



Understanding the Risks

Is Safe Computing Possible?

Bob Cowles

bob.cowles@slac.stanford.edu

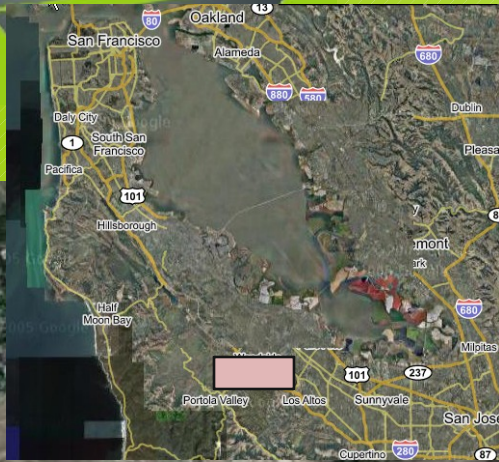
7th Internet Users Conference 2005



Work supported by U. S. Department of Energy contract DE-AC03-76SF00515



The image is a composite. The main part is an aerial photograph of the SLAC National Accelerator Laboratory. A long, straight, light-colored linear accelerator structure runs horizontally across the middle of the frame. To the right of this structure, a large, multi-looped circular accelerator is visible. The surrounding area includes green fields, some buildings, and roads. Labels on the map include 'Menlo Park', 'Sharon Park', 'Junipero Serra Fwy', 'Sand Hill Rd', and 'Alpine Rd'. In the top left corner, there is an inset map of the San Francisco Bay Area. This inset map shows major highways (101, 680, 880, 980, 101, 205, 87) and cities (San Francisco, Oakland, Alameda, Dublin, Pleasanton, Fremont, Milpitas, San Jose, Cupertino, Los Altos, Sunnyvale, Portola Valley, Hillsborough, Daly City, South San Francisco, Pacifica, Menlo Park). A red rectangle on the inset map indicates the location of the main aerial photograph. The background of the entire slide is a solid light blue color.





A Few of the Computers





Program for Today

- ◆ Security in the Internet Infrastructure
- ◆ Security for Network/Computer Admins
- ◆ Security at Work
- ◆ Security at Home
- ◆ Security for Kids

