Addressing C3:
Cyber Ethics, Safety, and Security in Web 2.0

Davina Pruitt-Mentle

Educational Technology Policy Research and Outreach

Linking Research to Practice

CyberWATCH

Nancy Willard

Center for Safe and Responsible Internet Use

Educational Technology Policy
Linking Research to Practice
Research and Outreach

CyberWATCH

Cyberethics
Cybersafety
C3 INSTITUTE
Educational Technology
Policy, Research, and Outreach
Cybersecurity

Cybersecurity
The Forgotten Element

Davina Pruitt-Mentle
Education Technology Policy, Research and Outreach
CyberWATCH

June 29, 2008

NECC

FTC 2007 Report

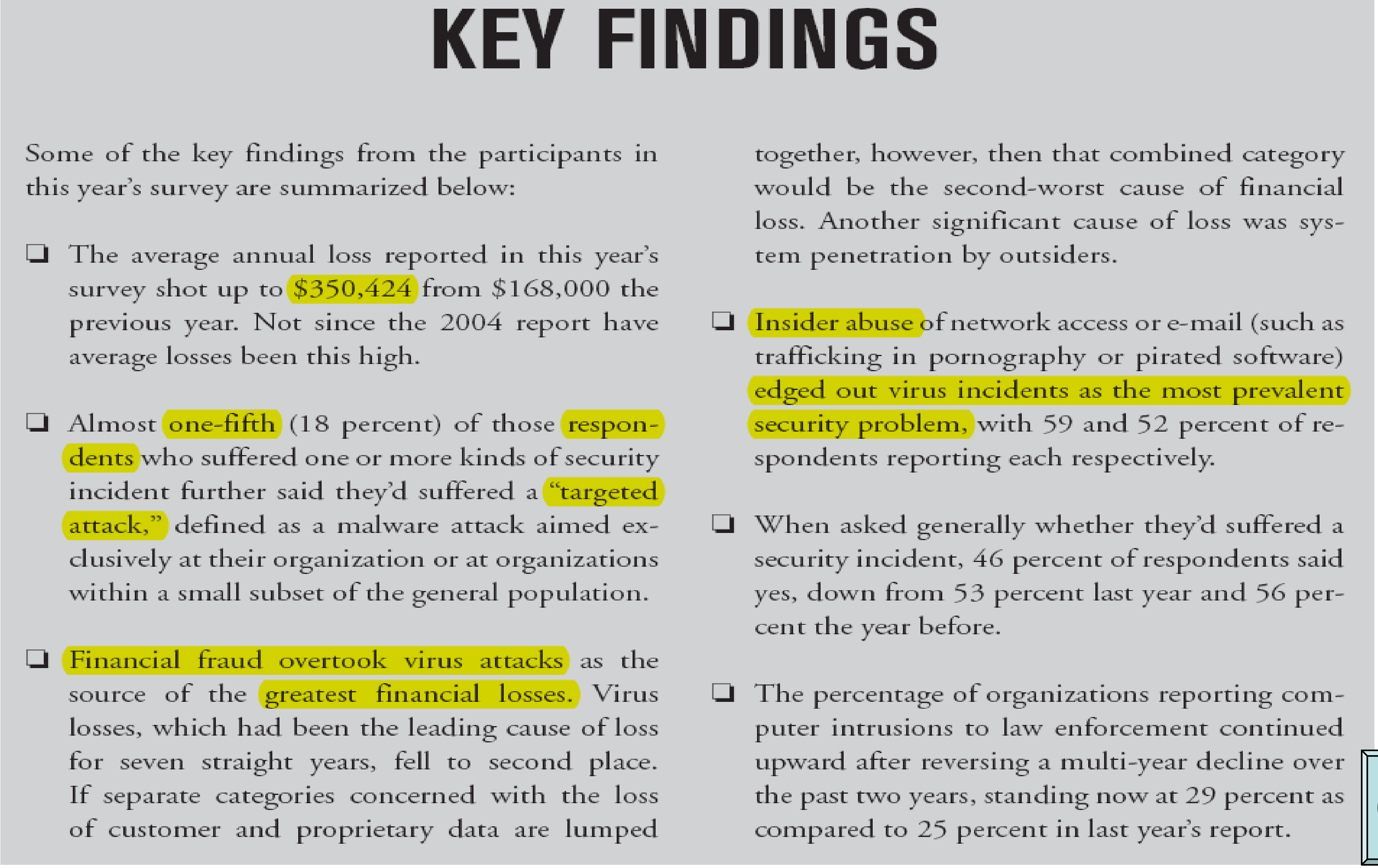
Consumer Fraud and Identity Theft Complaint Data

- 7th year in a row, **identity theft tops the list**, accounting for 36 percent of the 674,354 complaints received
- Consumers reported fraud losses totaling more than $1.1 billion; the median monetary loss was $500. 85 percent of the consumers reporting fraud also reported an amount lost.
- The percentage of fraud complaints with wire transfer as the reported payment method continues to increase. Twenty-three percent of the consumers reported wire transfer as the payment method, an increase of eight percentage points from calendar year 2005.
- Credit card fraud (25 percent) was the most common form of reported identity theft, followed by phone or utilities fraud (16 percent), bank fraud (16 percent), and employment fraud (14 percent).
- FTC reports that identity theft now affects more than 10 million people every year representing an annual cost to the economy of $50 billion

Slightly Down From 2006
http://www.privacyrights.org/ar/idtheftsurveys.htm#Jav2007

http://www.ftc.gov/
On Guard http://onguardonline.gov/phishing.html

2007 CSI Computer Crime and Security Survey



KEY FINDINGS

Some of the key findings from the participants in this year's survey are summarized below:

- The average annual loss reported in this year's survey shot up to $350,424 from $168,000 the previous year. Not since the 2004 report have average losses been this high.

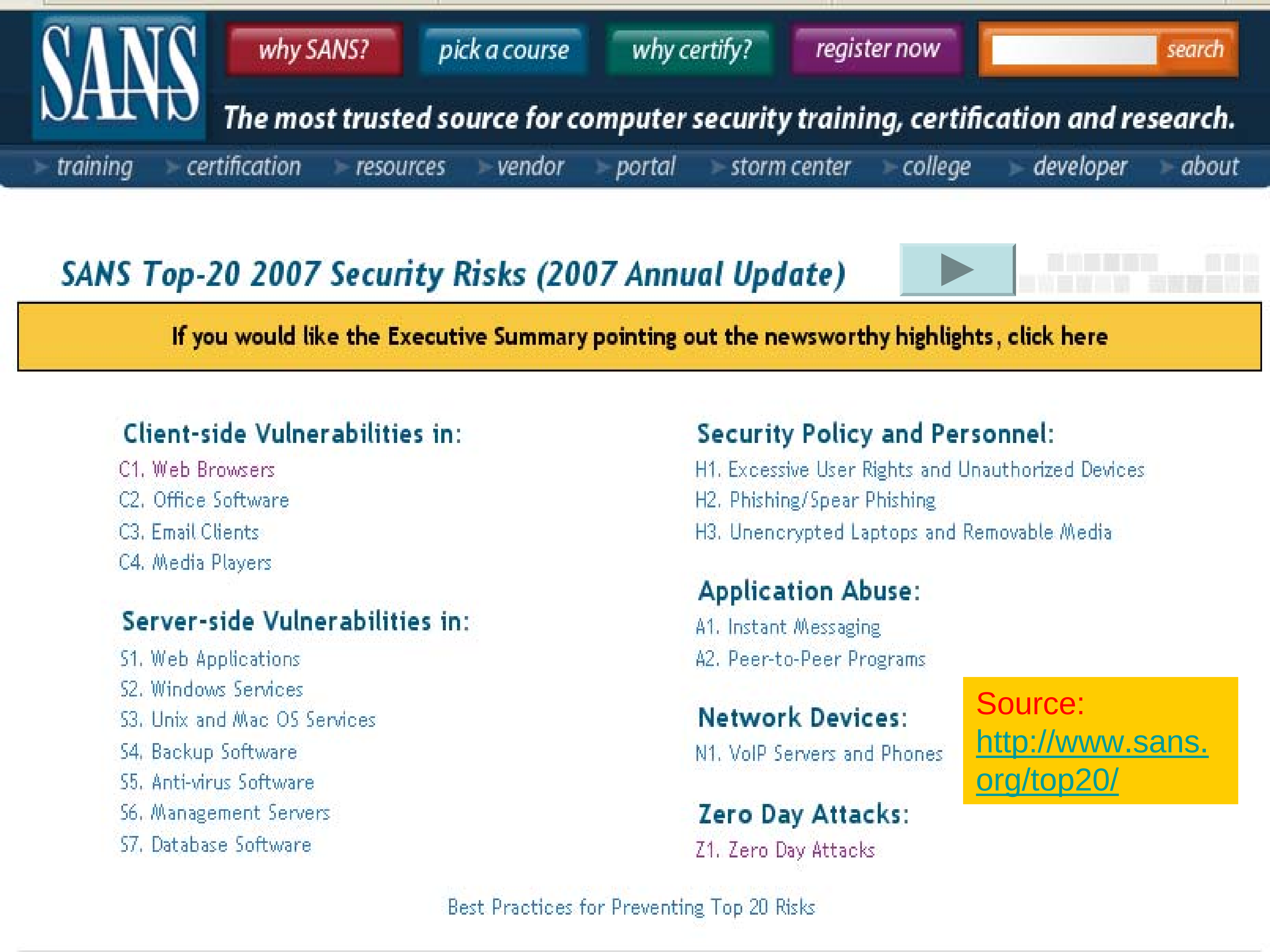
- Almost one-fifth (18 percent) of those respondents who suffered one or more kinds of security incident further said they'd suffered a "targeted attack," defined as a malware attack aimed exclusively at their organization or at organizations within a small subset of the general population.

- Financial fraud overtook virus attacks as the source of the greatest financial losses. Virus losses, which had been the leading cause of loss for seven straight years, fell to second place. If separate categories concerned with the loss of customer and proprietary data are lumped together, however, then that combined category would be the second-worst cause of financial loss. Another significant cause of loss was system penetration by outsiders.

- Insider abuse of network access or e-mail (such as trafficking in pornography or pirated software) edged out virus incidents as the most prevalent security problem, with 59 and 52 percent of respondents reporting each respectively.

- When asked generally whether they'd suffered a security incident, 46 percent of respondents said yes, down from 53 percent last year and 56 percent the year before.

- The percentage of organizations reporting computer intrusions to law enforcement continued upward after reversing a multi-year decline over the past two years, standing now at 29 percent as compared to 25 percent in last year's report.



SANS Top-20 2007 Security Risks (2007 Annual Update)

If you would like the Executive Summary pointing out the newsworthy highlights, click here

Client-side Vulnerabilities in:

C1. Web Browsers
C2. Office Software
C3. Email Clients
C4. Media Players

Server-side Vulnerabilities in:

S1. Web Applications
S2. Windows Services
S3. Unix and Mac OS Services
S4. Backup Software
S5. Anti-virus Software
S6. Management Servers
S7. Database Software

Security Policy and Personnel:

H1. Excessive User Rights and Unauthorized Devices
H2. Phishing/Spear Phishing
H3. Unencrypted Laptops and Removable Media

Application Abuse:

A1. Instant Messaging
A2. Peer-to-Peer Programs

Network Devices:

N1. VoIP Servers and Phones

Zero Day Attacks:

Z1. Zero Day Attacks

Best Practices for Preventing Top 20 Risks

Source: http://www.sans.org/top20/

Georgia Tech's Information Security Center (GTISC) 2008 Top 5 Emerging Cyber Threats

- **Web 2.0 and Client-Side Attacks** – including social networking attacks and new attacks that will exploit Web 2.0 vulnerabilities
- **Targeted Messaging Attacks** – including Instant Messaging attacks and malware propagation via online video-sharing
- **Botnets** – specifically the spread of botnet attacks to wireless and peer-to-peer network
- **Threats Targeting Mobile Convergence** – including voice spam, vishing and smishing
- **Threats to Radio Frequency Identification (RFID) Systems** – evolving and varied threats in this emerging technology sector

http://www.gatech.edu/news-room/release.php?id=1531

Think Your Home Computer Is Safe?

- **2007 McAfee-NCSA Online Safety Study**
  - conducted a comprehensive consumer online security research study
  - compared online Americans' *opinions* of their computer security to the *reality* – what security software they were actually running
  - telephone survey and then participated in a remote scan which collected the type of security software installed on the respondents' computer

SOURCE:
http://staysafeonline.org/features/ncsalibrary.html

2007 McAfee/NCSA Survey

- **Viruses Are Common**
  - **54%** Americans reported that they have had a **virus** on their computer
  - **15%** of Americans **aren’t sure** if they’ve had a virus or not
- **I Spy**
  - More than **4 in 10** Americans believe they currently have **spyware or adware** on their home computer (44%)
- **Something Phishy**
  - 3 out of 4 Americans **(74%)** have received a **phishing email**
  - 92% of this group says at least some of the emails looked legit at first glance
- **Pop-Up Problems.**
  - **1 in 3** Americans (32%) still get **pop up ads** even when using a pop up blocker on their computer
  - 39% said that they were redirected to another site or received a pop-up when doing an online search

Consumers Know Security is Important

- **Security is a Priority** Majority of Americans think they have the following security software installed on their computer
  - **87%** believe they have anti-virus software
  - **73%** believe they have a firewall
  - **70%** believe they have anti-spyware software

- **Awareness of Online Threats** Americans also know about the many online dangers that exist
  - 99% have heard about of spyware
  - 75% have heard about phishing

False Sense of Security

When it comes to the security software on their computer, what Americans say they have doesn't match up with what's actually there.

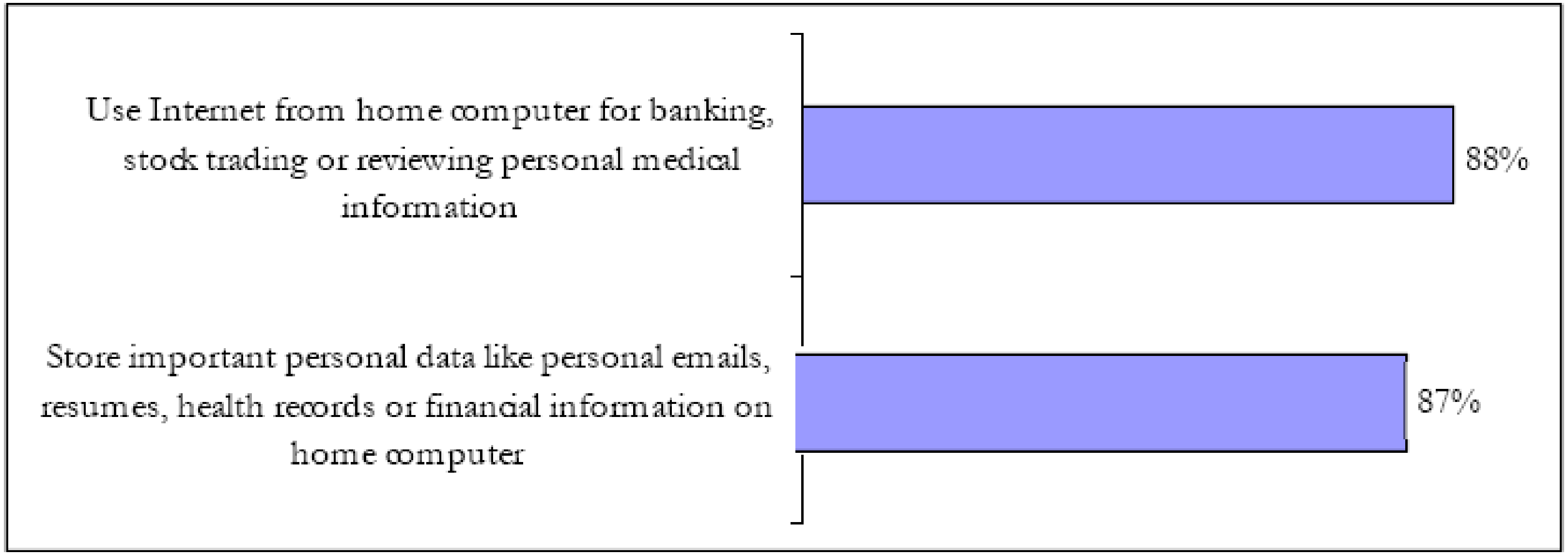
- **Expired Anti-Virus Software**
  - **92%** of Americans think that their anti-virus software is up to date
  - **51%** have current anti-virus software that has received an **updated** DAT* file within the past week. (49% do not)
- **Disabled Firewall**
  - **73%** of Americans think they have a firewall installed
  - **64%** actually have it enabled
- **Less than half have anti-spyware protection**
  - **70%** think they have anti-spyware software
  - barely half actually have it installed (55%)
- **No Phishing Protection**
  - More than twice as many Americans report having anti-phishing software as actually have it installed (27% vs. 12%)

Americans are Underprotected

- **Fully Protected? You’re One of the Few**
- Less than 1 in 4 Americans are fully protected against viruses and malware.
  - Just **22%** have anti-spyware software installed, an enabled firewall and anti-virus protection that has received an updated virus definition file within one week.

