Chapter 2:
Personal Safety Online

Web 101
Third Edition

by Wendy G. Lehnert & Richard L. Kopec
Learning Objectives

- Understand the importance of acceptable use policies, passwords, and constant vigilance while online.
- Learn why 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 your online activities violate copyright or software piracy laws.
Learning Objectives

• 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 you see warnings and advice on the Net.
• Learn what you can do to protect yourself from identity theft.
Taking Charge

• While you may feel secure in the privacy of your own home, each time you connect to the Internet you enter a public place
• Your conduct is visible to many different people
• You have both rights and responsibilities
• The Internet has its own code of conduct
• You need to minimize your personal risk as you work and play online
• Actions that you take have consequences
Acceptable Use Policies

• All computer accounts and some public servers are subject to an Acceptable Use Policy (AUP)
• An AUP is a policy that outlines appropriate use of the Internet and is enforced by system administrators
• Violating the AUP can result in the withdrawal of your Internet access privileges
Acceptable Use Policies

• The restrictions that pertain to an ISP account are called the terms of service.
• When you sign up for an account, you also agree to the terms of service or AUP.
• You should locate and periodically check your account’s AUP, as you are expected to know the AUP.
Acceptable Use Policies

• Common university AUPs include the prohibition of the use of university resources for:
  – Commercial activity
  – Academic dishonesty
  – Harassment

• Some universities also prohibit the use of specific Internet services, such as some music sharing sites
Password Security

• Your password is the first line of defense
• While you may think that your account has nothing to offer, someone can use it as a starting point to access other accounts
• System administrators have resources to maintain accounts and the system
• No system administrator will need to ask you for your password
Password Security

• Do not be tricked by an email, no matter how official looking, asking you for your password

• Hackers try tactics like this

• Do not share your password with anyone, as this is a security hole
Password Security

• Choose a good password
• Here are some tips to help you choose a good password:
  – Do not use a word from the dictionary
  – Do not use a proper name
  – Do not use the same password on more than one site
  – A good password has at least one number, has at least 6 characters, and has uppercase and lowercase letters
Phishing

- Phishing is a form of online fraud characterized by unsolicited e-mail messages seeking personal information for fraudulent purposes.
- Phish often appears to originate from reputable sources that maintain accounts for the recipient.
- Spear phishing is a large scale phishing effort directed at all employees of a company intended to capture an account name and password.
Phishing

• Here are some tips to help you identify phishing expeditions:
  – References to accounts that you do not have.
  – A general salutation (Dear Valued Customer) rather than one by name.
  – Grammar and spelling errors.
  – Mismatch in the URL of embedded links with that of the apparent source (URLs of links display in the status bar at the bottom of the web page when the cursor hovers over them).
  – Contact the apparent source directly using other trusted means first.
Phishing

• Some tips from the Federal Trade Commission:
  – Don’t provide personal information unless you initiate
    the contact or can verify the identity of the agent
    receiving it.
  – Never click on links from an unsolicited e-mail.
  – Legitimate organizations *never* request or seek
    confirmation of personal information via e-mail or
    phone.
  – Forward *phishages* to spam@use.gov,
    reportphishing@antiphishing.org and the company
    being impersonated.
Phishing

• Some tips from the Federal Trade Commission:
  – Keep your OS and security software updated.
  – Monitor sites like mailfrontier.com to keep abreast of the latest scams.
Identity Theft

• Occurs when stolen personal information is used to open accounts used to make fraudulent purchases.
• In many cases, information is stolen from third party business records.
• Not limited to internet activity
• Warning signs:
  – Late or missing bills.
  – Receipt of credit cards or other lines of credit not requested.
  – Requests for payment from debt collectors.
Identity Theft

• If your identity is stolen:
  – Notify any of three major credit bureaus: Equifax, Experian, or TransUnion
  – Close compromised accounts.
  – File report with local law enforcement office.
  – File a complaint with the FTC.
  – Contact relevant government agencies to cancel/replace stolen licenses or IDs. And flag your account appropriately.
  – Consult your financial institution about bank and other accounts.
Viruses, Trojan Horses, and Worms

• Some software is a security risk
• The mainstream news calls all such software “viruses”, but there are three different classes of such software
• A virus is a computer program that can replicate itself through files to move from computer to computer
  – Some viruses are benign
  – Others are very destructive
Viruses, Trojan Horses, and Worms

