

Christopher Wren Association

A10 Improve the Security of Your Computer



William
& Mary



January 27, February 3 and 10
Wightman Cup Room

Introduction

- The hand out is primarily for your use at home. I will make reference to the handout as the class progresses.
- Information is geared to:
 - Beginners
 - Advanced Users

Some of the reference materials are for highly skilled people. Some of their procedures can affect the way your computer works.

Introduction continued

- Start with the basics
 - Microsoft has listed 4 basic steps
 - Will show a Microsoft power point presentation
 - Will follow with other references for detail
 - Microsoft Help
 - www.Microsoft.com information
 - Other information from the “web”
 - Discuss documents written for professionals.
 - Microsoft documents
 - National Institute of Standards and Technology

Complete Security

- I have taken the flu shot. If I wear this mask continually, wash hands often, and avoid school children, can I be 100% sure of avoiding the flu?
- A quote from the National Institute of Standards and Technology: **“there is no 100% solution to computer security**; although having multiple layers of defense provides a much stronger solution than a single layer of defense, it is simply not possible to thwart every single attack” -- paragraph 3.3, page 47 of Special Publication 800-69, Guidance for securing XP Home edition.

Sources of Information

- Consult an Expert
- Check with the Vendor (Microsoft)
- Check with the United States Government
- Independent sources
 - Search the internet for Sans, read news.
 - Search the internet for DEFCON

<https://www.defcon.org/html/links/defcon-media-archives.html>

Sources of Information continued

Consult an Expert

The word “EXPERT” is made from two parts:

EX --- Has been

‘Spert --- Drip under pressure

Sources of Information continued

Check with the Vendor (Microsoft)

- Help

 - Demonstrate start/help/firewall

- Control panel security

 - Demonstrate start/control panel/security center/firewall

- Power point presentation

 - (roman numeral I in your handout)

- Microsoft security guide (Handout roman numeral V)

 - For XP
 - For Vista

Sources of Information continued

Check with the United States Government

National Institute of Standards and Technology Guides.

<http://csrc.nist.gov/itsec/>

- A. Guidance for Securing XP-Home Edition SP 800-69
- B. Guidance for Securing XP for IT Professional Operating system SP 800-68
- C. Guidance for VISTA Operating System
- D. Guidance for Windows 2000 Professional Operating System SP 800-43

Sources of Information continued

DEFCON Security Conference

- Lock hacks, contests, and intrigue at Defcon
- At the 16th annual Defcon security conference, hackers and hacker wannabes attend sessions on hacking Google Gadgets, Medeco M3 locks, and even their own conference badges.
- [Defcon ends with researchers muzzled, viruses written](#)
- Three-day hacker fest ends following a restraining order that killed one talk, a cable TV crew getting thrown out, and general software and hardware hacking tips shared.
(Posted in [Security](#) by Elinor Mills)
August 10, 2008 11:29 p.m. PDT

DEFCON Security Conference, continued

- [Judge orders halt to Defcon speech on subway card hacking](#)
- Federal judge grants the Massachusetts transit authority's request for an injunction preventing three MIT students from giving a presentation about hacking smartcards used in the Boston subway system.
(Posted in [Security](#) by Declan McCullagh)
August 9, 2008 10:31 a.m. PDT

