Social Implications of a Computerized Society

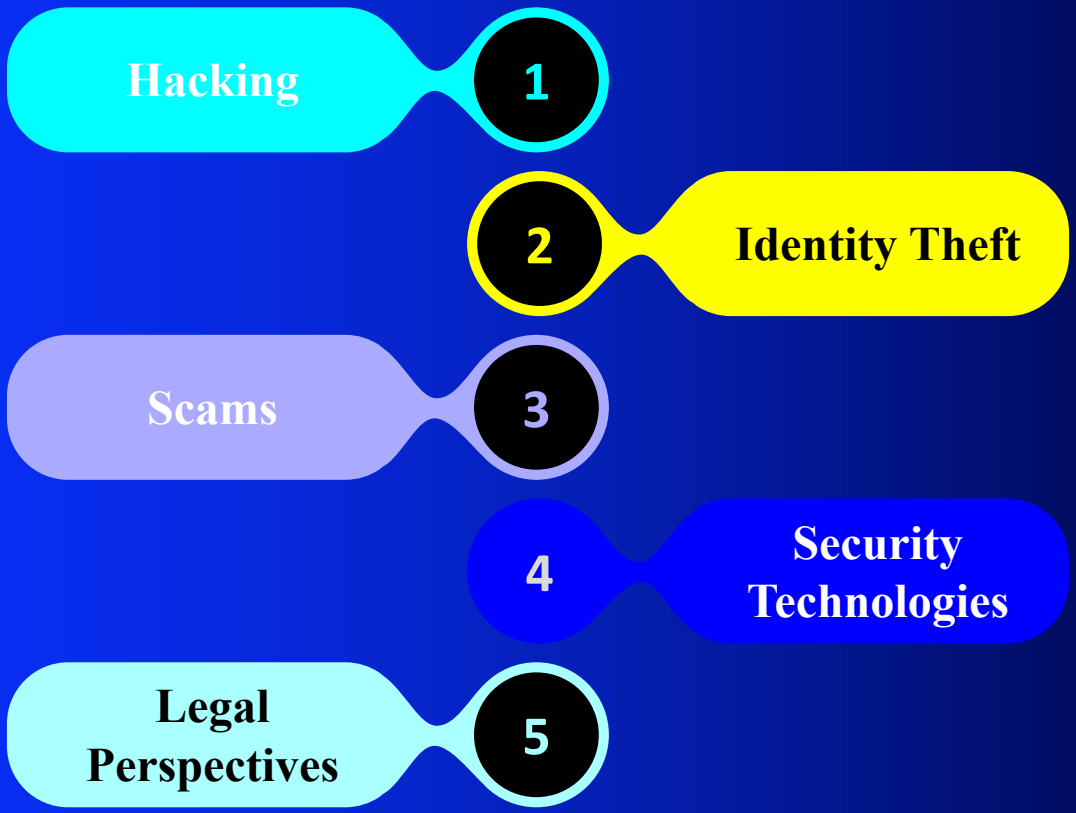
Computer Crime
Chapter 5

Instructor: Oliver Schulte

Simon Fraser University

Key Topics

EXAMPLE WITH 5 PARTS



Themes in Computer Crime

- We're going to review some general themes from this course as they apply to computer crime issues.
  - Anonymity
  - Security/Surveillance/Interception
  - Responsibility of Web Technology Providers

Anonymity and Cybercrime

Anonymity facilitates cybercrime compared to the "real" world.