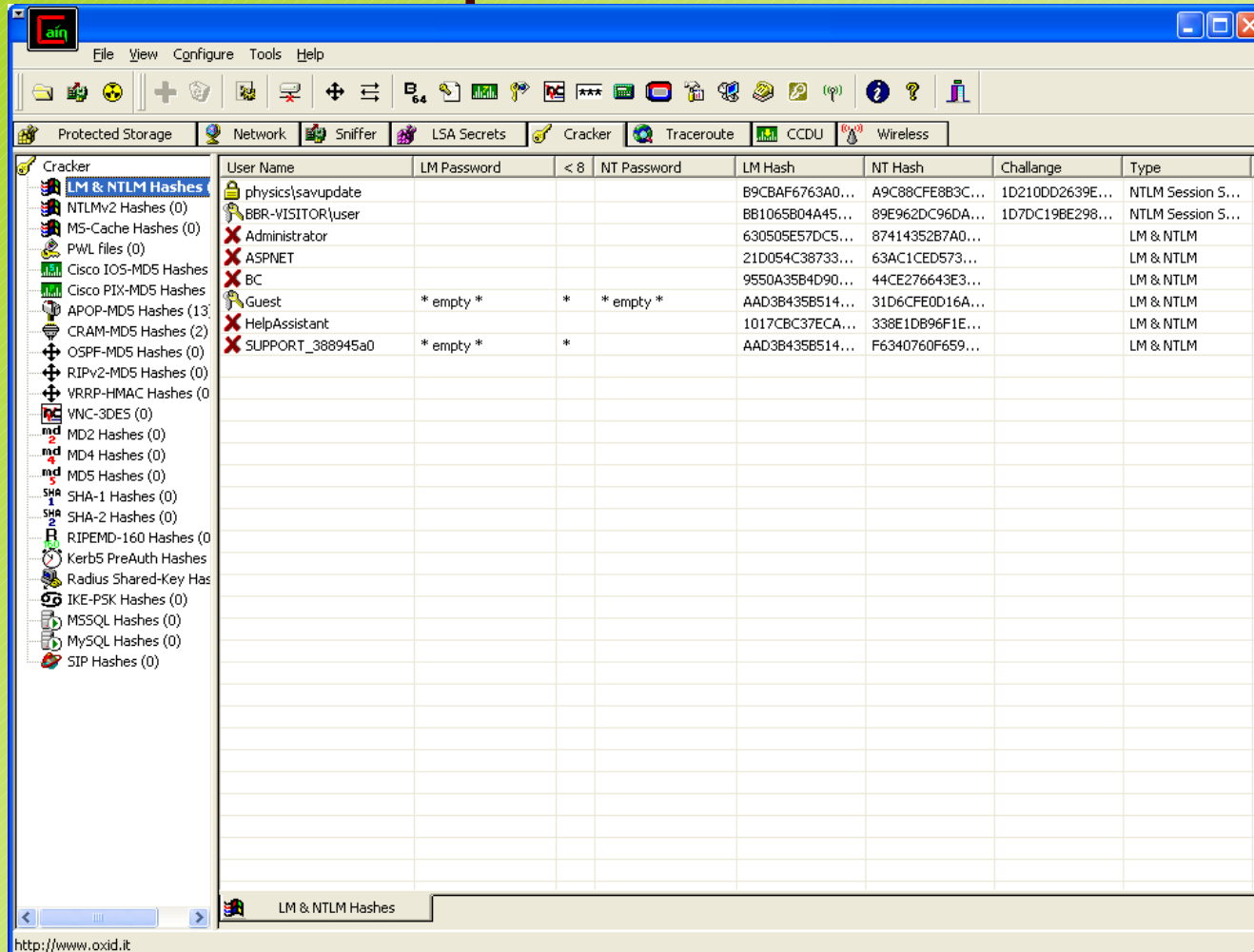




Security in the Internet Infrastructure



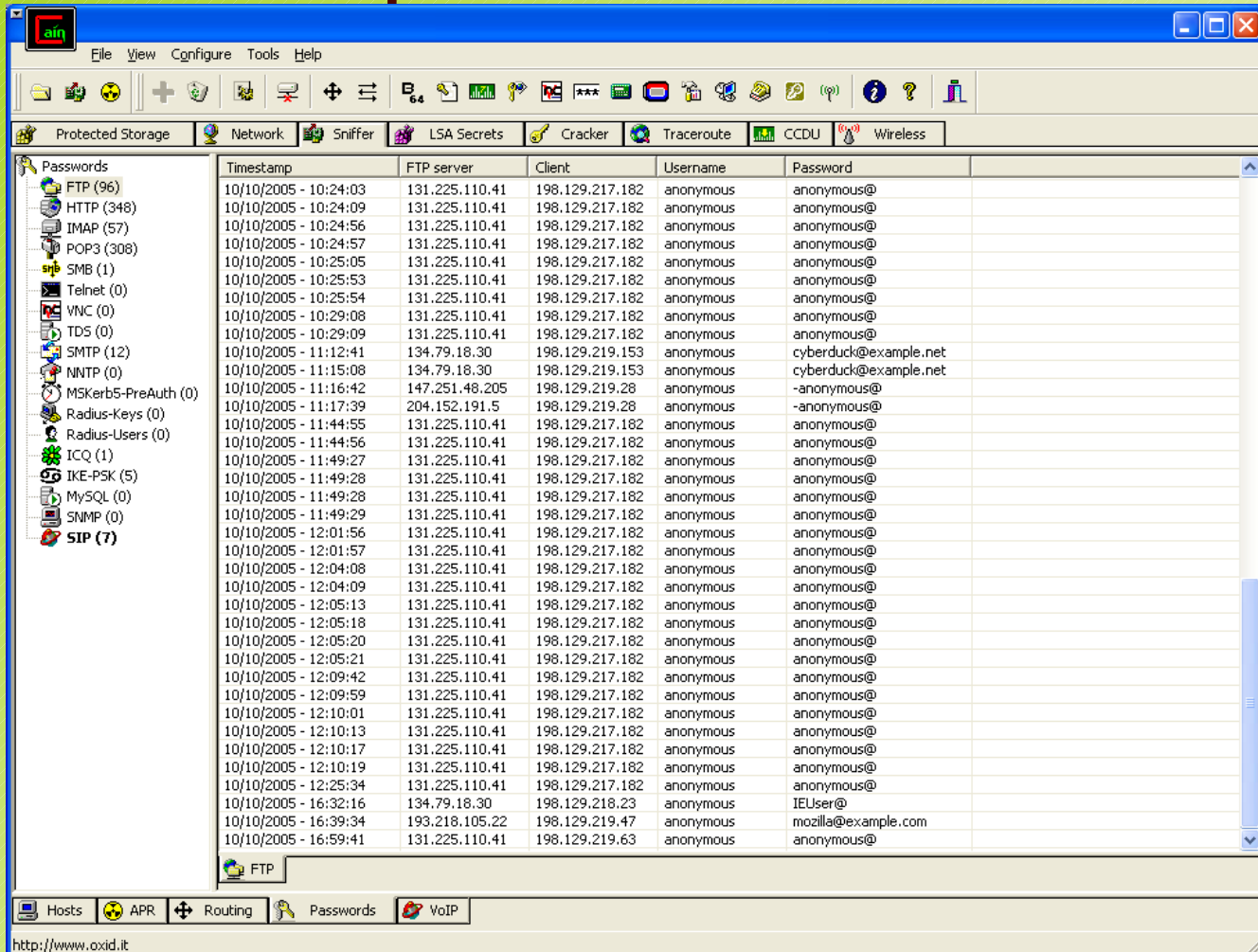
More Sophisticated Tools



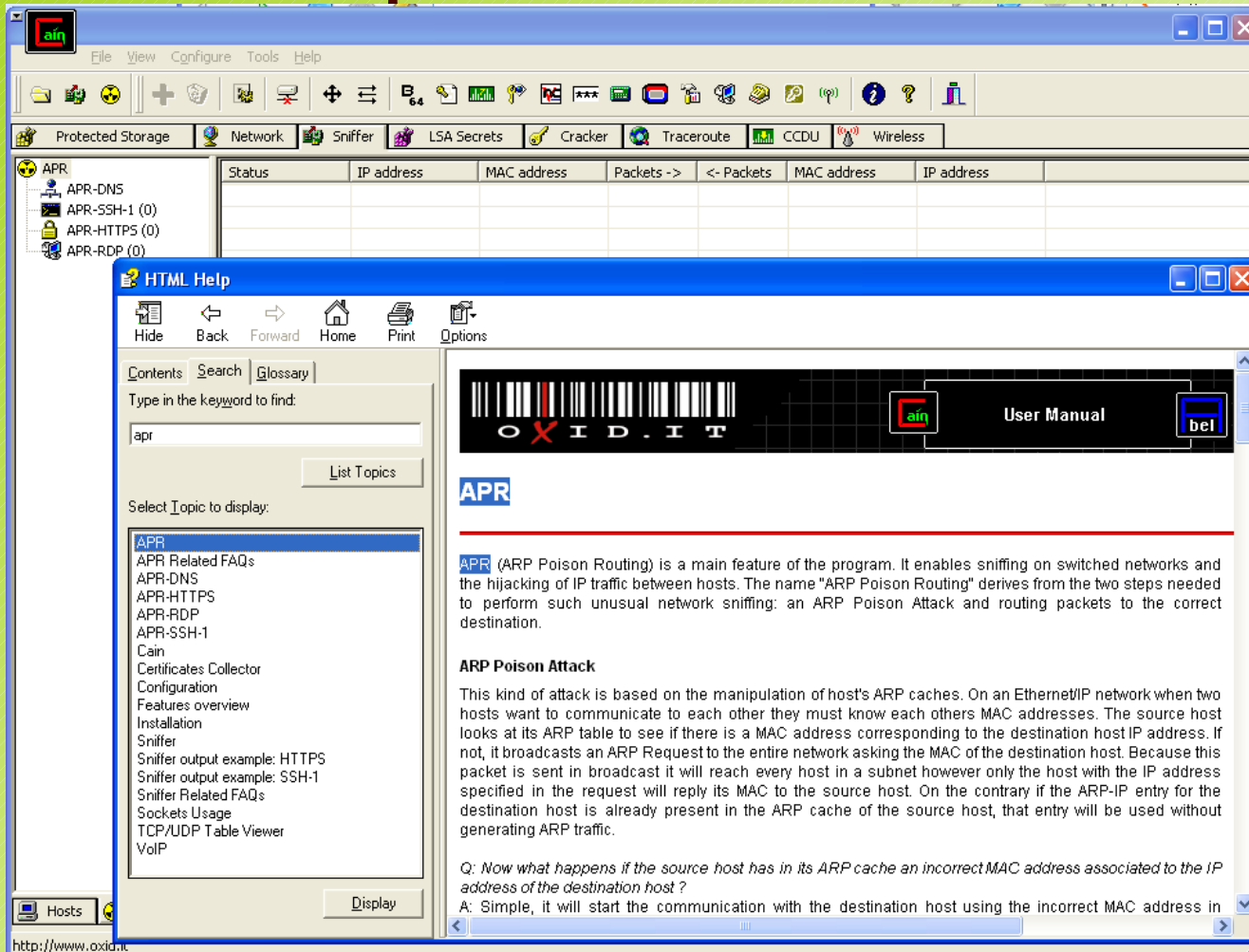
The screenshot shows the main window of the Cain & Abel network analysis tool. The 'Cracker' module is active, displaying a list of hashes on the left and a table of user credentials on the right. The table includes columns for User Name, LM Password, < 8, NT Password, LM Hash, NT Hash, Challenge, and Type.

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	Challenge	Type