- **Older And Wiser** Somewhat surprisingly, Americans ages 45 and older show more savvy than their younger counterparts when it comes to cyber security
  - 25% of them are fully protected versus just 18% of Americans ages 44 and younger.

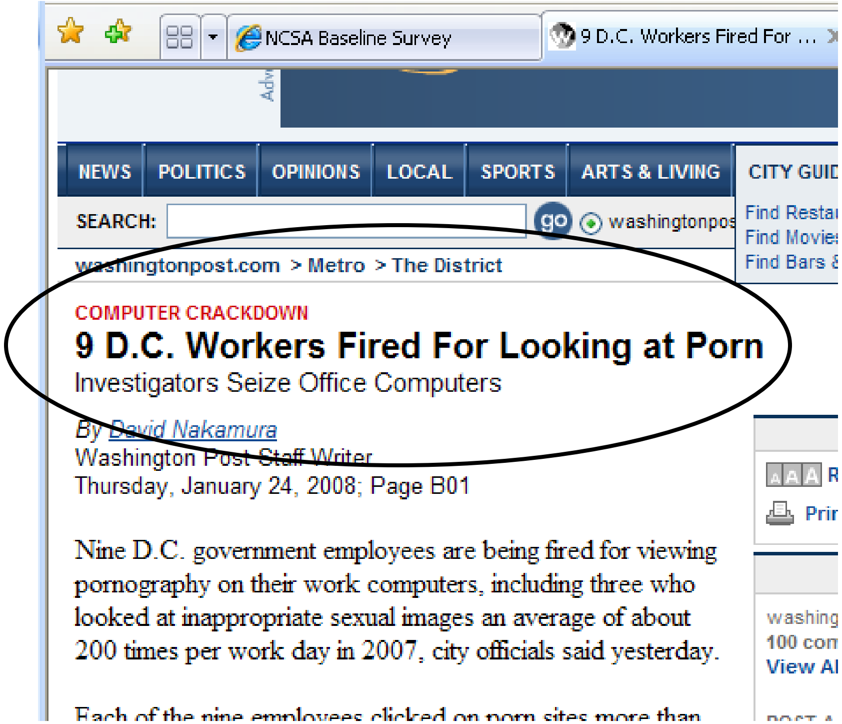
Putting Themselves at Risk



How Computer Savvy Are You?

- **Safe Search.** Almost all Americans agree that it is important to be able to know the risk level of a web site before visiting it (98%), but most do not know how to do this.
  - **64%** of Americans admit they don’t know how to determine if a website is safe before visiting it
  - Nearly eight in ten **(78%)** say that when they are viewing search results, they have no idea how to tell if any of them might lead to a high-risk website
- **What Is A Firewall, Anyway?** Just 4% of Americans say they understand firewalls “completely” and more than four out of ten Americans (44%) don’t understand how firewalls work.
- **The Facts of Phishing.** One in four Americans have not even heard of the term “phishing” before (25%). And just half of those who claim to know what phishing is can accurately define it (54%).

In the News



COMPUTER CRACKDOWN

9 D.C. Workers Fired For Looking at Porn

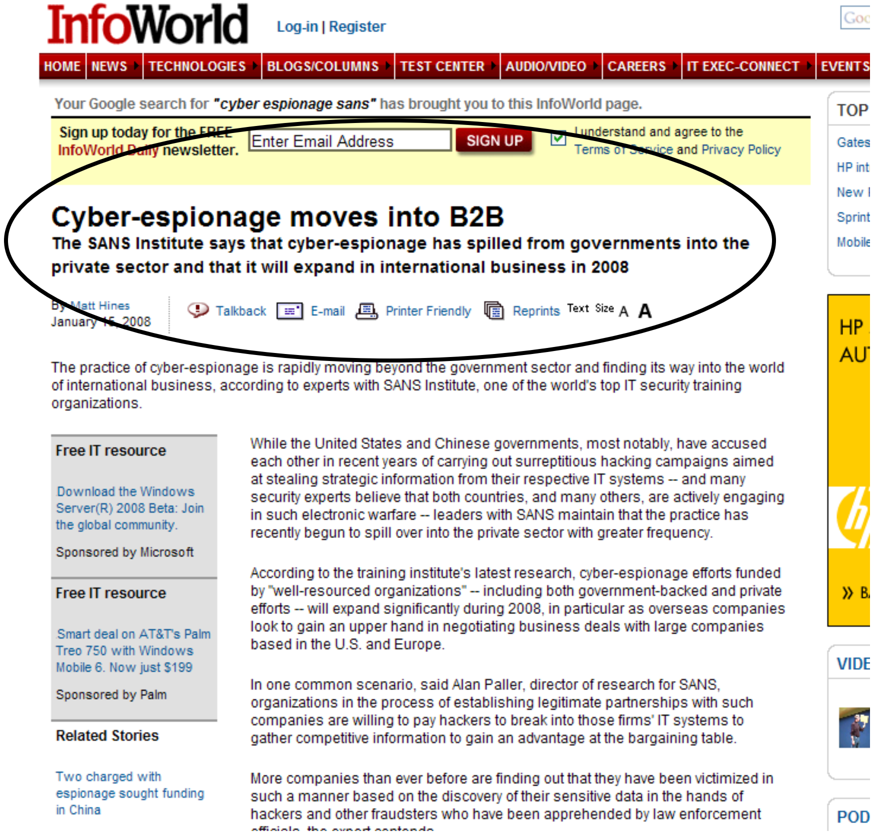
Investigators Seize Office Computers

By David Nakamura
Washington Post Staff Writer
Thursday, January 24, 2008; Page B01

Nine D.C. government employees are being fired for viewing pornography on their work computers, including three who looked at inappropriate sexual images an average of about 200 times per work day in 2007, city officials said yesterday.

Each of the nine employees clicked on porn sites more than

http://www.washingtonpost.com/wp-dyn/content/article/2008/01/23/AR2008012302511.html?wpisrc=_rsstechnology



Your Google search for ***"cyber espionage sans"*** has brought you to this InfoWorld page.

Sign up today for the FREE InfoWorld Daily newsletter. Enter Email Address SIGN UP ☑ I understand and agree to the Terms of Service and Privacy Policy

Cyber-espionage moves into B2B

The SANS Institute says that cyber-espionage has spilled from governments into the private sector and that it will expand in international business in 2008

By Matt Hines
January 15, 2008

The practice of cyber-espionage is rapidly moving beyond the government sector and finding its way into the world of international business, according to experts with SANS Institute, one of the world's top IT security training organizations.

While the United States and Chinese governments, most notably, have accused each other in recent years of carrying out surreptitious hacking campaigns aimed at stealing strategic information from their respective IT systems -- and many security experts believe that both countries, and many others, are actively engaging in such electronic warfare -- leaders with SANS maintain that the practice has recently begun to spill over into the private sector with greater frequency.

According to the training institute's latest research, cyber-espionage efforts funded by "well-resourced organizations" -- including both government-backed and private efforts -- will expand significantly during 2008, in particular as overseas companies look to gain an upper hand in negotiating business deals with large companies based in the U.S. and Europe.

In one common scenario, said Alan Paller, director of research for SANS, organizations in the process of establishing legitimate partnerships with such companies are willing to pay hackers to break into those firms' IT systems to gather competitive information to gain an advantage at the bargaining table.

More companies than ever before are finding out that they have been victimized in such a manner based on the discovery of their sensitive data in the hands of hackers and other fraudsters who have been apprehended by law enforcement officials, the expert contends.

Free IT resource

Download the Windows Server(R) 2008 Beta: Join the global community.

Sponsored by Microsoft

Free IT resource

Smart deal on AT&T's Palm Treo 750 with Windows Mobile 6. Now just $199

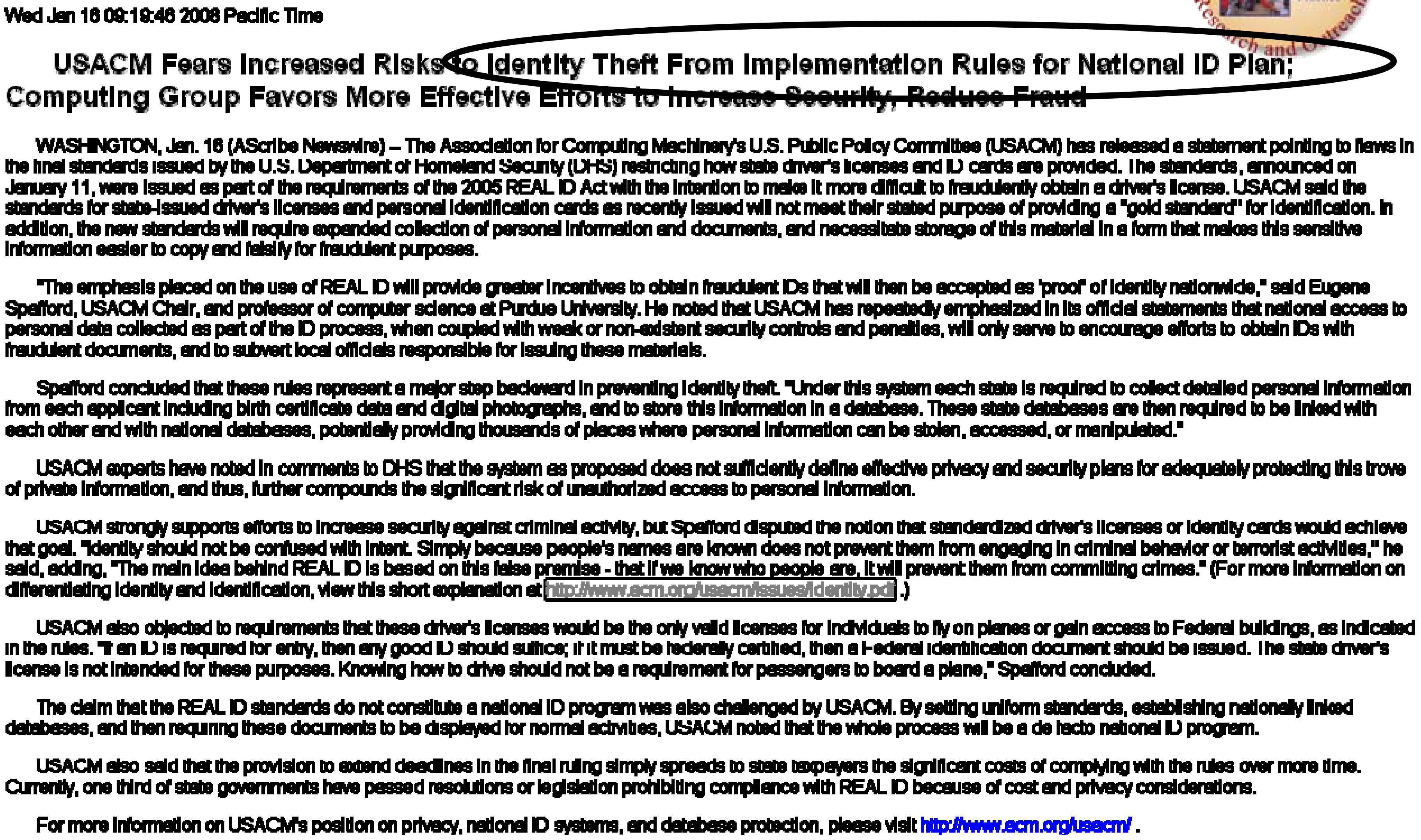
Sponsored by Palm

Related Stories

Two charged with espionage sought funding in China

http://www.infoworld.com/article/08/01/15/Cyber-espionage-moves-into-B2B_1.html

In the News



Wed Jan 16 09:19:46 2008 Pacific Time

USACM Fears Increased Risks to Identity Theft From Implementation Rules for National ID Plan; Computing Group Favors More Effective Efforts to Increase Security, Reduce Fraud

WASHINGTON, Jan. 16 (AScribe Newswire) -- The Association for Computing Machinery's U.S. Public Policy Committee (USACM) has released a statement pointing to flaws in the final standards issued by the U.S. Department of Homeland Security (DHS) restricting how state driver's licenses and ID cards are provided. The standards, announced on January 11, were issued as part of the requirements of the 2005 REAL ID Act with the intention to make it more difficult to fraudulently obtain a driver's license. USACM said the standards for state-issued driver's licenses and personal identification cards as recently issued will not meet their stated purpose of providing a "gold standard" for identification. In addition, the new standards will require expanded collection of personal information and documents, and necessitate storage of this material in a form that makes this sensitive information easier to copy and falsify for fraudulent purposes.

"The emphasis placed on the use of REAL ID will provide greater incentives to obtain fraudulent IDs that will then be accepted as 'proof' of identity nationwide," said Eugene Spafford, USACM Chair, and professor of computer science at Purdue University. He noted that USACM has repeatedly emphasized in its official statements that national access to personal data collected as part of the ID process, when coupled with weak or non-existent security controls and penalties, will only serve to encourage efforts to obtain IDs with fraudulent documents, and to subvert local officials responsible for issuing these materials.

Spafford concluded that these rules represent a major step backward in preventing identity theft. "Under this system each state is required to collect detailed personal information from each applicant including birth certificate data and digital photographs, and to store this information in a database. These state databases are then required to be linked with each other and with national databases, potentially providing thousands of places where personal information can be stolen, accessed, or manipulated."

USACM experts have noted in comments to DHS that the system as proposed does not sufficiently define effective privacy and security plans for adequately protecting this trove of private information, and thus, further compounds the significant risk of unauthorized access to personal information.

USACM strongly supports efforts to increase security against criminal activity, but Spafford disputed the notion that standardized driver's licenses or identity cards would achieve that goal. "Identity should not be confused with intent. Simply because people's names are known does not prevent them from engaging in criminal behavior or terrorist activities," he said, adding, "The main idea behind REAL ID is based on this false premise - that if we know who people are, it will prevent them from committing crimes." (For more information on differentiating identity and identification, view this short explanation at http://www.acm.org/usacm/issues/identity.pdf .)

USACM also objected to requirements that these driver's licenses would be the only valid licenses for individuals to fly on planes or gain access to Federal buildings, as indicated in the rules. "If an ID is required for entry, then any good ID should suffice; if it must be federally certified, then a Federal identification document should be issued. The state driver's license is not intended for these purposes. Knowing how to drive should not be a requirement for passengers to board a plane," Spafford concluded.

