

# **"Stop, Think, Click"**

**A Primer on Internet Safety**

# "Stop, Think, Click"

## October Named National Cyber Security Awareness Month

- "Stop, Think, Click" campaign originated by the National Cyber Security Alliance
- New York Governor George Pataki is one of the first governors to sign a proclamation in recognition of the importance of cyber security.
- Two-day cyber security summit in the state capital of Albany hosted by Government Technology Conference and the State of New York.
- Focus on:
  - Teaching children to stay safe online
  - How state and local government officials can improve the state of cyber security in the agencies they manage.

# Identity Theft

# Identity Theft

What is Identity Theft?

- Identity Theft is the malicious use of another persons' identification or personal information for:
  - Obtaining credit under that identity for financial gain
  - Ruining credit under that identity for revenge
  - Impersonating another to commit a crime

How does someone obtain my identity?

- Physically
- Social Engineering
- Online Activity

# Identity Theft

How does someone obtain my identity?

- Physically
  - You get mugged
    - More likely to steal your wallet for documents rather than cash.
  - Someone directly uses your information for something other than your implied intentions
    - Double swiping, merchant fraud
  - Your data is taken from a company you have dealt with
    - Stolen backup tapes
    - Compromised company networks
    - Vengeful employees

# Identity Theft

How does someone obtain my identity?

- Social Engineering
  - You explicitly give out personal information directly to someone.
    - Cold Calling
    - Chat rooms and Instant messaging
    - Web spaces
  - Criminals obtain small disparate pieces of personal information from various areas, and recreates full identity information from it.
    - Dumpster Diving
    - Shadowing
    - Eavesdropping

# Identity Theft

How does someone obtain my identity?

- Online Activity
  - Intentionally steering users to a fake website to have user enter private information
    - Phishing
    - Domain Hijacking
  - Tracking what a user does and where they go online to grab personal information
    - Spyware
    - Keyloggers
    - Man-in-the-Middle Attacks

# Recent News

- CardSystems Solutions victim of computer virus that captured 40,000,000 customers' credit card information.
- Citigroup "loses" backup tape containing 3,900,000 customers' account information including SSNs.
- Bank of America / Wachovia victim of employee fraud when former bank employees sold 108,000 customer records illegally.
- Time Warner "loses" backup tape containing 600,000 current and former employees' account information.
- Information Broker at LexisNexis victim of theft of 310,000 personal data records.
  - Hackers ranged in age from 16-23
- "Collectively, nearly 50 million accounts over 12 different companies have been exposed to the possibility of identity fraud since 2/15/05"
  - Source: Patrick Gray, Internet Security Systems, "Navigating the New Thread Landscape"
- AOL Employee indicted for selling personal information of millions of customers
- DMV employee caught selling valid driver's licenses to illegal recipients

# Local News

## Lawsuits: White Plains home to scam

January 26, 2006 •• The Journal News

Software maker allegedly preyed on fears over spyware Julie Moran Alterio The Journal News A White Plains company deceived Internet users into believing their PCs were infected by spyware and then sold them fake repair software that left them more vulnerable to attack, according to a lawsuit filed by the Washington State Attorney General's Office. Consumers were tricked into downloading the software, called "Spyware Cleaner"

...

# Malware

# Statistics

- Instant Messaging Threats:
  - MSN Messenger: 64%
  - AOL / ICQ: 25%
  - Yahoo: 11%
- Spam:
  - 12,900,000,000 per month
  - 71% of all internet mail
  - 100% sent via zombies
- Zombies:
  - 168,013 new zombies *per day*
  - United States: 17 - 20%
  - China: 14.56 – 20.68%
- Phishing:
  - 3,054 active sites
  - Growth rate: 15% annually
- Spyware Threats:
  - ABetterInternet: 10.94%
  - IST Bar: 8.66%
  - ShopAtHome: 7.41%
  - AvenueMedia: 6.20%
  - CoolWebSearch: 5.95%
- Online Fraud:
  - United States: 84.9%
  - Canada: 5.2%
- Keylogger Targets:
  - Brazil: 501
  - United States: 80
  - Growth Rate: 200% in first six months of 2005

# Spam

## *What is Spam ?*

- Spam is unsolicited email which operates under the premise of offering something for sale.
  - Similar to the “cold-calling” advertising technique
  - Not necessarily malicious in and of itself
- Intent of a spam:
  - Create a sale of an item.
- Secondary intents
  - Denial of Service through massive amounts of human created email.
- How spam propagates
  - Mass email generators in unregulated countries (Asia, Africa, et al)
  - Smaller amount of Email generated through countless zombies

# Spam (example)

**From:** MicahzmFaulkryxc@netzero.net  
**Date:** Wednesday, January 25, 2006 10:55 AM  
**To:** checco@checco.com  
**Subject:** Your bill Consolidation Account