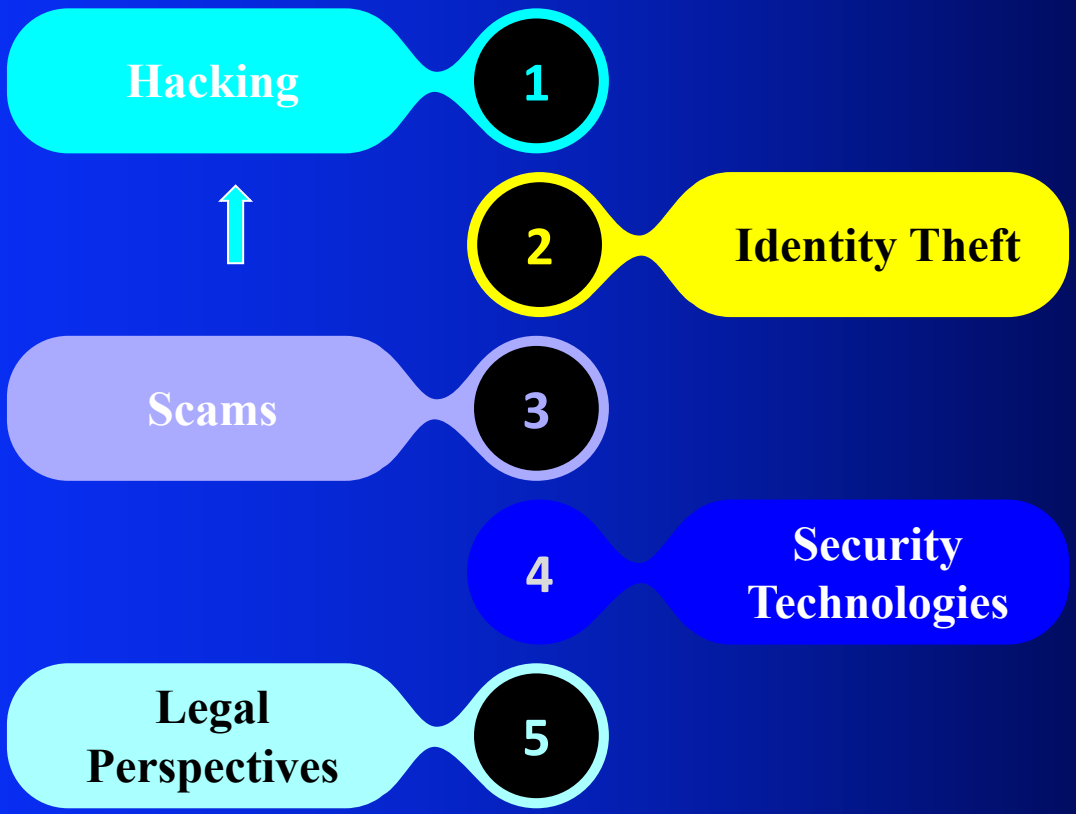
- Anonymity requires identification for legitimate purchases ⇒ Identity theft makes it easy to **impersonate** someone.
- Anonymity makes it easier to get away with fraud and deception.
  - E-bay scams.
  - Phishing
  - Click Fraud.
- Anonymity facilitates hacking as trespassing (use other people's computer, username).

Security/Surveillance/Interception

- Much personal information is stored or transmitted on the web insecurely.
- “Big Hacker is watching you”.
- Also an issue for privacy.

Key Topics

EXAMPLE WITH 5 PARTS



Web scale hacking

Hacking and the Web

Phase 3: beginning with the mid 1990s

- Changed the scale of computer crime: #victims, sites, computers attacked
- Large scale theft of personal and financial information.
- Viruses and worms can be spread rapidly
- Political hacking (Hacktivism) surfaced
- Denial-of-service (DoS) attacks used to shut down Web sites

