Hacking and International Investigations

Presented By:

Nenette Day

Harvard University Extension School

Context

- Federal Law Enforcement is interested in business computers (interstate commerce)
- Title 18 Section 1030 ($5,000 damage)
- Personal Computer hacks, call the State or Local Police
- Identity Theft, call the Federal Trade Commission

Hacking the Business

- Targets
  - Business Computers
  - Cell phones (especially Camera Phones)
  - Conference Call/Phone Systems
  - Laptops
  - PDAs
  - Wireless Connections
  - Business Partners w/ trusted connections
  - Web Sites

The Suspects

- Organized Crime
- Motivated Insiders
- Economic Espionage
- Individual Hacker
- Teenage Punks
- State Sponsored Actors: China for Example

Tools of the Trade

- Any network connected computer
- Vulnerabilities in software or operating system
- Social Engineering
- Classic Trojan Horse delivered through e-mail, web site, infected CD, etc.
- Unsecured wireless connection
- Mobile computing in an unsecure environment

Tools of the Trade cont…

- Loss of physical security over computing device (keystroke loggers, theft, etc)
- Outsourced partner
- Lack of passwords and encryption
- Letting someone use your cell phone

Bottom Line

- Wetware (humans) are the most vulnerable link in the computer security chain
- Technology advances at a speed that outpaces security
- Hacking is a growth business