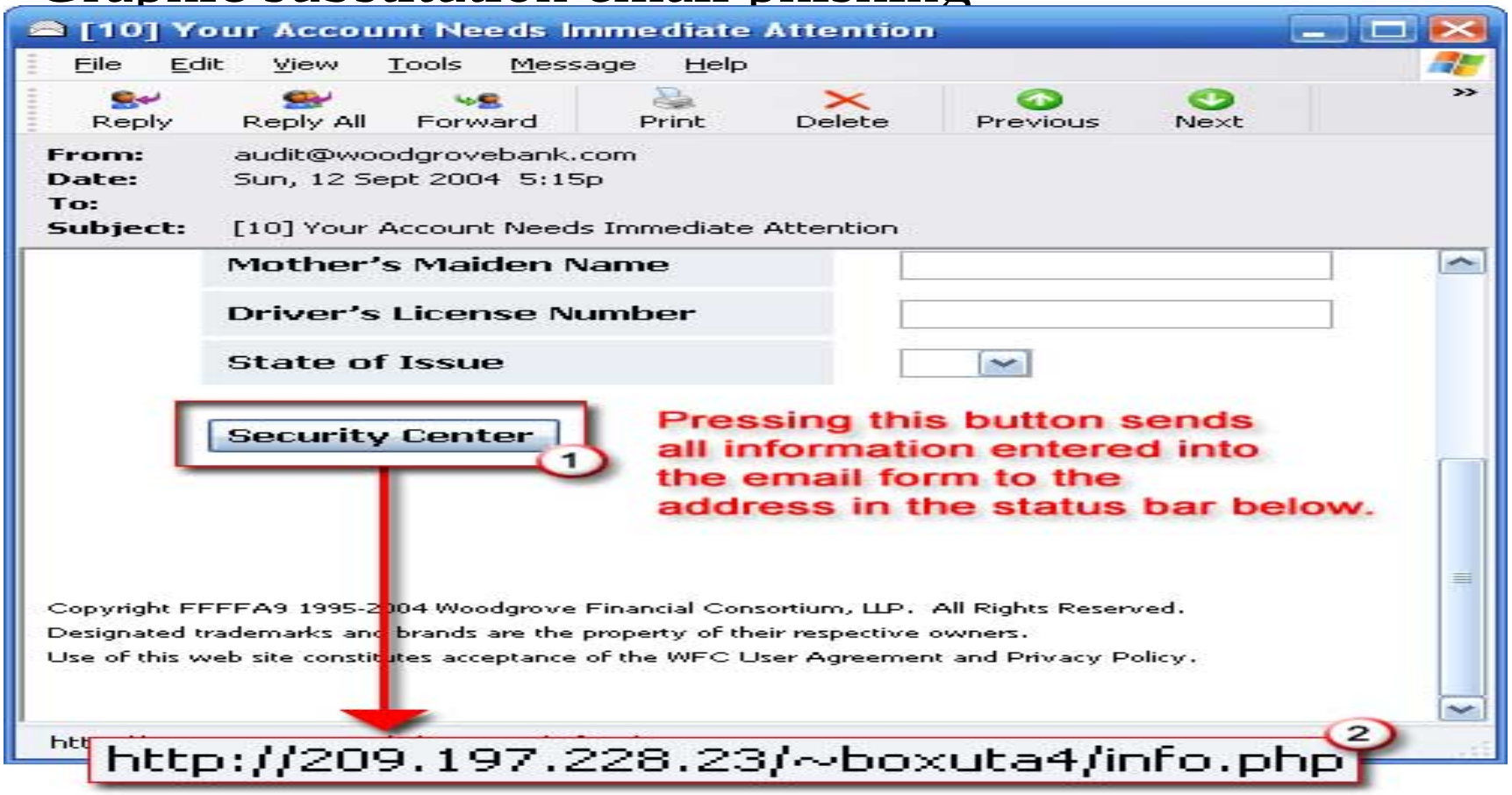
Phishing (Cont. 1)

Address bar and security status substitution



Phishing (Cont. 2)