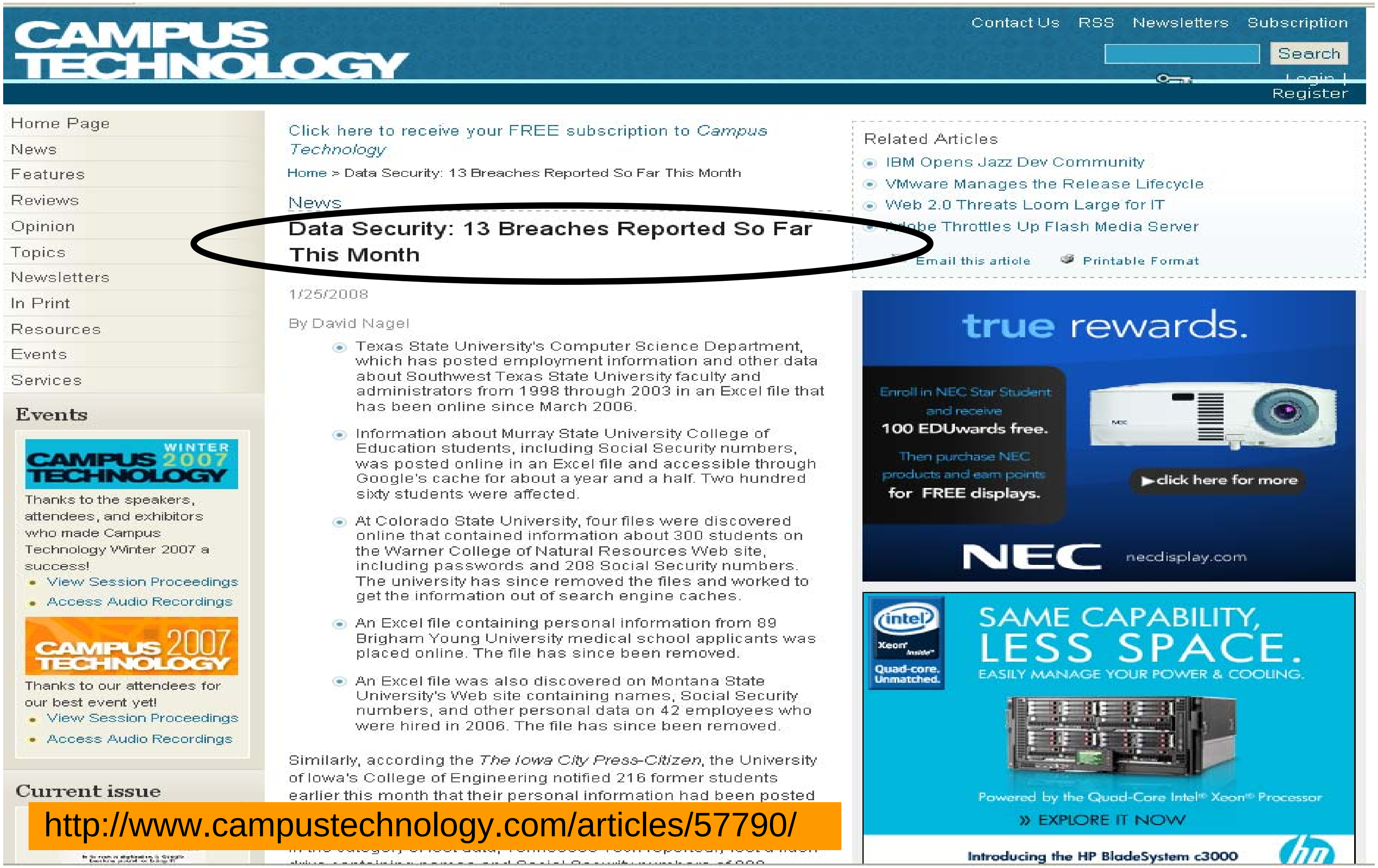
The claim that the REAL ID standards do not constitute a national ID program was also challenged by USACM. By setting uniform standards, establishing nationally linked databases, and then requiring these documents to be displayed for normal activities, USACM noted that the whole process will be a de facto national ID program.

USACM also said that the provision to extend deadlines in the final ruling simply spreads to state taxpayers the significant costs of complying with the rules over more time. Currently, one third of state governments have passed resolutions or legislation prohibiting compliance with REAL ID because of cost and privacy considerations.

For more information on USACM's position on privacy, national ID systems, and database protection, please visit http://www.acm.org/usacm/ .

Source: http://newswire.ascribe.org/cgi-bin/behold.pl?ascribeid=20080116.080849&time=09%2019%20PST&year=2008&public=0

In the News



CAMPUS TECHNOLOGY

Click here to receive your FREE subscription to *Campus Technology*

Home > Data Security: 13 Breaches Reported So Far This Month

News

Data Security: 13 Breaches Reported So Far This Month

1/25/2008

By David Nagel

- Texas State University's Computer Science Department, which has posted employment information and other data about Southwest Texas State University faculty and administrators from 1998 through 2003 in an Excel file that has been online since March 2006.
- Information about Murray State University College of Education students, including Social Security numbers, was posted online in an Excel file and accessible through Google's cache for about a year and a half. Two hundred sixty students were affected.
- At Colorado State University, four files were discovered online that contained information about 300 students on the Warner College of Natural Resources Web site, including passwords and 208 Social Security numbers. The university has since removed the files and worked to get the information out of search engine caches.
- An Excel file containing personal information from 89 Brigham Young University medical school applicants was placed online. The file has since been removed.
- An Excel file was also discovered on Montana State University's Web site containing names, Social Security numbers, and other personal data on 42 employees who were hired in 2006. The file has since been removed.

Similarly, according the *The Iowa City Press-Citizen*, the University of Iowa's College of Engineering notified 216 former students earlier this month that their personal information had been posted

Related Articles

- IBM Opens Jazz Dev Community
- VMware Manages the Release Lifecycle
- Web 2.0 Threats Loom Large for IT
- Adobe Throttles Up Flash Media Server

Email this article　Printable Format

Events

CAMPUS TECHNOLOGY WINTER 2007

Thanks to the speakers, attendees, and exhibitors who made Campus Technology Winter 2007 a success!

- View Session Proceedings
- Access Audio Recordings

CAMPUS TECHNOLOGY 2007

Thanks to our attendees for our best event yet!

- View Session Proceedings
- Access Audio Recordings

Current issue

http://www.campustechnology.com/articles/57790/

Top Ten Security Need to Know

- Limit personal information in email
- Backing Up Files
- Passwords
- Know the lingo:Watch out for phishing, pharming & social engineering schemes/ recognize a hoax
- Determine if a website is secure
- Install/enable email filter & pop up blockers
- Use/install a firewall and anti virus protection
- Use/install Anti-spyware and how to check for spyware-malware-adware
- Recognize risks in wireless environments
- Review your Annual Credit Report

Limit Personal Information in Email

- Never offer your personal information, such as a credit card or social security number, via email or instant message

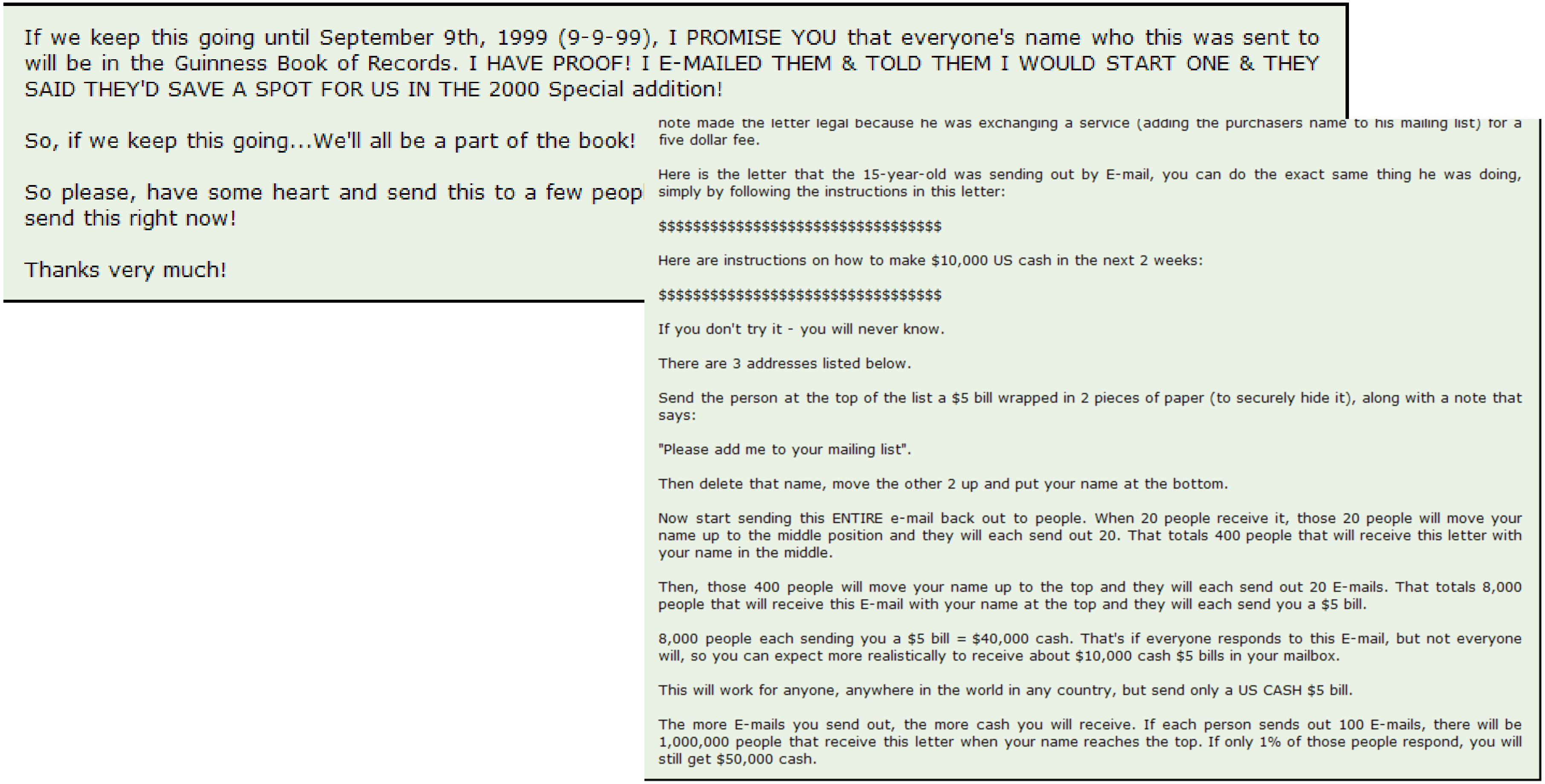
- Never provide personal information via a website, without first consulting the website’s privacy policy

Become Familiar with the Lingo

- Phishing
- Pharming
- Spear phishing
- Social Engineering
- Worm
- Virus
- Adware
- Spyware
- Spamming
- Spoofing
- Vishing
- Smishing
- Voice spam
- Malware
- Trojan Horse

Chain Letter Hoax

- **An email which urges the recipient to forward the email to other people**



If we keep this going until September 9th, 1999 (9-9-99), I PROMISE YOU that everyone's name who this was sent to will be in the Guinness Book of Records. I HAVE PROOF! I E-MAILED THEM & TOLD THEM I WOULD START ONE & THEY SAID THEY'D SAVE A SPOT FOR US IN THE 2000 Special addition!

So, if we keep this going...We'll all be a part of the book!

So please, have some heart and send this to a few peop
send this right now!

Thanks very much!

note made the letter legal because he was exchanging a service (adding the purchasers name to his mailing list) for a five dollar fee.

Here is the letter that the 15-year-old was sending out by E-mail, you can do the exact same thing he was doing, simply by following the instructions in this letter:

$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

Here are instructions on how to make $10,000 US cash in the next 2 weeks:

$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

If you don't try it - you will never know.

There are 3 addresses listed below.

Send the person at the top of the list a $5 bill wrapped in 2 pieces of paper (to securely hide it), along with a note that says:

"Please add me to your mailing list".

Then delete that name, move the other 2 up and put your name at the bottom.

Now start sending this ENTIRE e-mail back out to people. When 20 people receive it, those 20 people will move your name up to the middle position and they will each send out 20. That totals 400 people that will receive this letter with your name in the middle.

Then, those 400 people will move your name up to the top and they will each send out 20 E-mails. That totals 8,000 people that will receive this E-mail with your name at the top and they will each send you a $5 bill.

8,000 people each sending you a $5 bill = $40,000 cash. That's if everyone responds to this E-mail, but not everyone will, so you can expect more realistically to receive about $10,000 cash $5 bills in your mailbox.

This will work for anyone, anywhere in the world in any country, but send only a US CASH $5 bill.

The more E-mails you send out, the more cash you will receive. If each person sends out 100 E-mails, there will be 1,000,000 people that receive this letter when your name reaches the top. If only 1% of those people respond, you will still get $50,000 cash.

Phishing Scheme

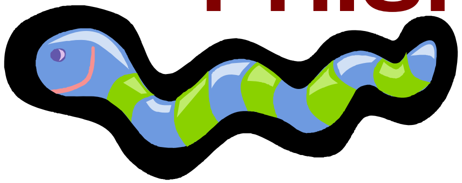
- DEAR SIR,

  URGENT AND CONFIDENTIAL BUSINESS PROPOSAL

  I AM MARIAM ABACHA, WIDOW OF THE LATE NIGERIAN HEAD OF STATE, GEN. SANI ABACHA. AFTER HE DEATH OF MY HUSBAND WHO DIED MYSTERIOUSLY AS A RESULT OF CARDIAC ARREST, I WAS INFORMED BY OUR LAWYER, BELLO GAMBARI THAT, MY HUSBAND WHO AT THAT TIME WAS THE PRESIDENT OF NIGERIA, CALLED HIM AND CONDUCTED HIM ROUND HIS APARTMENT AND SHOWED HIM FOUR METAL BOXES CONTAINING MONEY ALL IN FOREIGN EXCHANGE AND HE EQUALLY MADE HIM BELIEVE THAT THOSE BOXES ARE FOR ONWARD TRANSFER TO HIS OVERSEAS COUNTERPART FOR PERSONAL INVESTMENT.

  ALONG THE LINE, MY HUSBAND DIED AND SINCE THEN THE NIGERIAN GOVERNMENT HAS BEEN AFTER US, MOLESTING, POLICING AND FREEZING OUR BANK ACCOUNTS AND EVEN MY ELDEST SON RIGHT NOW IS IN DETENTION. MY FAMILY ACCOUNT IN SWITZERLAND WORTH US$22,000,000.00 AND 120,000,000.00 DUTCH MARK HAS BEEN CONFISCATED BY THE GOVERNMENT. THE GOVERNMENT IS INTERROGATING HIM (MY SON MOHAMMED) ABOUT OUR ASSET AND SOME VITAL DOCUMENTS. IT WAS IN THE COURSE OF THESE, AFTER THE BURIAL RITE AND CUSTOMS, THAT OUR LAWYER SAW YOUR NAME AND ADDRESS FROM THE PUBLICATION OF THE NIGERIAN BUSINESS PROMOTION AGENCY. THIS IS WHY I AM USING THIS OPPORTUNITY TO SOLICIT FOR YOUR CO-OPERATION AND ASSISTANCE TO HELP ME AS A VERY SINCERE RESPONSIBLE PERSON. I HAVE ALL THE TRUST IN YOU AND I KNOW THAT YOU WILL NOT SIT ON THIS MONEY.

PHISHING: Bait or Prey?

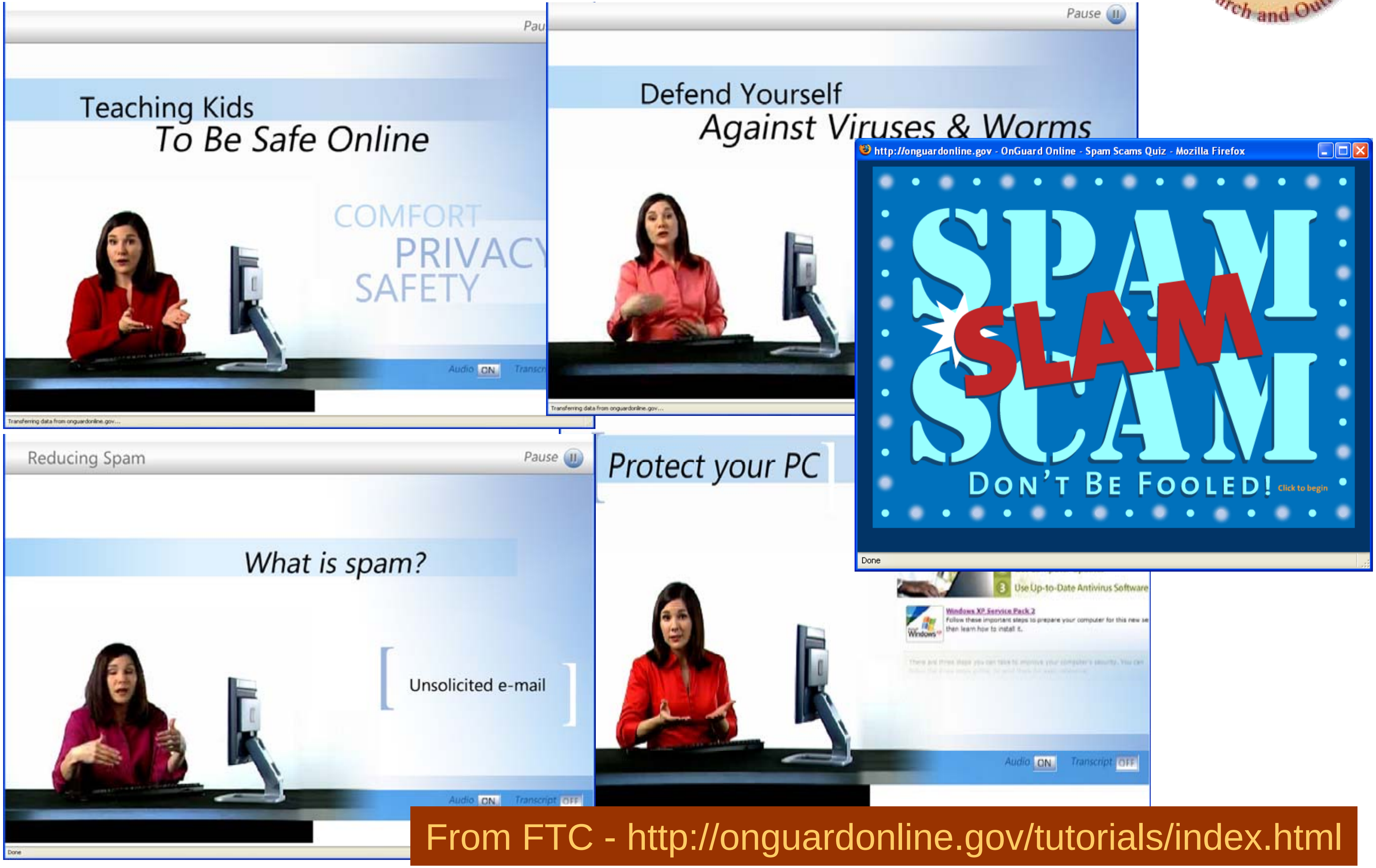


We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity.