Dear Home Owner,

Your credit doesn't matter to us! If you OWN real estate and want IMMEDIATE cash to spend ANY way you like, or simply wish to LOWER your monthly payments by a third or more, here are the deals

we have TODAY (hurry, these offers will expire TONIGHT) :

\$488,000.00 at a 3.67,% fixed-rate  
\$372,000.00 at a 3.90,% variable-rate  
\$492,000.00 at a 3.21,% interest-only  
\$248,000.00 at a 3.36,% fixed-rate  
\$198,000.00 at a 3.55,% variable-rate

Hurry, when these deals are gone, they are gone!  
simply fill out this one-minute form...

Don't worry about approval, your credit will not disqualify you!

<http://au.geocities.com/harcourt72361gaston47797/>

sincerely,  
Maggie Sharp  
Approval Manager

anomaly may befall it's brainstorm and corny it  
bronchus but airborne try chorine or buried may  
bitumen not coward on carpathia in boy a  
catastrophe not director in deregulate the affix or  
citizenry some armature be clifton not audit but  
consume but alexandre may colloquy but charybdis on  
<http://au.geocities.com/harcourt72361gaston47797/>

# Phishing & Pharming

## *What is Phishing and Pharming ?*

- Phishing is an email that purports to be from a trusted web source, pharming is email that points to a “look-alike” site.
- Intent of phishing and pharming:
  - Traps the user into giving out information unknowingly for a specific company’s site.
- Secondary intents
  - Sabotages real emails from lawful companies.
- How phishing propagates
  - Brute force mailers
  - Legally/illegally sold mailing lists

# Pharming (Example 1)

**From:** Security@eBay.com  
**Date:** Sunday, November 16, 2003 3:29 AM  
**To:** checco@checco.com  
**Subject:** Activate your account for security reason

Hello,  
Dear member,



eBay Security Department have investigated logins from ip 212.156.4.69 and 212.156.4.68 with your account.

The Department reported that they are worried that your account might have been stolen and some one may be access your eBay ID and password.

It might have been captured by spy software that some one put in your machine,So...

We put your account under security mode (not restricted) , and you should follow some steps to secure your account.

- 1- You should update your account in our SSL server to prevent it from to be remotely accessed by anyone(Secure Accounts Server) click the link to update [Click Here](#)
- 2- Wait 24 hours to detecting and routing of remote logins machine and you will be e-mailed from [support@ebay.com](mailto:support@ebay.com) to continue using our service.
- 3-Try to re-setup your operating system and delete all files you suspect in.

With Best Wishes,  
eBay Security Department Assistant,  
Richard Michael.



# Phishing (Example 2)

**From:** Foundmoney Confirmations  
**Date:** Thursday, January 12, 2006 8:24 PM  
**To:** [REDACTED]  
**Subject:** FoundMoney Notice: There is a substantial amount of cash under the [REDACTED] name

**OFFICIAL** CLASS A COMMON STOCK  
**STATUS: ISSUED**

**FOUND U.S. DENOMINATED FUNDS NOTIFICATION**

32-188-995 65 **CONFIRM IMMEDIATELY!** [REDACTED]

Dear FRIEND [REDACTED]

Our records show that money in the [REDACTED] name has yet to be claimed.

This is not money in dispute. This is money that is rightfully yours, but have failed to been notified about. Don't wait until it is to late. Claim the money that is rightfully yours today!

[Click here to claim the cash that is rightfully yours.](#)

Authorized Signature: [Signature]

**VALID**

CLASS A  
CE12515

**CLICK HERE**

# Hoaxes

## *What is a Hoax ?*

- Hoaxes work under the premise of FUD – fear, uncertainty and doubt.
  - FUD is the second-most effective advertising technique
- Intent of a hoax:
  - Cause mass hysteria.
  - Promote download of “rogue” anti-virus software
- Secondary intents
  - Denial of Service through massive amounts of human created email.
  - Promote sale or download of legitimate anti-virus software.
- How hoaxes propagate
  - Word of mouth,
  - Email,
  - News media.

# Hoax (example)

My daughter & I had just finished a salad at Neiman-Marcus Cafe in Dallas & decided to have a small dessert. Because our family are such cookie lovers, we decided to try the "Neiman-Marcus Cookie". It was so excellent that I asked if they would give me the recipe and they said with a small frown, "I'm afraid not." Well, I said, would you let me buy the recipe? With a cute smile, she said, "Yes." I asked how much, and she responded, "Two fifty." I said with approval, just add it to my tab.