physics\savupdate				B9CBAF6763A0...	A9C88CFE8B3C...	1D210DD2639E...	NTLM Session S...
BBR-VISITOR\user				BB1065B04A45...	89E962DC96DA...	1D7DC19BE298...	NTLM Session S...
Administrator				630505E57DC5...	87414352B7A0...		LM & NTLM
ASPNET				21D054C38733...	63AC1CED573...		LM & NTLM
BC				9550A35B4D90...	44CE276643E3...		LM & NTLM
Guest	* empty *	*	* empty *	AAD3B435B514...	31D6CFE0D16A...		LM & NTLM
HelpAssistant				1017CBC37ECA...	338E1DB96F1E...		LM & NTLM
SUPPORT_388945a0	* empty *	*		AAD3B435B514...	F6340760F659...		LM & NTLM

More Sophisticated Tools - 2



More Sophisticated Tools - 3





On the Increase

- ◆ phishing (including IM)

<http://www.infosecwriters.com/texts.php?op=display&id=229>

- ◆ pharming

<http://www.infosecwriters.com/texts.php?op=display&id=323>

- ◆ spyware (p2p)

- ◆ Tailored viruses

- ◆ Identity theft (in general)

http://www.emergentchaos.com/archives/cat_breaches.html

<http://www.privacyrights.org/ar/ChronDataBreaches.htm>





New Technologies

- ◆ bluetooth
 - voice recognition
- ◆ VoIP (skype, Google Talk, ...)
- ◆ smartcards, One Time Passwords (OTP)

- ◆ Will they make a difference?