Graphic substitution email phishing



Property Theft

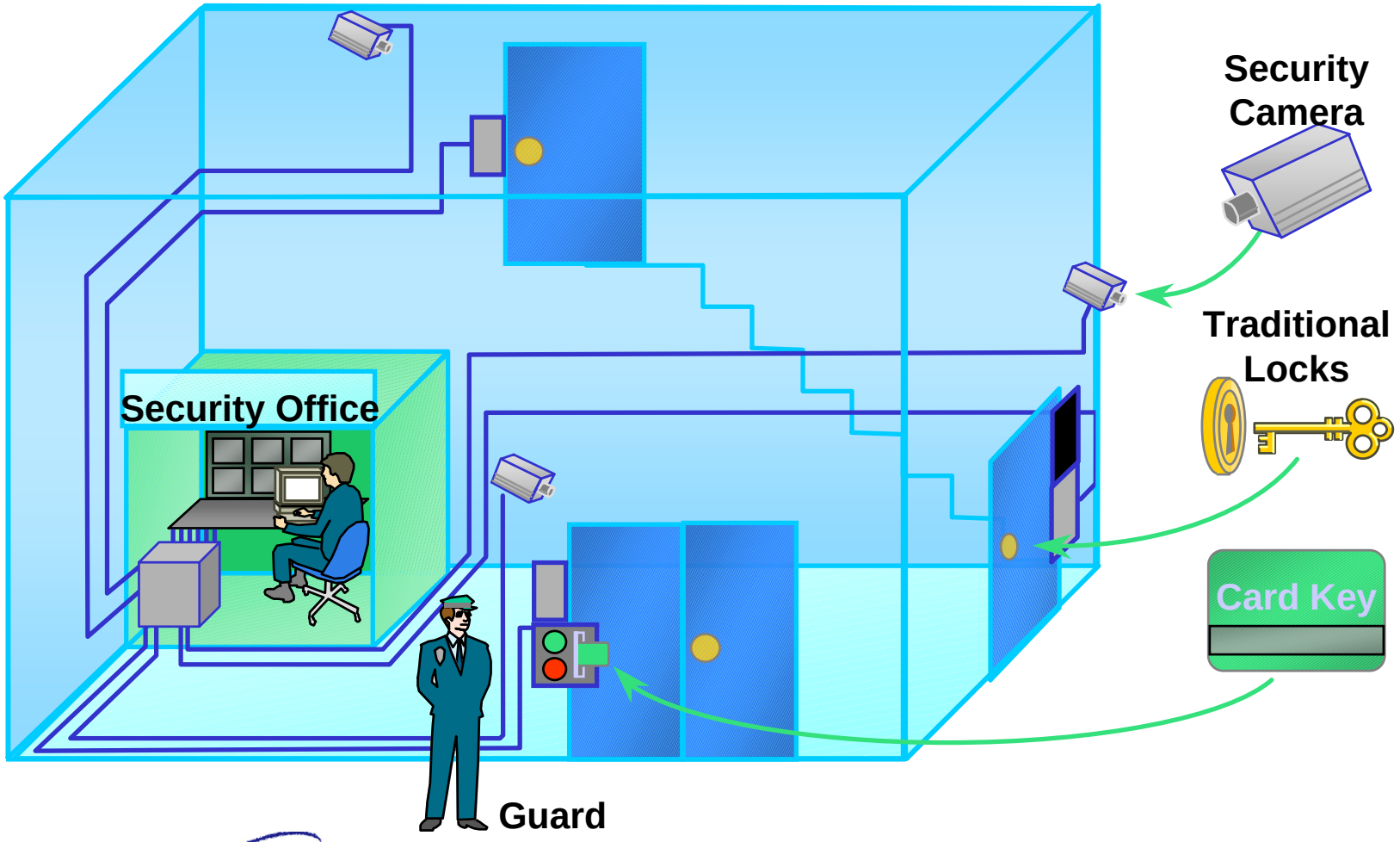
- Stolen computer with you personal and financial information
- Stolen unencrypted USB drives with your personal information