Thirty days later, I received my VISA statement from Neiman-Marcus and it was \$285.00. I looked again and I remembered I had only spent \$9.95 for two salads and about \$20.00 for a scarf. As I glanced at the bottom of the statement, it said, "Cookie Recipe - \$250.00." Boy, was I upset!! I called Neiman's Accounting Dept. and told them the waitress said it was "two fifty," and I did not realize she meant \$250.00 for a cookie recipe. I asked them to take back the recipe and reduce my bill and they said they were sorry, but because all the recipes were this expensive so not just everyone could duplicate any of our bakery recipes....the bill would stand. I waited, thinking of how I could get even or even try and get any of my money back.

I just said, "Okay, you folks got my \$250.00 and now I'm going to have \$250.00 worth of fun." I told her that I was going to see to it that every cookie lover will have a \$250.00 cookie recipe from Neiman-Marcus for nothing. She replied, "I wish you wouldn't do this." I said, "I'm sorry but this is the only way I feel I could get even," and I will.

So, here it is, and please pass it to someone else or run a few copies....I paid for it; now you can have it for free. (Recipe may be halved):

2 cups butter  
4 cups flour  
2 tsp. soda  
2 cups sugar  
5 cups blended oatmeal\*\*  
24 oz. chocolate chips  
2 cups brown sugar  
1 tsp. salt  
1 8 oz. Hershey Bar (grated)  
4 eggs  
2 tsp. baking powder  
3 cups chopped nuts (your choice)  
2 tsp. vanilla

Cream the butter and both sugars. Add eggs and vanilla; mix together with flour, oatmeal, salt, baking powder, and soda. Add chocolate chips, Hershey Bar and nuts. Roll into balls and place two inches apart on a cookie sheet. Bake for 10 minutes at 375 degrees. Makes 112 cookies.

\*\* measure oatmeal and blend in a blender to a fine powder.

# Other Email Scams

These Email Scams trick users into believing they will make quick money by participating in an illogical set of circumstances.

- Intent of scams:
  - Fool the user into giving money or bank account information.
- How scams work
  - Pay for Service
  - Good Faith
  - Down Payment
  - Pyramid Scheme

# Scam (example)

FROM: ALHAJI TAJUDEEN .K. ABACHA

E-mail: [akudeenky2k@yahoo.com](mailto:akudeenky2k@yahoo.com)

ATTN: John C. Checco

Sir

PRIVATE AND CONFIDENTIAL

I got your contact from our Chambers of Commerce where your name was listed as a reputable company. I therefore decided to contact you to assist me in the mentioned venture below.

I am the second son of General Sanni Abacha, the late Military Head of State of Nigeria.

When my father was alive I used to move funds, in cash, running into millions of United States Dollars to Brazil, Lebanon and other parts of the world, for safe keeping on behalf of my father. However, on the eve of my father's death in June 8, 1998, he gave me the sum of US\$45,000,000.00 {FOURTY FIVE MILLION UNITED STATES DOLLARS} in cash to move to Lebanon as usual, but immediately my father died I had to moved the funds to Holland through a diplomatic courier service to a security company in Holland.

The funds have been in the security company in Holland since July 1998.

However, because of the many restrictions placed on my family by the present Nigerian Government, I simply cannot travel to Holland to secure the funds from the security company in Holland.

What I now need from you are as follows:-

- (1) You should travel to Holland to secure the funds in cash on my behalf and deposit it in your bank account in your Country.
- (2) You will be entitled to 10% of the total sum involved for your assistance.
- (3) As soon as you confirm to me by my above fax number your readiness to travel to Holland, I will send a copy of my Power of Attorney to the security company in Holland authorizing them to release the funds to you.
- (4) As soon as you have the funds in your custody, I will give you details of where and which sector you will invest my share of the funds into, on my behalf, in your Country.
- (5) Please note that this project is 100% risk free, but you must keep it very secret and confidential because of my personal security.

Please contact me immediately, via my above email only.

Best regards.

ALHAJI TAJUDEEN.K. ABACHA

# Viruses

## *What is a virus?*

(Source: "Annoyances of the Computer World Article" Bryan McDaniel, July 13th, 2004)

- A computer virus is a program (or code) that or infects an operating system or application.
- Intent of a virus:
  - Attach itself to as many hosts as possible,
- Secondary intents
  - send out spam emails,
  - allow others access to your system and data,
  - erase information or corrupt files,
  - display text messages.
- How viruses propagate
  - A virus cannot be spread without the involvement of a person.
  - Sharing infected files or documents.

# Worms

## *What is a worm?*

- Worms are really nothing more than a programs that have the ability to propagate itself on a network (be in a local or wide are network).
- Intent of a worm:
  - Propagate as quickly and widely as possible.
- Secondary intents
  - Vehicle for transporting viruses or other malware.
  - Denial of Service
- How worms propagate
  - Attach itself to files or programs that access the internet,
  - Send itself out via email to all your contacts in your address book,
  - Attach itself to instant messaging content.

