Security and Ethics in Information Systems


What is Ethics?

• **Ethics**, also known as moral philosophy, is a branch of philosophy that addresses questions about morality—that is, concepts such as good and evil, right and wrong

Principles of Technology Ethics

• **Proportionality** – the good achieved by the technology must outweigh the harm or risk
• **Informed Consent** – those affected by the technology should understand and accept the risks

Ethical Responsibility

• **Business professionals** — have a responsibility to promote ethical uses of information technology in the workplace.

Computer Crime

• The unauthorized use, access, modification, and destruction of hardware, software, data, or network resources
• The unauthorized release of information
Computer Crime
• Using or conspiring to use computer or network resources illegally to obtain information or tangible property

Common Hacking Tactics
○ Sniffer
• Programs that search individual packets of data as they pass through the Internet

Hacking
• The forced access and use of networked computer systems

Common Hacking Tactics
○ Spoofing
• Faking an e-mail address to trick users into passing along critical information like passwords or credit card numbers
○ Phishing
• An attempt to trick a person into giving away their private account information by confirming it at the phisher’s Web site.
• Spoofed E-mails are sent to a randomly chosen group of prospective victims with hope that a portion will be received by actual customers.

Common Hacking Tactics
○ Denial of service (attack)
• Hammering a website’s equipment with too many requests for information
○ Scans
• Widespread probes of the Internet to determine types of computers, services, and connections

Common Hacking Tactics
○ Trojan Horse
• A program that, unknown to the user, contains instructions that exploit a known vulnerability in some software
• Unlike viruses, they cannot replicate. They need to be invited usually when a user opens an e-mail attachment.
Common Hacking Tactics

- **Malicious Applets**
  - Tiny Java programs that misuse your computer’s resources, modify files on the hard disk, send fake e-mail, or steal passwords

- **Back Doors**
  - A hidden point of entry to be used in case the original entry point has been detected or blocked

- **Logic Bombs**
  - An instruction in a computer program that triggers a malicious act

- **Buffer Overflow**
  - A technique for crashing by sending too much data to the buffer in a computer's memory

Common Hacking Tactics

- **Password Crackers**
  - Software that can guess passwords

- **Social Engineering**
  - Gaining access to computer systems by talking unsuspecting company employees out of valuable information such as passwords

Common Hacking Tactics

- **Dumpster Diving**
  - Sifting through a company's garbage to find information to help break into their computers

- **Keystroke Logging**
  - Technique embedded in some program that enables the recording and reporting of a user’s keystrokes

Cyber Theft

- **Computer crime involving the theft of money**

Freedoms vs. Censorship Issues

- **Spamming**
  - Indiscriminate sending of unsolicited e-mail messages to many Internet users (*Junk mail*)

- **Flaming**
  - Sending extremely critical, derogatory, and often vulgar e-mail messages or newsgroup postings to other users on the Internet or online services (*Flame mail*)

  - Racist or defamatory messages or sexually explicit material have led to calls for censorship and laws for libel
Internet Abuses in the Workplace

• General e-mail abuses

Internet Abuses in the Workplace

• Leisure use of the Internet (time and resource theft)

Internet Abuses in the Workplace

• Unauthorized usage and access

Internet Abuses in the Workplace

• Copyright infringement/plagiarism
• Newsgroup postings

Internet Abuses in the Workplace

• Transmission of confidential data
• Pornography – accessing sexually explicit sites

Internet Abuses in the Workplace

Hacking
Non-work related download or upload
Internet Abuses in the Workplace

• Usage of external ISPs
• Moonlighting

Software Piracy

• Unauthorized copying of computer programs

Licensing

• Purchase of software is really a payment for a license for fair use
• Site license allow a certain number of copies

A third of the software industry's revenues are lost due to piracy

Theft of Intellectual Property

• Intellectual property

- Copyrighted material
- Peer-to-peer networking techniques have made it easy to trade pirated intellectual property

Viruses and Worms

• Computer Virus

  - Self-replicating computer program intended to alter how a computer operates, without the permission or knowledge of the user
  - File virus: infects executable files. When the virus runs, it searches for files of specific name or type and infects them.

• Worm

  - Self-replicating (like a virus) but does not need to attach itself to an existing program for transport.
  - E-Mail Worm: spread via e-mail, but once implanted take responsibility for their own replication and distribution.

