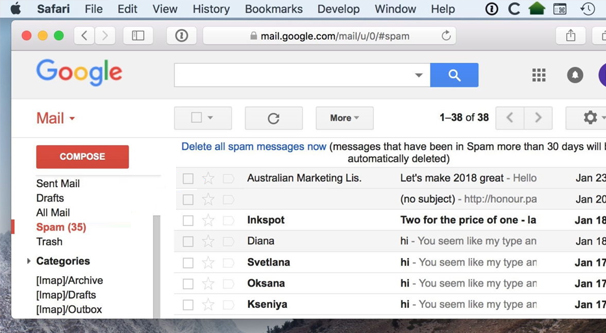
# Attack Propagation

## Spam

* Act of sending irrelevant, inappropriate and unsolicited messages
* Prolific due to low barrier to entry
* Estimated figure for spam messages was around seven trillion in 2011 (APWG, 2011)
  + Between 88–92% of email messages carried spam
  + Considerable cost associated with loss of productivity and fraud
  + Extra capacity needed to cope with the spam.
* Unsolicited Electronic Messages Act 2007 (NZ)
  + IMG was ordered to pay $120, 000 for sending spam via email and text messages to half a million New Zealanders



## Phishing

* Act of attempting to acquire sensitive information by masquerading as a trustworthy entity
* Deceives users into visiting a malicious web site claiming to be from legitimate businesses and agencies
* Unsuspecting user enters private information in the malicious web site which is then subsequently used by malicious criminals.



## Phishing Variations

* **Spear Phishing**
  + Targets only specific users
  + Customized to the recipients including their names and personal info to make it appear legitimate
* **Whaling**
  + Going after “big fish” e.g., wealthy individuals or senior executives
  + Highly tuned message
* **Vishing (also known as “Voice Phishing”)**
  + Attacker calls a victim masquerading to be from a trusted third party e.g., bank manager

## Drive-by-download

* Visit a website
  + Legitimate site that has been hacked
  + Evil site arrived at via a link
* Websites with popular content
  + Games: 60% of websites contain executable content, one-third contain at least one malicious executable
  + Celebrities, adult content, everything except news
* Code on site exploits vulnerability in web browser
* Drops malware onto your machine

# Anti-Malware Techniques

## Integrity Checkers



* Viruses make size of file grow
* Computer keeps a list of the lengths
* Periodically checks against the list
* Any unexpected change indicates a problem

## Signature Detection



* Database of malware signatures (sometimes called DAT files).
* Search for bit pattern.
* Requires regular updates.
* Limited to detection of known malware.

## Zero Day Exploits

* A zero-day exploit is an attack that exploits a previously unknown security vulnerability



* Especially vulnerable to Encrypted and Polymorphic Viruses
  + These both change their code as they spread.
  + This means our signature no longer will work.
  + For example, every file with “BAD” in it is a virus.
  + Virus mutates and changes this to “ADB”, it will no longer be detected.