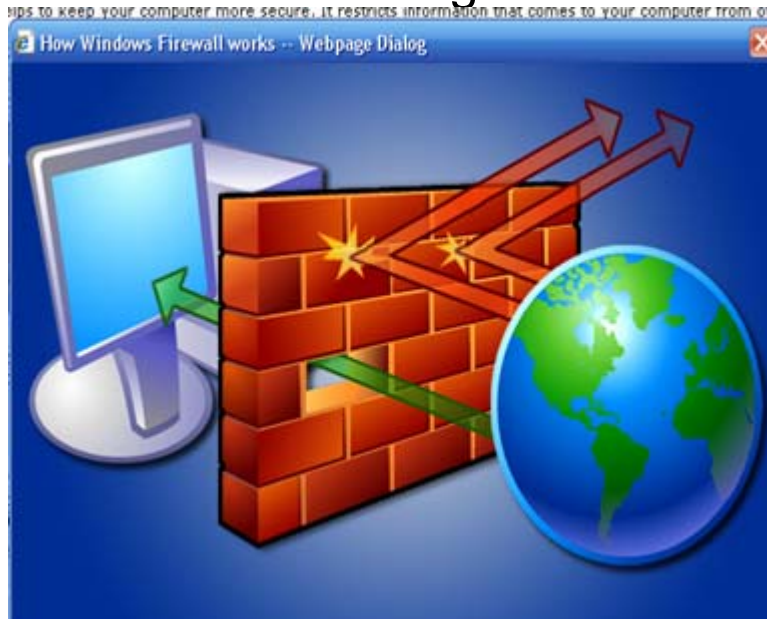
Microsoft Presentation

(Roman numeral III in your handout)

- A. Use an Internet firewall and keep it turned on. (firewall included in XP SP2 and VISTA.)
- B. Keep your operating system up to date, preferably by using automatic update features in Windows. (Automatic update included in XP and VISTA)
- C. Install and maintain antivirus software. (Microsoft “Windows Live OneCare” package for XP and Vista available for a fee.) (NIST identifies freeware antivirus software.)
- D. Install and maintain antispyware software, such as Windows Defender. (Free download is available from Microsoft-Home, included in VISTA.)

Use a Firewall

1. Demonstrate start/help then search for firewall (use a firewall that your computer does not find)
2. Demonstrate start/control panel/security center/ firewall.
3. Demonstrate start/control panel/firewall.
4. Demonstrate two firewalls running at the same time.



Keep your operating system up to date

- Microsoft responds to new hacker threats as they are discovered. Updates are generated by Microsoft, and are made available to users.

<http://www.microsoft.com/windowsxp/using/setup/maintain/autoupdate.aspx>

- Demonstrate start/control panel/security center/update

Correction for Handout

- Paragraph III _ C :

Install and maintain antivirus software.

Change :

(Microsoft package for XP available for a fee, Included in VISTA.)

TO Read:

(Microsoft package for XP and VISTA available for a fee.)

Correction for Handout, continued

<http://www.microsoft.com/protect/products/computer/compare/antivirusandantispyware.msp>

- [Windows Live OneCare safety scanner](#) is free and will manually:
 - Check for and remove viruses
 - Get rid of junk on your hard disk
 - Improve your PC's performance
- [Malicious Software Removal Tool](#) free and runs once a month. A security tool that checks your computer for specific viruses and other malicious software and helps remove any infection found.
- [Windows Live OneCare](#)
A set of security tools that runs quietly on your computer, with little or no intervention needed from you to maintain it.-- Free trial -- Costs \$49.95

Install and Maintain Antivirus Software

- Microsoft One Care package is available for a fee for XP and VISTA

<http://onecare.live.com/standard/en-us/3/helpsupport/default.htm>

<http://www.microsoft.com/protect/products/computer/default.aspx>

- NIST SP 800-69 identifies a free antivirus program. (Search sp800-69 for AVIRA).

