IMPORTANT

Common Internet Crime Schemes

http://www.ic3.gov/crimeschemes.aspx
Current and ongoing Internet trends and schemes identified by the Internet Crime Complaint Center along with its description.

- Auction fraud
- Counterfeit cashier's check
- Credit card fraud
- Debt elimination
- Parcel courier e-mail scheme
- Employment/ Business opportunities
- Escrow services fraud
- Identity theft
- Internet extortion
- Investment fraud
- Lotteries
- Nigerian Letter or "419"
- Phishing/spoofing
- Ponzi/pyramid
- Reshipping
- Spam
- Third-party receiver of funds

http://www.ic3.gov/preventiontips.aspx
How to prevent these crimes through individual actions.

35

Sources of Laws

- Statutory law
  - Statutory laws are the laws passed by local, state, and federal legislative bodies.
  - Specific statutory laws, such as the Computer Fraud and Abuse Act (CFAA), govern behavior.
- Administrative law
  - Power granted to government agencies through legislation.
  - This power of lies in the ability to enforce behaviors through administrative rule making.
  - Example: Federal Trade Commission (FTC), have made their presence felt in the Internet arena with respect to issues such as intellectual property theft and fraud.
- Common law
  - Laws derived from previous events or precedence and originates in the judicial branch of government.
  - As new cybercrime cases continue to unfold in the courts, precedents are being made on which future crimes involving computers can be judged.

36

Computer Trespass

- Unauthorized access of a computer system
  - Independent of access method
  - Considered a crime in many countries
  - May warrant significant punishment
  - Treaties between countries regulate ways to deal with the cyber offenders

37

Convention on Cybercrime (2004)

- First international treaty that addresses crimes committed through the Internet and other computer networks.
- Ratified by EU, U.S., Canada, Japan, and others
- Created common policies to handle cybercrime
- Focused on:
  - Copyright infringement
  - Computer-related fraud
  - Child pornography
  - Violations of network security

38

Significant U.S. Laws

- **The United States**
  - A leader in the development and use of computer technology.
  - As such, it has a long history associated with computers, and with cybercrime.
  - Because legal systems tend to be reactive and move slowly, this leadership position has translated into a leadership position from a legal perspective as well.
- **Some significant US laws dealing with cybercrime**
  - Electronic Communications Privacy Act
  - Stored Communications Act
  - Computer Fraud and Abuse Act
  - Controlling the Assault of Non-Solicited Pornography and Marketing Act
  - USA Patriot Act
  - Gramm-Leach-Bliley Act
  - Sarbanes-Oxley Act

39

Electronics Communications Privacy Act (ECPA)

- Addresses legal privacy issues related to computer use and telecommunications
- A common practice with respect to computer access and privacy today is the use of a warning banner
- **Warning Banners are common practice in**:
  - Establishing the level of expected privacy
  - Serving notice of intent to conduct real-time monitoring
    - Real-time monitoring can be conducted for
      - Security reasons
      - Business reasons
      - Technical network performance reasons.
  - Obtaining user's consent to monitoring. Typically displayed upon login
  - Providing consent to law enforcement search

40

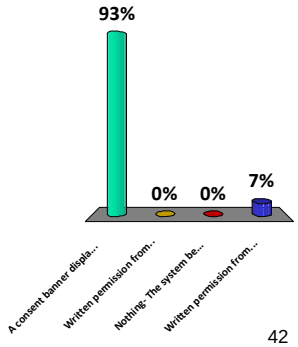
Computer Fraud and Abuse Act (1986)

- Provides the foundation of U.S. law on unauthorized access
- Criminalizes activities such as:
  - to knowingly access a computer, either considered a government computer or a computer used in interstate commerce, without permission
  - Using a computer in interstate crime
  - Trafficking in passwords or access information
  - Transmitting code, commands, or programs that result in damage

41

The VP of IS wants to monitor user actions on the company's intranet. What is the best method of obtaining the proper permission

1. A consent banner displayed upon login
2. Written permission from a company officer
3. Nothing- The system belongs to the company
4. Written permission from the user



42

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM)

- Established spam e-mail regulations
- **Provided rules of compliance**
  - Unsubscribe
    - Requires an obvious opt-out provision to allow users to unsubscribe, with these requests being honored within ten days.
  - Content
    - The content must be clear and not deceptive.
    - Header Information- Adult content must be clearly labeled and subject lines must be clear and accurate.
  - Sending Behavior
    - Sending behavior rules include not using harvested e-mail addresses, not falsifying headers, and not using open relays.
    - CAN-SPAM criminalizes header manipulation
- Has had a poor track record of convictions

