

# INTERNET & COMPUTER SECURITY

March 20, 2010

Scoville Library  
[ccayne@biblio.org](mailto:ccayne@biblio.org)

# Internet:

- Password strength
- Phishing
- Malware
- Email scams
- Identity Theft
- Viruses

# Computer

- Windows updates
- Browser updates
- Backup
- Firewall

# Password Strength

- Effectiveness of a password is measured in resisting guessing and brute-force attacks
- The strength of a password is a function of length, complexity, and randomness.
- Don't use the same password for all your accounts.
- Use the same password, sometimes with small variations, for low level accounts
- Use a good password for high level accounts such as online banking and change that password some time within every 100 days.
- Some security experts recommend writing down your password and carrying it on a piece of paper in your wallet.
- If passwords are written down, they should never be kept in obvious places such as address books, rolodex, etc.

# Password Strength - High level passwords:

- Include numbers, symbols, upper and lowercase letters in passwords
- Password length should be around 12 to 14 characters
- Avoid any password based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, or biographical information (eg, dates, ID numbers, ancestors names or dates, ...).
- If the system is case sensitive use capital and lower-case letters
- Password should be easy to remember for the user
- Great way to pick a hard password: use the first letters of the words in a classic song's chorus.
- Ex.: "1itlntyed2cbaba1." That stood for "One is the loneliest number that you'll ever do. Two...can be as bad as one..."
- <https://www.microsoft.com/protect/fraud/passwords/checker.aspx> - test your password's strength.

# Password Manager

- A program that keeps track of all your passwords using a master password to access the information
- [www.lastpass.com](http://www.lastpass.com), a free download, has been recommended by PC Magazine, PC World, The Economist and Fox News and CNet as one of the top products of 2009, T is a better choice than having your browser remember passwords which is not very secure.
- Last Pass encrypts all the logons and passwords stored on your computer. Access is through a master password. So, be warned: forget your master password and you could be in trouble—especially if you have let the program delete (as it urges you to let it do) all the vulnerable logons and passwords on your own computer.
- Nice feature is the use of one time only passwords to access your password vault

# PHISHING

- **phishing** is the fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.
- Phishing is typically carried out by email or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
- Secure websites have a padlock symbol and in Firefox and Google Chrome the background of the URL bar will be yellow for secure sites.

- Phishing Protection is turned on by default in Firefox 3 or later, and works by checking the sites that you browse against a list of known phishing sites. This list is automatically downloaded and regularly updated within Firefox when the Phishing Protection feature is enabled.
- Phishing protection is also turned on automatically in Google Chrome
- If you go to a site deemed to be a phishing site, a popup window will appear giving you the choice of “get me out of here” or continue. The "Get me out of here!" link will back out of a suspected phishing site and redirect you to the Firefox Start page. The "Ignore this warning" link will allow you to continue to the suspected phishing site.

# MALWARE

- Malware, short for malicious software, is software designed to infiltrate a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.
- In Firefox 3 and later and Google Chrome, malware protection is turned on automatically.
- If you wish to scan your computer, Malwarebytes Anti-Malware is an effective antimalware tool: [www.malwarebytes.org](http://www.malwarebytes.org). A quick scan takes about 8 minutes. Real-time protection is restricted to the paid version, as is the scheduler for updates and scans.

# EMAIL SAFETY

- Change your password often and keep it in a safe place
- Don't share the password with anyone.
- Don't open any attachments from anyone unless they are run through an anti-virus program.
- Log off when done.
- Don't reply to spam, harassing, or offensive e-mail or forward chain e-mail letters.
- Use common sense and keep personal information personal.
- Delete all e-mails, unread, from people you don't know
- Don't be caught by the spammers' favorite trick, "Remember me?"

# IDENTITY THEFT

**Identity theft** is a term used that is to refer to fraud that involves someone pretending to be someone else in order to steal money or get other benefits.

Government website with excellent information on what to do if you are the victim of identity theft:

<http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm>

# VIRUSES, ETC.

- A **virus** is a small piece of software that piggybacks on real programs. Each time the real program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.
- **E-mail viruses** - An e-mail virus travels as an attachment to email messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. Some e-mail viruses don't even require a double-click -- they launch when you view the infected message in the preview pane of your e-mail software

- **Trojan Horse** - A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard drive). Trojan horses have no way to replicate automatically.
- **Worms** - A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

# ANTIVIRUS SOFTWARE

- AVG Anti-Virus Free Edition is an anti-virus protection tool free to home users.
- Rapid virus database updates are available for the lifetime of the product, thereby providing the high level of detection capability.
- AVG Anti-Virus Free Edition gives you free rock solid protection for your basic security needs. Additionally, version 9.0 comes with basic anti-rootkit protection to ensure protection against sophisticated hidden threats.

5 star editor's rating on Cnet.com

Free download: <http://free.avg.com/us-en/homepage>

# ANTIVIRUS SOFTWARE

- Microsoft Security Essentials provides real-time protection for your home PC that guards against viruses, spyware, and other malicious software.
- It is a free\* download from Microsoft that is simple to install, easy to use, and always kept up to date so you can be assured your PC is protected by the latest technology.

[http://www.microsoft.com/Security\\_Essentials/default.aspx?  
mkt=en-us#dlbutton](http://www.microsoft.com/Security_Essentials/default.aspx?mkt=en-us#dlbutton)

4.5 stars by CNet.com

# WINDOWS UPDATES

- Control Panel - Settings - Control Panel
- Recommended to select Automatic Updates
- If you do not change the default schedule, updates that have been downloaded to your computer will be installed at 3 A.M.
- If your computer is turned off during a scheduled update, Windows will install the updates the next time you start your computer.
- When you turn on Automatic Updates, Windows routinely checks the Windows Update Web site for high-priority updates that can help protect your computer from the latest viruses and other security threats. These updates can include security updates, critical updates, and service packs. Depending on the setting you choose, Windows automatically downloads and installs any high-priority updates that your computer needs, or notifies you as these

# BROWSERS

- Recommended browsers are Firefox, Google Chrome and Safari for Macs.
- Always make sure you are running the latest version of your browser.
- Do not have browser remember passwords
- In Firefox 3.5 and up, you can enable private browsing. If private browsing is enabled, sites visited will not appear in the browsing history. More info: <http://support.mozilla.com/en-US/kb/Private+Browsing?bl=n&s=private%20browsing&as=q>

# BACKUP

- Backing up is saving the data on your computer to a location outside of your computer
- It is one of the most important things you can do
- Hard drives (where your data is stored) last 3-5 years
- If that is the only place where your information is, you can lose all of it
- You should back up everything on your computer which you would not want to lose
- You can back up to an external piece of hardware, like a CD, large flash drive or external hard drive
- Windows: connect external storage
  - start-programs-accessories-system tools-backup**
  - Follow instructions in the wizard which will open

# ONLINE BACKUP

- Online backup services encrypt your data and it is stored on servers at the host location.
- You can schedule automatic online backups more easily than scheduling through Windows
- **www.jungledisk.com.** \$2 per month; 5GB free; \$.15 @ GB; includes unlimited number of computers; works with PCs and Macs; only backs up files that have changed since the last backup.
- **www.mozy.com.** 2GB month free; \$4.95 per month more storage. I believe pricing is per computer.

# FIREWALL

- A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer.
- If an incoming packet of information is flagged by the filters, it is not allowed through.

**Windows: Start - Control Panel - Security Center**