http://csrc.nist.gov/itsec/guidance_WinXP_Home.html

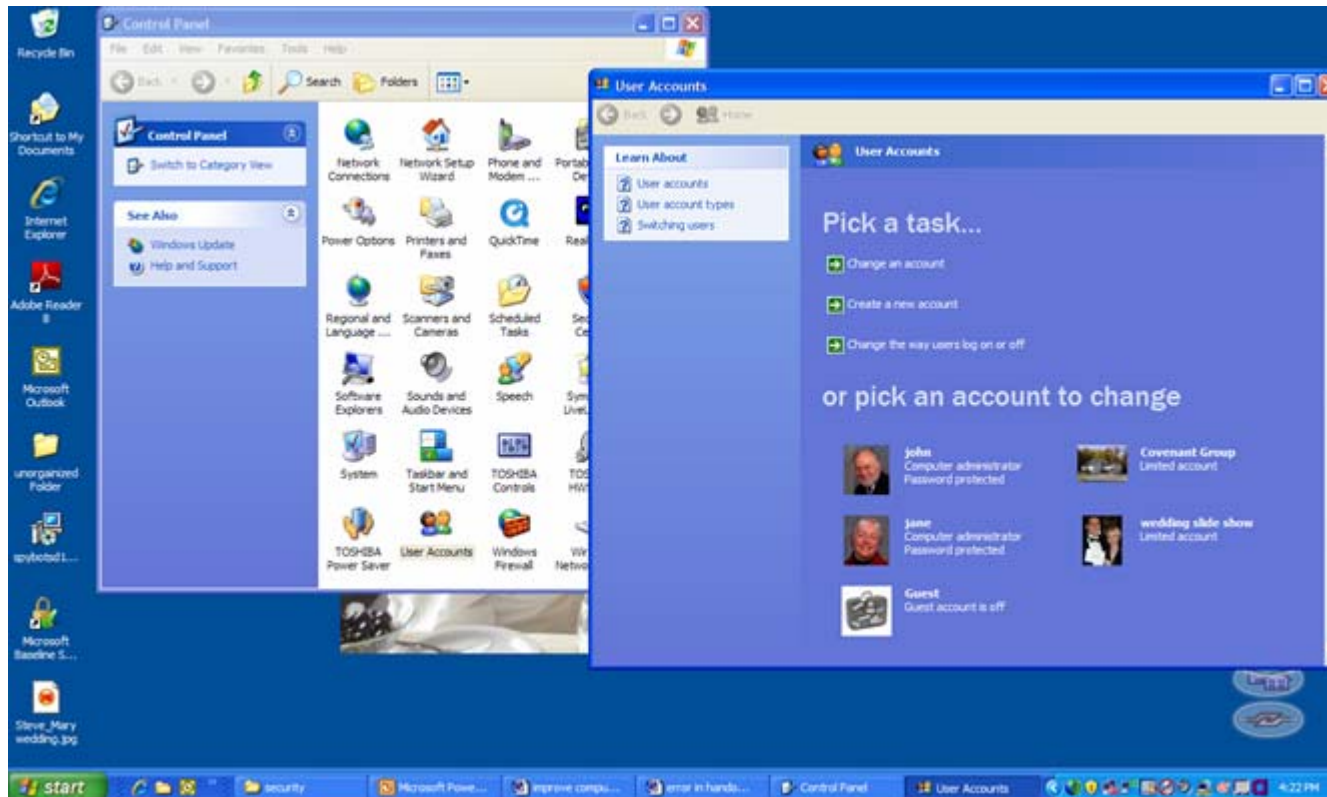
Install and maintain antispyware software

- Defender, an antispyware program is included with the VISTA operating system
 - A free download for XP is available from Microsoft.
- <http://www.microsoft.com/windows/products/winfamily/defender/default.mspx>
- A freeware program, SPYBOT is identified in NIST sp800-69

User Accounts and Privileges

<http://www.microsoft.com/protect/computer/advanced/useraccount.mspx>

Start/control panel/user accounts



John Nichols

A10 Improve the Security of Your
Computer

Sharing files/ folders

<http://www.microsoft.com/windowsxp/using/networking/security/permissions.msp#2>

- This does not work for Windows XP Home
In XP home, there is a shared folder that all users logged in can see and use.

<http://support.microsoft.com/kb/307874>

Passwords

- Use passwords to control access to your computer
 - Demonstrate start/control panel/user accounts
- Use strong Passwords and consider storing them in a safe place
 - <http://www.microsoft.com/protect/yourself/password/create.mspix>
 - <http://www.microsoft.com/protect/yourself/password/checker.mspix>

Guest Account

If the guest account is enabled, a user without a user account on the computer can log on to the computer at the Welcome screen.

To turn the guest account on or off

You must have a computer administrator account to turn on and turn off the guest account.

Demonstrate start/control panel/user accounts.

Click **Guest**.

Do one of the following:

To turn on the guest account, click **Turn On the Guest Account**.