- *“Phishers” send spam or pop-up messages*
- DON’T click on the URL in the pop up
- Open a new browser window and type the URL into the address field, watching that the actual URL of the site you visit doesn't change and is still the one you intended to visit.

Forward spam that is phishing for information to spam@uce.gov

Watch out for phishing, pharming social engineering schemes



Teaching Kids
To Be Safe Online

COMFORT
PRIVACY
SAFETY

Transferring data from onguardonline.gov...

Defend Yourself
Against Viruses & Worms

Transferring data from onguardonline.gov...

http://onguardonline.gov - OnGuard Online - Spam Scams Quiz - Mozilla Firefox

SPAM SCAM SLAM

DON'T BE FOOLED! Click to begin

Done

Reducing Spam

What is spam?

Unsolicited e-mail

Done

Protect your PC

3 Use Up-to-Date Antivirus Software

Windows XP Service Pack 2
Follow these important steps to prepare your computer for this new se
then learn how to install it.

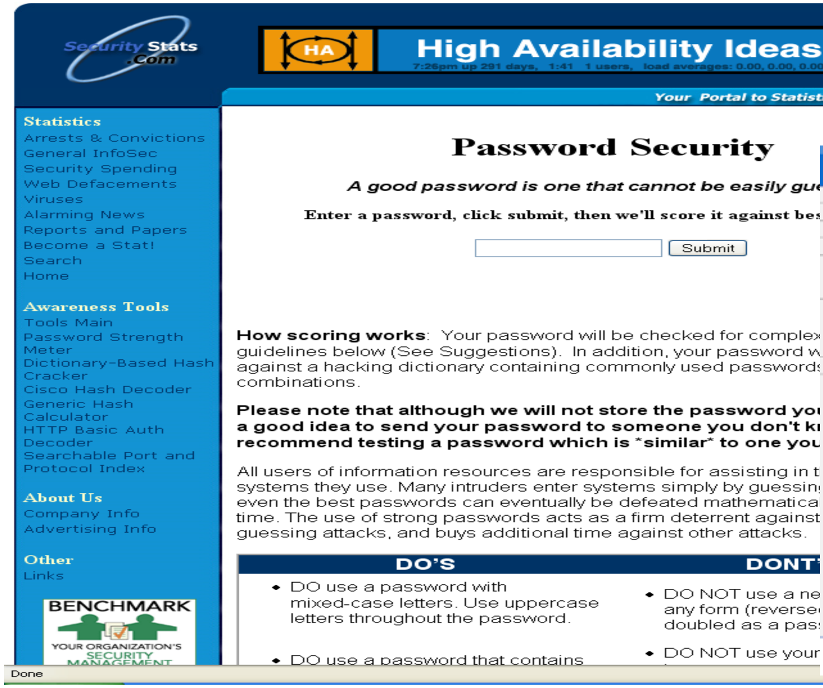
From FTC - http://onguardonline.gov/tutorials/index.html

Passwords

- 8+ character
- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Punctuation marks (!@#$%^&*()_+=-

Humorous Video from George Mason

- http://itu.gmu.edu/security/practices/



Password Security

A good password is one that cannot be easily gue

Enter a password, click submit, then we'll score it against bes

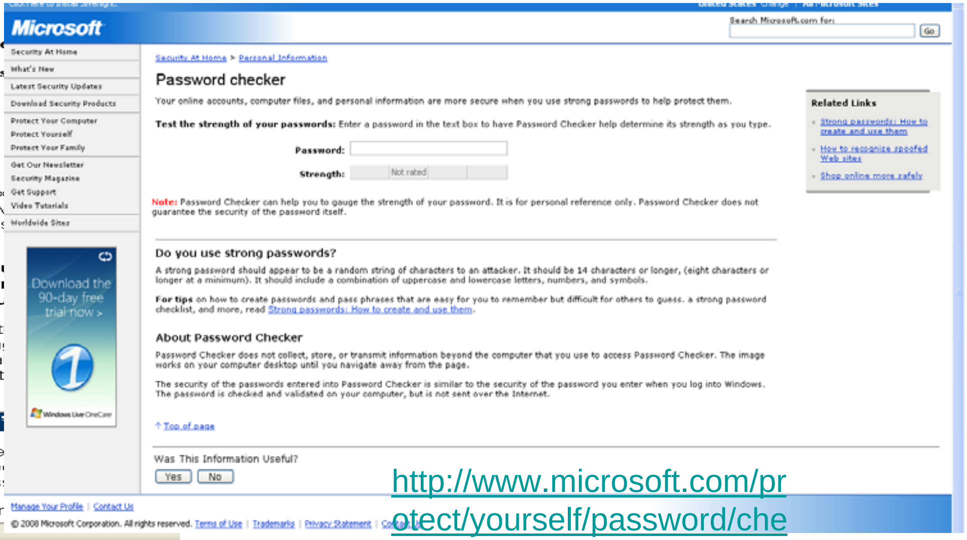
How scoring works: Your password will be checked for complex guidelines below (See Suggestions). In addition, your password w against a hacking dictionary containing commonly used passwords combinations.

Please note that although we will not store the password you a good idea to send your password to someone you don't kı recommend testing a password which is *similar* to one you

All users of information resources are responsible for assisting in t systems they use. Many intruders enter systems simply by guessin even the best passwords can eventually be defeated mathematica time. The use of strong passwords acts as a firm deterrent against guessing attacks, and buys additional time against other attacks.

DO'S	DONT'
• DO use a password with mixed-case letters. Use uppercase letters throughout the password.	• DO NOT use a ne any form (reverse doubled as a pas
• DO use a password that contains	• DO NOT use your

http://www.securitystats.com/tools/password.php


United States Change | All Microsoft Sites
Microsoft
Search Microsoft.com for:
Go
Security At Home
What's New
Latest Security Updates
Download Security Products
Protect Your Computer
Protect Yourself
Protect Your Family
Get Our Newsletter
Security Magazine
Get Support
Video Tutorials
Worldwide Sites
Download the 90-day free trial now >
Windows Live OneCare
Related Links
Strong passwords: How to create and use them
How to recognize spoofed Web sites
Shop online more safely
Manage Your Profile | Contact Us
© 2008 Microsoft Corporation. All rights reserved. Terms of Use | Trademarks | Privacy Statement | Contact Us

Security At Home > Personal Information

Password checker

Your online accounts, computer files, and personal information are more secure when you use strong passwords to help protect them.

Test the strength of your passwords: Enter a password in the text box to have Password Checker help determine its strength as you type.

Password:

Strength: Not rated

Note: Password Checker can help you to gauge the strength of your password. It is for personal reference only. Password Checker does not guarantee the security of the password itself.

Do you use strong passwords?

A strong password should appear to be a random string of characters to an attacker. It should be 14 characters or longer, (eight characters or longer at a minimum). It should include a combination of uppercase and lowercase letters, numbers, and symbols.

For tips on how to create passwords and pass phrases that are easy for you to remember but difficult for others to guess. a strong password checklist, and more, read Strong passwords: How to create and use them.

About Password Checker

Password Checker does not collect, store, or transmit information beyond the computer that you use to access Password Checker. The image works on your computer desktop until you navigate away from the page.

The security of the passwords entered into Password Checker is similar to the security of the password you enter when you log into Windows. The password is checked and validated on your computer, but is not sent over the Internet.

↑ Top of page

Was This Information Useful?

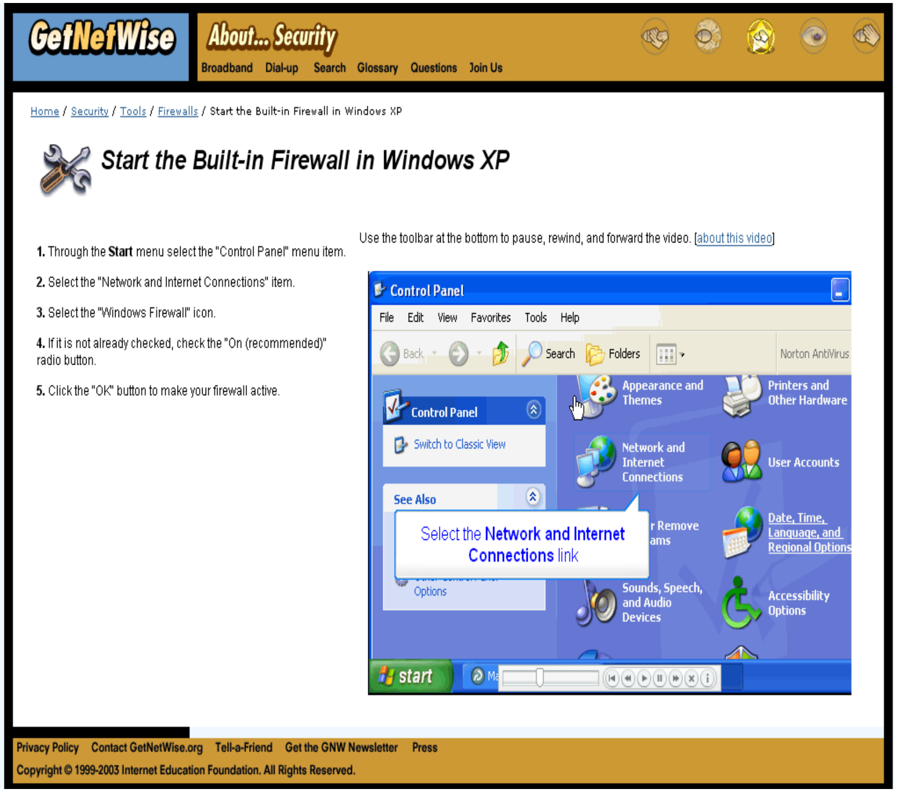
Yes No

http://www.microsoft.com/protect/yourself/password/checker.mspx

Install a Firewall

- Activate your built-in firewall or download/install a firewall for your computer.
- Prevents unauthorized Internet traffic from entering or leaving your computer.
- A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources

- http://security.getnetwise.org/tools/firewall


GetNetWise
About... Security
Broadband
Dial-up
Search
Glossary
Questions
Join Us
Home / Security / Tools / Firewalls / Start the Built-in Firewall in Windows XP

Start the Built-in Firewall in Windows XP

1. Through the **Start** menu select the "Control Panel" menu item.

2. Select the "Network and Internet Connections" item.

3. Select the "Windows Firewall" icon.

4. If it is not already checked, check the "On (recommended)" radio button.

5. Click the "OK" button to make your firewall active.

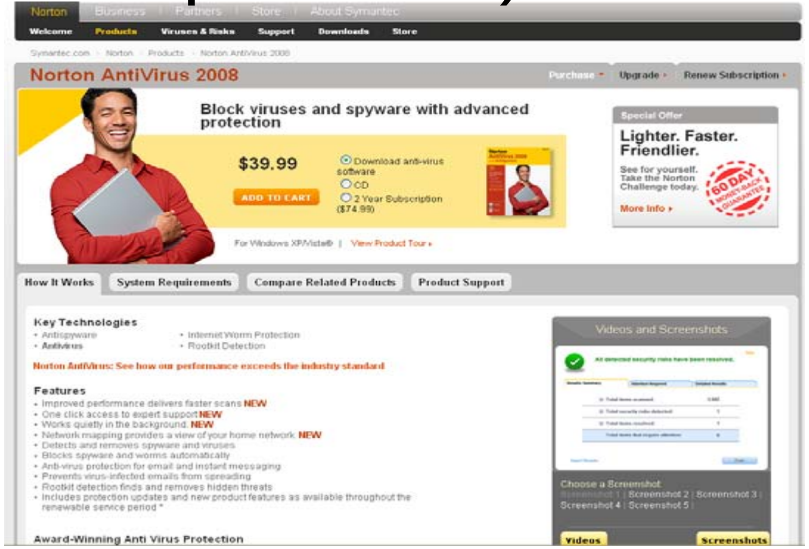
Use the toolbar at the bottom to pause, rewind, and forward the video. [about this video]

Select the **Network and Internet Connections** link

Copyright © 1999-2003 Internet Education Foundation. All Rights Reserved.

Anti-Virus Protection

- Detects and removes computer viruses
- Most programs can check every day for new DAT (virus definition-description files)


Norton | Business | Partners | Store | About Symantec
Welcome Products Viruses & Risks Support Downloads Store
Symantec.com › Norton › Products › Norton AntiVirus 2008
Purchase ▸ Upgrade ▸ Renew Subscription ▸

Norton AntiVirus 2008

Block viruses and spyware with advanced protection

$39.99

ADD TO CART

● Download anti-virus software
○ CD
○ 2 Year Subscription ($74.99)

For Windows XP/Vista® | View Product Tour ▸

Special Offer

Lighter. Faster. Friendlier.

See for yourself. Take the Norton Challenge today.

More Info ▸

60 DAY MONEY-BACK GUARANTEE
How It Works | System Requirements | Compare Related Products | Product Support

Key Technologies
- Antispyware
- Antivirus
- Internet Worm Protection
- Rootkit Detection

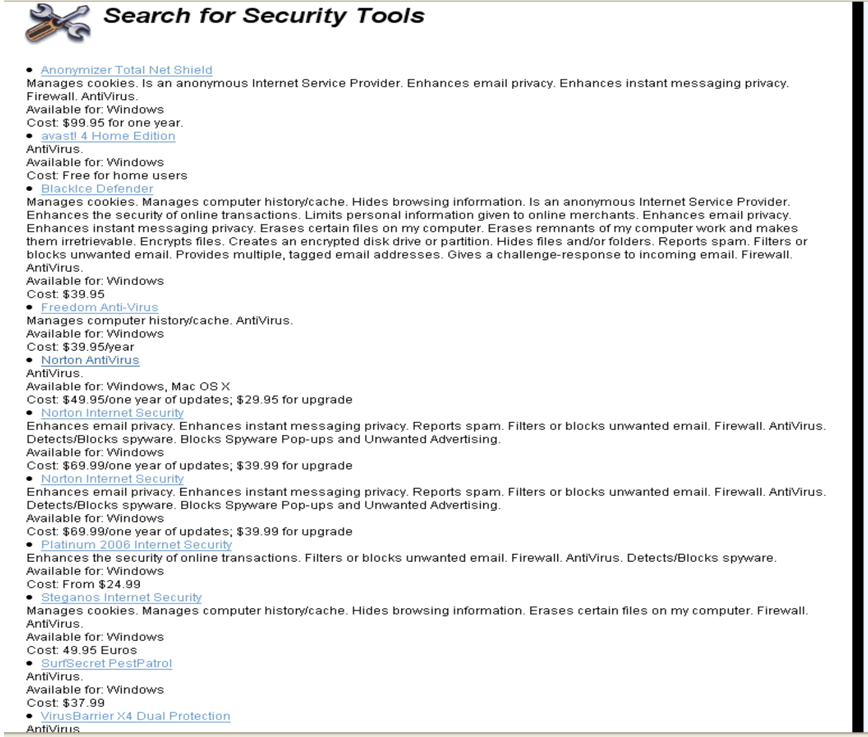
Norton AntiVirus: See how our performance exceeds the industry standard

Features
- Improved performance delivers faster scans NEW
- One click access to expert support NEW
- Works quietly in the background. NEW
- Network mapping provides a view of your home network. NEW
- Detects and removes spyware and viruses
- Blocks spyware and worms automatically
- Anti-virus protection for email and instant messaging
- Prevents virus-infected emails from spreading
- Rootkit detection finds and removes hidden threats
- Includes protection updates and new product features as available throughout the renewable service period *

Award-Winning Anti Virus Protection

Videos and Screenshots
Choose a Screenshot
Screenshot 1 | Screenshot 2 | Screenshot 3 | Screenshot 4 | Screenshot 5 |
Videos
Screenshots

http://www.symantec.com/norton/products/overview.jsp?pcid=mp&pvid=nis2008



Search for Security Tools

- Anonymizer Total Net Shield

Manages cookies. Is an anonymous Internet Service Provider. Enhances email privacy. Enhances instant messaging privacy. Firewall. AntiVirus.
Available for: Windows
Cost: $99.95 for one year.

