Legal Issues

Objectives

- Discuss types of computer crime
- Discuss why it’s important to get authorization

Disclaimer

- I am not an attorney
- Nor do I pretend to be one
- Please consult with your own attorney for any of the content related to computer crime

Computer Crime

- To help understand computer crime and what it means, the Convention on Cybercrime was ratified in 2001
  - “The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.
  - Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.”

Articles

- 2: Illegal Access
- 3: Illegal Interception
- 4: Data Interference
- 5: System Interference
- 6: Misuse of Devices
- 7: Computer-releated forgery
- 8: Computer-related fraud
- 9:Offenses related to child pornography
- 10: Infringements of copyright and related rights
- 11: Attemp and aiding or abetting

US Computer Fraud and Abuse Act

- 1986 US Code outlining different computer crimes
- Most important and perhaps widely used
- 18 U.S.C. § 1030(a)(1): Computer Espionage.
- 18 U.S.C. § 1030(a)(2): Computer trespassing, and taking government, financial, or commerce info
- 18 U.S.C. § 1030(a)(3): Computer trespassing in a government computer
- 18 U.S.C. § 1030(a)(4): Committing fraud with computer
- 18 U.S.C. § 1030(a)(5): Damaging a protected computer (including viruses, worms)
- 18 U.S.C. § 1030(a)(6): Trafficking in passwords of a government or commerce computer
- 18 U.S.C. § 1030(a)(7): Threatening to damage a protected computer
- 18 U.S.C. § 1030(b): Conspiracy to violate (a)
- 18 U.S.C. § 1030(c): Penalties

First conviction US vs Morris

- *United States v. Morris* (1991)
- Intentionally caused damage
- Unauthoized

States – DON'T PUT THESE SLIDES ON VIDEO

- Many local jurisdictions have similar laws
- **18-5.5-102**
  Computer Crime.
- (1) A person commits computer crime if the person knowingly:
- (a) **Accesses a computer, computer network, or computer system or any part thereof without authorization**; **exceeds authorized access**
- (b) **Accesses any computer, computer network, or computer system, or any part thereof for the purpose of devising** to defraud
- (c) **Accesses any computer, computer network, or computer system, or any part thereof to obtain passwords, private information**
- (d) Accesses any computer, computer network, or computer system, or any part thereof to commit theft; casues damages
- (f) Causes the transmission of a computer program, to cause damage

Privacy Acts

- Privacy is serious business
- Many states and governments have laws governing privacy
- You need to think about your customers
- If you customers are residents of a jurisdiction, you may be held to those laws
- Upcoming is GDPR – General Data Protection Regulation
- Privacy policies can go a long way to ensure data remains private