To turn off the guest account, click **Turn off the guest account**.

The Simple File Sharing feature of Windows XP Home Edition, which is always enabled, allows only the Guest account to be used to gain access to the computer through the network. This means that attackers cannot gain remote access by guessing passwords to other accounts, such as the Administrator account.(SP800-69)

Wireless Router Issues

- WEP/WPA encryption -- 128 bit encryption
http://www.microsoft.com/windowsxp/using/networking/expert/bowman_03july28.msp
http://docs.lucidinteractive.ca/index.php/Cracking_WEP_and_WPA_Wireless_Networks
- Access restricted to specific devices
- Change network name from default
- Change router administrator name (if possible) and password from factory default
<http://www.netgear.com>
Model mr814 v2 support/downloads/wireless/ ...

Microsoft Outlook Express Backup

- Open Outlook Express then click on help, enter backup
- <http://support.microsoft.com/kb/270670>
 - Differences Between Outlook and Outlook Express
- [SUMMARY](#)
- [MORE INFORMATION](#)
 - [How to back up Outlook Express items](#)
 - [Step 1: Copy message files to a backup folder](#)
 - [Step 2: Export the Address Book to a .csv file](#)
 - [Step 3: Export the mail account to a file](#)
 - [Step 4: Export the newsgroup account to a file](#)
 - [How to restore Outlook Express items](#)
 - [Step 1: Import messages from the backup folder](#)
 - [Step 2: Import the Address Book file](#)
 - [Step 3: Import the mail account file](#)
 - [Step 4: Import the newsgroup account file](#)
 - [How to preserve the Blocked Senders list and other e-mail rules](#)
- SUMMARY
 - This article describes how to back up and to restore the following items in Microsoft Outlook Express:

Generic Email Backup

- Open your email
- Add a new folder (example “class_demo”) close email program
- Search for the new folder (start/search/class_demo)
- Record location of “class_demo”
- Open windows explorer, navigate to Location.
- Right click, drag to desktop, select “copy here”.

Data Backups

- Microsoft discussion of tools for backups
http://www.microsoft.com/windowsxp/using/setup/learnmore/bott_03july14.mspx
http://www.microsoft.com/protect/educators_us.mspx search for backups
- Other solutions
 - Flash drive
 - CD or DVD disk

NTFS vs FAT

- File Allocation Table, FAT16 file system was introduced way back with MS-DOS in 1981
- FAT32 was originally introduced in Windows 95 Service Pack 2
- NT File System, the NTFS file system, introduced with first version of Windows NT, is a completely different file system from FAT. It provides for greatly increased security, file-by-file compression, quotas, and even encryption. It is the default file system for new installations of Windows XP, and if you're doing an upgrade from a previous version of Windows, you'll be asked if you want to convert your existing file systems to NTFS. Don't worry. If you've already upgraded to Windows XP and didn't do the conversion then, it's not a problem. You can convert FAT16 or FAT32 volumes to NTFS at any point.

– http://www.microsoft.com/windowsxp/using/setup/expert/russel_october01.msp

Additional Topics continued

- Microsoft Baseline Analyzer
<http://www.microsoft.com/technet/security/tools/mbsahome.aspx>
- Parental Controls
<http://www.microsoft.com/protect/products/family/vista.aspx>
- Encrypt files and data
<http://technet.microsoft.com/en-us/library/cc875821.aspx>

Service Pack Blockers

- <http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127068>
- January 30, 2009 (Computerworld) [Microsoft Corp.](#) is warning customers that tools for blocking automatic upgrades to the newest service packs of [Windows Vista](#) and [Windows XP](#) will expire in the coming months.
- The tools, which were [released in December 2007](#), prevent service packs from reaching PCs via Windows Update, Microsoft's default update service, and are primarily used by corporations that have not yet tested or approved the newest upgrades.

Router Reports

7/7/2008 3:55:10 PM

Intrusion: MSSQL_Stack_Overflow.

Intruder: 218.75.199.50(3632).

Risk Level: High.

Protocol: UDP.