Security Breach

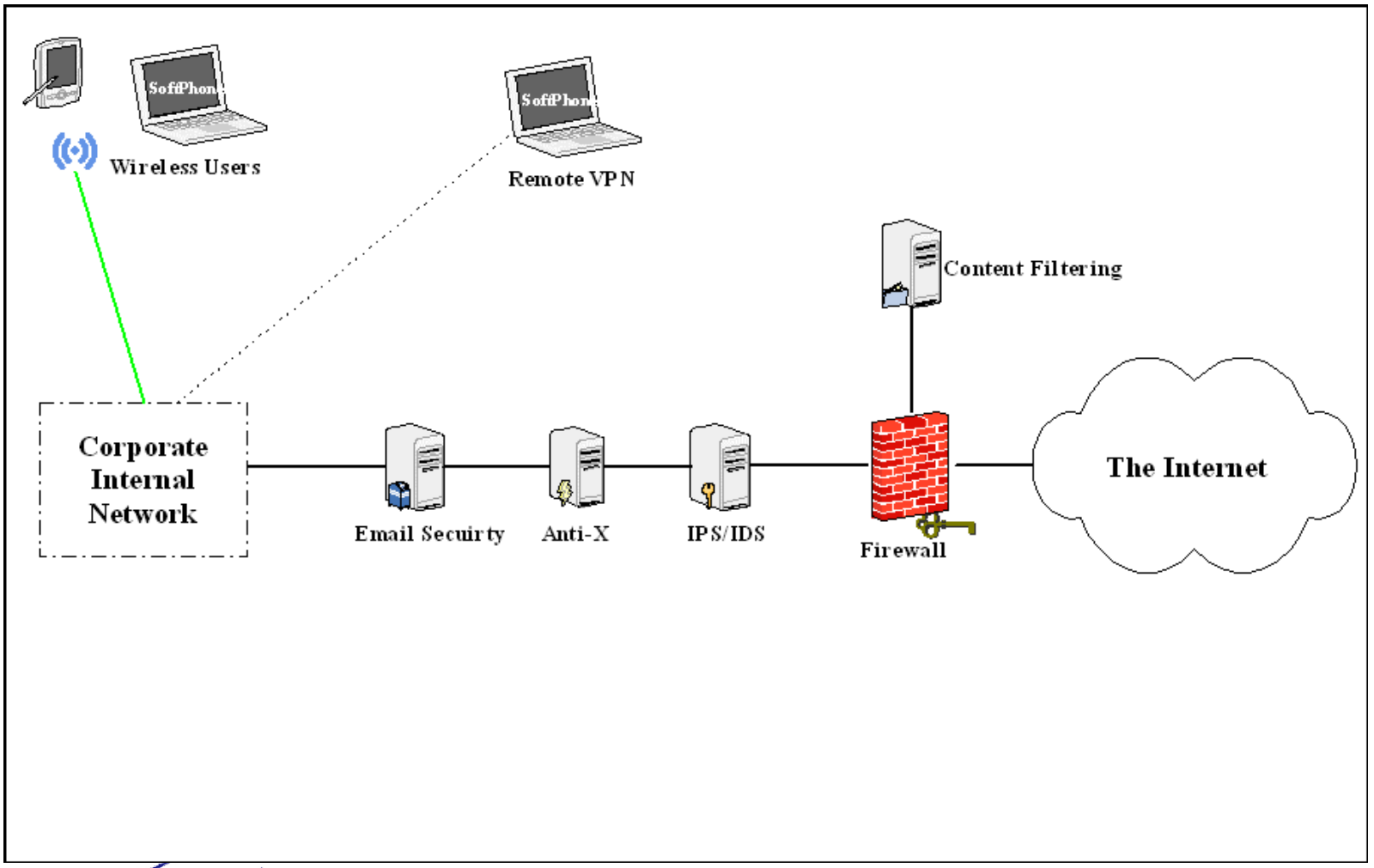
- Compromising of your firewall
- Wireless network intrusion
- Virus infection
- Malware and Trojans installed unkown to you
- Hackers Can Now Deliver Viruses via Web Ads