• A Trojan horse is a program that slips into a computer under the guise of another program
  – Someone could e-mail a game to you that contains a Trojan horse. If you run the game you also run the Trojan horse
  – The Trojan horse could record your keystrokes or allow someone to access your computer
Viruses, Trojan Horses, and Worms

- A worm is a program that is similar to a virus, but spreads through a network.
- Software can be exploited by worms.
- Some worms run over several computers.
- Others communicate among themselves over the network.
- A worm may be malicious or may take up system resources, causing a slowdown in performance.
Viruses, Trojan Horses, and Worms

• You can take control and secure your computer

• Use antivirus software and keep it updated
  – Antivirus software can scan files moving from the computer onto disks and CDs
  – Your email and downloaded files can also be scanned
  – Since new viruses are created every day, the data files needed to detect these viruses needs to be kept up-to-date
Viruses, Trojan Horses, and Worms

• Keep bootable disks out of your drive unless you are actively working with the files on the disk
  – Some viruses can hide on the boot sector on a disk
  – These are triggered when the computer starts up and accesses the disk

• If you need to work without a virus scanner running in the background, you should manually scan each file before opening or executing it
Viruses, Trojan Horses, and Worms

- Install a firewall on your home computer (especially if you use a broadband connection)
- Do not download files offered to you in chat rooms or personal Web pages
- For maximum safety, encrypt all files that contain sensitive information or store them offline on removable media
- Do not leave your computer connected to the Internet any longer than necessary
E-Mail Viruses

• E-mail is the number one source of computer viruses

• Attachments are the most common culprit

• Some attachments contain scripts

• A script is a small program written in a scripting language (e.g. Visual Basic)

• You can take precautions
  – Configure your mailer to not open attachments automatically
  – Save attachments and scan them first
E-Mail Viruses

• Microsoft Word documents are a popular source of viruses
• Someone can spread a virus unknowingly
• Precautions include:
  – Keeping your antivirus software up-to-date
  – Saving an attachment and make sure that it is scanned before you open it
  – Not opening a document that contains a macro
E-Mail Viruses

• Mailers that render messages into Web-like displays are susceptible to script attacks
  – Some messages contain scripts
  – If the script is automatically executed, it can cause harm

• Some threats can contain a blend of different types of attacks
  – Nimda
  – Love Letter
Internet Scams

• Scams are nothing new, but the Internet makes it easier for them to reach you
• Examples include:
  – Get rich quick offers
  – Miracle health cures
  – Guaranteed loans or credit
  – Your credit report repaired for a fee
• If it sounds too good to be true, then it probably is
Hacker Attacks and Intrusions

- Hacker intrusions are less likely than viruses, but are more devastating.
- Many companies monitor their computers, so home computers are easier targets.
- It doesn’t take much effort to break into a computer that is not protected.
  - Tools exist to make breaking into a computer as easy as point-and-click.
  - The existence of such tools doesn’t mean that it is okay.
Hacker Attacks and Intrusions

• The results can range from:
  – A hacker changing your wallpaper to
  – Adding, changing, or deleting files

• You can take precautions to protect your computer
  – The precautions are similar to those discussed earlier in regard to viruses
  – Install a firewall, a software program that acts as a boundary between your computer and the outside world
Firewalls

• A firewall is software that
  – monitors all attempts to move bytes over the Internet in either direction and
  – notifies you when such movement is attempted.

• Firewalls previously were only used by large organizations but now home users can install them on their computers.

• They can prevent a Trojan horse from stealing your files or spyware from “phoning home.”
Firewalls

• Both the Macintosh and PC have firewalls.

• Examples include:
  – Zone Alarm
  – Symantec Internet Security

• The software can be configured or used with default settings.

• Read software reviews to help you choose what firewall to buy.
Protecting Your Privacy

• The Internet has provided opportunities for data collection that go far beyond a marketer’s wildest dreams
• Your browser contains information about you, including the types of sites you visit
• Web pages can also be programmed to collect information about you, such as when you visited the site
• The Online Personal Privacy Act (2002) limits the kinds of information that is collected
• For information about the current status of this bill, visit www.netcoalition.com/keyissues
Protecting Your Privacy

• To protect your privacy:
  – Do not provide personal information unless it is needed for a credit card transaction
  – Do not provide your Social Security Number or other sensitive information

• When you do provide personal information, read the site’s Privacy Policy

• Some companies sell your information, but you can opt-out of this
Protecting Your Privacy

• If you plan to use a portal, and have a personalized page, then you may need to supply personal information

• Be aware that this same information can be used by advertisers

• Two federal laws exist to protect privacy
  – Children’s Online Privacy Protection Act of 1998 - children under 13 years old
  – Online Personal Privacy Act of 2002 - everyone
Libel and Lawsuits

- Libel is any written or pictorial statement that damages a person or an organization.
- Posting libelous statements can result in legal action against the poster.
- Some companies even monitor Web pages and online forums to protect themselves and their products.
- While libel is not criminal, it can result in civil litigation.
Statements against a company or their product is libelous if it results in lost revenues for the company.

