



# Electronic Commerce

Michael O'Herlihy

---

---

---


---

---

---

---

---



## Agenda

- Discussion on Spam and Spam Legislation
- Encryption
  - Symmetric
  - Asymmetric

---

---

---


---

---

---

---

---



## SPAM Definition

- *“Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups”*

---

---

---

---

---

---

---

---

## European Directives

Directive 2002/58/EC, implemented as:

**European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003**  
(SI 535/2003)

*in force 6 November 2003*

---

---

---

---

---

---

---

---

## Spam

- The new Irish laws also place restrictions on direct marketing via telephone, fax, automated calling system and, importantly, SMS and MMS, or mobile spam

---

---

---

---

---

---

---

---

## Where do Spammers Get their Email Addresses?

- From Web pages
- From Domain Contact Pointers
- By guessing & cleaning
- Using social engineering
- From the address book and emails on other people's computers (Worms)
- Buying lists from others

---

---

---

---

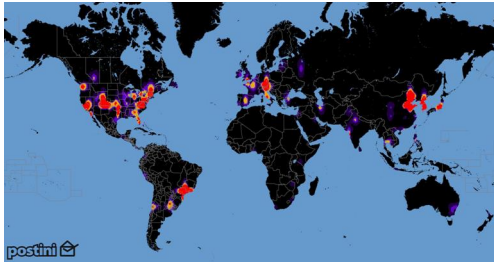
---

---

---

---

## World Spam Map



---

---

---

---

---

---

---

---

## Irish SPAM Legislation

- Positives
  - It's opt-in, rather than opt-out
  - Each spam counts as a separate offence
  - Forging / disguising of originating header info is prohibited
- Negatives
  - No private right of action
  - Spamming to mailing lists is not prohibited
  - No good against non European based spammers

---

---

---

---

---

---

---

---

## First Anti-Spam Conviction

- 4's A Fortune Limited
  - The company – which describes itself as "Ireland's first online casino-like cash game"
  - Made a total of 165,000 calls to O2 customers
  - Most calls made by auto diallers that hung up after 2 rings
  - When recipients noticed a missed call on their phones, some of them called back to the landline number displayed
  - They were then put through to a recorded message which encouraged them to call a premium rate number and play a game to win money

[http://www.theregister.co.uk/2005/09/07/irish\\_spam\\_conviction/](http://www.theregister.co.uk/2005/09/07/irish_spam_conviction/)

---

---

---

---

---

---

---

---

### Question?

- There is a maximum €3,000 per message penalty
- How much were the company fined?

---

---

---

---

---

---

---

---

### Answer

- They were fined €300 per message
- €49,500,000?
- The Commissioner's office is only empowered to investigate those calls that become the subject of complaints
- In this case 5 Complaints were received
- Therefore a fine of just €1,500!

---

---

---

---

---

---

---

---

### SPAM Legal Actions 23-Jan

- A Danish court fined a local telecoms equipment firm a record 400,000 Danish crowns (\$68,000) for sending up to 15,000 unsolicited faxes

---

---

---

---

---

---

---

---

## Data Protection Stopping Spam

- Data Protection Regulations
  - National "Opt Out" Register – Personal
  - National "Opt Out" Register – Company
  - Automatic Dialing Machines – SPAM fax
  - SPAM text messages SMS
  - Companies can SPAM customers

---

---

---

---

---

---

---

---

## Encryption

---

---

---

---

---

---

---

---

## Encryption

- The translation of data into a secret code
- To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it
- Unencrypted data is referred to as plain text
- Encrypted data is referred to as cipher text
- Two Types of Encryption
  - Symmetric
  - Asymmetric (public-key)

---

---

---

---

---

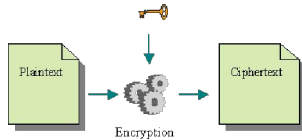
---

---

---

## Symmetric (Private Key) Encryption

- An encryption system that uses the same key to encrypt and decrypt the message



---

---

---

---

---

---

---

---

## Major problems of Symmetric Encryption

- **Data Integrity:** Receiver can not verify that a message has not been altered
- **Repudiation:** Receiver can not make sure that the message has been sent by the claimed sender
- **Scalable Key Distribution**

---

---

---

---

---

---

---

---

## Asymmetric – Public Key Encryption

- Public key encryption is different as it operates using a combination of two keys
  - A private key and
  - A public key
  - Which together form a pair of keys
- The *private key* is kept secret on your computer since it is used for decryption
- The *public key*, which is used for encryption, is given to anybody who wants to send encrypted mail to you
- Decryption of a message enciphered with a public key can only be done with the matching private key

---

---

---

---

---

---

---

---

## Asymmetric – Public Key Encryption

### ■ Example

- John wants to send a secure message to Jane
- He uses Jane's public key to encrypt the message
- Jane then uses her private key to decrypt the message

---

---

---

---

---

---

---

---

## Asymmetric – Public Key Encryption

- An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them
- It is virtually impossible to deduce the private key if you know the public key

---

---

---

---

---

---

---

---

## Asymmetric – Public Key Encryption

- Public-key systems, such as Pretty Good Privacy (PGP), are becoming popular for transmitting information via the Internet
- They are extremely secure and relatively simple to use
- The only difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for him or her

---

---

---

---

---

---

---

---