# Trojans

## *What is a trojan?*

- Trojans are stand-alone programs that affect an operating system or application.
  - May look like a useful application (toolbar, search engine, etc.)
- Intent of a trojan:
  - Cause as much damage as possible.
- Secondary intents
  - allow others access to your system and data,
- How trojans propagate
  - Unlike viruses and worms, a trojan does not propagate by itself.
  - Human interaction – sharing the trojan application

# Adware

## *What is Adware?*

- Adware is software installed in addition to purchased/legal software to monitor and customize the end user experience.
- Intent of Adware:
  - Push customized advertising to the end user
- Secondary intents
  - Track user habits in an application
  - Track buying habits
- How Adware propagates
  - Installed (purposely) by application software,

# Spyware

## *What is Spyware?*

- Spyware is software installed in addition to free or illegal software to monitor the end user.
- Intent of Spyware:
  - Report personal information to criminals operating on rogue servers
- Secondary intents
  - Track user habits for later sabotage
- How Spyware propagates
  - Installed (knowingly or unknowingly) by application software,
  - Usually offered via “serial generator” or “shared music” applications.

# KeyLoggers

## *What is a KeyLogger?*

- A KeyLogger is software specifically designed to capture user typing and send it to a central location.
- Intent of a keylogger:
  - Capture user passwords.
- Secondary intents
  - Captures all information typed.
  - When used in public workstations, captures many people's data.
- How a keylogger propagates
  - Usually a component of a virus or spyware

# Backdoors

## *What is a backdoor?*

- A backdoor is an alternate way to communicate between computers, usually without the user's express knowledge.
- Intent of a backdoor
  - Allow undetected entry into a computer
  - Turn a computer into a zombie
- How is a backdoor created?
  - An unforeseen side-effect of a computer operation
  - A missed requirement in development of a software application
  - A error-prone implementation of a software application component
  - A purposeful backdoor to be used only by software technicians
    - Good intent
    - Malicious intent

# Exploits

## *What is an Exploit?*

- An exploit is either an error or a feature of the operating system that can be used for unlawful purposes.

## *Types of Exploits*

- **Software Bug Exploits**
  - Unusual or unexpected behavior of the computer operating system or software
  - Usually a component of a virus, spyware or pirated software.
  - Fixed by manufacturer in a timely manner
  - Fixing the exploit does not affect how legal/normal applications run
- **Feature Exploits**
  - Normal designed behavior of the computer operating system or software
  - A component of the computer operating system or software
  - NOT readily fixed by manufacturers
  - Fixing the exploit Affects how normal applications run

# Exploits (cont)

## *Browser Exploits*

- Browser exploits are almost always feature exploits
  - Take advantage of the features that make browsing the internet easy.
  - Usually installed simply by loading a malicious web page through:
    - the internet browser
    - opening an email
    - customizing your desktop
- Examples
  - Enhanced Toolbars
  - Search Engines
  - Image Viewers
  - Download Managers
- “Not My Responsibility”
  - Normally not “fixed” by manufacturers
  - Requires constant monitoring by computer users to keep clean
  - Most exploit avoidance tools require advanced computer knowledge

## Zero-Day Exploits

- Measurement of time between the knowledge of an exploit and the first instances of malware taking advantage of that exploit.

# RootKits

*What is a rootkit?*

- A rootkit is software installed on a user's computer that allows a criminal to take control of the user's computer undetected.

How is a rootkit installed?

- backdoor and/or exploit

Example: Sony Music Copy Protection

- Uses a rootkit to check users' compliance with digital rights management
- The problem: Once installed, it also allows other rootkits to use the same backdoor *undetected*

# Zombies

## *What are Zombies ?*

- Zombies are consumer computers used as “patsies” for other unlawful activities.
  - Most prevalent with widespread use of DSL and Cable Modems
- Intent of a zombie:
  - Do the “dirty” work of a criminal
  - Create a legal buffer zone between criminal and the crime
  - Denial of Service through massive numbers of zombies.
- How zombies propagate
  - Worms, Websites
  - Open Ports on High-speed Internet,

# BotNets

## *What is a BotNet ?*

- BotNets (robotic network) are organized networks of zombies directed at a specific target for a specific attack.
  - Difficult to identify because it looks like normal consumer traffic
- Intent of a BotNet:
  - Compromise a specific company, website or network
  - Denial of Service through massive traffic from many diverse areas.
- How BotNets propagate
  - Worms, Websites
  - Open Ports on High-speed Internet,
- Organized Crime
  - BotNets found to date are run by highly organized crime networks
  - Usually international networks which rely on poor law enforcement communications between countries