Viruses and Worms

- Virus and worms copy annoying or destructive routines into networked computers
- Often spread via e-mail or file attachments or shareware
Viruses and Worms

- A virus copies itself into the files of the operating system
- Then it spreads to the primary memory and copies itself throughout the hard disk, flash drives, disks, etc.
- Then it spreads through e-mail or infected devices

Most Costly Worms and Viruses

- **ILOVEYOU** – 2000
  - Caused over $15 billion in damages.
  - Spread through emails that had a subject of “ILOVEYOU”
  - More than 3 million opened the attachment
  - Shut down email servers around the world
  - Was one of the first to attach to an email

Most Costly Worms and Viruses

- **MyDoom** – 2004
  - Caused over $38 billion in damages. When a user was infected with the virus it creates network openings which allowed others to have access to your computer.
  - In 2004, an estimated 25% of all emails had been infected by the virus.
  - Slowed down Internet access globally by 10%

Most Costly Worms and Viruses

- **Sasser Worm** – 2008
  - Caused over $18 billion in damages.
  - Brought down Delta Airlines causing cancellation of numerous flights
  - Resulted in 300,000 railway passengers to be stranded in Australia

Most Costly Worms and Viruses

- **SirCam** – 2001
  - Caused over $1 billion in damages in 2001.
  - Had the ability to compromise confidential information, delete items or use up space on your hard drive until there was not enough memory to store anything else.

Most Costly Worms and Viruses

- **In 2003, the SoBig virus caused over $37.1 billion in devastation. This fast-spreading virus circulated through email as viral spam, and if exposed, the virus had the capability to copy files, emailing itself to others and causing serious damage to computer software and hardware.**
Most Costly Worms and Viruses

- Melissa – 1999
- Particularly slimy virus that sent out infected MS Word documents through Outlook, delivering viral messages to everyone listed in the address book.
- The message: "Here is that document you asked for ... don't show anyone else." There would be a word document attached with the Melissa virus.
- Caused $1.2 billion in damages.

Cost of viruses and worms

- Over 300 million computers were infected in 2011
- As many as 11 million computers are believed to be permanently infected
- Total economic damage estimated to be greater than $388 billion per year according to Norton
- Average damage per installed Windows-based machine is between $277 and $366

CAN-SPAM Act

- permits e-mail marketers to send unsolicited commercial e-mail as long as it adheres to 3 basic types of compliance
  1. Unsubscribe compliance (Visible Opt-out)
  2. Content compliance – label if adult content, legitimate and visible address, relevant subject
  3. Sending behavior compliance – can’t have a false header, can’t send on open relay (sending through a third-party)

Adware and Spyware

Adware

- Software that purports to serve a useful purpose but also allows Internet advertisers to display advertisements (pop-up and banner ads)

Spyware

- Adware that employs the user’s Internet connection in the background without your permission or knowledge.
- It usually sends information to a third party for identity theft.
Cookies
• Information about you can be captured legitimately and automatically each time you visit a website
• This information is recorded as a “cookie” on your disk
• Then the website owners may sell the information from cookies to third parties
• Cookies can also be intercepted or retrieved from your hard disk by hackers

Privacy: Opt-in versus Opt-out

• Opt-in
  – You (the customer) explicitly consent to allow data to be compiled about you.

Privacy Issues

Violation of Privacy:
• Accessing individuals’ private e-mail conversations and computer records,
• Collecting and sharing information about individuals gained from their visits to Internet websites

Privacy Issues

Computer Monitoring:
• Always knowing where a person is, especially as mobile and paging services become more closely associated with people rather than places
• Computers used to monitor the productivity and behavior of employees as they work

Privacy Issues

Computer Matching
• Using customer information gained from many sources to market additional business services

Unauthorized Personal Files
• Collecting telephone numbers, e-mail addresses, credit card numbers, and other personal information to build individual customer profiles
Protecting your Privacy on the Internet

- E-mail can be encrypted
- ISP can be asked not to sell your name and personal information to mailing list providers and other marketers
- Decline to reveal personal data and interests on online service and website user profiles

Encryption

- Symmetric Key
- Asymmetric Key
- Three Pass Protocol Asymmetric Key

How to protect yourself from cybercrime

- Use different passwords for different websites
- Don’t open e-mail attachments unless you know the source of the incoming message
- Install all operating system patches and upgrades

Encryption

- Use the most up-to-date version of your e-mail software and browser
- Send credit card numbers only to secure sites (look for a padlock or a key icon at the bottom of the browser)
- Use a security program that give you control over “cookies” that send information back to websites

IT Code of Conduct

- Contribute to society and to human well-being
- Avoid harm to others
- Be honest and trustworthy
- Be fair and take action not to discriminate
- Honor property rights including copyrights and patents
- Respect the privacy of others
- Honor confidentiality

How to protect yourself from cybercrime

- Use anti-virus software (update it regularly)
- Don’t allow merchants to store your credit card information for future purchases
Cyber Security and Ethics
The End