http://online.wsj.com/public/article_print/SB118480608500871051.html

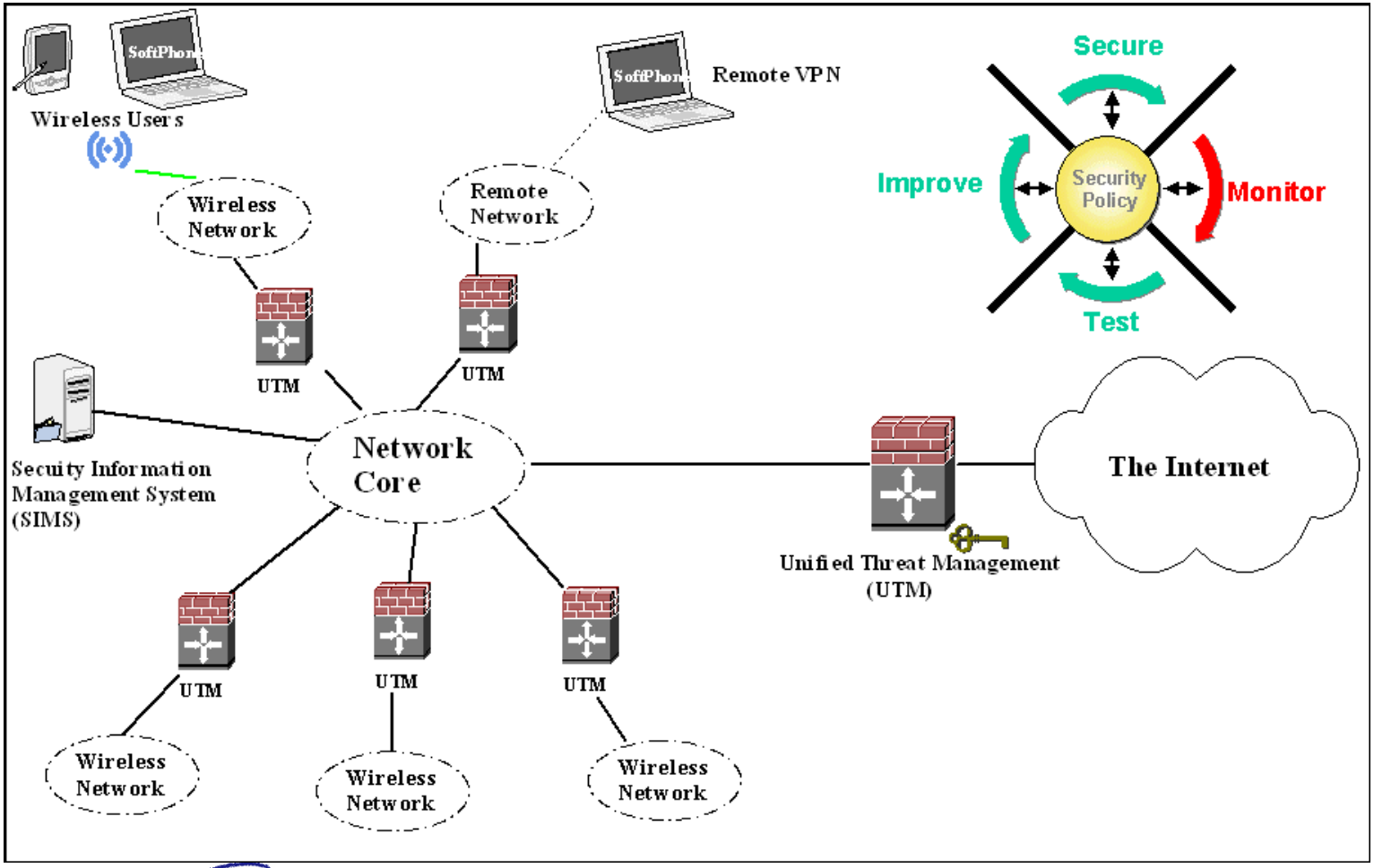
Effective Defenses is a security system working together



Effective Defenses for Enterprises (Old Security Model)



Effective Defenses for Enterprises (New Security Model)



Effective Defenses

- Two things in life are 100% certain:Death and Taxes.
- 100% security unfortunately is not one of them, doesn't matter how much money and effort is thrown at it.
- Security is about managing risks. Minimalist approach.

Risk = Probability + Consequence

Effective Defenses (Cont.)