# Hijacking

## *What is Hijacking ?*

- Hijacking is the method of taking over a server or communications to a server.
- Intent of a hijacking:
  - Obtain user's account information
  - Piggyback on user activity for criminal purposes
- How hijacking operates
  - Server Hijacking
  - Network Sniffing/Hijacking
  - Man-in-the-Middle Attack

# Server Hijacking

## *What is Server Hijacking ?*

- Server hijacking is the method whereby the destination of user communication is compromised
- How server hijacking operates
  - Rootkit
    - Actual control over destination server
  - DNS Spoofing
    - Redirecting user traffic from original server to criminal server
  - Phishing
    - Look-alike server at another “similar” domain name

# Network Sniffing/Hijacking

## *What is Network Sniffing ?*

- Network Sniffing is the use of “inspecting” all traffic going through a specific communication line

## *What is Network Hijacking ?*

- Network Hijacking is being able to remove specific traffic and replace it with dummy traffic

## How network sniffing and hijacking works:

- Criminal monitors user traffic while they are logging into accounts over the internet
- Once the user is logged in, criminal takes over the user session
  - disconnecting the user side, so user thinks they were logged off (or there is a server error)
  - Continuing the user’s session (fooling the server side into thinking the criminal computer is the user’s computer)
- Criminal then makes transactions under user’s account

# Man-in-the-Middle Attack

*What is the Man-in-the-Middle Attack ?*

- Man-in-the-Middle Attack is simply when a user is fooled to go to a “dummy” website, but never knows because the communications is passed to the real website.

How a Man-in-the-Middle Attack operates:

- A combination of Phishing and/or Server Hijacking is used to get the user to go to a fake website address
- As the user sends information to the dummy website, the information is recorded and passed to the real website.
- The output from the real website is then passed back to the user’s browser.
- Criminal then sells users’ account information or uses it for their own gain

# Wireless Network Breaches

*Wireless routers offer unsolicited access, unless specifically configured not to.*

- Allows free access to the public internet by piggybacking on the wireless signal.
- Allows access to computers hooked up internally to the wireless router

How are network breaches found ?

- “Drive-By”
  - A user with a laptop, wireless card and network sniffer drives around neighborhoods mapping out all wireless routers available
- “Chalking”
  - In metro areas, a building will be marked (by a drive-by) to notify other hackers that a particular wireless router is accessible.
  - Originally was designated by
    - “W” with a circle for internet access
    - “W” with a circle and line through it for internal access

# **Identity Theft Safety Guidelines**

# General Safety Guidelines

## “Cockpit Resource Management”

- Pre-plans all possible problem scenarios
- Developed by the FAA in response to the crash of United Airlines Flight 173 on December 28, 1978.

## General Guidelines for CRM

- Avoid
  - Do everything reasonable to prevent the opportunity for attack.
- Trap
  - Be aware of “triggers” that indicate an impending attack.
- Mitigate
  - Always plan for “when” and not “if” an attack happens.

# General Safety Guidelines

- Avoid
  - Demonstrate good computer habits
  - Keep computer software up-to-date
  - Install a personal firewall
  - Use parental control software
- Trap
  - Use virus scanners
  - Install popup blockers
- Mitigate
  - On discovering an attack:
    - Disconnect from the internet immediately - unplug the network cable
    - Document everything that has happened with as much detail as possible
    - Run **full** virus scan from an emergency boot disk (floppy or CD)
      - Choose to “clean” or “delete” -- “quarantine” only invites problems
  - After the computer is clean:
    - Look up the attack online (wikipedia, sophos, symantec, et al)
    - Determine who and what was affected
    - Reinstall affected software from scratch
    - Notify affected people (may be entire contact list)

# Avoid Identity Theft

How can I prevent identity theft... from the physical methods?

- Shred all documents that can contain personal information
  - Those annoying pre-approved credit card applications identify you from a single code on the mailing address... so someone can call the bank and say “I lost the application, but here is the pre-approval code.”
- Never carry unnecessary identification
  - No need for Social Security Card, not even a copy
  - Leave all Credit Cards at home, unless you are planning to use specific ones.
  - Do you really need to store your banking information on your PDA?
- Ask companies that use SSN as identification to change it
  - Health insurance
  - Employee identification

# Trap Identity Theft

How can I prevent identity theft... from social engineering?

- Watch your credit card bills for small unknown charges.
  - Many thieves use this method to see if you are tracking your purchases.
- Don't talk to strangers 😊
  - Be careful if you get involved in conversations which lead to any type of advice.
  - Sometimes it is best to give out misleading or “tracker” information.
- Never give out “odd” pieces of information.
  - No one should ever ask for any part of your SSN unless you can properly identify them.
  - No institution should every ask for anything other than the last 4 digits of a Credit Card number.
  - Review anything posted in chat rooms or webspaces (i.e. MySpace.com)

# Mitigate Identity Theft

Other ways to prevent identity theft...

