PowerPoint® Slides to Accompany

A Gift of Fire: Social, Legal, and Ethical Issues for Computers and the Internet

(2nd Edition)

by **Sara Baase**

San Diego State University

PowerPoint slides created by Sherry Clark

A Gift of Fire

Computer Crime

Introduction

Hacking

Online Scams

Fraud, Embezzlement, Sabotage, Information Theft, and Forgery

Crime Fighting Versus Privacy and Civil Liberties

Introduction

Computers Are Tools

Computers assist us in our work, expand our thinking, and provide entertainment.

Computers Are Used to Commit Crimes

Preventing, detecting, and prosecuting computer crime is a challenge.

Hacking

The Phases of Hacking

Phase One: The early years

- 1960s and 1970s.
- Originally, *hacker* referred to a creative programmer wrote clever code.
- The first operating systems and computer games were written by hackers.
- The term hacking was a positive term.
- Hackers were usually high-school and college students.

Hacking

The Phases of Hacking (cont'd)

Phase Two: Hacking takes on a more negative meaning.

- 1970s through 1990s.
- Authors and the media used the term hacker to describe someone who used computers, without authorization, sometimes to commit crimes.
- Early computer crimes were launched against business and government computers.
- Adult criminals began using computers to commit their crimes.

Hacking

The Phases of Hacking

Phase Three: The Web Era

- Beginning in the mid-1990s.
- The increased use of the Internet for school, work, business transactions, and recreation makes it attractive to criminals with basic computer skills.
- Crimes include the release of malicious code (viruses and worms).
- Unprotected computers can be used, unsuspectingly, to accomplish network disruption or commit fraud.
- Hackers with minimal computer skills can create havoc by using malicious code written by others.

Hacking

Hactivism

…is the use of hacking expertise to promote a political cause.

- This kind of hacking can range from mild to destructive activities.
- Some consider hactivism as modern-age civil disobedience.
- Others believe hactivism denies others their freedom of speech and violates property rights.

Hacking

The Law

Computer Fraud and Abuse Act (CFAA, 1986)

- It is a crime to access, alter, damage, or destroy information on a computer without authorization.
- Computers protected under this law include:
  - government computers,
  - financial systems,
  - medical systems,
  - interstate commerce, and
  - any computer on the Internet.

Hacking

The Law (cont’d)

USA Patriot Act (USAPA, 2001)

- Amends the CFAA.
- Allows for recovery of losses due to responding to a hacker attack, assessing damages, and restoring systems.
- Higher penalties can be levied against anyone hacking into computers belonging to criminal justice system or the military.
- The government can monitor online activity without a court order.

Hacking

Catching Hackers

… requires law enforcement to recognize and respond to myriad hacking attacks.

Computer forensics tools may include:

- Undercover agents,
- Honey pots (sting operations in cyberspace),
- Archives of online message boards,
- Tools for recovering deleted or coded information.

Computer forensics agencies and services include:

- Computer Emergency Response Team (CERT),
- National Infrastructure Protection Center (NIPC),
- Private companies specializing in recovering deleted files and e-mail, tracking hackers via Web site and telephone logs, etc..

Hacking

Questions About Penalties

Intent

- Should hackers who did not intend to do damage or harm be punished differently than those with criminal intentions?

Age

- Should underage hackers receive a different penalty than adult hackers?

Damage Done

- Should the penalty correspond to the actual damage done or the potential for damage?

Hacking

Security

Security weaknesses can be found in the computer systems used by:

- businesses,
- government (classified and unclassified), and
- personal computers.

Causes of security weakness:

- characteristics of the Internet and Web,
- human nature,
- inherent complexity of computer systems.

Hacking

Security can be improved by:

- Ongoing education and training to recognize the risks.
- Better system design.
- Use of security tools and systems.
- Challenging “others” to find flaws in systems.
- Writing and enforcing laws that don’t stymie research and advancement.

Online Scams

Auctions

Selling and buying goods online has become popular.

Problems:

- sellers don’t send the goods,
- sellers send inferior goods,
- price is driven up by shill bidding, and
- illegal goods sold.

Solutions:

- educate customers,
- read seller “reviews,”
- use third-party escrow, and
- more…

Fraud, Embezzlement, Sabotage, Identity Theft, and Forgery

Some Causes of Fraud

Credit-Card

- Stolen receipts, mailed notices, and cards.
- Interception of online transaction or weak e-commerce security.
- Careless handling by card-owner.

ATM

- Stolen account numbers and PINs.
- Insider knowledge.
- A counterfeit ATM.

Telecommunications

- Stolen long-distance PINs.
- Cloned phones.

Fraud, Embezzlement, Sabotage, Identity Theft, and Forgery

Some Defenses Against Fraud

Credit-Card

- Instant credit-card check.
- Analysis of buying patterns.
- Analysis of credit card applications (to detect identity theft).
- Verify user with Caller ID.

ATM

- Redesigned ATMs.
- Limited withdrawal.

Telecommunications

- match phone “signature” with serial number.
- identify phone without broadcasting serial number.

Fraud, Embezzlement, Sabotage, Identity Theft, and Forgery

Embezzlement and Sabotage

Some Causes

- Insider information.
- Poor security.
- Complex financial transactions.
- Anonymity of computer users.

Some Defenses

- Rotate employee responsibility.
- Require use of employee ID and password .
- Implement audit trails.
- Careful screening and background checks of employees.

Fraud, Embezzlement, Sabotage, Identity Theft, and Forgery

Identity Theft

Some Causes of Identity Theft

- Insecure and inappropriate use of Social Security numbers.
- Careless handling of personally identifiable information.
- Weak security of stored records.
- Insufficient assistance to identity theft victims.

Some Defenses for Identity Theft

- Limit use of personally identifiable information.
- Increase security of information stored by businesses and government agencies.
- Improve methods to accurately identify a person.
- Educate consumers.

Fraud, Embezzlement, Sabotage, Identity Theft, and Forgery

Forgery

Some Causes

- Powerful computers and digital manipulation software.
- High-quality printers, copiers, and scanners.

Some Defenses

- Educate consumers and employees.
- Use anti-counterfeiting techniques during production.
- Use counterfeit detection methods.
- Create legal and procedural incentives to improve security.

Crime Fighting vs Privacy and Civil Liberties

Scams

Crime Fighting

- Automated surveillance software to look for suspicious Web activity.

Privacy and Civil Liberties

- No search warrant nor proof of probable cause.

Biometrics

Crime Fighting

- Exact match of biological characteristics to a unique person.

Privacy and Civil Liberties

- Easy to build complete dossier on people.

Crime Fighting vs Privacy and Civil Liberties

Search and Seizure of Computers

Crime Fighting

- Obtain evidence of a crime.

Privacy and Civil Liberties

- Day-to-day business ceases; non-criminal contact with others ends.

The Cybercrime Treaty

Crime Fighting

- U.S. and European governments agree to cooperate with investigations.

Privacy and Civil Liberties

- Potential for government spying is great.