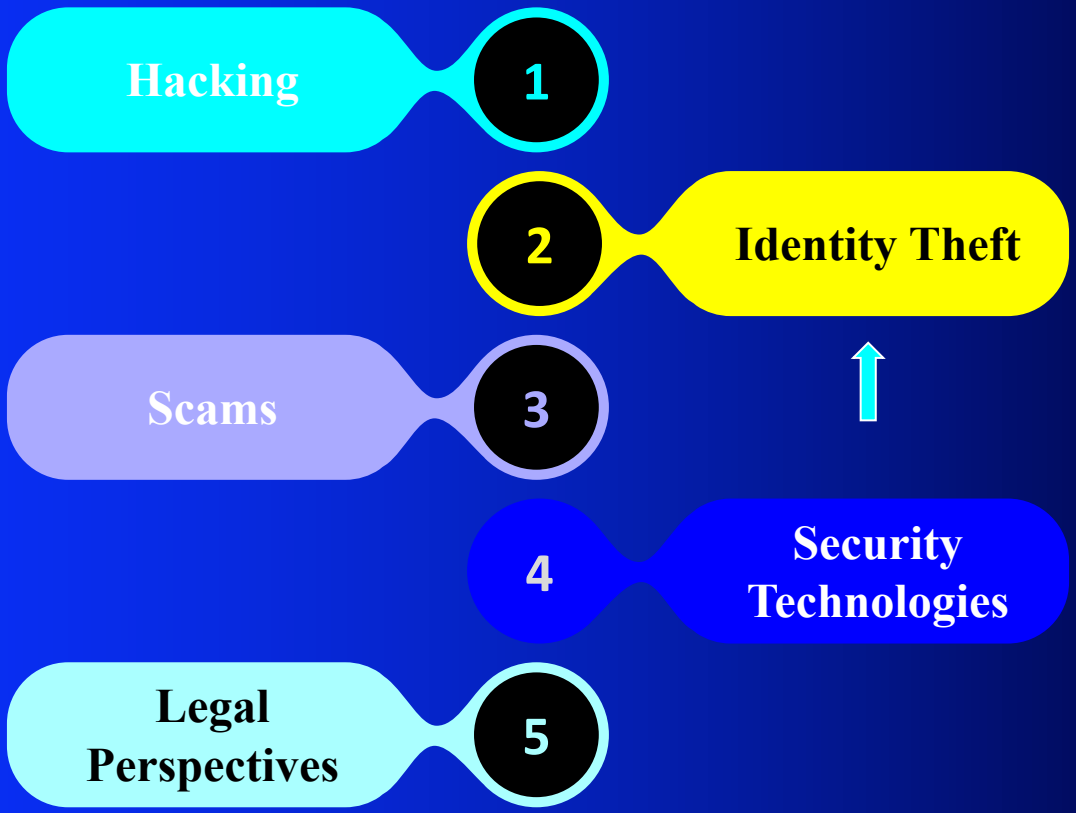
Internet hacking: examples

- The Internet Worm 1988, Robert Morris from Cornell.
- A **worm** is a program that copies itself to other computers.
- A **virus** is a malicious program hidden inside a file, program or document (e.g. Word macro).
- Mellisa virus (1999): mail copies of itself to 50 e-mail addresses in address book. Infected 1 mill computers.
- Love bug (2000): also mailing itself. Infected 80% of U.S. agencies, millions of computers, $10 billion in damages.

Internet hacking: more examples

- **Denial of Service attack** (DoS).
- Overload target site with 10^5 requests for web pages.
- 15-year old Canadian aka “mafiaboy” shut down Yahoo, eBay, Amazon etc, $1.7 billion damage.
- Estonian government was attacked.

Key Topics


Hacking
1
2
Identity Theft
Scams
3
4
Security Technologies
Legal Perspectives
5

See Canvas Survey Computer Crime

Identity theft

Identity Theft, Spam: Phase 4

- E-commerce has experienced huge growth, estimated around $200 Billion in the U.S.

⇒ many people send passwords, credit cards on-line.

⇒ Opportunities for fraud and impersonation: e-bay, Nigerian account scheme.

- Emergence of organized cybercrime rings: targets e-business by stealing IDs, often international.
- FTC estimates 8.3 million victims of identity theft, $15.6 billion losses.

Cybercrime Tools: Identity Theft

- **Phishing** - e-mail fishing for personal and financial information disguised as legitimate business e-mail. SFU attack
- **Pharming** - false Web sites that fish for personal and financial information by planting false URLs in Domain Name Servers.
- **Social Engineering**: manipulating people into releasing information that violates security protocols.
  - used to launch Melissa and ILOVEYOU viruses

Cybercrime Tools: Malware

- Already discussed viruses and worms
- **Trojan Horse**: apparently benign software with malicious component
  - e.g. send spam to all contacts
- **Ransomware**: encrypts files on computer, demands payment for the key (bitcoin)
  - 1 attack every 11 sec in 2021
- **Spyware**: record user activities
- **backdoor**: software that allows access at a future time

Cybercrime Tools: Botnets

- Zombie viruses, **botnets**: normal computers remotely controlled by distributor. Typically millions of infected machines. Botnet Article
- "A botnet is a controlled army of compromised devices"
- Mirai is a big current IoT botnet

Identity Theft: The Target Breach

Target Security Breach (Fall 2013)