Attacked IP: 69.117.108.96.

Attacked Port: ms-sql-m(1434).

7/7/2008 3:55:10 PM

Intrusion detected and blocked. All communication with
218.75.199.50 will be blocked for 30 minutes.

– Google seach for who is

Telephonic Pfishing text msg

From: <7577844539@VTEXT.COM>

To: <jnichols@home.hrcoxmail.com>

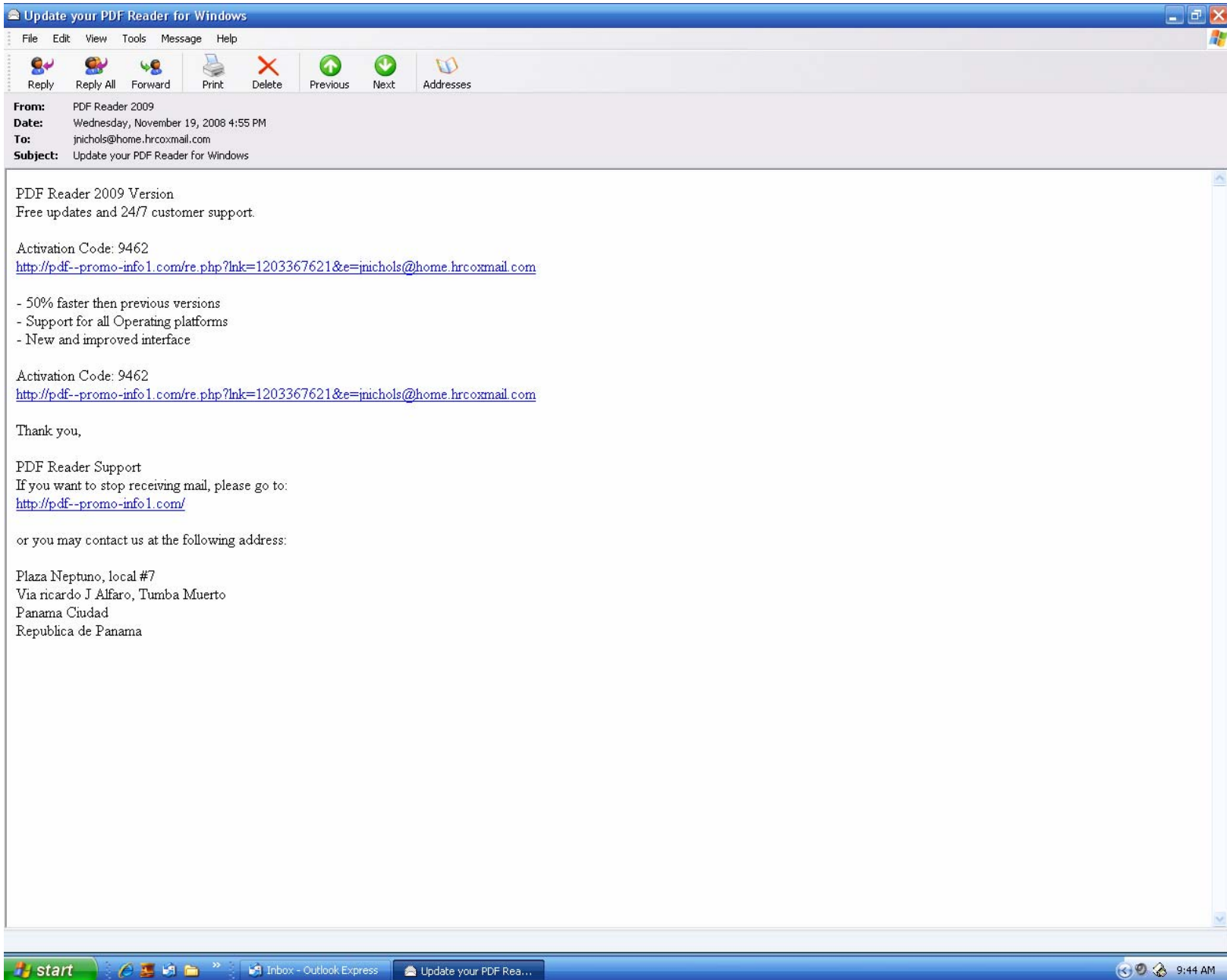
Sent: Thursday, January 15, 2009 9:53 AM