Advances in Security

◆ Common Malware Enumeration

<http://cme.mitre.org/>

◆ Common Vulnerability Scoring System

<http://www.first.org/newsroom/releases/20050919.html>

◆ MS Office 2003 SP2 – anti-phishing

Extra click to activate links in email



Map of Bots

<http://nepenthes.sourceforge.net/visualisation>

visualisation [Nepenthes - finest collection -] - Mozilla Firefox Beta 2

File Edit View Go Bookmarks Yahoo! Tools Help

http://nepenthes.sourceforge.net/visualisation

Getting Started Latest Headlines News - Gaim iDefense : Power Of I... Kevin Kelly -- Cool Tools Gmail - Inbox (1)

Search Web My Yahoo! Yahoo! Mail Movies Travel Maps Reference

nepenthes
finest collection

- Home
- Download
- Documentation
- Installation
- FAQ
- Help us
- Howtos
- Virus Removal Help
- Bugs
- Forum
- Mailing-Lists
- Patches
- Statistics
- Visualisation
- Code Snippets
- Links
- Papers and News
- Recommendations
- Sample Analysis
- TODO
- Contact
- sf.net nepenthes

SOURCEFORGE
net


POWERED BY
Google

Orange	< 25 samples	Easy task
Red	< 250 samples	Should think about security
Black	> 250 samples	Worms heaven, admins hell

10.10.2005 flushed database to support city & country
26.10.2005 to increase time used to draw the table, we use a 15 minute cached result for the last 2 days now
17.10.2005 caching, but without timewindow for the select, as this seems to nonwork with mysql DISTINCT It may take some time till the markers show up

just wait some (lets say 30) seconds

You can click the map, zoom, crawl, whatever you can do with a map, this is not a static picture**



Maps provided by Google Maps.

Disclaimer: Given the nature of the internet and the involvement of third-party services, we cannot guarantee the accuracy of the information presented.

visualisation.txt - Last modified: 2005/11/17 04:55

Show pagesource Old revisions Login Index Back to top

Done

23 Novemb



Security for Network/Computer Administrators





Passwords

◆ POP3

- kastela3, kcoct21, dec3.141, baum2kid, abouki99, jasperD9, pi16tchou

◆ IMAP

- 15Kajetan, vrvs@Toshi, jef, worib4

◆ SMTP

- lworib4u, frtaljkruha, ha66il33

◆ ICQ

- infograf, sutivan, nelavodo, 9Ll@jkl2, tehsup, joeking, kmhm116

◆ FTP

- aw3edcft6





Passwords (http) - 2

- ◆ d115872m
- ◆ Hammerhead
- ◆ mrakovnjacha
- ◆ 268jld823
- ◆ bravodb
- ◆ ovidVM1
- ◆ sebastian
- ◆ 2005
- ◆ bazzzy
- ◆ 637xre286
- ◆ argxb@\$
- ◆ e4077a97
- ◆ peggy101
- ◆ guest
- ◆ fin_maggie
- ◆ frump
- ◆ pingpass
- ◆ anais
- ◆ admin
- ◆ cband
- ◆ tig4yet
- ◆ pincopallino
- ◆ Mammoths





DOE Site Assistance Visit

- ◆ We're from the government and here to help
- ◆ Help with documentation required by new government standards (NIST 800-xx)
- ◆ Included penetration test





Penetration Test - results

- ◆ Win 2000 SP3 server
- ◆ MS dropped support as of June 30
- ◆ No warning of August vulnerability
- ◆ LM hashes for local admin password
 - Rainbow tables
 - 64GB – 99.9% success at LM passwords
- ◆ Defenders have to be perfect – attackers only have to succeed once





The Security Plan

◆ Prepare

- Policies
- User awareness

◆ Patch & protect

- Anti-virus & spyware
- Update when patches are available

◆ Response and containment

◆ Recovery – reinstall





Train Users & Admins on first response

- ◆ Stop and report to your security team
- ◆ Do NOT retaliate
- ◆ Do NOT power off system
 - unless immediate danger
- ◆ Do preserve evidence
 - backups, logs, traces, listings