- Reducing the probability of infection.
- Understand the impact if you were an ID theft victim before you become a victim so you can plan ahead and reduce the damage.
- You are in less risk if you reduce the sum of these two.
- Use common sense. If it looks too good to be true. It probably is!
- Obtain and check your credit report annually.

http://www.annualcreditreport.com 877-322-8228; Equifax;Experian;TransUnion

Effective Defenses (Cont 1.)

- Do not post your email address on public websites or user forums. This will greatly reduce amount of SPAM sent to you.
- If something looks out of place on a web page or in an email, beware.
- Email addresses can be easily spoofed. bank, financial and medical industry will never send you emails asking for confidential information. These industries are regulated and governed by laws such as HIPAA, Sarbanes-Oxley.

Basic Security

- The most basic: turn on firewall on your Windows XP. Use anti-virus and anti-spyware applications. Many such good applications are free.

  - AVG anti-virus from http://www.grisoft.com/

  - Spybot from http://www.safer-networking.org/en/index.html

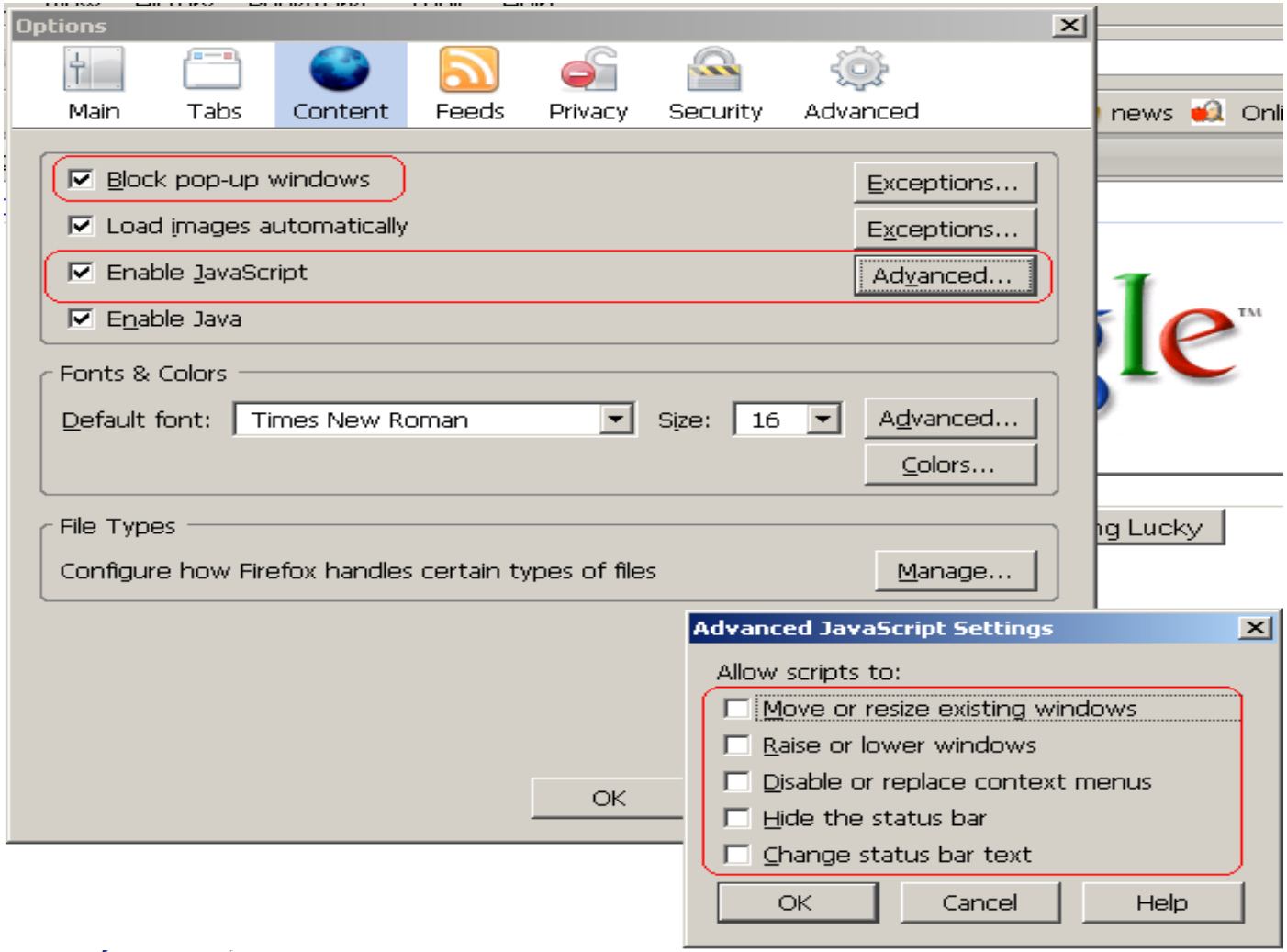
  - Free online virus scanning http://housecall.trendmicro.com/

