Welcome to Windows – Week 3
Personal Safety
E-mail Management

Personal Safety - Objectives
• Understand the importance of acceptable use policies, passwords, and constant vigilance while online
• Learn how your computer is not secure on the Internet unless you make it secure
• Discover what you can do to protect your computer and personal data while you are online
• Know when you own online activities violate copyright and software piracy laws
• Become aware of privacy issues, and learn what you can do to protect your personal privacy
• Find out how to separate fact from fiction when using warnings and advice on the Net

Take Charge
• Each time you're on the net, you expose your information and yourself to the Net and the world
• Acceptable Use Policies (AUP)
  – Restrictions on ISP Accounts are known as Terms of Service (ToS)
Password Security

- Passwords are the key protection to your account and yourself
  - Once someone hacks your account, they can gain administrative access to the network, and can look like you did it
- No system administrator will ever ask you for your password
  - Only privileged (or trusted) administrators have special passwords that allow access to your account

Password Security

- If you receive an e-mail asking for password and looks like an official, refuse and notify network admin ASAP
  - These hackers are also known as social engineering
  - If you receive an e-mail asking for password, forward a copy of the e-mail with "URGENT: PASSWORD THEFT ATTEMPT" to System Admin

Password Security

- Passwords DOs and DON'Ts
  - DO select a Password that is at least 5 characters long, and if possible, mix with numbers
  - DO select a password that you can remember
  - DO consider making a password combining two or more words, or the first letter of a poem or phrase
  - DO change you password if you think someone discovered it
  - DON'T select a password that can be found in a dictionary
  - DON'T use your name, nickname, social security number, birth date, or name of a close relative
  - DON'T write your password where it is easy to find – under the keyboard is the first place they will look
Viruses, Trojans and Worms

- **Open Door on your System**
  - If your computer is on broadband, your system is always online and open.
  - Online is not the only way viruses spread.

- **Virus**
  - An executable program that attaches itself to another program and has a "trigger" and has a series of commands to carry out nasty tasks.
  - Can be replicated through floppies or other media.

- **Trojan Horse**
  - An executable program that slips into a system as a disguise as a system program.
  - It has to do something undocumented and intended by the programmer that the user would not approve.
  - There are some Trojans that records every keystroke you hit, capture credit card numbers, and even take over your system.

- **Worm**
  - Similar to Virus, but reproduces differently.
  - Worm depends on network connections and a variety of hosts to reproduce.
  - One part of the worm can do some vicious on one computer while only doing a log on another.
Viruses, Trojans and Worms

- **Macro Virus**
  - A virus that is written in a macro, commonly used in Microsoft Office products under Macros and VBA
  - The most famous was The Melissa Virus (3/26/00)
    - The macro virus went into everyone’s address books of e-mail software and send e-mail to propagate itself
  - If not sure, you can prevent macro viruses by sending RTF (Rich Text Format) documents
  - Never have e-mail program open a Word or Excel document automatically
  - These viruses spread so fast since just about everyone uses Microsoft Office products and almost all word processors have macro writing capabilities

Viruses, Trojans and Worms

- **Protection**
  - Use Anti-Virus Software
  - The key to complete protection is the antivirus program updated regularly
  - Keep floppy disks out of floppy drives unless you are using them
  - If you are NOT using a virus scanner, disable Java and JavaScript in your browser as they are virus potentials
  - For maximal safety, encrypt all files contain sensitive information or store them offline on floppies or removable media
  - Do not leave your computer online longer than necessary unless you have virus protection and firewall
  - Computers using UNIX, Linux and Macintosh have much far less virus issues

E-mail Viruses

- You can not get a virus from just reading an e-mail, but you can get one from an e-mail attachment, especially scripts
  - "Mail attachments can carry viruses, and reading a mail attachment can cause a virus to swing into action."
  - Save the attachment in a folder on the hard drive and have it scanned by the virus scanner software
  - Page 62 in text has directions on setting up e-mail software how to make sure attachments are never opened
E-mail Viruses

• What to do if you receive an e-mail attachment
  – If you receive an unsolicited e-mail attachment from an
    unknown person, delete it without opening it first
  – If you receive an e-mail attachment with an empty message
    body, delete it, even if it is from someone you know
    • Besides someone sending you something and not telling you
      what it is, is rude
  – If you receive an unexpected e-mail attachment from
    someone you know and the message body looks generic,
    contact the sender to make sure that they sent the e-mail.
  – Before opening any attachments, have it scanned

• Besides someone sending you something and not telling you
  what it is, is rude
  – If you receive an unexpected e-mail attachment from
    someone you know and the message body looks generic,
    contact the sender to make sure that they sent the e-mail.
  – Before opening any attachments, have it scanned

E-mail Viruses

• What to do if you are sending an e-mail attachment
  – Have a body in the e-mail, letting them know what the
    attachment is
  – By all means, if there are no graphics in your Word
    document, send an RTF
  – Have your e-mail scanned upon sending and let the recipient
    know it was scanned upon sending

Shopping Online

• When purchasing anything online, do it with a
  well known vendor or cleaning house. Do not
  use a generic company! Most likely a scam!
  • What to look for in the browsers before
    purchasing
    – The URL should have “https.....” for Secured
    Channels
    – There should be either a padlock or key on the lower
      part of browser screen
      • DO NOT use public computers such as schools since
        cookies can keep credit card information
    – Make sure there is a customer service phone number
      if there is a problem with the order
Protecting Your Privacy

- No matter what you are doing...computer or not...online or offline, your privacy is not protected in the USA
  - It is your responsibility to ensure your own privacy
- Give out as little information as possible about and your family
  - Under no circumstances should you divulge your social security number, age, income or other sensitive information.
  - It is against the law making it required data for ANYTHING
- Check for privacy policy/statement before completing any questionnaire online

Internet Scams

- Whenever you feel unease or uncomfortable about anything online, do not do it.
- Tips on avoiding scams
  - Beware of get rich quick offers...that's a joke
  - Don't trust an operation just because their website looks slick
  - Be wary of anyone pressuring you to buy
  - Never send cash....if no credit card is available, use COD

Online Auctions

- Online auctions topped fraud list in 1997 according to FTC
- Before bidding on anything, do your homework!
  - Look for sites that post fraud warnings and offer the following
    - Escrow services
    - Feedback areas
    - Easy-to-follow complaint procedures
    - A policy to remove problem vendors
  - Use the BBB (Better Business Bureau) when deemed necessary
- When bidding, use credit cards utilizing a clearing house such as Billpoint or PayPal since they can assist with purchasing problems
Software Piracy and Copyright Infringements

• "It is a willful reproduction or distribution of one or more copies of one or more copyrighted works that have collectively a total of retail value of more than $1,000."
  – It is not only for profits...it is any kind of unauthorized duplicating
  – It is punishable by law, jail time and fines

Software Piracy and Copyright Infringements

• When you buy a software, you do not OWN the software...you are an end user with limited license rights
  – Software distributed over the net, including shareware are accompanied by a license agreement
  • If you did not get a license agreement, discard it...could be a piracy or virus issue
  • Under the 1997 NET (No Electronic Theft) Act, the RIAA (Recording Industry Association of America) is keeping a lookout for piracy music
    – This was prompt by Napster as well as a 22-year old senior of University of Oregon who was sentenced 3 years in prison and charged $250,000 fine
    – Basic Rule, "If you download an audio file that is being distributed illegally, you are guilty of copyright infringement."