Subject: FWD: (NOTICE) Your Langley FCU

> FWD: (NOTICE) Your Langley FCU web service is expired, for renewal please login using www.langleyfcuweb.org ASAP

>

-
- Correct web address for Langley FCU is:
 - ***www.langleyfcu.org/*** -



John Nichols

A10 Improve the Security of Your
Computer

Cuckoo's Egg

- ***The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*** is a 1990 book written by [Clifford Stoll](#). It is his first-person account of the hunt for a [computer hacker](#) who broke into a computer at the [Lawrence Berkeley National Laboratory](#) (LBL).

Subway Card Hacking

- August 9, 2008 10:31 AM PDT
- Judge orders halt to Defcon speech on subway card hacking
- Posted by [Declan McCullagh](#)
- LAS VEGAS--A federal judge on Saturday granted the Massachusetts transit authority's request for an injunction preventing three MIT students from giving a presentation about hacking smartcards used in the Boston subway system.
- The Electronic Frontier Foundation, which is representing the students, anticipates appealing the ruling, said EFF senior staff attorney Kurt Opsahl.
- The undergraduate students had been scheduled to give a presentation Sunday afternoon at the Defcon hacker conference here that they had [said](#) would describe "several attacks to completely break the CharlieCard," an RFID card that the Massachusetts Bay Transportation Authority uses on the Boston T subway line. They also planned to release card-hacking software they had created, but canceled both the presentation and the release of the software.
- U.S. District Judge Douglas Woodlock on Saturday ordered the students not to provide "program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System." Woodlock granted the MBTA's request after a hastily convened hearing in Massachusetts that took place at 8 a.m. PDT on Saturday.

Wall St Journal article

<http://finance.yahoo.com/banking-budgeting/article/106508/Cyber-Scams-on-the-Uptick-in-Downturn>

Course Outline

INTRODUCTION

The class presentation will focus on basic steps to improve security. Microsoft's four basic steps will be discussed and demonstrated.

Instead of recommending a text book, numerous web sites are identified. A perusal of these sites will demonstrate the extensive amount of information on the World Wide Web.

References and brief discussion will be made to advanced topics for the benefit of the advanced student as well as those students who wish to do independent study and are eager to delve deep into the workings of the system.

A quote from the National Institute of Standards and Technology: “**there is no 100% solution to computer security**; although having multiple layers of defense provides a much stronger solution than a single layer of defense, it is simply not possible to thwart every single attack” -- paragraph 3.3, page 47 of Special Publication 800-69, Guidance for securing XP Home edition.

- I. Microsoft presentation: Fundamentals of Computer Security.
http://www.microsoft.com/protect/educators_us.mspx
- II. Introduce National Institute of Standards and Technology Guides.
<http://csrc.nist.gov/itsec/>
 - A. Guidance for Securing XP-Home Edition SP 800-69
http://csrc.nist.gov/itsec/guidance_WinXP_Home.html
 - B. Guidance for Securing XP for IT Professional Operating system SP 800-68
http://csrc.nist.gov/itsec/guidance_WinXP.html
 - C. Guidance for VISTA Operating System
http://csrc.nist.gov/itsec/guidance_vista.html
<http://www.microsoft.com/downloads/details.aspx?familyid=A3D1BBED-7F35-4E72-BFB5-B84A526C1565&displaylang=en>
 - D. Guidance for Windows 2000 Professional Operating System SP 800-43
http://csrc.nist.gov/itsec/guidance_W2Kpro.html
- III. Microsoft recommends four basic steps to **help** secure your computer from many malicious software attacks.
<http://www.microsoft.com/protect/computer/default.mspx>