Security at Work





Email Security

- ◆ Read email as plain text, not html
- ◆ Never download executable attachments
 - Best if your site quarantines attachments & spam
- ◆ Do not click on links that are not clear
- ◆ Do not run with administrative privileges
- ◆ Never disclose your email password
- ◆ What you say in email lives forever
- ◆ Consider implications of userid reuse





Instant Messaging

- ◆ Central servers can log/expose information
 - AIM, Gtalk, etc.
 - Blackberry and other PIM; SMS?
- ◆ Clients must be updated frequently
- ◆ Often unsupported by IT infrastructure
- ◆ Popular vector for spyware, viruses, other malware





IM Worms

<http://www.scmagazine.com/uk/news/article/528542/plague-mutant-worms-targets-im-systems/>

Plague of mutant worms targets IM systems

William Eazel 18 Nov 2005 10:24

Instant Messaging (IM) systems are coming under sustained attack from a record number of mutant worms, security watchers have warned.

According to IMlogic Threat Center, the recent jump in worm mutations poses the largest threat to corporate and consumer IM use due to the difficulty in consistently maintaining up-to-date virus protection on local and mobile systems. It notes that, as a leading indicator for the number of mutations to expect, the Kelvir worm has mutated 123 times during the last 11 months.





Backups

◆ Recovery

- From user error
- From hardware error
- From disaster
- From compromised machine

◆ Used in legal proceedings

- Opposing attorneys





Security at Home





Sony CDs

- ◆ Digital Rights Management (DRM)
 - Corporations vs. individuals
 - 52 protected CDs on the market
- ◆ Asset Protection
 - At the expense of the consumer
- ◆ Removal tool fiasco
 - Created yet another vulnerability





419 Scams

Dear Friend,

Greetings to you.

I wish to accost you with a request that would be of immense benefit to both of us. Being an executor of wills, it is possible that we may be tempted to make fortune out of our client's situations, when we cannot help it, or left with no better option. The issue I am presenting to you is a case of my client who willed a fortune to his next-of-kin. It was most unfortunate that he and his next-of-kin died on the same day the 31st October 1999 in an Egyptian airline 990 with other passengers on board. You can confirm this from the website below which was published by BBC WORLD NEWS.

WEBSITE.

<http://news.bbc.xx.xx/1/hi/world/americas/502503.stm>. (altered URL)

I am now faced with confusion of who to pass the fortune to.





Trojans in Email

Delete Reply Forward Spam Move...

This message is not flagged. [[Flag Message](#) - [Mark as Unread](#)] [Printable View](#)

From: postmaster@rrwd.dst.il.us [Add to Address Book](#) [Add Mobile Alert](#)

To: emailserv@yahoo.com

Date: Mon, 21 Nov 2005 23:01:45 GMT

Subject: Registration_Confirmation

Account and Password Information are attached!