- avast! 4 Home Edition

AntiVirus.
Available for: Windows
Cost: Free for home users

- BlackIce Defender

Manages cookies. Manages computer history/cache. Hides browsing information. Is an anonymous Internet Service Provider. Enhances the security of online transactions. Limits personal information given to online merchants. Enhances email privacy. Enhances instant messaging privacy. Erases certain files on my computer. Erases remnants of my computer work and makes them irretrievable. Encrypts files. Creates an encrypted disk drive or partition. Hides files and/or folders. Reports spam. Filters or blocks unwanted email. Provides multiple, tagged email addresses. Gives a challenge-response to incoming email. Firewall. AntiVirus.
Available for: Windows
Cost: $39.95

- Freedom Anti-Virus

Manages computer history/cache. AntiVirus.
Available for: Windows
Cost: $39.95/year

- Norton AntiVirus

AntiVirus.
Available for: Windows, Mac OS X
Cost: $49.95/one year of updates; $29.95 for upgrade

- Norton Internet Security

Enhances email privacy. Enhances instant messaging privacy. Reports spam. Filters or blocks unwanted email. Firewall. AntiVirus. Detects/Blocks spyware. Blocks Spyware Pop-ups and Unwanted Advertising.
Available for: Windows
Cost: $69.99/one year of updates; $39.99 for upgrade

- Norton Internet Security

Enhances email privacy. Enhances instant messaging privacy. Reports spam. Filters or blocks unwanted email. Firewall. AntiVirus. Detects/Blocks spyware. Blocks Spyware Pop-ups and Unwanted Advertising.
Available for: Windows
Cost: $69.99/one year of updates; $39.99 for upgrade

- Platinum 2006 Internet Security

Enhances the security of online transactions. Filters or blocks unwanted email. Firewall. AntiVirus. Detects/Blocks spyware.
Available for: Windows
Cost: From $24.99

- Steganos Internet Security

Manages cookies. Manages computer history/cache. Hides browsing information. Erases certain files on my computer. Firewall. AntiVirus.
Available for: Windows
Cost: 49.95 Euros

- SurfSecret PestPatrol

AntiVirus.
Available for: Windows
Cost: $37.99

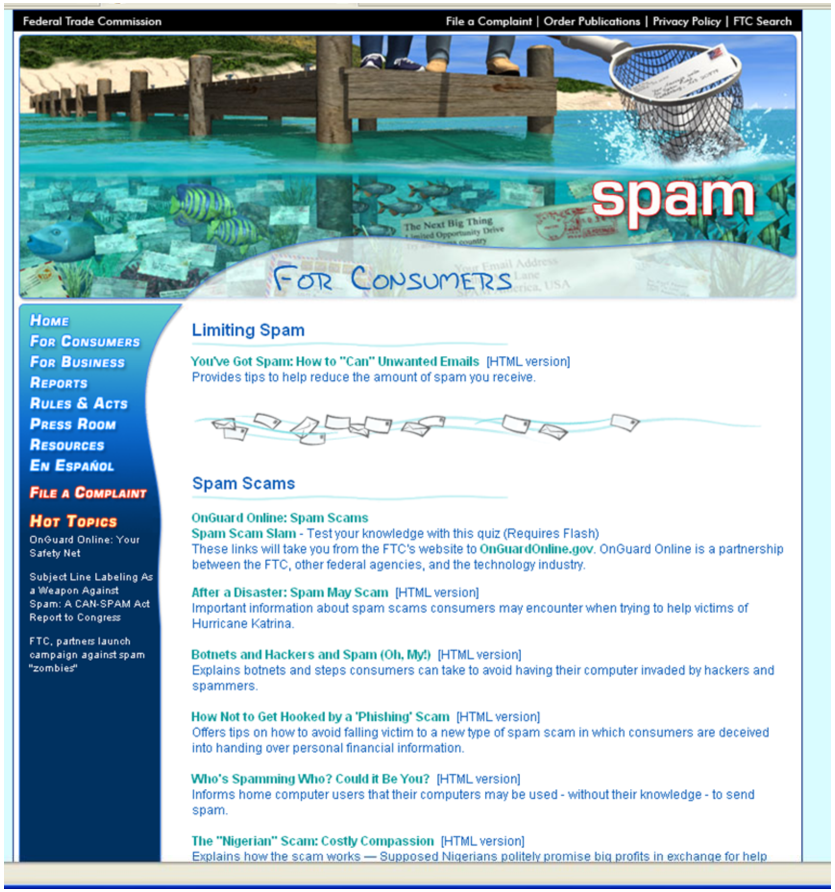
- VirusBarrier X4 Dual Protection

AntiVirus

http://security.getnetwise.org/tools/search

Anti-Spam Protection

- Program used to detect unsolicited and unwanted email and prevent those messages from getting to a user's inbox.
- Looks for certain criteria on which it bases judgments
- Can use email program, filter or server software



Federal Trade Commission

File a Complaint | Order Publications | Privacy Policy | FTC Search

Home
For Consumers
For Business
Reports
Rules & Acts
Press Room
Resources
En Español

File a Complaint

Hot Topics

OnGuard Online: Your Safety Net

Subject Line Labeling As a Weapon Against Spam: A CAN-SPAM Act Report to Congress

FTC, partners launch campaign against spam "zombies"

Limiting Spam

You've Got Spam: How to "Can" Unwanted Emails [HTML version]
Provides tips to help reduce the amount of spam you receive.

Spam Scams

OnGuard Online: Spam Scams
Spam Scam Slam - Test your knowledge with this quiz (Requires Flash)
These links will take you from the FTC's website to OnGuardOnline.gov. OnGuard Online is a partnership between the FTC, other federal agencies, and the technology industry.

After a Disaster: Spam May Scam [HTML version]
Important information about spam scams consumers may encounter when trying to help victims of Hurricane Katrina.

Botnets and Hackers and Spam (Oh, My!) [HTML version]
Explains botnets and steps consumers can take to avoid having their computer invaded by hackers and spammers.

How Not to Get Hooked by a 'Phishing' Scam [HTML version]
Offers tips on how to avoid falling victim to a new type of spam scam in which consumers are deceived into handing over personal financial information.

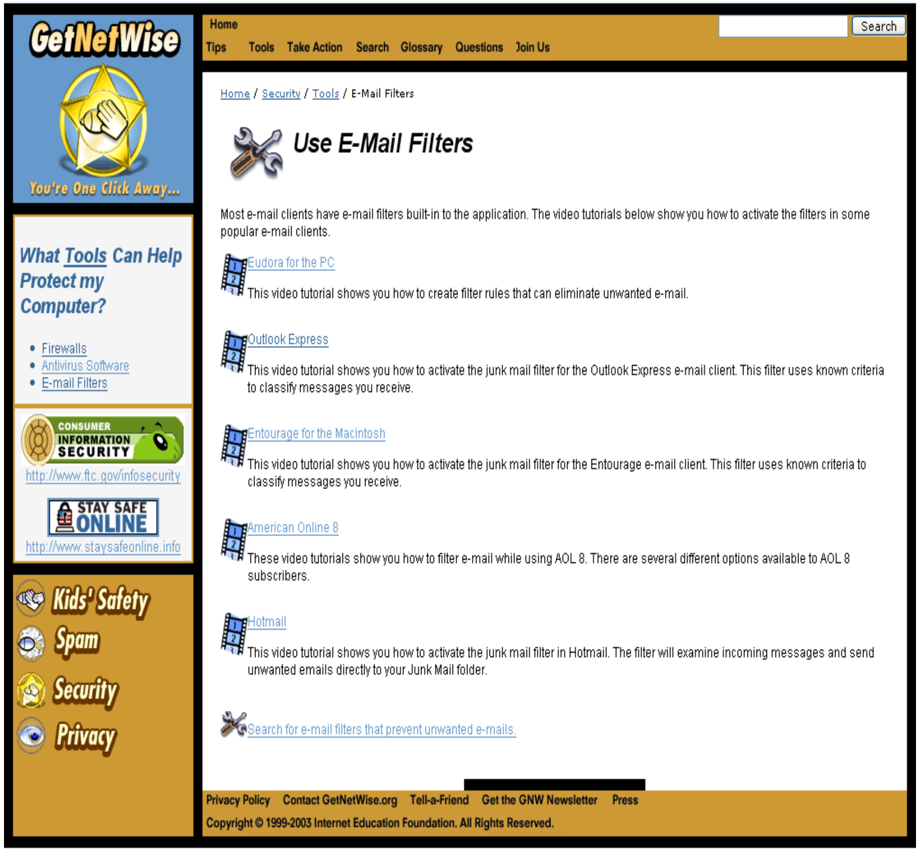
Who's Spamming Who? Could it Be You? [HTML version]
Informs home computer users that their computers may be used - without their knowledge - to send spam.

The "Nigerian" Scam: Costly Compassion [HTML version]
Explains how the scam works — Supposed Nigerians politely promise big profits in exchange for help

http://www.ftc.gov/bcp/conline/edcams/spam/consumer.htm

E-mail filters

- Web-based e-mail services provide filters to limit e-mail that flows into your inbox
- Filter --known criteria such as phrasing, font style (ex: all caps), and symbols (ex: dollar signs, exclamation points) to classify messages as junk.



Home / Security / Tools / E-Mail Filters

Use E-Mail Filters

Most e-mail clients have e-mail filters built-in to the application. The video tutorials below show you how to activate the filters in some popular e-mail clients.

Eudora for the PC
This video tutorial shows you how to create filter rules that can eliminate unwanted e-mail.

Outlook Express
This video tutorial shows you how to activate the junk mail filter for the Outlook Express e-mail client. This filter uses known criteria to classify messages you receive.

Entourage for the Macintosh
This video tutorial shows you how to activate the junk mail filter for the Entourage e-mail client. This filter uses known criteria to classify messages you receive.

American Online 8
These video tutorials show you how to filter e-mail while using AOL 8. There are several different options available to AOL 8 subscribers.

Hotmail
This video tutorial shows you how to activate the junk mail filter in Hotmail. The filter will examine incoming messages and send unwanted emails directly to your Junk Mail folder.

Search for e-mail filters that prevent unwanted e-mails.

Copyright © 1999-2003 Internet Education Foundation. All Rights Reserved.

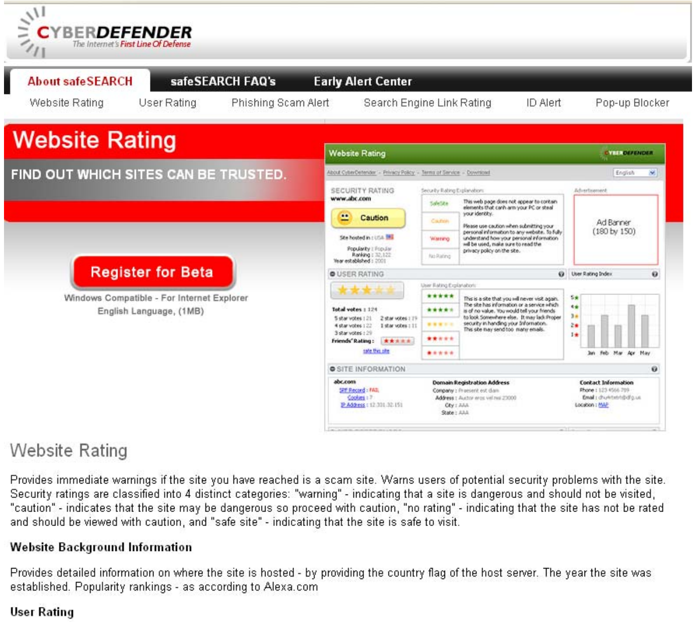
Use e-mail filters
http://security.getnetwise.org/tools/filters

Who’s on the Other Side?

- Dealing w/ new site?
  - Call the seller’s/contact
    - can’t find a working phone number, take your business elsewhere
- Type the site’s name into a search engine: If you find unfavorable reviews posted, you may be better off doing business with a different seller
- Read the site’s privacy policy to learn how it uses and shares your personal information

Secure Website?

- Use software toolbar that rates websites and warns you if a site has gotten unfavorable reports from experts and other Internet users
  - http://beta.cyberdefender.com/



Website Rating

Provides immediate warnings if the site you have reached is a scam site. Warns users of potential security problems with the site. Security ratings are classified into 4 distinct categories: "warning" - indicating that a site is dangerous and should not be visited, "caution" - indicates that the site may be dangerous so proceed with caution, "no rating" - indicating that the site has not be rated and should be viewed with caution, and "safe site" - indicating that the site is safe to visit.

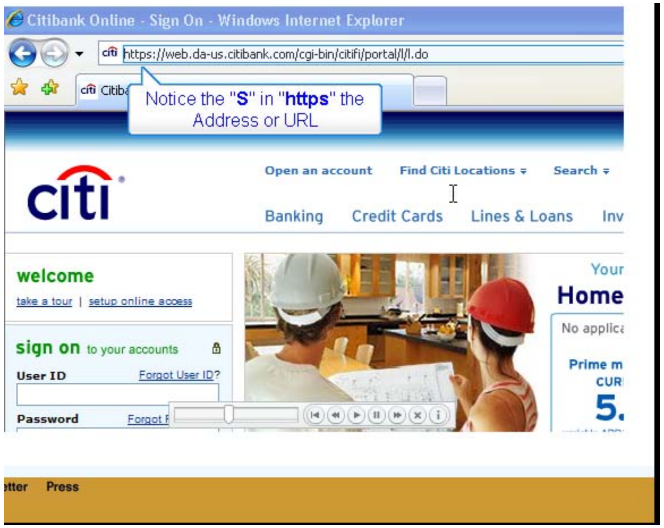
Website Background Information

Provides detailed information on where the site is hosted - by providing the country flag of the host server. The year the site was established. Popularity rankings - as according to Alexa.com

User Rating

- **Signs of Safe Site**
  - closed padlock on the browser's status bar, before you enter your personal and financial information When you're asked to provide payment information, the beginning of the *Web site's URL address should change from http to shttp or https*, indicating that the purchase is encrypted or secured

    View secure SSL tutorial http://security.getnetwise.org/tips/secure-web.php


Citibank Online - Sign On - Windows Internet Explorer
https://web.da-us.citibank.com/cgi-bin/citifi/portal/l/l.do
Notice the "S" in "https" the Address or URL
citi
Open an account
Find Citi Locations
Search
Banking
Credit Cards
Lines & Loans
Inv
welcome
take a tour | setup online access
sign on to your accounts
User ID
Forgot User ID?
Password
Your
Home
Press

What to do if you have Malicious Software

- Signs of infection
  - May seem sluggish or slow down significantly
  - Might ‘lock up’ more often than usual
  - Browser program may not work correctly
  - Pop-up ads
  - Unusual hard drive activity

- Ways to get rid of
  - Use your anti-virus software (you have one right!!!)
    - Scan all your drives
  - Use Microsoft Malicious Software Removal Tool
    - http://www.microsoft.com/security/malwareremove/default.mspx
  - McAfee: http://ts.mcafeehelp.com/?siteID=1&resolution=1280x1024&rurl=vrContactOptions.asp
  - Symantec: http://security.symantec.com/sscv6/default.asp?productid=symhome&langid=ie&venid=sym