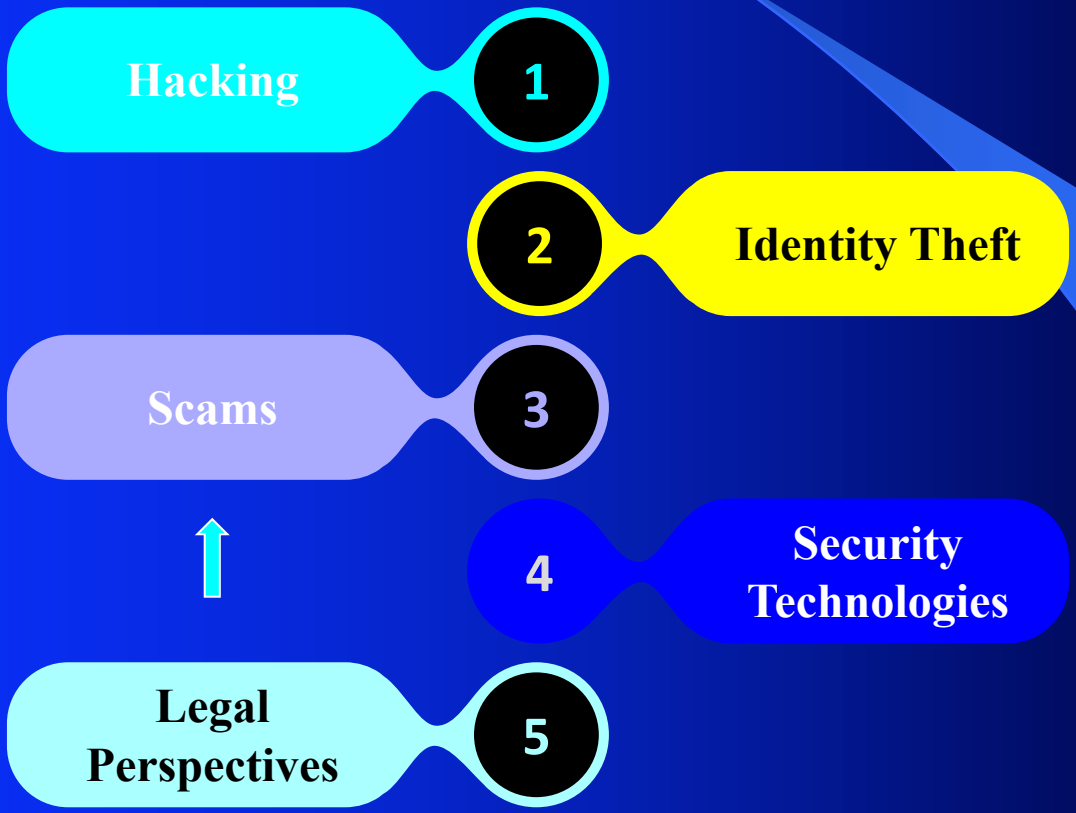
- Data on 40 million credit cards stolen
- Over 70 million customer records stolen
- Started with phishing email sent to Fazio Mechanical
  - A small company with 200 employees
- Target had to compensate consumers

Discussion Question

- The Federal Trade Commission (U.S.) has said that that “companies that collect sensitive consumer information have a responsibility to keep it secure”.
- Do you agree with that? How much responsibility do users/customers have? For example, using firewalls, encryption, coded credit cards, strong passwords?

Key Topics

EXAMPLE WITH 5 PARTS



Scams and Forgeries

Ad/Cllick Fraud

- Recent major ad fraud case (google post)

1. Make or acquire a popular Android app
2. Track user behaviour (spyware)
3. Use zombies in botnet to mimic users
4. Send to app bot traffic with real human traffic to escape fraud detection
5. Bots click on ads ➔ more money for developers!