- Upgrade to IE7 or Firefox 2.0

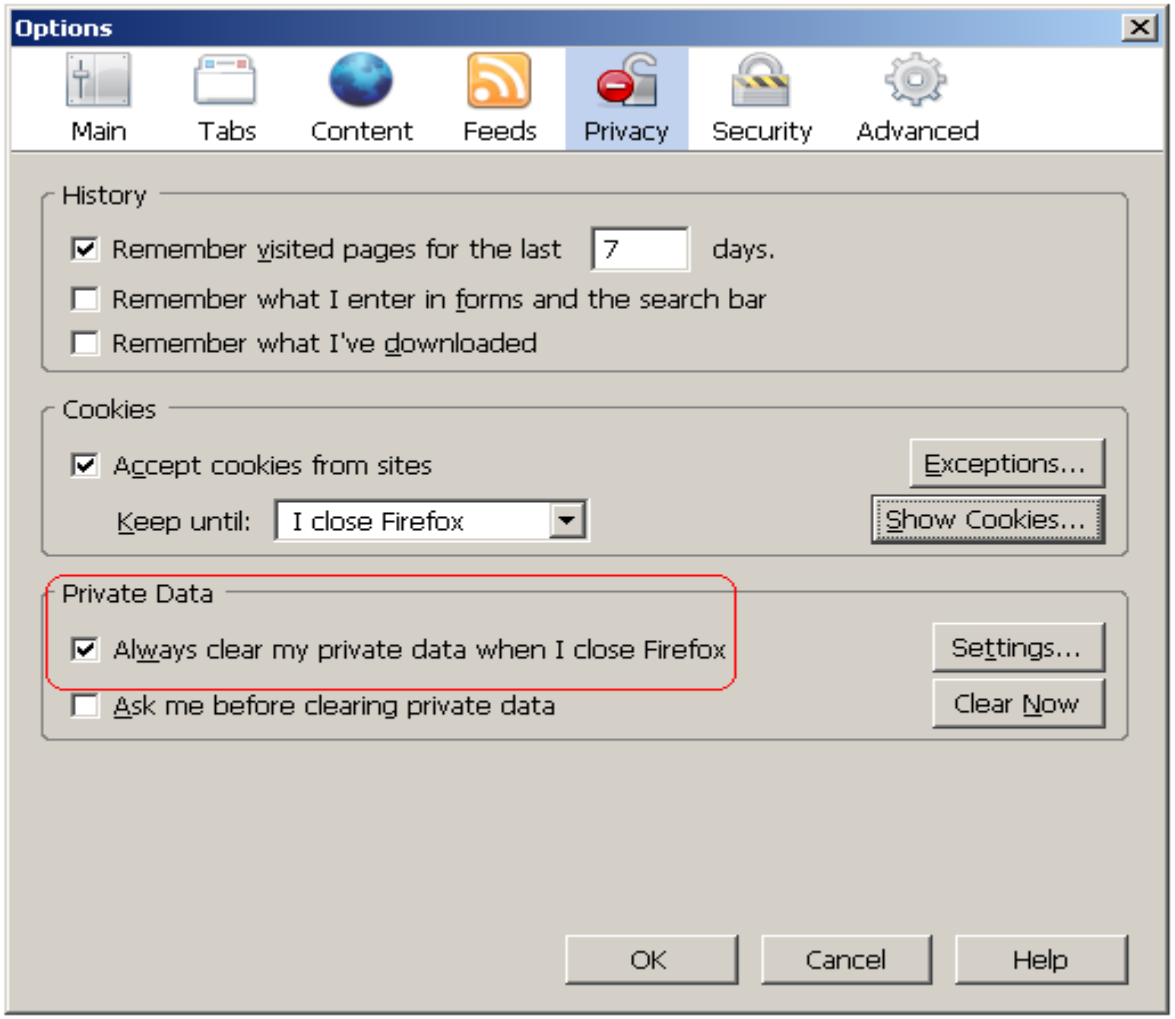
- Signup for Opt Out of NAI Member Ad Networks. Do not call equivalent