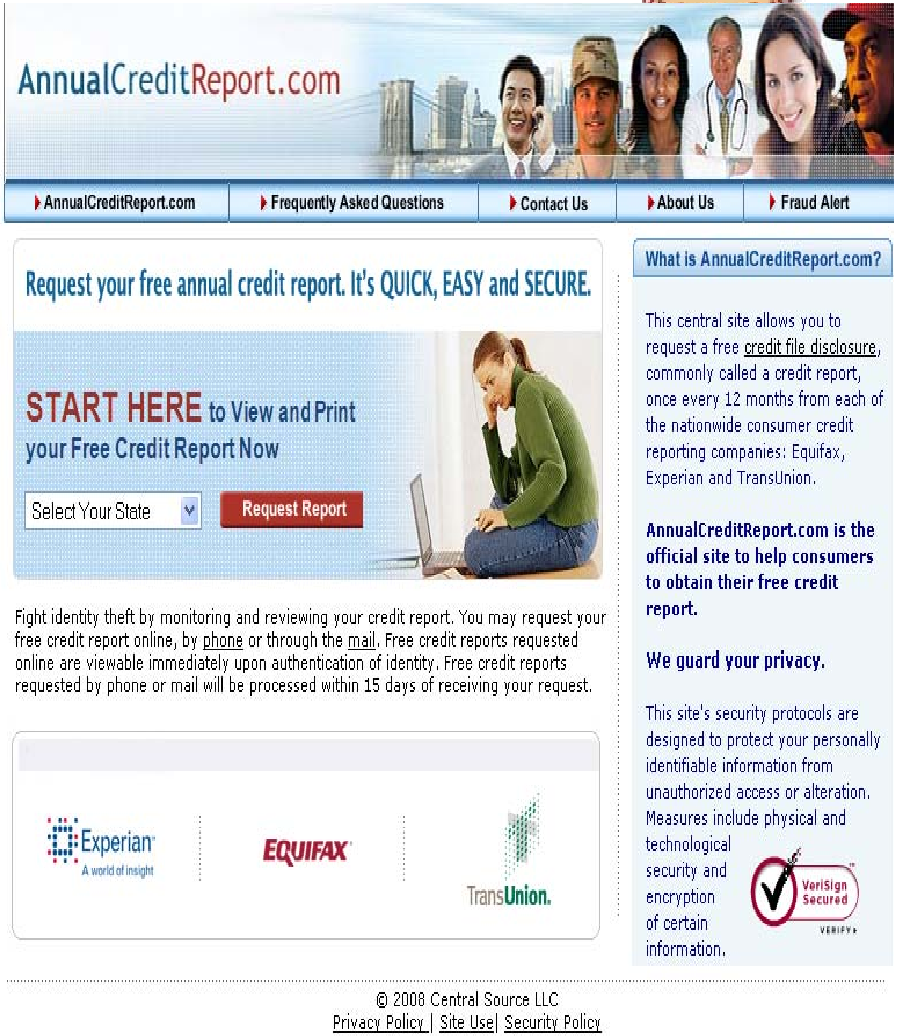
What to do if you have your share of adware/spyware

- Signs of infection
  - An affected computer can rapidly become infected with large numbers of spyware components
  - Pop-up advertisements
  - Unwanted behavior and degradation of system performance.
  - Significant unwanted CPU activity, disk usage, and network traffic
    - Slows down other programs
    - Stability issues—application or system

- Ways to get rid of or protect
  - **Anti-spyware programs**
    - *OptOut*
    - *Ad-Aware SE*
    - *Spybot - Search & Destroy*

Annual Credit Report

- **annualcreditreport.com**
  - *only* site you should be using (the sound and look-alikes are all subscription based scam artists)
- The credit reporting agencies *can* and *will* try to sell you things (FICO scores, monitoring, insurance, etc)
- You do not need to give anyone your credit card number to obtain your free credit report



Request your free annual credit report. It's QUICK, EASY and SECURE.

START HERE to View and Print your Free Credit Report Now

Fight identity theft by monitoring and reviewing your credit report. You may request your free credit report online, by phone or through the mail. Free credit reports requested online are viewable immediately upon authentication of identity. Free credit reports requested by phone or mail will be processed within 15 days of receiving your request.

What is AnnualCreditReport.com?

This central site allows you to request a free credit file disclosure, commonly called a credit report, once every 12 months from each of the nationwide consumer credit reporting companies: Equifax, Experian and TransUnion.

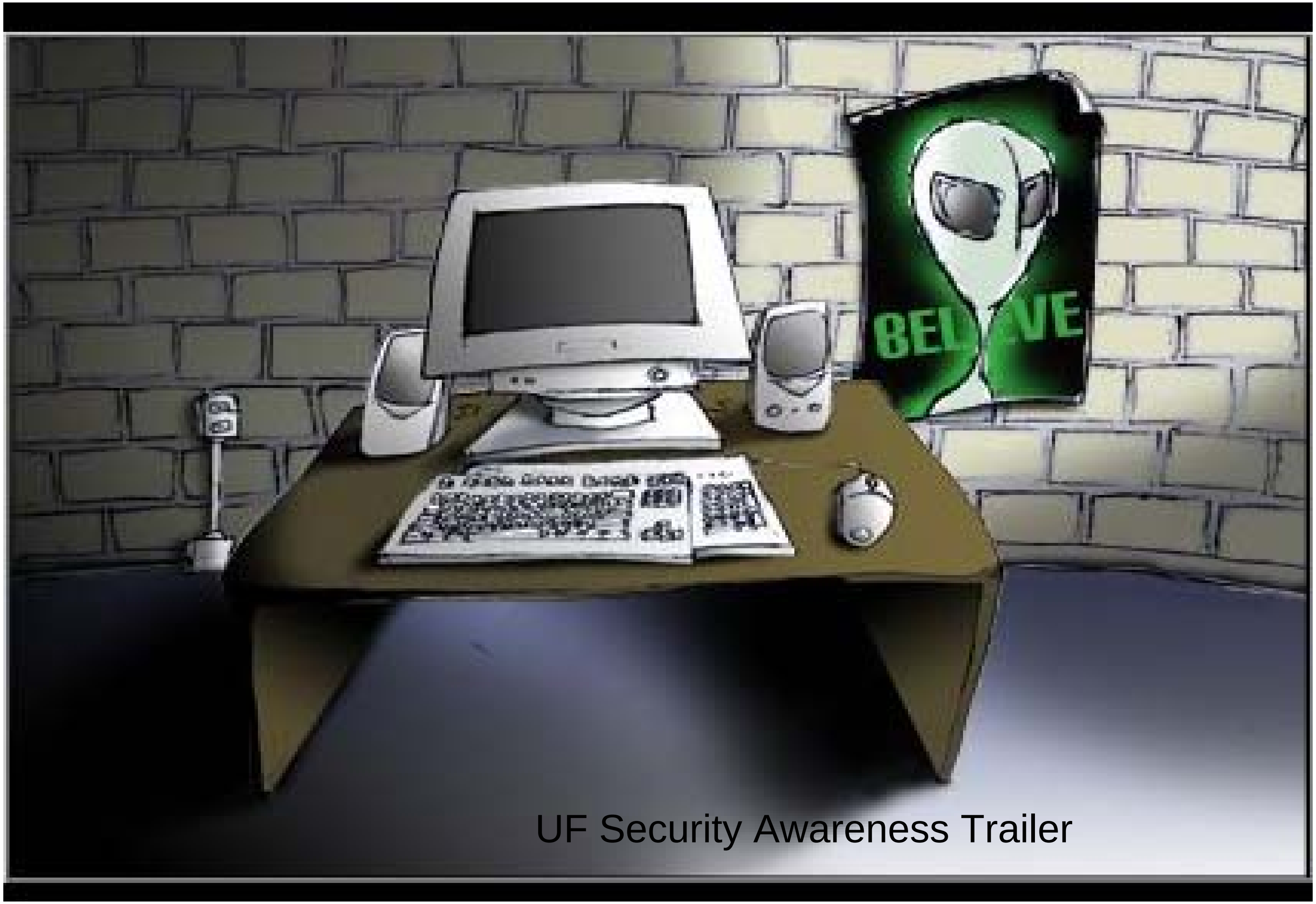
AnnualCreditReport.com is the official site to help consumers to obtain their free credit report.

We guard your privacy.

This site's security protocols are designed to protect your personally identifiable information from unauthorized access or alteration. Measures include physical and technological security and encryption of certain information.

© 2008 Central Source LLC
Privacy Policy | Site Use| Security Policy

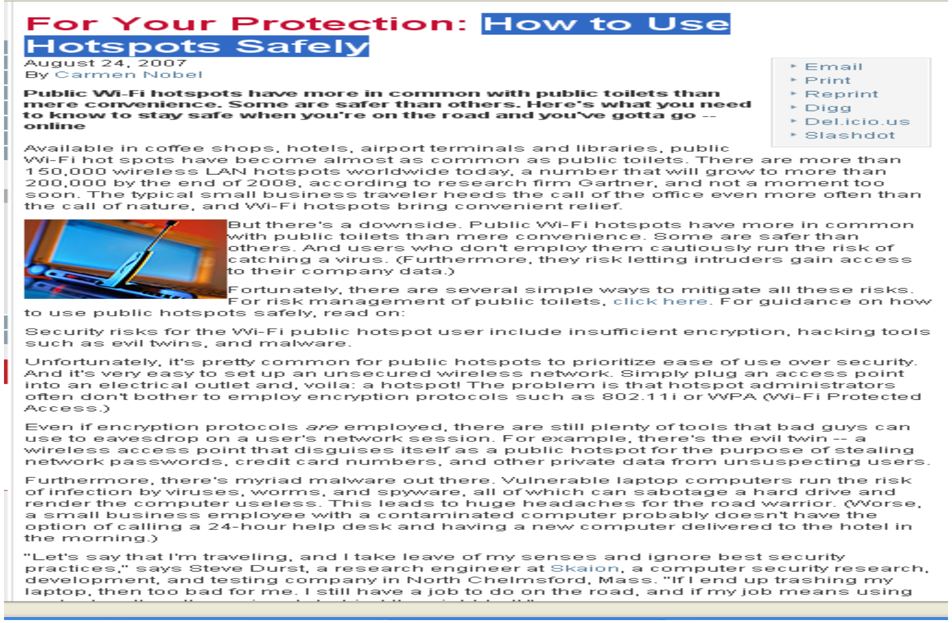
http://www.itsa.ufl.edu/trailer/



UF Security Awareness Trailer

How to Use Hotspots Safely

- Connect only to legitimate wi-fi hot-spots - "Know your network"
- Encrypt sensitive data
- Use and update your Anti-virus software
- Use a firewall
- Update your operating system



For Your Protection: How to Use Hotspots Safely

August 24, 2007
By Carmen Nobel

- Email
- Print
- Reprint
- Digg
- Del.icio.us
- Slashdot

Public Wi-Fi hotspots have more in common with public toilets than mere convenience. Some are safer than others. Here's what you need to know to stay safe when you're on the road and you've gotta go -- online

Available in coffee shops, hotels, airport terminals and libraries, public Wi-Fi hot spots have become almost as common as public toilets. There are more than 150,000 wireless LAN hotspots worldwide today, a number that will grow to more than 200,000 by the end of 2008, according to research firm Gartner, and not a moment too soon. The typical small business traveler heeds the call of the office even more often than the call of nature, and Wi-Fi hotspots bring convenient relief.

But there's a downside. Public Wi-Fi hotspots have more in common with public toilets than mere convenience. Some are safer than others. And users who don't employ them cautiously run the risk of catching a virus. (Furthermore, they risk letting intruders gain access to their company data.)

Fortunately, there are several simple ways to mitigate all these risks. For risk management of public toilets, click here. For guidance on how to use public hotspots safely, read on:

Security risks for the Wi-Fi public hotspot user include insufficient encryption, hacking tools such as evil twins, and malware.

Unfortunately, it's pretty common for public hotspots to prioritize ease of use over security. And it's very easy to set up an unsecured wireless network. Simply plug an access point into an electrical outlet and, voila: a hotspot! The problem is that hotspot administrators often don't bother to employ encryption protocols such as 802.11i or WPA (Wi-Fi Protected Access.)

Even if encryption protocols *are* employed, there are still plenty of tools that bad guys can use to eavesdrop on a user's network session. For example, there's the evil twin -- a wireless access point that disguises itself as a public hotspot for the purpose of stealing network passwords, credit card numbers, and other private data from unsuspecting users.

Furthermore, there's myriad malware out there. Vulnerable laptop computers run the risk of infection by viruses, worms, and spyware, all of which can sabotage a hard drive and render the computer useless. This leads to huge headaches for the road warrior. (Worse, a small business employee with a contaminated computer probably doesn't have the option of calling a 24-hour help desk and having a new computer delivered to the hotel in the morning.)

"Let's say that I'm traveling, and I take leave of my senses and ignore best security practices," says Steve Durst, a research engineer at Skaion, a computer security research, development, and testing company in North Chelmsford, Mass. "If I end up trashing my laptop, then too bad for me. I still have a job to do on the road, and if my job means using

Public Hotspots Prioritize Ease of Use Over Security

- Use a **firewall and a VPN-**Virtual Private Network
- Use **antivirus** software
- **Turn off ad-hoc networking features--** *before* they arrive at a wireless hot spot
- **Turn off file share mode**
- **Turn off Wi Fi**
- **Encrypt**

Source: Carmen Nobel: http://bmighty.com/security/showArticle.jhtml?articleID=201801882

How to Turn Off Ad-hoc Mode in Windows

- In the Network Connections menu, click "***Wireless Network Connection***."
- Click "***change the settings of this connection***"
- ***Wait*** for the Windows Network Connection Properties window to open.
- Click the little tab that says "***Wireless Networks***"
- In that tab, click "**Advanced**"
- In the "Advanced" window, click "**Access point (infrastructure) networks only**"

Source: Carmen Nobel:
http://bmighty.com/security/showArticle.jhtml?articleID=201801882

How to Turn Off the File Sharing Feature

- File sharing feature is turned on by default
- On the Start menu, select ***Settings***
- Select ***Network Connections***
- Find the Internet connection and right-click to select ***Properties***
- Find the General tab. If there's a check mark next to File and Printer Sharing for Microsoft Networks, then click to ***uncheck it***. (If it's already unchecked, then leave well enough alone)

Source: Carmen Nobel: http://bmighty.com/security/showArticle.jhtml?articleID=201801882

How to Turn off Wi Fi Connection

- Turn off the radio when you don't need it
- Right-click on the wireless network icon in the right-hand corner of the screen. (That's the picture of the computer with radio waves coming out of it.)
- Click disable or wireless off

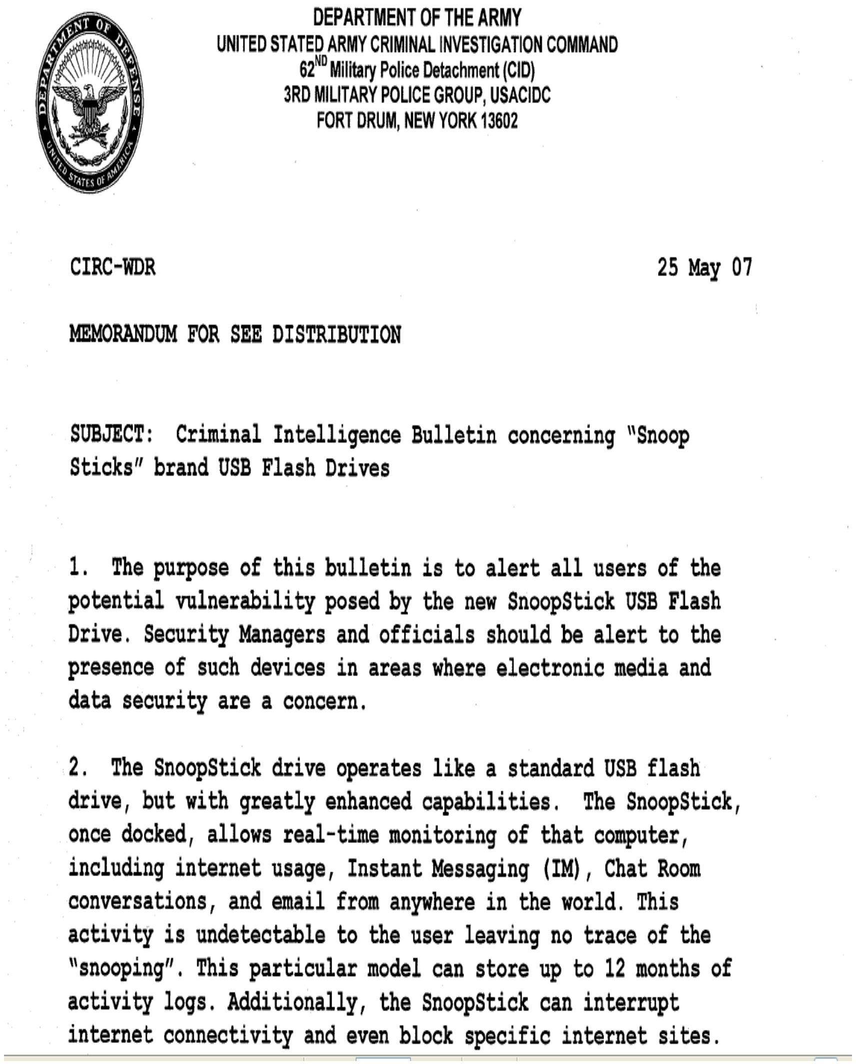
Source: Carmen Nobel:
http://bmighty.com/security/showArticle.jhtml?articleID=201801882

