Computer Crimes

Computers are tools

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

Computers are used to commit crimes

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

First Cyber Crime

- Happened in 1820
- Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom
- This device allowed the repetition of a series of steps in the weaving of special fabrics
- This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened
- They committed acts of sabotage to discourage Jacquard from further use of the new technology
- This is the first recorded cyber crime

Categories of Computer Crime

- "There are three general categories of computer crime: targets, means, and incidentals" – Britz, 2009, p.51
- However, these three are not necessarily mutually exclusive of one another. Many computer crimes "involve a multiplicity of intentions"

Targets

- The computer is the intended target of a criminal, as may (or may not) be the case with hacking
- Hacking, DDoS Attack, etc

Means

- In this instance, the computer is the means through which the criminal can gain access of stored information
- Harassing, stalking, and crimes against persons, including physical and psychological harm, etc.
- Crimes have occurred in both instances: the use of the computer by the criminal, the targeted theft of information from the hacked computer system

Incidentals

- Computer crimes dealing with incidentals exist when a computer has played a minor role in an offense
- Malware, Trojan Horse, etc.

Types of Computer Crime

- Child Pornography
- Cyberbully
- Creating Malware
- Enrollment Process
- Identity Theft
- Cyber Terrorism
- Money Laundering
- Malware

- Phishing
- Software Piracy
- Unauthorized Access
- Doxing
- Fraud
- Scam
- Spamming

Hacking

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

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 Update Softwarecrimes

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

Hactivism

- 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

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

- PH Counterpart: The Philippine Congress enacted Republic Act No. 10175 or "Cybercrime Prevention Act of 2012"

Revised E-Commerce Law

- 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

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.

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 be the penalty correspond to the actual damage done or the potential for damage?

Security

- Security weaknesses can be found in the computer systems used by: businesses, government, and personal computers
- Causes of security weakness: characteristics of the internet and web, human nature, inherent complexity of computer systems

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

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…

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

Defense Against Fraud

Credit Card

- Instant credit-card check
- Analysis of buying patterns
- Analysis of credit card applications
- Verify user with Caller ID

ATM

- Redesigned ATMs
- Limited withdrawal

Telecommunications

- Match phone “signature: with serial number
- Identify phone without broadcasting serial number

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

Identity Theft

Some Causes of Identity Theft

- Insecure and inappropriate use of Social Security numbers
- Careless handling of personality 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

Forgery

Causes

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

Defense

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

Scams

Crime Fighting

- Automated surveillance software to look for suspicious Web Activity

Privacy and Civil Liberties

- No search warrant not 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

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 government agree to cooperate with investigations

Privacy and Civil Liberties

- Potential for government spying is great

"A liberal education is about…The wisdom to connect." - William Cronon

What's with the terminology?

- Distance Education
- Distance Learning
- Web-Assisted
- Hybrid
- Online Learning

IN PUP…

Institute of Open and Distance Education / Transnational Education (PUP-OUS)

- Distance education provides option in terms of where and when you learn. You may study independently, with the guidance of a teacher or a tutor who grads and comments on your work or you may study online, communicating with your teacher and other students in your "online" classroom.

Communication Tools

Asynchronous

- Telephone – individual
- Email- individual or group
- Print – group
- Web Page – group
- Discussion Board – group

Synchronous

- Chat Rooms – all participants log on at once
- MS Teams
- Google Classroom
- Skype
- Zoom

Communication Models

Carnegie Model

- Higher Education must move beyond "critical thinking" to the idea of "practical reasoning" as a focal point for curriculum and teaching
- It is important for students to learn to think, to reason, to interrogate text, AND understand it
- Engage faculty in collaborative dialogue, writing and reflection, inquiring into what teaching for practical reason means for their university/college
- Foster connections between individuals and fields; provide faculty with a place to ask hard questions
- Serve as pedagogical exemplars for one another

Computer-Mediated Model (CMI)

- Human social life online is a future in which friendships, social groups, organizations, and work teams operate in "cyberspace", transcending physical restraints.

Computer-Supported Collaborative Learning (CSCL)

- The concept of collaborative or group learning whereby instructional methods are designed to encourage or require students to work together on learning tasks

Laurillard's Conversational Model

There are four main aspects of the teaching-learning process:

- Discussion between the teacher and the learner
- Adaptation of the learner's actions and of the teachers's constructed environment
- Interaction between the learner and the environment defined by the teacher
- Reflection of the learner's performance by both teacher and learner

Pedagogical Elements

Meaningful Learning occurs when learners are:

- Active
- Constructive
- Collaborative

Learning Styles:

- Visual
- Auditory
- Kinesthetic

Learning Environments are best when

- Intentional
- Complex
- Contextual

Bloom's Taxonomy

- **Remember**
  - Recognizing and recalling facts
- **Understand**
  - Understanding what the facts mean
- **Apply**
  - Applying the facts, rules, concepts, and ideas
- **Analyze**
  - Breaking down information into component parts
- **Evaluate**
  - Judging the value of information or ideas
- **Create**
  - Combining parts to make a new whole

Learning as a Social Act

- Blending Learning
- Communities of Practice

We are Social Beings who benefit from learning that is

- Conversational
- Reflective

Instructor Concerns

Evaluation

- Provide opportunities for students to reflect on their own learning and contribution
- Feedback on the learning experience
- Evaluation of your performance

Rules for Discussion Groups

Be courteous, participate responsibly

Participate actively

Write clearly

Build ideas on what others say

Be Credible, back up your statements

Stick to the subject

Student Concerns

Overcoming Isolation

- Distance education students often feel very isolated
- Overcoming this isolation is a big challenge – “Get to know me!”
- Good access to a tutor is essential i.e., some face –to-face time with the instructor