- A. Use an Internet firewall and keep it turned on. (firewall included in XP SP2 and VISTA.)
<http://www.howstuffworks.com/firewall.htm>
<http://en.wikipedia.org/wiki/Firewall>
<http://www.microsoft.com/windowsxp/using/networking/security/winfirewall.mspix>
- B. Keep your operating system up to date, preferably by using automatic update features in Windows. (Automatic update included in XP and VISTA)
<http://www.microsoft.com/windowsxp/using/setup/maintain/autoupdate.mspix>
- C. Install and maintain antivirus software. (Microsoft package for XP available for a fee, Included in VISTA.)
<http://onecare.live.com/standard/en-us/3/helpsupport/default.htm>
<http://www.microsoft.com/protect/products/computer/default.mspix>
NOTE: Section C-1 of NIST Special Publication 800-69 gives directions for obtaining installing, and configuring three different versions of free, open source Antivirus programs. (Search sp800-69 for AVIRA).
- D. Install and maintain antispyware software, such as Windows Defender. (Free download is available from Microsoft-Home, included in VISTA.)
<http://www.microsoft.com/windows/products/winfamily/defender/default.mspix>

IV. Case histories of Hackers.

- A. The Cuckoo's egg
[http://en.wikipedia.org/wiki/The_Cuckoo's_Egg_\(book\)](http://en.wikipedia.org/wiki/The_Cuckoo's_Egg_(book))
- B. Hacking smartcards used in the Boston subway system
http://news.cnet.com/Lock-hacks%2C-contests%2C-and-intrigue-at-Defcon/2009-1029_3-6245076.html?tag=mncol;txt
http://news.cnet.com/8301-1009_3-10012612-83.html
http://blogofbile.com/wp-content/uploads/2008/08/11/defcon_presentation.pdf

V. Additional topics for the interested student.

- A. Microsoft's security guide for Windows XP
<http://www.microsoft.com/downloads/details.aspx?FamilyId=2D3E25BC-F434-4CC6-A5A7-09A8A229F118&displaylang=en>
- B. Microsoft's security guide for VISTA
<http://www.microsoft.com/downloads/details.aspx?familyid=A3D1BBED-7F35-4E72-BFB5-B84A526C1565&displaylang=en>
- C. User Accounts Privileges
<http://www.microsoft.com/protect/computer/advanced/useraccount.mspix>

Sharing files/ folders

<http://www.microsoft.com/windowsxp/using/networking/security/permissions.msp#2>

Passwords (strong) (stored)

<http://www.microsoft.com/protect/yourself/password/create.msp>

Delete/disable GUEST account and other unnecessary accounts.
(help, search for guest).

D. NTFS file system

http://www.microsoft.com/windowsxp/using/setup/expert/russel_october01.msp

E. Disable file sharing

<http://www.microsoft.com/windowsxp/using/networking/security/permissions.msp#2>

F. Block unnecessary/unused services (ports)
Section 3.1.5 of NIST SP 800-69

G. Perform Data and System Backups. (Consider off-site storage)

http://www.microsoft.com/protect/educators_us.msp

search NIST SP 800-69 for backup

H. Microsoft Baseline Security Analyzer

<http://www.microsoft.com/technet/security/tools/mbsahome.msp>

I. Examples of intrusion attempts (“attacks”) reported by Firewall.
(Instructor’s notes)

J. Enable Data Execution Prevention (DEP).

<http://support.microsoft.com/kb/875352>

<http://technet.microsoft.com/en-us/library/cc700810.aspx>

K. Wireless router Issues

WEP/WAP encryption -- 128 bit encryption

http://www.microsoft.com/windowsxp/using/networking/expert/bowman_03july28.msp

Access restricted to specific devices

Change network name from default

Change router administrator name (if possible) and password from factory default

http://www.netgear.com/Community/Blog/ThreeEasyStepsSecurity_10_10_2006.aspx

L. Encrypt files and data

Microsoft provisions for encrypting data on hard drive

<http://technet.microsoft.com/en-us/library/cc875821.aspx>

M. Parental Controls.

<http://www.microsoft.com/protect/products/family/vista.msp>

N. Less risky way of paying online.
www.allaccessgift.com