http://www.networkadvertising.org/managing/opt_out.asp

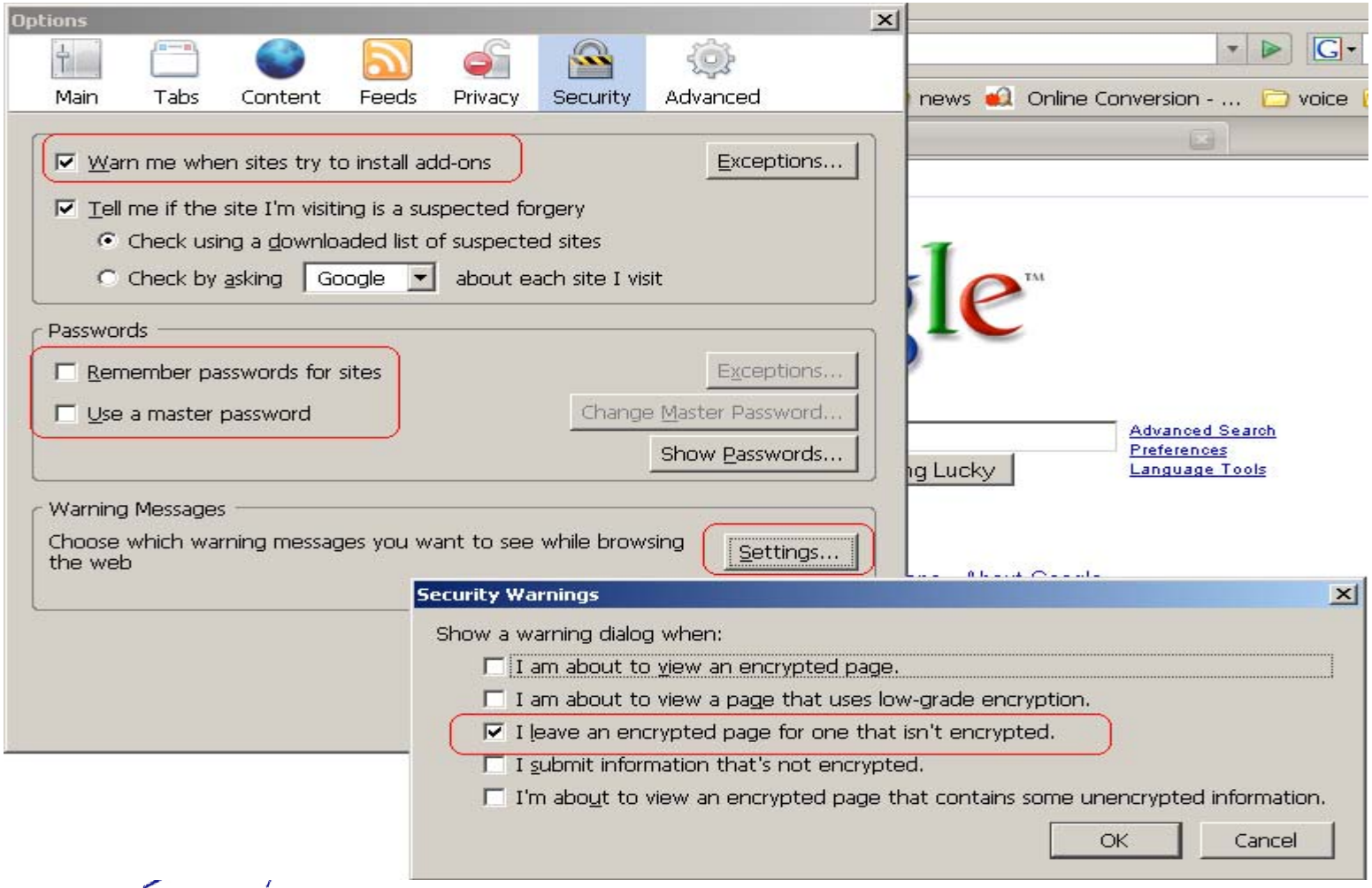
Basic Security-Use What You Already Have