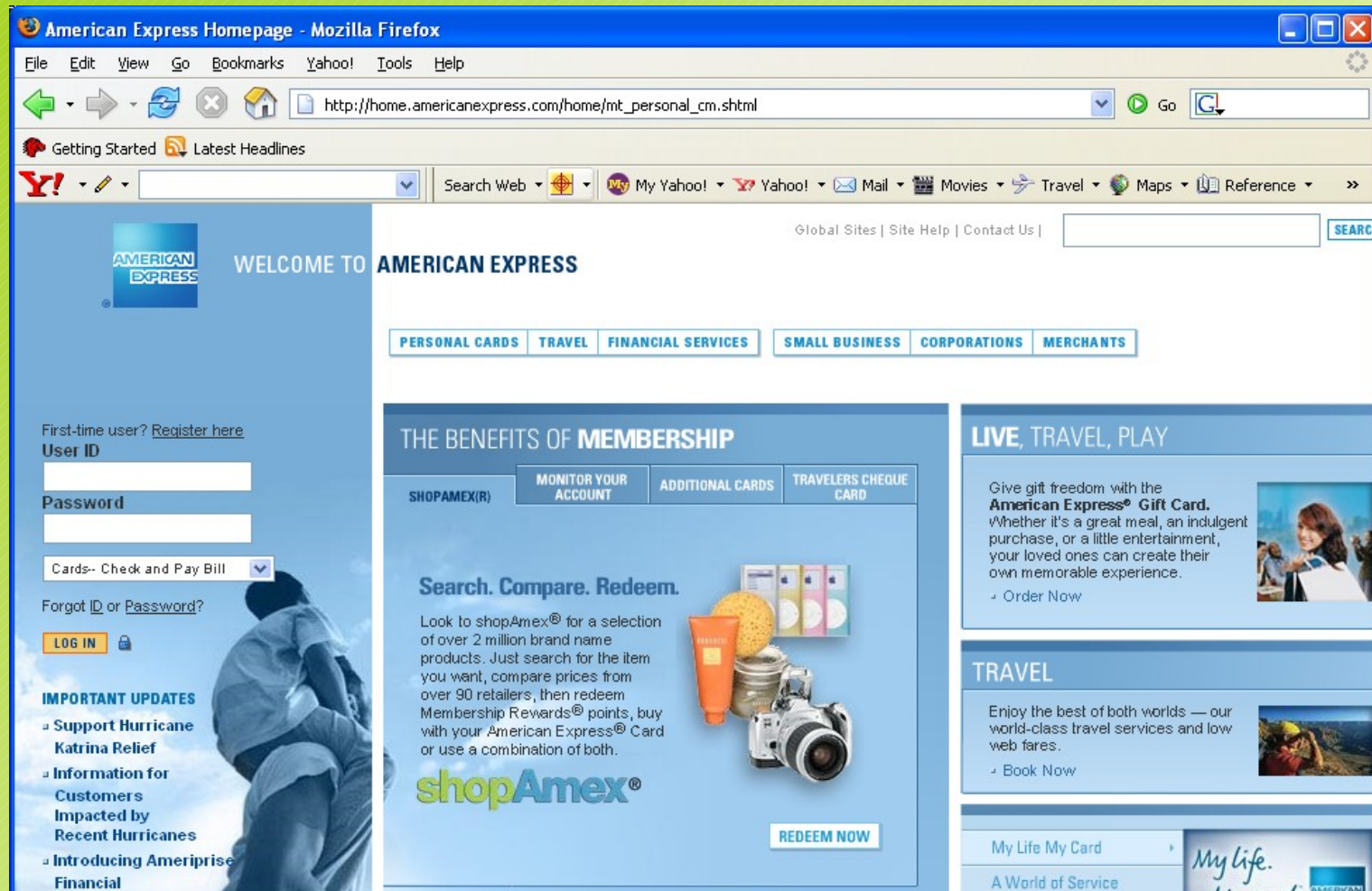
Attachments Attachment scanning provided by:

Files:

reg_pass.zip (54k) [Save to Computer](#) - [Save to Yahoo! Briefcase](#)



Bad Practices





Protecting From Identity Theft

<http://www.bradenton.com/mld/bradenton/13146939.htm>

- ◆ Look for the “s” in https://
- ◆ Keep OS updated and use firewall
- ◆ If contacted by mail, email, phone about your account(s), don’t respond. Call back main office from your statement.
- ◆ Use credit card with low limit online





Software Needing Regular Update

- ◆ Windows (you knew that!)
- ◆ MS Office
- ◆ Anti-virus, Anti-spyware
- ◆ Macromedia Flash
- ◆ Realplayer, Quicktime MS Media Player
- ◆ mp3 players
- ◆ IM clients





Dangers for Home Machines

- ◆ Unsecured wireless network
- ◆ Missing or misconfigured firewall
- ◆ Poorly trained users who access dangerous web sites using vulnerable web browsers
- ◆ Software poorly maintained
- ◆ Virus & spyware protection not updated
- ◆ Kids & teenagers