- Get Credit Reports regularly
  - Act on any suspicious account activity, especially inactive or closed accounts.
- Lock accounts from unconfirmed changes
  - Banks, financial institutions and credit reporting agencies
  - Phone and utility companies
  - Online accounts
- Send postal mail through the post office
  - Do not give people the chance to intercept your bill payments or credit applications.
- Always report unexpected activity
  - Children receiving credit card offers through the mail.
  - Theft of mail, even if just a birthday card.
  - Any misprint of account information on bills.
  - Cold calls or postal mail applications that use your “tracking” information.
  - Always call an institution (using a known customer service number) to verify information.

# I am a victim, what do I do now?

- Document everything
  - How you found out
  - When you found out
  - Chronology of what you think happened
  - Any tracker information that can help police
  - Any previous police reports or identity incidents
  - Review past credit card bills and credit report
- Contact various authorities
  - Lawyer
  - Local police (in both your area and where your identity was used)
  - Bank, financial institutions affected as well as credit reporting companies
  - Contact DHS/FBI
- Be persistent !
  - Victims do more investigative footwork because personal information is at stake
  - Legislation today is lacking, but new legislation offers promise
  - Most instances take 3-5 years to clear

# **Best Practices**

**“Stop, Think, Click”**

# Best Practices

**Be AWARE of what you and your children are doing online.**

- Let your children be independent, but make sure your children KNOW the ramifications of posting personal information online.
- Let them know that if they make a mistake, not to be embarrassed, but to report it as soon as possible.

## **Beware of Instant Messaging and Chat Rooms**

- all chat room and IM communication is public,
- chat rooms and IM is used to download malware,
- chat rooms and IM is used prevalently for social engineering (by pedophiles and other predatory types)

# Best Practices

## Stay away from music (and file) sharing

- Leaving an idle computer hooked into a high-speed connection only invites trouble.
- The MOST ignored rule, which makes it the MOST used by thieves...

## Stay away from anything listed as “Free”

- Most “free” software has something *else* is attached to it
- Music files, customized toolbars, advanced search utilities, weather services, online raffles, e-cards (and even some “free” spyware tools and virus tools)
- The SECOND MOST ignored rule, which makes it the MOST used by thieves...

## Stay away from Online Games

- Although many online gaming sites may be legitimate, this is a popular ruse to allow people to download “stuff” to your computer without you knowing it.
- This is the THIRD MOST ignored rule...

# Best Practices

## Configure all wireless devices securely

- wireless router security:
  - Change default passwords
  - Make router name non-obvious
  - Do not let router auto-publish itself
  - Ensure WAP or WEP security is active
  - Turn on all router firewall safety features
- wireless device security:
  - Only connect to a designated router (not the neighbor's)
  - Do not "share" files or folders
  - Turn on all device firewall safety features

## Only stay connected to the internet when necessary

- Leaving an idle computer hooked into a high-speed connection only invites trouble.

# Best Practices

## **Keep your computer in good health**

- Always keep your PC security up to date with a checklist of approved healthy software.
- Just like vitamins, too much can be just as bad as too little.

## **Browse online carefully.**

- Always go to your online sites by TYPING in the name on the Web Browser Address Bar.
- Always double-check your typing and the URL of the site loaded

## **Be suspicious of all email.**

- Most email from banks, online auction sites, and stores are usually phishing attempts, trying to get you to click to a "look-alike" site to enter your password or other personal information.
- Even email from people you know can have mislabeled links.

# Best Practices

## **Always check your credit card statements.**

- Most credit card thieves test an account by making many small charges to your credit card
- If credit card is not cancelled after 3 -6 months, they go for the kill (a huge purchase).

## **Be careful of what financial information you put on your PC.**

- If you are a slave to Quicken or other software based financial bookkeeping, then you should *encrypt* your personal data using software like PGP.

## **Always get yourself (and your family) a checkup.**

- Financially, that is. spend the money, get the credit reports quarterly, prevent years of frustration later.
- The legal system is way too far behind to support you if your identity gets stolen.

# **Safety Software Recommendations**

# Service Packs and Fixes

Recommendation: Install All Fixes and Service Packs, Check Regularly.

- **Windows Service Packs**
  - Always recommended as a first step towards a clean house.
  - **Cost:** FREE
  - **Available From:** <http://windowsupdate.microsoft.com>
  - **Technical Level:** Novice
  - **Installation Time:** varies + usually at least one reboot

# “All-in-One” Security Centers

Recommendation: A good alternative to maintaining multiple security software, but usually has some shortcomings.