Don't be Lazy About Encryption

- Process may vary depending on the version of Windows on any given machine
- EX: Windows XP
  - Open Windows Explorer
  - Right-click the file or folder that you want to encrypt, and then click ***Properties***
  - On the General tab, click ***Advanced***
  - Check the box that says, "***Encrypt contents to secure data check"***

Source: Carmen Nobel:
http://bmighty.com/security/showArticle.jhtml?articleID=201801882

Snoop Sticks



DEPARTMENT OF THE ARMY
UNITED STATED ARMY CRIMINAL INVESTIGATION COMMAND
62ND Military Police Detachment (CID)
3RD MILITARY POLICE GROUP, USACIDC
FORT DRUM, NEW YORK 13602

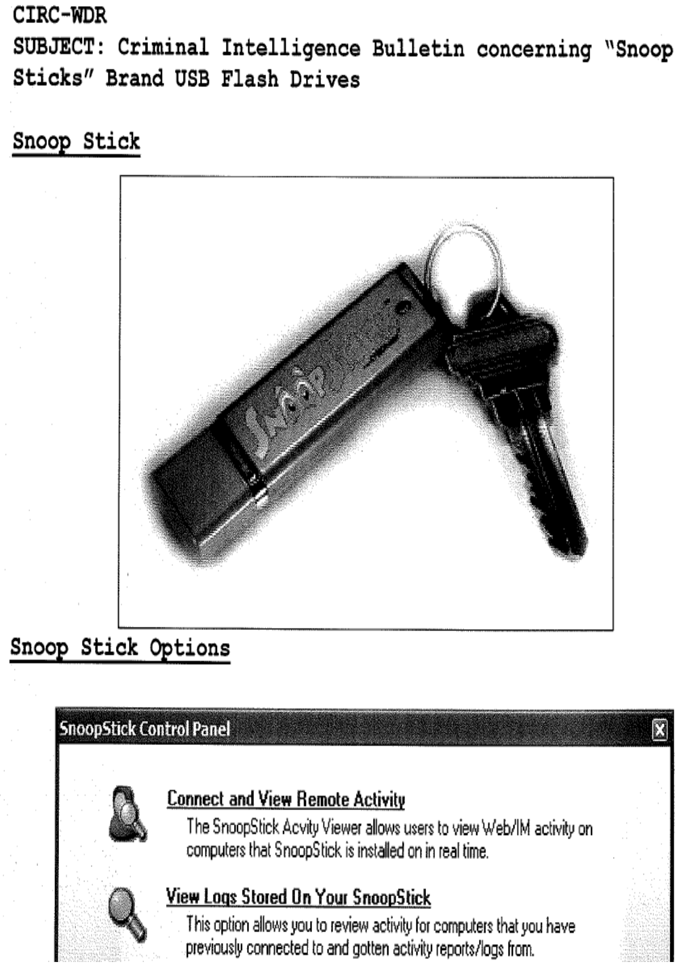
CIRC-WDR 25 May 07

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Criminal Intelligence Bulletin concerning "Snoop Sticks" brand USB Flash Drives

1. The purpose of this bulletin is to alert all users of the potential vulnerability posed by the new SnoopStick USB Flash Drive. Security Managers and officials should be alert to the presence of such devices in areas where electronic media and data security are a concern.

2. The SnoopStick drive operates like a standard USB flash drive, but with greatly enhanced capabilities. The SnoopStick, once docked, allows real-time monitoring of that computer, including internet usage, Instant Messaging (IM), Chat Room conversations, and email from anywhere in the world. This activity is undetectable to the user leaving no trace of the "snooping". This particular model can store up to 12 months of activity logs. Additionally, the SnoopStick can interrupt internet connectivity and even block specific internet sites.



CIRC-WDR
SUBJECT: Criminal Intelligence Bulletin concerning "Snoop Sticks" Brand USB Flash Drives

Snoop Stick

Snoop Stick Options

SnoopStick Control Panel

Connect and View Remote Activity
The SnoopStick Acvity Viewer allows users to view Web/IM activity on computers that SnoopStick is installed on in real time.

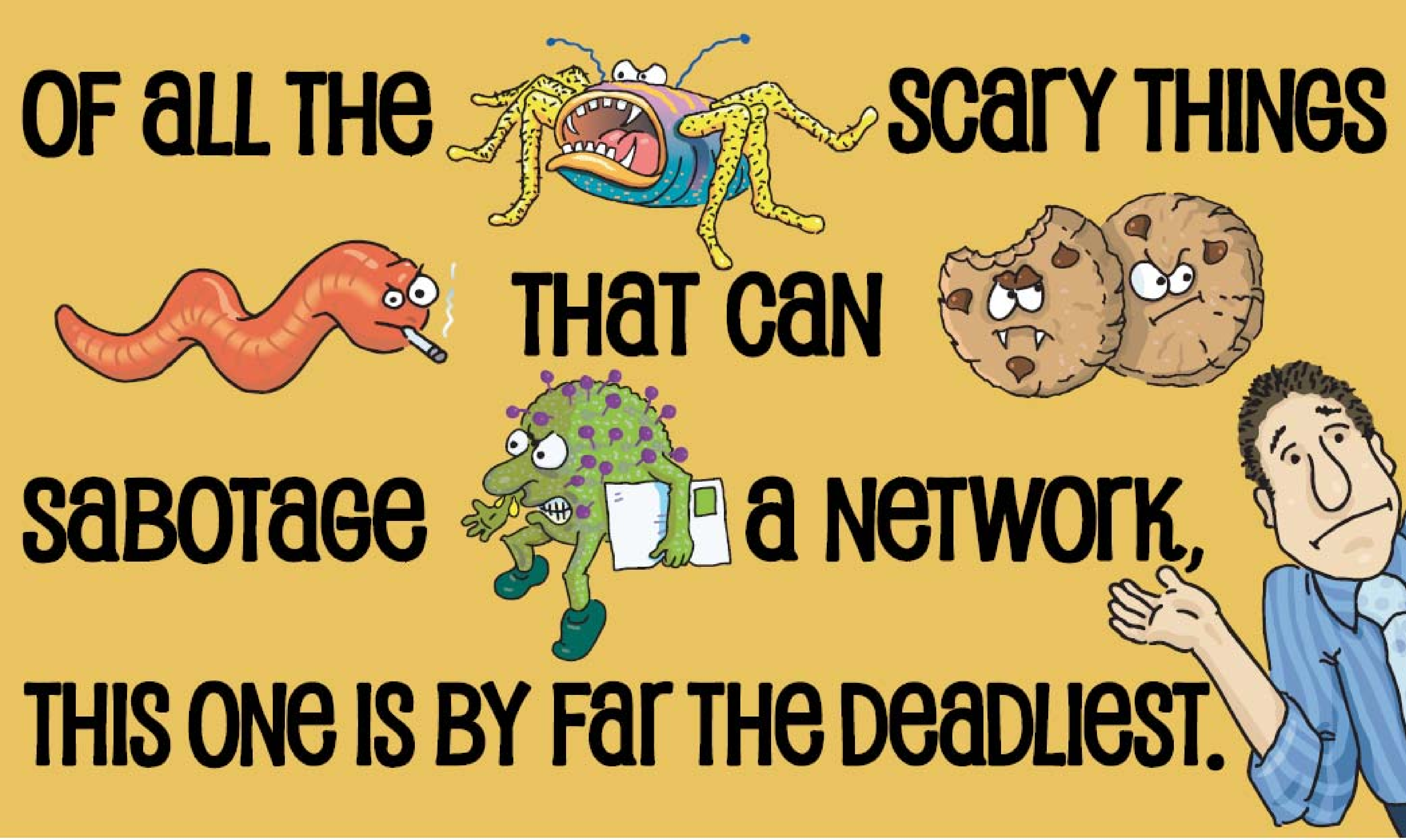
View Logs Stored On Your SnoopStick
This option allows you to review activity for computers that you have previously connected to and gotten activity reports/logs from.

Activities

- NCSA StaySafeOnline http://staysafeonline.org/basics/quiz.html
- James Mason's Computer Security Awareness tutorial page
  - http://www.jmu.edu/computing/security/ -
- George Mason University's IT Security Quiz
  - http://itu.gmu.edu/security/quiz/
- Carnegie Mellon's Home Computer Security tutorial site
- Microsoft Spyware Quiz part 1 and part 2 http://www.microsoft.com/nz/athome/security/quiz/default.mspx

Activities

- Humorous video on Passwords at George Mason's Security Website http://itu.gmu.edu/security/practices/.
- The University of Arizona's Security Awareness Posters http://security.arizona.edu/posters
- and the http://www.itd.umich.edu/posters/ University of Michigan's posters (my favorite).



Human Error Is The Single Biggest Cause Of Information Security Breaches.

Statistics show that up to 80% of security problems are caused by people. So instead of focusing on securing hardware and software, it's crucial to consider another kind of security: education. (ISC)^2 is the non-profit global leader in educating and certifying information security professionals. Our members have benchmark credentials which allow them to anticipate and fend off attacks. So look into (ISC)^2. Because you never know. You could be the target of some creepy cybercrime as you read this.

For details please visit us at www.isc2.org/awareness.

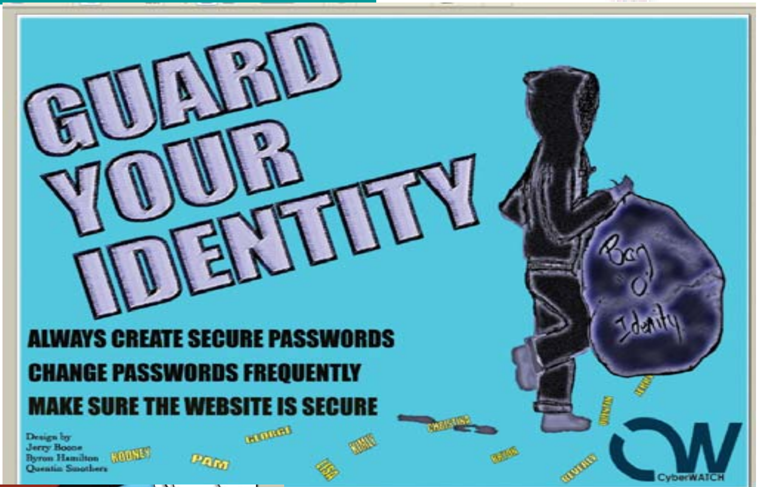
(ISC)^2®

SECURITY TRANSCENDS TECHNOLOGY®

2008 CyberWATCH Security Awareness Contest Winners

They're watching you !
Beware the Spies
They love to know everything about you
A public service announcement from

Poster Designed by Latysha Franklin

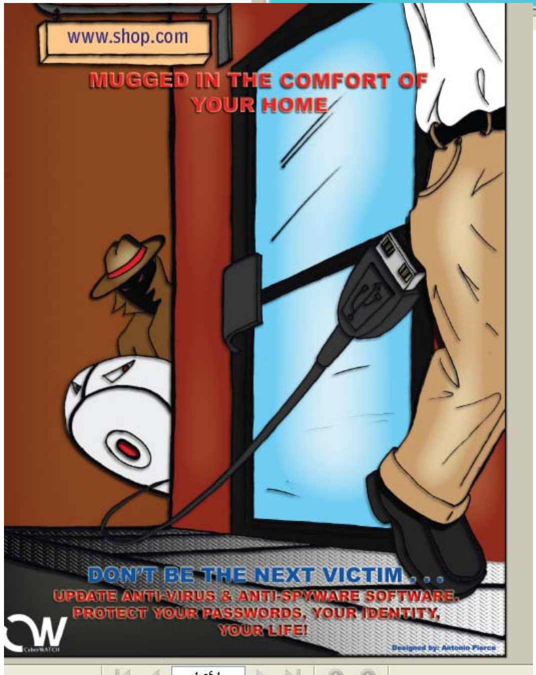

GUARD YOUR IDENTITY
ALWAYS CREATE SECURE PASSWORDS
CHANGE PASSWORDS FREQUENTLY
MAKE SURE THE WEBSITE IS SECURE
Bag O' Identy
RODNEY
PAM
GEORGE
LISA
CHRISTINA
BEVERLY
CyberWATCH

Design by
Jerry Boone
Byron Hamilton
Quentin Smothers

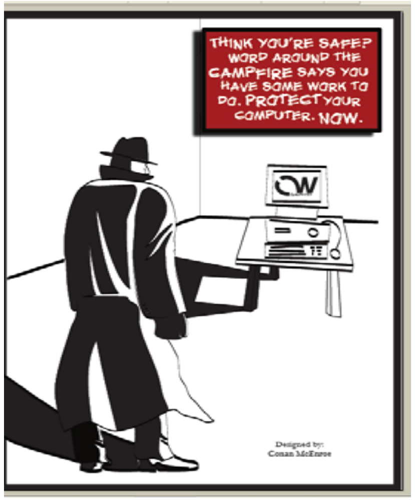
iHack
CyberWATCH

Every two seconds a different computer gets hacked into. It's sabotaged with spyware, trojan horses, viruses, and more. Protect your computer with anti-malware software, update passwords often, and be wary of unsecure websites. The next computer hacked may be yours.

Designed By Aidan Boyd

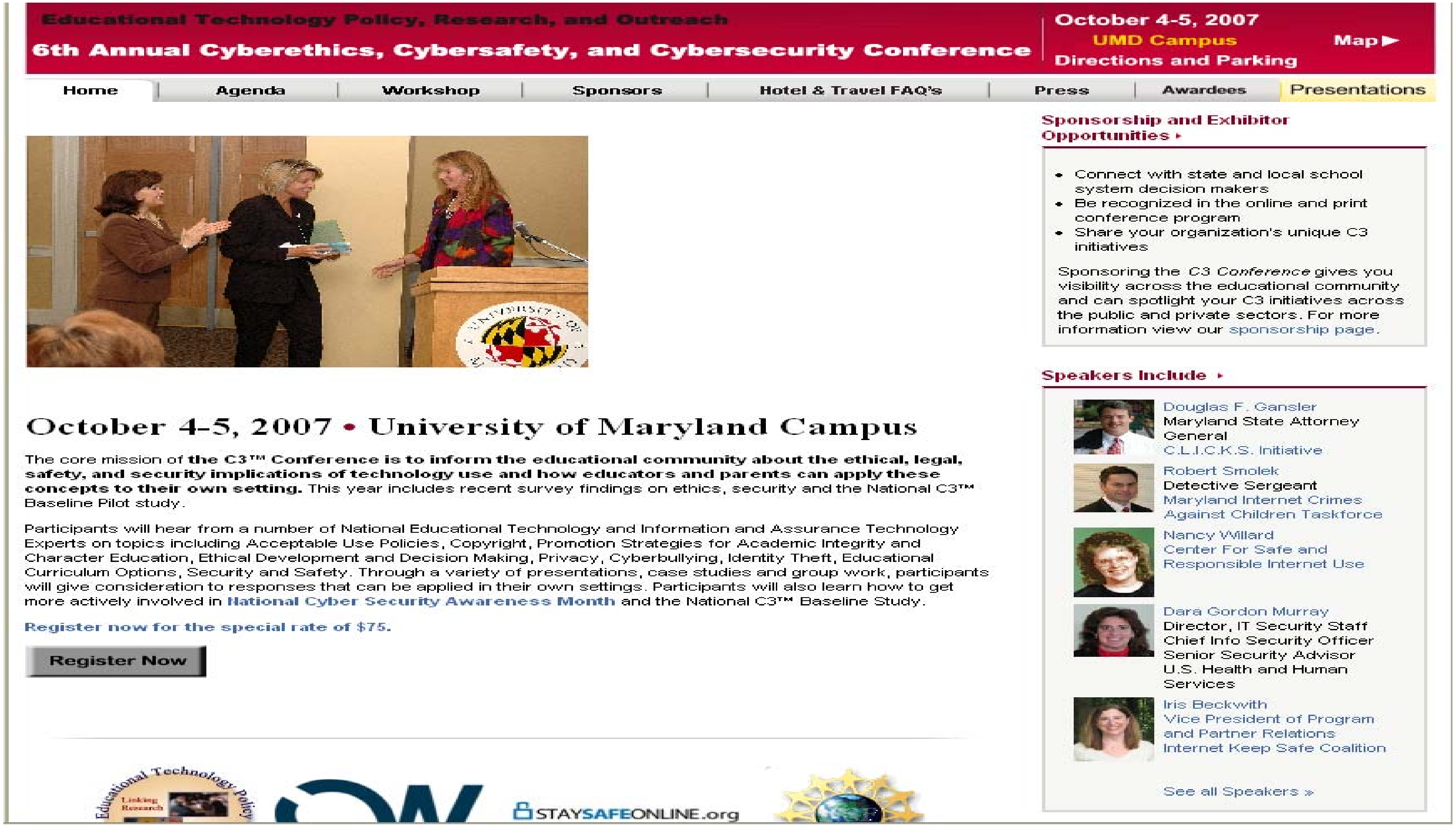

www.shop.com
MUGGED IN THE COMFORT OF YOUR HOME
DON'T BE THE NEXT VICTIM . . .
UPDATE ANTI-VIRUS & ANTI-SPYWARE SOFTWARE.
PROTECT YOUR PASSWORDS, YOUR IDENTITY, YOUR LIFE!
CyberWATCH

Designed by: Antonio Pierce


THINK YOU'RE SAFE? WORD AROUND THE CAMPFIRE SAYS YOU HAVE SOME WORK TO DO. PROTECT YOUR COMPUTER. NOW.

