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

Davina Pruitt-Mentle

Nancy Willard
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/idtheftsurvey.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.

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 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

- Use Internet from home computer for banking, stock trading or reviewing personal medical information: 88%
- Store important personal data like personal emails, resumes, health records or financial information on home computer: 87%
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

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

Cyber-espionage moves into B2B

http://www.infoworld.com/article/08/01/15/Cyber-espionage-moves-into-B2B_1.html
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. 18 (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 dismissed 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 spread 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/].
In the 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 1993 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 301 students on the Warner College of Natural Resources Web site, including passwords and 288 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 to the The Iowa City Press-Citizen, the University of Iowa's College of Engineering notified 215 former students earlier this month that their personal information had been posted.

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 people 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:

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

$\ldots$

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.
• 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

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/](http://itu.gmu.edu/security/practices/)

Password Security

A good password is one that cannot be easily guessed. Enter a password, click submit, then we'll score it against 120 different criteria:

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

Please note that although we will not store the password you enter, a good idea is to send your password to someone you don't trust and recommend testing a password which is "similar" to one you use.

All users of information resources are responsible for assisting in the systems they use. Many intruders enter systems simply by guessing, and even the best passwords can eventually be defeated mathematically.

The use of strong passwords acts as a firm deterrent against guessing attacks, and buys additional time against other attacks.

DO'S
- DO use a password with mixed-case letters. Use uppercase letters throughout the password.
- DO use a password that contains symbols.
- DO use a password with mixed-case letters. Use uppercase letters throughout the password.
- DO use a password with mixed-case letters. Use uppercase letters throughout the password.

DON'TS
- DO NOT use a password that contains any form (reverse, doubled, as a pass).
- DO NOT use your name, personal information is more secure when you use secure passwords to help protect them.
- DO NOT use your name, personal information is more secure when you use secure passwords to help protect them.
- DO NOT use your name, personal information is more secure when you use secure passwords to help protect them.

Related Links:
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
Anti-Virus Protection

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


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

1/29/08 2008 Copyright ETPRO
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.

http://www.ftc.gov/bcp/online/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.

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/

- 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
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
  – McAfee: [http://ts.mcafeehelp.com/?siteID=1&resolution=1280x1024&rurl=vrContactOptions.asp](http://ts.mcafeehelp.com/?siteID=1&resolution=1280x1024&rurl=vrContactOptions.asp)
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
http://www.itsa.ufl.edu/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 Carrian Hoke

Public Wi-Fi hotspots have more in common with public toilets than more 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 hotspots 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 small number of them are not safe to use. People tend to forget that a network is more likely than the cat’s nature, and Wi-Fi hotspots bring convenient relief.

Unfortunately, there are several simple ways to mitigate all these risks. Fortunately, there are several simple ways to mitigate all these risks. Fortunately, there are several simple ways to mitigate all these risks. Fortunately, there are several simple ways to mitigate all these risks. Fortunately, there are several simple ways to mitigate all these risks.

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

Vulnerable networks still exist even though the Wi-Fi standard now requires that new networks be encrypted. Unfortunately, it’s pretty common for public hotspots to prioritize ease of use over security. In some cases, you may even access a network’s configuration file and change its name to a more meaningful description. For example, there’s the evil twin wireless access point that masquerades itself as a public hotspot for the purpose of stealing network passwords, credit card numbers, and other private data from unsuspecting users.

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 wireless access point that masquerades 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 excrete a hard drive and render the computer useless. This leads to people abandoning their trust in wireless networks and thus in the public Wi-Fi realm.

Don’t be one of those who find themselves the victim of a hot-spot phishing scam. A phishing scam is a popular way for identity thieves to obtain your personal financial information (credit card numbers, Social Security numbers and passwords) by contacting you by email or by phone to persuade you to give them your financial information.

On the positive side, there are some hotspot users who have taken it upon themselves to guard against these risks. One such network is called “hotspotters,” a group of people who use public wireless networks to help others stay safe online.

The hotspotters are a diverse group, ranging from students and professionals to retirees and entrepreneurs. Some are full-time hotspotters, while others use the network only occasionally.

Unfortunately, the hotspotters’ efforts are often overlooked or dismissed by others. But the hotspotters are making a difference, and they’re not alone. Other groups are also working to make the wireless network safer and more secure.

One such group is Hotspot Shield, which offers a free software tool that helps protect users from online threats. Hotspot Shield uses a combination of encryption and advanced security features to secure users’ data and keep them safe online.

Another group is the Wi-Fi Protected Access (WPA) forum, which develops standards for wireless networks. WPA provides stronger security than the original Wi-Fi security standard, WEP, and is recommended for all wireless users.

In addition, there are many other organizations that are working to improve wireless security. These include the Wi-Fi Alliance, which promotes wireless security standards, and the Wi-Fi Foundation, which develops and promotes wireless security technologies.

In conclusion, while wireless networks are convenient and easy to use, they come with risks. By following these simple steps, you can protect yourself from these risks and enjoy the benefits of wireless networking.

1/29/08 2008 Copyright ETPRO 35
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 STATES 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 Snoop Stick drive operates like a standard USB flash drive, but with greatly enhanced capabilities. The Snoop Stick, 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 Snoop Stick 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

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

View Logs Stored On Your Snoop Stick
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).
OF ALL THE SCARY THINGS
THAT CAN SABOTAGE A NETWORK,
THIS ONE IS BY FAR THE DEADLIEST.

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 at any time.

For details please visit us at www.isc2.org/awareness.
2008 CyberWATCH Security Awareness Contest Winners
SAVE THE DATE
C3 Conference
October 2-3, 2008

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.

Speakers Include:

Douglas G. Barnier
Maryland State Attorney General

Robert Smolar
Detective Sergeant
Maryland Internet Crimes Against Children Taskforce

Nancy Willard
Center For Safe and Responsible Internet Use

Dana Gordon Murray
Director, IT Security Staff

Iris Beckwith
Vice President of Program and Partner Relations

See all Speakers »
Questions

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

- Yes: 46%
- No: 45%
- Don’t Know: 10%
Types of Attacks or Misuse Detected in the Last 12 Months

- Insider abuse of Net access: 58%
- Virus: 52%
- Laptop/mobile device theft: 50%
- Phishing where your organization was fraudulently represented as sender**: 20%
- Instant messaging misuse**: 25%
- Denial of service: 25%
- Unauthorized access to information: 25%
- Bot 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): 6%
- 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.

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.