Auction Fraud

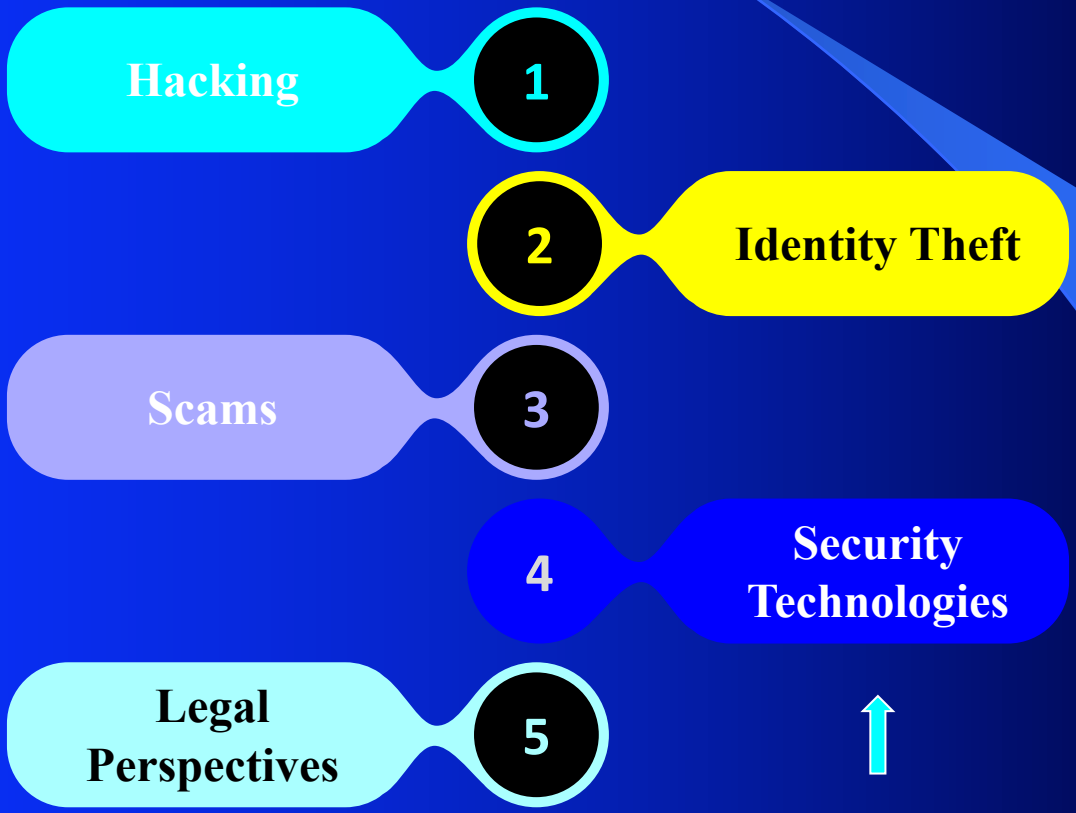
- FTC reports that online auction sites are one of the top sources of fraud complaints
  - Some sellers do not send items or send inferior products
  - Shill bidding is used to artificially raise prices
  - Sellers give themselves or friends glowing reviews to garner consumer trust
- Auction sites use various techniques to counter dishonest sellers.

Other Examples

- **Stock fraud** - most common method is:
  1. buy a stock low
  2. send out messages urging others to buy
  3. sell when the price goes up
  - GameStop story showed power of web communication to change stock prices
- **Digital Forgery** - new technologies (scanners and high quality printers) are used to create fake checks, passports, visas, birth certificates, etc.
  - Requires little skill and investment.
- Canadian Case: 400 SIN numbers stolen by government employee, $7m fraud. sin case

Key Topics

EXAMPLE WITH 5 PARTS



Fighting cybercrime

Security Technologies

- Big business: e-mail security sales $1.2 bn in 2008.
- **Firewalls** monitor network traffic.
- Web browsers check websites for proper authorization.
- Biometrics are new way to identify yourself.
  - Do you use them?
- Public-key encryption: important theoretical tool.
- New **authentication** methods?
- **Fundamental trade-off**: security versus convenience.

Encryption and Biometrics

- Public-key encryption: Encryptor makes two keys, one secret, one public. With public key, anyone can encrypt, but only encryptor can decrypt.
- Biometrics: fingerprint, face, Iris, Voice.
- Desired false positive and false negative rate: < 0.1%.
- Currently no single technology gets this rate, maybe we need to use combinations.

System Professionals

- **Software designers and system administrators** should put time and resources into system security.
- **Cybersecurity professionals** protect systems and networks. Three broad goals
  - Confidentiality: keep private data private
  - Integrity: allow only authorized access
  - Availability: ensure system and data are accessible when needed