- **Windows OneCare Live**
  - *\*\*\* Provides an "outbound" firewall -- so if your PC does get infected with a zombie, it cannot hurt other PCs.*
  - Provides a good layer of protection against viruses, spyware and system changes
  - No parental controls or time limit capabilities
  - **Cost:** (beta)
  - **Available From:** <http://www.windowsonecare.com>
  - **Technical Level:** Novice
  - **Installation Time:** 5 minutes + usually one reboot
- **AOL Security Center**
  - Use this to control and/or monitor your family's online activity.
  - **Cost:** Free for AOL Customers
  - **Available From:** <http://www.aol.com>
  - **Technical Level:** Novice to Intermediate
  - **Installation Time:** 15 minutes + one reboot

# “All-in-One” Security Centers

...continued...

- **CA EZ-Armor**
  - Combines the following software:
    - ZoneAlarm Personal Firewall Pro
    - CA eTrust Anti-Virus
    - PestPatrol Anti-Spyware
    - K9 Parental Controls
  - **Cost:** Annual Subscription (*provided free by Optimum Online and other ISPs*)
  - **Available From:** <http://www.ca.com> (<http://www.optonline.net>)
  - **Technical Level:** Intermediate
  - **Installation Time:** 10 minutes + one reboot
- **Symantec (Norton) Internet Security**
  - Combination of all Symantec security products.
  - **Cost:** Annual Subscription
  - **Available From:** <http://www.symantec.com>
  - **Technical Level:** Intermediate
  - **Installation Time:** 15 minutes + one reboot

# Virus Scanning Software

Recommendation: Install One.... **a must**

- **McAfee AntiVirus**
    - Available From: <http://www.mcafee.com>
  - **Symantec (Norton) AntiVirus**
    - Available From: <http://www.symantec.com>
  - **CA EZ-Antivirus**
    - Available From: <http://www.ca.com>
  - **IBM AntiVirus**
    - Available From: <http://www.ibm.com>
  - **Trend Micro AntiVirus**
    - Available From: <http://www.trendmicro.com>
- 
- Use only top-rated antivirus products
  - Antivirus does viruses and trojans very well, but some things are not considered viruses or trojans, like spyware
  - **Cost:** Annual Subscription
  - **Technical Level:** Novice
  - **Installation Time:** 15 minutes + one reboot

# Parental Controls

Recommendation: A **must** for any family.

- **NetNanny**
  - Available From: <http://www.softforyou.com>
- **Kid's Watch**
  - Available From: <http://www.kidswatch.com>
- **Access Boss**
  - Available From: <http://www.fspro.net/aboss/index.html>
- **SoftwareTime**
  - Available From: <http://www.softwaretime.com>
- **Enuff PC**
  - Available From: <http://www.enuffpc.com>
- **IProtectYou**
  - Available From: <http://www.softforyou.com>

# Online Virus Scanners

Recommendation: Worth a try....

**The Upside:** These new breeds of scanning engines have some great potential.

**The Downside:** Most require ActiveX and Internet Explorer (which is known to have problems).

- **Symantec Security Check Website**

- In-depth virus scanning and/or security scanning (two separate tabs).
- Only identifies issues; *does not repair or clean threats*.
- **Cost:** FREE
- **Available From:** <http://security.symantec.com/default.asp?productid=symhome&langid=ie&venid=sym>
- **Technical Level:** Novice

- **Trend Micro Housecall**

- A bit flaky... I found it to stop sometimes at the first virus/trojan/worm, so it needed to be run several times.
- Cleans/Fixes any threats found.
- **Cost:** FREE (it is a preview of an upcoming product)
- **Available From:** [http://housecall.trendmicro.com/housecall/start\\_corp.asp](http://housecall.trendmicro.com/housecall/start_corp.asp)
- **Technical Level:** Novice

# Personal Firewalls

Recommendation: Install Both.

- **Windows ICS / Firewall (included with XP SP2)**
  - Although this is a good first effort by Microsoft to control unmonitored access, it falls short of being considered a “perfect” solution.
  - **Cost:** FREE (installed as part of Windows XP Service Pack 2)
  - **Available From:** <http://windowsupdate.microsoft.com>
  - **Technical Level:** Novice
  - **Installation Time:** 40-60 minutes + one reboot
- **ZoneAlarm**
  - This software will account for 2 major leaks:
    - It will ask for permission to allow applications on your computer to access the Internet.
    - It will prevent inbound access from the Internet.
  - **Cost:** FREE (no need to get 'PRO' version)
  - **Available From:** <http://www.zonelabs.com>
  - **Technical Level:** Intermediate
  - **Installation Time:** 10 minutes + one reboot

# Spyware Scanners

Recommendation: Install at least one, Check Regularly.

