Computers and Crime: Cybercrime

Carter Halamka
What is Cybercrime?

- Crime involving computers / networks
- Varieties of cybercrime include:
  - Fraud
  - Extortion/Harassment
  - Espionage
- Cybercrime involves individuals / corporations / governments
- Nearly as old as computers themselves
Brief History of Cybercrime

- Early cybercrime involved computer phone systems
- Stealing information became a popular tactic
- Denial of Service attacks are now popular
  - First DoS attack launched by 15 year old
- Computer fraud targets vulnerable individuals
- Corporate espionage
Cybercrime Today

- Identity theft and fraud are common
- Extortion and blackmail
- Denial of Service attacks continue to be popular
  - Used by individuals as well as organizations
  - Use large networks of compromised machines (Distributed)
- Intellectual property issues / theft
- Computer viruses continue to advance technologically
Problems Caused by Cybercrime

- Identity theft costs the U.S. billions of dollars
- Theft of schematics / data by governments / corporations
- Websites can be taken down by DDoS attacks
- Children/Elderly are often victims
How can Cybercrime be Prevented?

- Security measures (and attack techniques) improve constantly
- Governments are increasingly paying attention
- Computers can be used to prevent cybercrime
  - Human factors are typically exploited
  - So called “Social Engineering”
- Raising awareness / preventing common mistakes
Cybercrime and the Future

- Cybercrime has typically followed computer development
- Mobile devices are extremely popular
- Vulnerabilities will be patched and discovered
- Legislation may address problems
- Hard to predict the next type of crime
Resources

1. http://content.time.com/time/nation/article/0,8599,1902073,00.html
4. Images via google.com