Designed by:
Conan McEnroe

SAVE THE DATE
C3 Conference
October 2-3, 2008



Educational Technology Policy, Research, and Outreach

6th Annual Cyberethics, Cybersafety, and Cybersecurity Conference

October 4-5, 2007
UMD Campus
Directions and Parking

October 4-5, 2007 • University of Maryland Campus

The core mission of **the C3™ Conference is to inform the educational community about the ethical, legal, safety, and security implications of technology use and how educators and parents can apply these concepts to their own setting.** This year includes recent survey findings on ethics, security and the National C3™ Baseline Pilot study.

Participants will hear from a number of National Educational Technology and Information and Assurance Technology Experts on topics including Acceptable Use Policies, Copyright, Promotion Strategies for Academic Integrity and Character Education, Ethical Development and Decision Making, Privacy, Cyberbullying, Identity Theft, Educational Curriculum Options, Security and Safety. Through a variety of presentations, case studies and group work, participants will give consideration to responses that can be applied in their own settings. Participants will also learn how to get more actively involved in **National Cyber Security Awareness Month** and the National C3™ Baseline Study.

Register now for the special rate of $75.

Sponsorship and Exhibitor Opportunities ▸

- Connect with state and local school system decision makers
- Be recognized in the online and print conference program
- Share your organization's unique C3 initiatives

Sponsoring the *C3 Conference* gives you visibility across the educational community and can spotlight your C3 initiatives across the public and private sectors. For more information view our sponsorship page.

Speakers Include ▸

Douglas F. Gansler
Maryland State Attorney General
C.L.I.C.K.S. Initiative

Robert Smolek
Detective Sergeant
Maryland Internet Crimes Against Children Taskforce

Nancy Willard
Center For Safe and Responsible Internet Use

Dara Gordon Murray
Director, IT Security Staff
Chief Info Security Officer
Senior Security Advisor
U.S. Health and Human Services

Iris Beckwith
Vice President of Program and Partner Relations
Internet Keep Safe Coalition

See all Speakers »

Questions

Contact Information:
Davina Pruitt-Mentle
Educational Technology Policy, Research and Outreach
(301) 503-8070
dpruitt@umd.edu

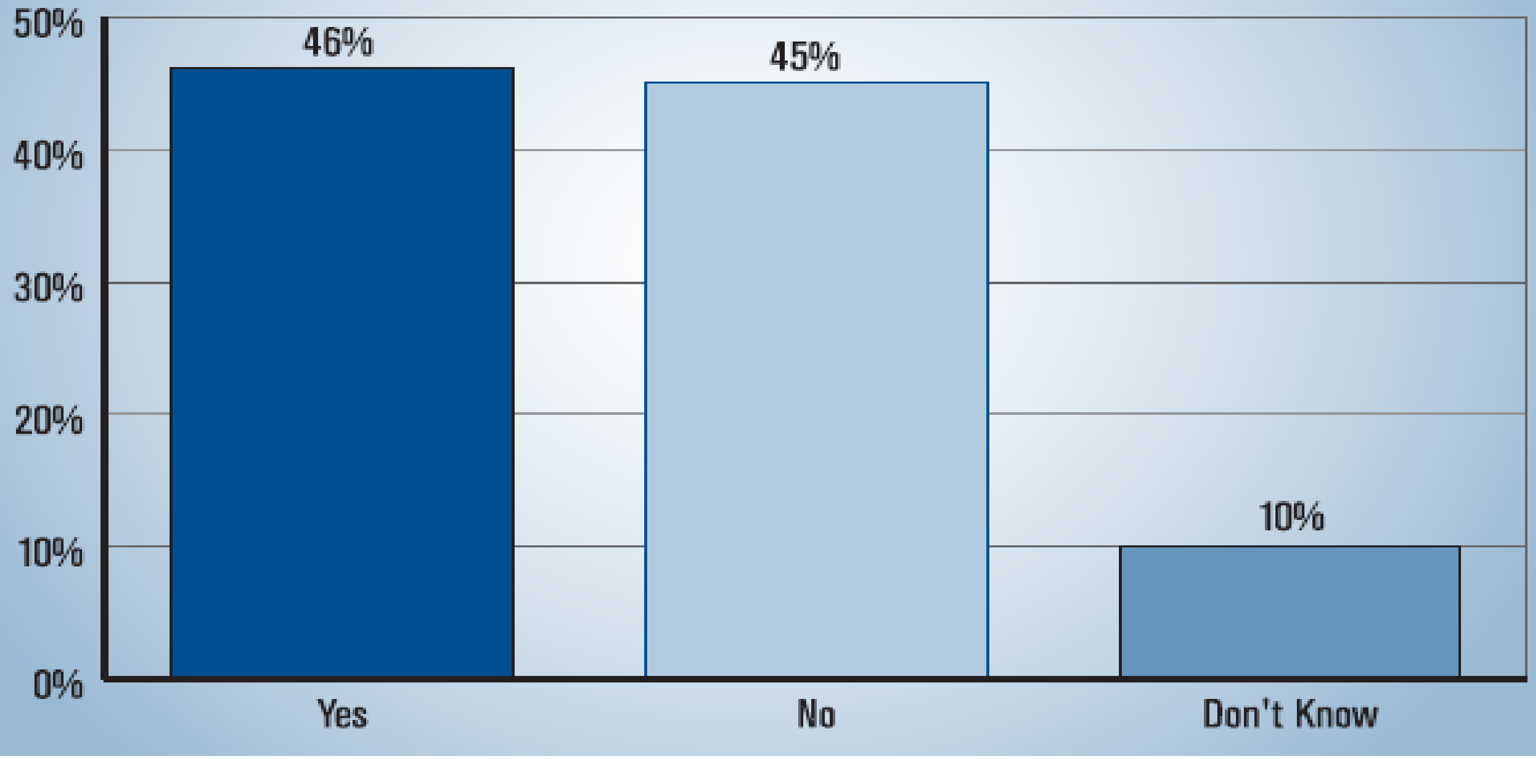
CSI/FBI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

Full Report: http://www.gocsi.com/

Figure 11. Did Your Organization Experience a Security Incident in the Past 12 Months?

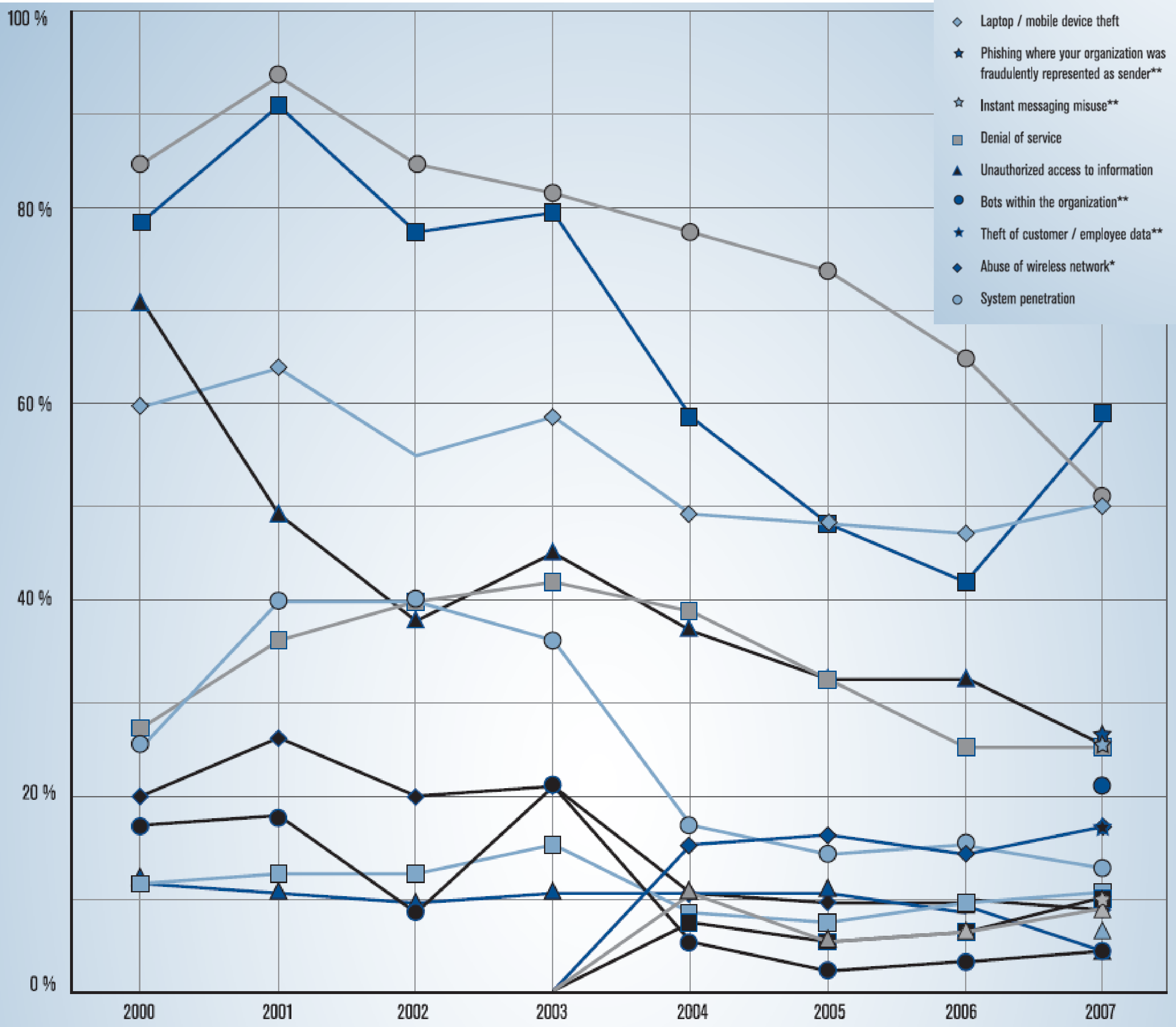
By Percent of Respondents

(Numbers do not add up to 100% due to rounding.)



2008 Copyright ETPRO

Types of Attacks or Misuse Detected in the Last 12 Months



	TYPE OF ATTACK	2007
■	Insider abuse of Net access	59%
●	Virus	52%
◇	Laptop / mobile device theft	50%
★	Phishing where your organization was fraudulently represented as sender**	26%
☆	Instant messaging misuse**	25%
□	Denial of service	25%
▲	Unauthorized access to information	25%
●	Bots within the organization**	21%
★	Theft of customer / employee data**	17%
◆	Abuse of wireless network*	17%
○	System penetration	13%
□	Financial fraud	12%
☆	Password sniffing**	10%
■	Web site defacement*	10%
△	Misuse of public Web application*	9%
◆	Theft of proprietary information (intellectual property)	8%
△	Exploit of the organization's DNS server**	6%
▲	Telecom fraud	5%
●	Sabotage	4%

*Added in 2004 survey
**Added in 2007 survey

CSI 2007 Computer Crime and Security Survey

Figure 14

http://www.gocsi.com/

Identity Theft

- **Phishing**
  - Phishing is a popular and growing method of identity theft, typically performed either through email or through the creation of a Web site that appears to represent a legitimate company. Victims are asked to provide personal information such as passwords and credit card numbers in a reply email or at the bogus Web site.
- **Spear phishing**
  - The practice of targeting an attack to a specific group is gaining in sophistication and frequency.
- **Pharming**
  - A scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. Pharming has been called "phishing without a lure."

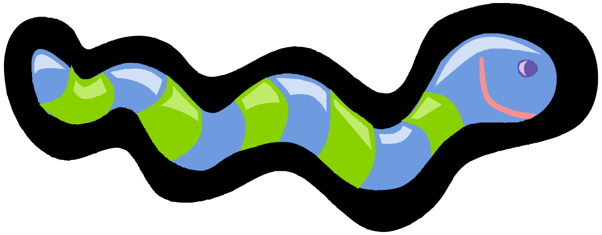
Lingo

- **Spamming**
  - Sending of unsolicited bulk unsolicited e-mail and received by multiple recipients
- **Solutions**
  - Source-based blocking solutions prevent receipt of spam
  - Content filtering solutions identify spam after it’s been received
  - Disposable identities
- **Spoofing**
  - One person or program successfully pretends to be another by falsifying data and thereby gains an illegitimate advantage
- **Webpage spoofing**
  - A legitimate web page such as a bank's site is reproduced in "look and feel" on another server under control of the attacker. They fool users into thinking they are connected to a trusted site, to gather user names and passwords.

Lingo

- **Vishing**
  - (Voice phISHING) Also called "VoIP phishing," SPIT (spam over Internet telephony), or sometimes known as vam -- is the voice counterpart to phishing. Instead of being directed by e-mail to a Web site, an e-mail message asks the user to make a telephone call. The call triggers a voice response system that asks for the user's credit card number. The initial bait can also be a telephone call with a recording that instructs the user to phone an 800 number.

    In either case, because people are used to entering credit card numbers over the phone, this technique can be effective. Voice over IP (VoIP) is used for vishing because caller IDs can be spoofed, and the entire operation can be brought up and taken down in a short time, compared to a real telephone line.
- **Smishing**
  - The mobile phone counterpart to phishing. Instead of being directed by e-mail to a Web site, a text message is sent to the user's cellphone with some ploy to click on a link. The link causes a Trojan to be installed in the phone
- **Voice Spam**
  - schemes includes the use of Interactive Voice Response (IVR) systems in conjunction with automated telemarketing sales to repeatedly initiate call setups and fill voicemail boxes.



Lingo

- **Worm**: a self-replicating computer program, similar to a computer virus. It is self-contained and does not need to be part of another program to propagate itself.
  - Example: Sobig and Mydoom.
- **Virus**: attaches itself to, and becomes part of, another executable program;
  - Macro viruses are written in the scripting languages for Microsoft programs such as Word and Excel.
- In general, a virus cannot propagate by itself whereas worms can. A worm uses a network to send copies of itself to other systems and it does so without any intervention. In general, worms harm the network and consume bandwidth, whereas viruses infect or corrupt files on a targeted computer. Viruses generally do not affect network performance, as their malicious activities are mostly confined within the target computer itself.

From Wikipedia - http://en.wikipedia.org/wiki/Computer_worm

Lingo

- **Trojan Horse**: A malicious program that is disguised as legitimate software
  - These are often those attachments to email that entice you to open them
- **Malware**: Software designed to infiltrate or damage a computer system, without the owner's consent
  - Includes computer viruses, Trojan horses, spyware and adware

Lingo

- **Adware**
  - Software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.
- **Spyware**
  - designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user.

◀