Statements against a person may or may not be considered libelous:
- If the person is a public figure, he/she is open to ridicule.
- A public figure has fewer rights than someone who is not a public figure.
Threats and Harassment

- Our society takes threats very seriously nowadays
- Online stalking and hate mail incidents also need to be taken seriously
- As people communicate in chat rooms and email over long distances, some people lose their temper
  - A flame is a message where the writer makes a personal attack against another individual
  - A flame war is an exchange of flames
Threats and Harassment

• Flame wars can make people nervous, as you may not know much about the person behind the communication

• Laws exist that make issuing threats illegal
  – This includes kidnapping or bodily harm
  – Threats against the President are investigated by the Secret Service
Threats and Harassment

- Employees are also protected against harassment in the workplace
- Students and staff are also protected at schools
- Title VII of the 1964 Civil Rights Act protects employees against workplace harassment
- E-mail is not private, and you never know who it may be forwarded to
- Save the questionable jokes for after work
Software Piracy and Copyright Infringements

- Software piracy is the willful reproduction or distribution of programs that prohibit such activity
- Piracy is against the law
- You do not have to profit to be guilty
- Purchasing commercial software, grants you the right to use the software under certain restrictions (the license rights)
Software Piracy and Copyright Infringements

• Intellectual property, in the form of text, images, and audio, is protected under copyright
  – Downloading MP3s has become popular
  – Unless they have been explicitly made public by an artist, they are protected

• Universities are starting to protect themselves by cracking down on students who violate copyright

• Some have also been prosecuted
Pornography and Other Lapses in Good Taste

• The Internet contains all sorts of material, including pornography
• The First Amendment protects against censorship, as well as obscene language
• Some material, such as child pornography is illegal to own and distribute
• Increasingly, employers monitor employees’ email and web activity
• Your employer determines your rights and freedoms in the workplace
Hoaxes and Legends

• The Internet contains both valuable information and misinformation
• Many hoaxes and urban legends persist
• A popular hoax is an email message that says not to read an email with a subject such as “Good times”, then pass it on
• You cannot get a virus through a plain text message
• Chain letters and scams are also common
• Don’t forward these messages
Laptops and Wireless Networks

• Because of their mobility and the ubiquity of wireless networks, laptops are especially prone to attack
• Many wireless networks are unsecured, allowing access to any and all
• Thieves can use packet sniffers to capture wireless transmissions
• If transmissions are not encoded, thieves can capture vital information
Laptops and Wireless Networks

• When joining a wireless network, keep these safety tips in mind:
  – Use encryption for communication, via a WPA or WEP encryption scheme (WPA is better) - an access key is required for these networks
  – Keep your antivirus and antispyware software up-to-date
  – Make sure your firewall is on
Laptops and Wireless Networks

• Safety tips continued:
  – Use a virtual private network (VPN) when connecting to your institution’s network (ask the IT staff for help)
  – Disable File and Printer Sharing
  – Keep your folders/directories private
  – Password protect your sensitive files
Summary of Threats

• AdWare - displays commercial advertisements, mostly a nuisance
• Pharming - redirects valid URLs to bogus sites, dangerous
• Phishing, Spear Phishing - emails requests for personal information, dangerous
• Rootkit - undetectable modifications to the OS that permit remote, surreptitious access to your computer, very dangerous
Summary of Threats

• Spam - unsolicited e-mail, low (unless you open an attachment)
• Spyware - monitors usage and/or keystrokes and sends data to remote user, dangerous
• Trojan Horse - embedded code in application that allows remote access to your computer, dangerous
• Virus - self-replicating software that inserts itself into other computer files, dangerous
Summary of Threats

- Worm - self-replicating, stand-alone program that sends copies of itself over the network, potentially jamming it, dangerous