Security for Kids





Trust



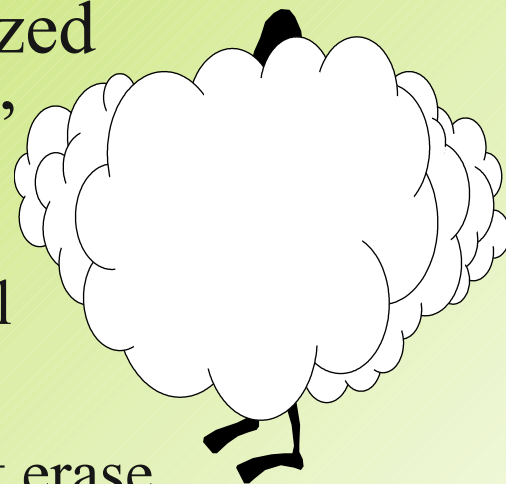
- ◆ We make trust decisions all the time
- ◆ We make mistakes all the time
- ◆ We (hopefully) learn from those mistakes
- ◆ We want people to trust us
- ◆ Trust and Computers
 - They get in the way of knowing someone
 - They allow us to know someone more deeply





Manners

- ◆ Agreements on how to behave – civilized
- ◆ “Virtual” world is different than “real”
 - email/chatting – what you type lives forever and is spread beyond your control
 - no way to hide if you upset someone – everything you do leaves traces you can’t erase
 - it’s all virtual – virtually **anything** can be faked – especially the things you want to believe
 - stupid / smart – both get amplified





Cartoon by Peter Steiner. *The New Yorker*, July 5, 1993 issue (Vol.69 (LXIX) no. 20) page 61





Risks

- ◆ We're very poor at understanding risks
 - Tend to believe familiar = safe
 - Risk judgment based on hype
- ◆ The Internet has many risks!
 - for you and your family
 - for your computer
- ◆ There are dangerous people on the Internet – very dangerous people





Risks for You



◆ Don't share personal information

- Real name, home address, phone, age, birth date, photos, family information, parents' income, etc., etc.

◆ Choose friends wisely – consult trusted adult

- OK to say “no” to ecards, “funny” downloads
- Your “friend” may be someone else
- No physical distance from other people – OK to ignore or block people who make you uncomfortable
- Use spam filters; don't open email from people you don't personally know





Risks for Your Family

◆ Using a family computer

- Keylogger that records userid/passwords for bank accounts, parents' work email, etc.
- Credit card, tax, and financial records; personal & identity information
- Remote access to microphone

◆ Using your computer

- Bypass home firewall protections
- Responsible for (possibly) illegal activities





Risks for Your Computer

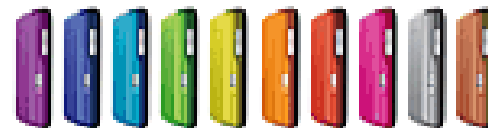
- ◆ keylogger – capture userid/ passwords – then pretend to be you
- ◆ bot – remotely controlled to spread viruses, spam
- ◆ “warez” – store pornography, illegal files
- ◆ erasing/changing files (homework, pictures)
- ◆ copyrighted material / infected files





ZEN
NEEON

The Charisma of Zen Neeon



Infected!!





Why do I Get So Much Spam?

What you see in the email

Learn more by visiting www.tips-it.com.





Why do I Get So Much Spam?

What you see in the email

Learn more by visiting www.tips-it.com.

Learn more by visiting www.tips-it.com

[<http://eletters-zannounce.com/gn4_AALeFwAIFuEB&emailid=WNNO90705>](http://eletters-zannounce.com/gn4_AALeFwAIFuEB&emailid=WNNO90705)

Where you really go when you click





For more information...



<http://www.microsoft.com/athome/security/children/kidpred.mspix>

<http://www.microsoft.com/athome/security/children/kidtips13-17.mspix>

<http://www.microsoft.com/athome/security/children/kidtips9-12.mspix>





Questions?

http://www.antsight.com/zsl/rainbowcrack/demo_rainbowcrack_cfg5.wmv