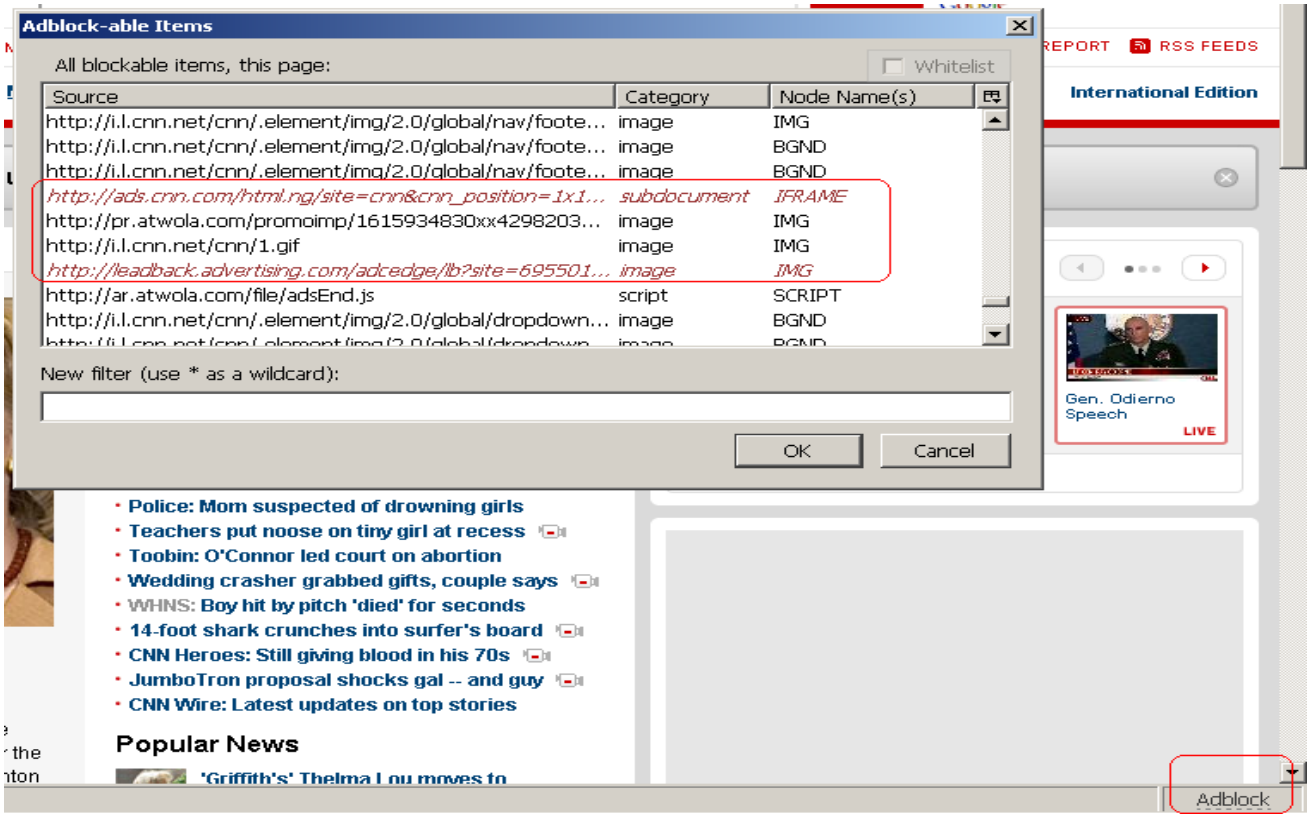
Basic Security-FireFox Privacy



Basic Security-FireFox Security



Basic Security-The best of FireFox



http://adblock.mozdev.org/

What you see is not what you will get

- How about this:

Be on the lookout

❖Be on the lookout for suspicious websites and emails. What does it tell you if your bank website prompts you with this:

Q&A