43

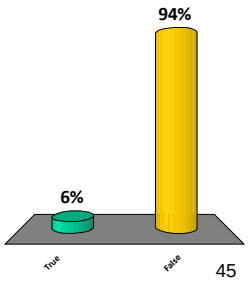
USA Patriot Act

- Response to the 9/11 terrorist attacks
- Altered U.S. laws on Internet wiretaps and tracing
- Permits the Justice department to rollout Carnivore program, an eavesdropping program for the Internet
  - The name Carnivore has now been retired but the right of the government to eavesdrop remains a hot topic
- Requires ISPs to facilitate Internet monitoring
- Provides for federal law enforcement investigation and adjudication of computer intrusions

44

Falsifying header information is not covered by the CAN-SPAM Act.

1. True
2. False



45

Gramm-Leach-Bliley Act (GLBA)

- Enacted in 1999
- Financial industry legislation to protect individual privacy.
- Key privacy tenet - Created an opt-out method providing individual control over the use of personal information
- Enforced by state, federal and securities laws
- Restricts information sharing with third-party firms, while still allowing for internal sharing in accordance with the Fair Credit Reporting Act.
  - For example: SSN, other facts kept by your bank

46

Payment Card Industry Data Security Standard (PCI DSS)

- Contractual rules governing exchange of credit card data between banks and merchants
  - Voluntary standard
- Noncompliance may result in:
  - Higher transaction fees
  - Expensive fines
  - Inability to process credit cards

47

Import/Export Encryption Restrictions

- Includes use to secure network communications
- U.S. export control laws handled by the Dept. of Commerce
- Administered by the Bureau of Industry and Security
- U.S. encryption export control policies rest on three principles:
  - Review of encryption products prior to sale
  - streamlined post-export reporting
  - License review of certain exports of strong encryption to foreign government end users.

48

Non-U.S. Laws

- Wassenaar Arrangement
  - International agreement on export controls dealing with dual-use goods and technologies.
  - Removed key length restrictions on encryption products to allow for mass-market distribution of encryption products
- Cryptographic use restrictions
  - Many countries tightly restrict the use and possession of cryptographic technology.

49

U.S. Digital Signature Laws

- **Signatures -**
  - A means of affixing a sign of one's approval for centuries
  - A ring and wax seal, a stamp, or a scrawl
- **Digital signatures-**
  - As communications have moved into the digital realm, there exists a need for signatures to move with the new medium
  - Means to show approval for electronic records
    - Cryptography provides integrity and non-repudiation.
    - Enables e-commerce transactions
  - Equivalent to notarized signatures for all transactions in the US for all transactions in which both parties agree to use digital signature
- **Electronic Signatures in Global and National Commerce Act (E-Sign Law)**
  - Electronic forms of signatures, contracts, and other records are just as valid and enforceable as those written on paper.

50

Other Digital Signature Laws

- United Nations
  - UN Commission on International Trade Law Model Law on Electronic Commerce
- Canada
  - Uniform Electronic Commerce Act
- European Union
  - Electronic Commerce Directive

51

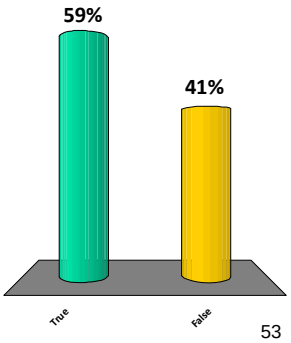
Digital Millennium Copyright Act (DCMA)

- **Digital Rights Management**
  - Generic term for access control technologies that can be used by hardware manufacturers, publishers, copyright holders and individuals to limit the usage of digital content and devices.
  - Used to describe any technology that inhibits uses of digital content not desired or intended by the content provider.
- **Digital Millennium Copyright Act (DCMA)**
  - Protects rights of recording artists.
  - Identifies how new computer technology relates to copyright laws.
  - Makes it illegal to develop, produce, and trade any device or mechanism designed to circumvent technological controls used in copy protection.

52

Digital signatures are equivalent to notarized signature **only for non-real property transactions** in the US in which both parties agree to use Digital signatures

1. True
2. False



53

MSDN Alliance

- Go to this web site:
http://msdn07.e-academy.com/stockton_cs/
- click on the “Register” button, and self-register by entering your student ID, a valid email address, and select your password
- The terms of use agreement

54