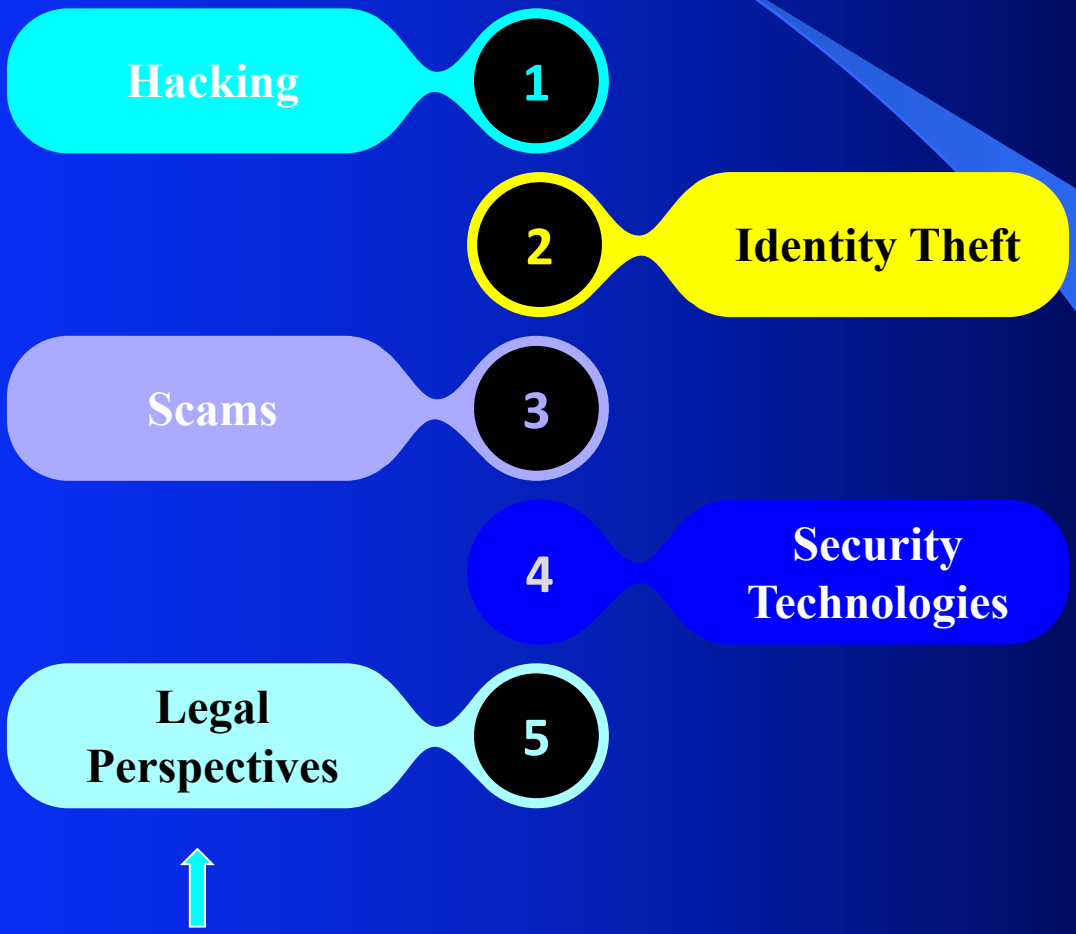
Pressure for Quick and Dirty Development

- Competitive pressure spurs companies to develop products without enough attention to security risks.
- Features and timely delivery are more important than the 3 security goals

➢ eventually this leads to updates, patches, extra maintenance, law suits,…**technical debt**

Key Topics

EXAMPLE WITH 5 PARTS



Legal perspectives

Law Enforcement and Security

- Security against unauthorized access → no access for law enforcement
- 1994 CALEA Telecommunications: communications equipment must have backdoor for FBI to eavesdrop
- FBI tried to get backdoor for encryption

Examples

- Terrorist couple killed 14 people in San Bernadino
- FBI could not unlock terrorist's Iphone.
- Asked Apple to create IOS version with no limit on login attempts
- Eventually found other access route

CFAA

- Computer Fraud and Abuse Act
- For devices connected to the internet, makes it illegal to
  - access without authorization
  - exceed authorization
  - in order to read or copy information
- Increased penalties for justice/military computers.

Canadian Law

- Part of Mischief: “Mischief in Relation to Computer Data”
- 2010: Government Cyber Security Strategy

Discussion Question

- Should it be a crime to write or post computer viruses?

Conclusion

- Hacking (modern meaning): breaking into computers without access
- Supports web-scale crimes:
  - identity theft
  - ad fraud
  - spam
- Often depend on **anonymity**
- National Jurisdiction is difficult to reconcile with international crime
  - See Kevin McQuiggin's slides

Criminal Techniques

- Phishing
- Pharming
- Social Engineering
- Malware: Viruses, Trojan Horses, Spyware, Ransomware

Security Techniques

- Public-Key Encryption
- Authentication against anonymity
- Security professionals aim for confidentiality, integrity, availability