Cybercrime and other pests

"Computer Crime"

- Computer as **target** of crime
  - Denial of service on eBay auction site
  - Cracking data stored on ChoicePoint network
- Computer as **instrumentality** of crime
  - Cracking bank computer to divert money to criminal's account
- Computer as **incident** to crime
  - Communicating by email about a robbery
- Which, if any, requires new law?

The Morris Worm

Not this one…

The Morris Worm

- Morris released a self-replicating computer program ("worm") that replicated beyond his expectations or control.
- Did he cause damage ("prevent authorized use of computers' information") ?
- Did he commit a crime?

How far is too far?

- Sending a worm that exploits holes, guesses passwords, and bogs down computer networks.
- Scraping screens from a publicly accessible website
- Even if tipped off to the organization of those screens by a misappropriated trade secret?

EF Cultural Travel v. Zefer

- EF Explorica
  (competitors)

  Zefer (contractor)

For what can you bring a civil action?

SPAM

Not this one either

How might we stop spam?

- CAN it?
- Block it?
- Ignore it?

How might we stop spam?

- CAN it? (law)
  - Place liability on the sender
  - Place liability on the advertiser
  - Place liability on the ISP
- Block it?
  - Where?
    - At the ISP level
    - At the user level
  - How?
    - Blacklists
    - Black hole lists
    - Whitelists
    - Trusted senders
    - Sender confirmation
    - Do-not-email registry
- Ignore it?

How should we evaluate anti-spam?

- Who is regulating / regulated?
- Who feels the impact?
  - Who apart from the target?
- How effective is the regulation?
  - Where are its errors?
- How easy to administer?
- How transparent is the regulation?

What are the effects of spam-blocks?

- On spammers?
- On email recipients?
- On non-spamming email senders?
- On developers of email software?
- On …

CAN-SPAM

- What's prohibited?
- Who can enforce?
- Against whom?

Special Medzz

- Bruno's Botanicals wants to introduce people to its new "healing compound." Can it harvest email addresses of potential customers from natural healing weblogs?
- Can it send emails to its prior customers?
  - If Bruno hasn't asked for their consent?
  - From bruno@amazon.com, because that's more likely to get opened?
  - If the list includes customers who have specifically opted out of email communications?

Technical measures

- MAPS RBL
  - Blackhole lists of IP addresses "that have been shown to send spam and/or allow their resources to be used by those who send spam."
  - "Loss of connectivity hurts us all. Spam hurts us all even more."
- DomainKeys sender authentication
  - Signatures linking email messages to the domain from which they are sent
  - "Finally, you could choose to send unauthenticated mail…. If you choose this path, you should carefully monitor the amount of authenticated mail over time to ensure that this strategy does not impact the deliverability of your email."

Technical measures…

- Local spam blockers
  - Spamassassin
  - DSPAM
  - Bayesian filtering
- Other sender verification
  - Bonded sender
  - Challenge-response
  - Whitelist

OptInRealBig v. SpamCop

- SpamCop runs a service to which users can forward spam they have received. SpamCop identifies ISPs from header information and URLs in the message, and forwards complaints mechanically to ISP abuse departments.
- OptInRealBig is a "sender of bulk commercial emails" whose ISPs limit or terminate service after complaints received via SpamCop.
- Can OptInRealBig recover from SpamCop?

How should we evaluate anti-spam?

- Who is regulating / regulated?
- Who feels the impact?
  - Who apart from the target?
- How effective is the regulation?
  - Where are its errors?
- How easy to administer?
- How transparent is the regulation?