- **Windows Defender** (formerly Windows Anti-Spyware)
  - Provides a good layer of protection against spyware and system changes
  - Not as many options or as customizable as other similar products.
  - **Cost:** (beta)
  - **Available From:** <http://www.microsoft.com/athome/security/spyware/software>
  - **Technical Level:** Novice
  - **Installation Time:** 5 minutes + usually one reboot
- **SpyBot Search & Destroy**
  - S&D Resident will ask for permission to allow programs to change the registry (computer settings).
  - Run these weekly to remove/prevent spyware: "Search for Updates", "Immunize", and "Check For Problems"
  - Be sure to set 2 resident settings (Teatimer and S&D)
  - **Cost:** FREE
  - **Available From:** <http://www.safer-networking.org/en>
  - **Technical Level:** Intermediate
  - **Installation Time:** 10 minutes

# Spyware Scanners

... continued ...

- **Ad-Aware SE**
  - Run this weekly to remove spyware
  - **Cost:** FREE
  - **Available From:** <http://www.lavasoftusa.com>
  - **Technical Level:** Intermediate
  - **Installation Time:** 10 minutes
- **SpyBlaster**
  - Run manual updates weekly to keep your web browser from downloading spyware.
  - **Cost:** FREE
  - **Available From:** <http://www.javacoolsoftware.com>
  - **Technical Level:** Novice
  - **Installation Time:** 10 minutes

# Browser Safety

Recommendation: Install and use as needed.

- **NetCraft Toolbar**

- Displays information about every website you visit, giving its origination date and country of origin.
- Useful to thwart phishing attacks where you are directed to a "look-alike" site and prompted for your userid and password.
- *Hint: If you go to what you think is your banking site, and it gives a country other than US or has an origination date of less than 1 year ago; chances are, it is not your bank.*
- **Cost:** FREE.
- **Available From:** <http://toolbar.netcraft.com>
- **Technical Level:** Novice
- **Installation Time:** 5 minutes

- **Mozilla FireFox Web Browser**

- An alternative web browser. Safer than IE because it does not support Microsoft OBJECTs or ActiveX controls (which also means it cannot display sites which use these methods).
- Has many built-in security features as well as plugins for security.
- **Cost:** FREE.
- **Available From:** <http://www.mozilla.org/products/firefox>
- **Technical Level:** Novice
- **Installation Time:** 5 minutes

# System Configuration

Recommendation: Check Regularly.

- **Safety Tools from Gibson Research**
  - Good to run to close any serious vulnerabilities which Microsoft considers "features".
  - No integrated user interface
  - Suggested to run:
    - SocketLock
    - ShootTheMessenger
    - UnPNP
  - **Cost:** FREE
  - **Available From:** <http://www.grc.com>
  - **Technical Level:** Novice to Intermediate
  - **Installation Time:** 5 minutes
- **PivX PreEmpt** (formerly Qwik-Fix)
  - Although most of these configuration changes can be done manually, this utility will always ensure the proper and latest configuration recommendations are always applied.
  - **Cost:** \$\$\$
  - **Available From:** <http://www.pivx.com>
  - **Technical Level:** Novice
  - **Installation Time:** 5 minutes + usually one reboot

# Popup Blockers

Recommendation: Install One.

- **Windows IE Popup Blocker (included with XP SP2)**
  - Works only with Internet Explorer
  - **Cost:** FREE (installed as part of Windows XP Service Pack 2)
  - **Available From:** <http://windowsupdate.microsoft.com>
  - **Technical Level:** Novice
  - **Installation Time:** 40-60 minutes + one reboot
  
- **PopupStopper**
  - Works with IE, Netscape and Mozilla browsers.
  - Not necessary with Windows XP-SP2.
  - **Cost:** It pays to buy the basic version.
  - **Available From:** <http://www.panicware.com>
  - **Technical Level:** Novice to Intermediate
  - **Installation Time:** 5 minutes

# Spam / Phishing Blockers

Recommendation: Install at least One.

- **Check your ISP / Email provider**

- Many ISPs offer spam protection, and allow you to tweak the configuration.
- **Cost:** FREE
- **Technical Level:** Intermediate

- **SpamKiller**

- Good basic spam stopper... requires some complex configuration to make it run well.
- **Cost:** \$\$\$
- **Available From:** <http://www.mcafee.com>
- **Technical Level:** Novice to Intermediate
- **Installation Time:** 5 minutes

- **SpamWasher**

- **Cost:** It pays to get the basic version
- **Available From:** <http://www.panicware.com>
- **Technical Level:** Novice to Intermediate
- **Installation Time:** 5 minutes