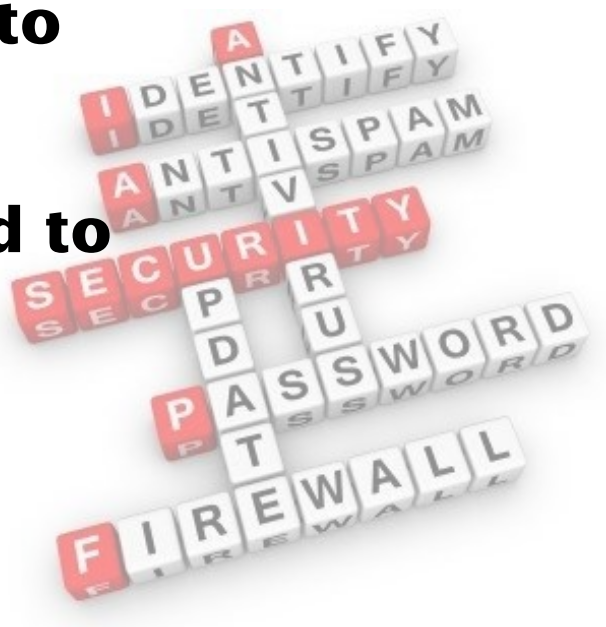
Internet Security

Internet security

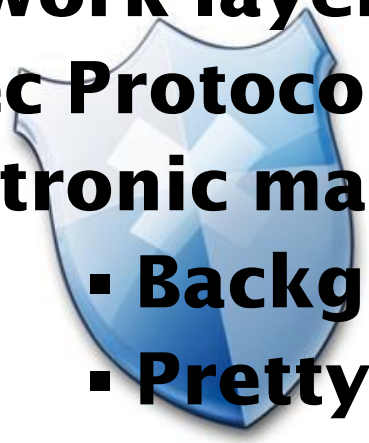
Is a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole.

Its objective is to establish rules and measures to use against attacks over the Internet.The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing.

Different methods have been used to protect the transfer of data, including encryption.



Types of security:



- Network layer security
- IPsec Protocol
- Electronic mail security (E-mail)
  - Background
  - Pretty Good Privacy (PGP)
  - Multipurpose Internet Mail Extensions (MIME)
  - Message Authentication Code

Firewalls

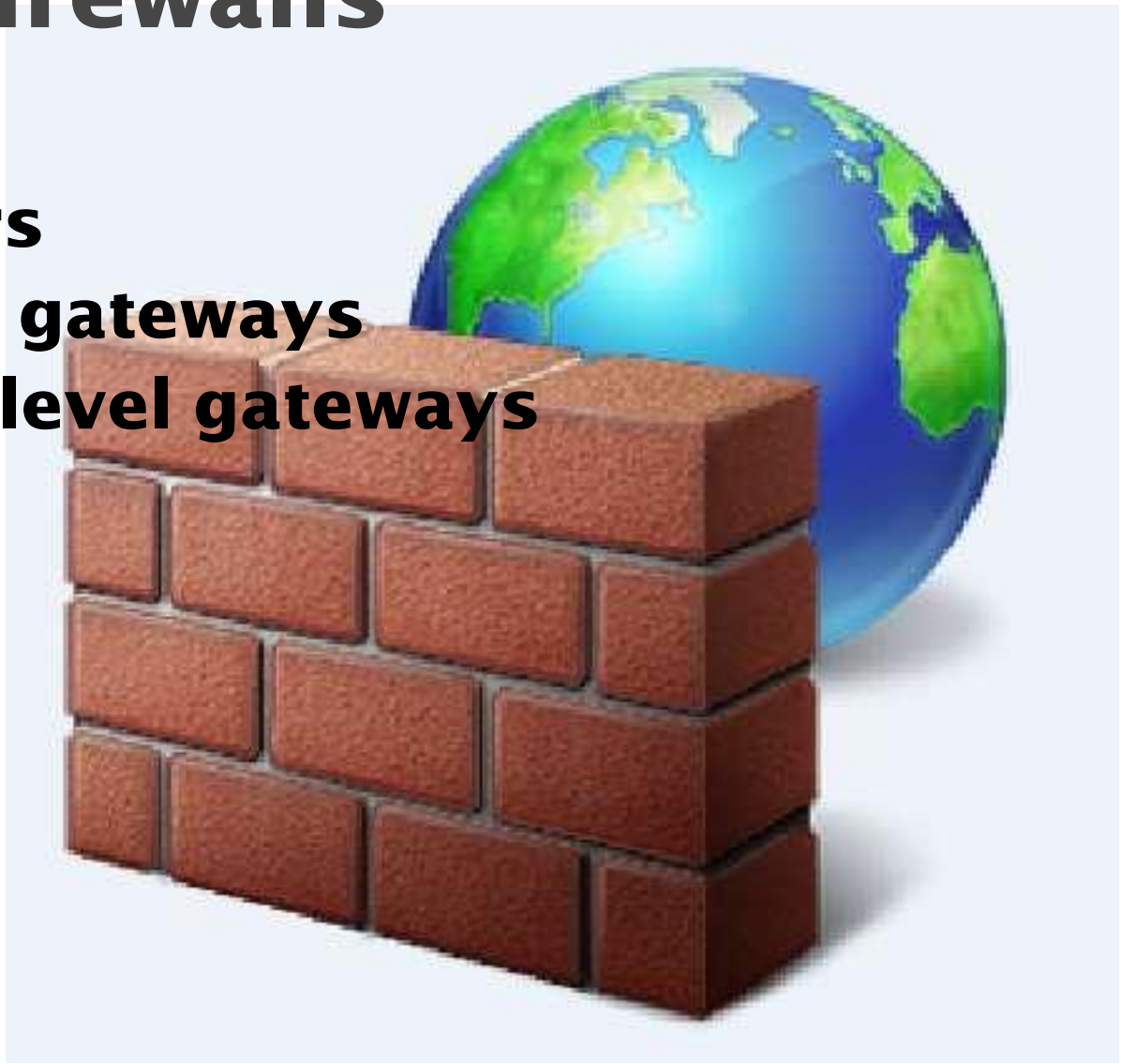
A firewall controls access between networks. It generally consists of gateways and filters which vary from one firewall to another. Firewalls also screen network traffic and are able to block traffic that is dangerous. Firewalls act as the intermediate server between SMTP and HTTP connections.

Role of firewalls in Internet security and web security

Firewalls impose restrictions on incoming and outgoing packets to and from private networks. They can also serve as the platform for IPsec. Using tunnel mode capability, firewall can be used to implement VPNs. Firewalls can also limit network exposure by hiding the internal network system and information from the public Internet.

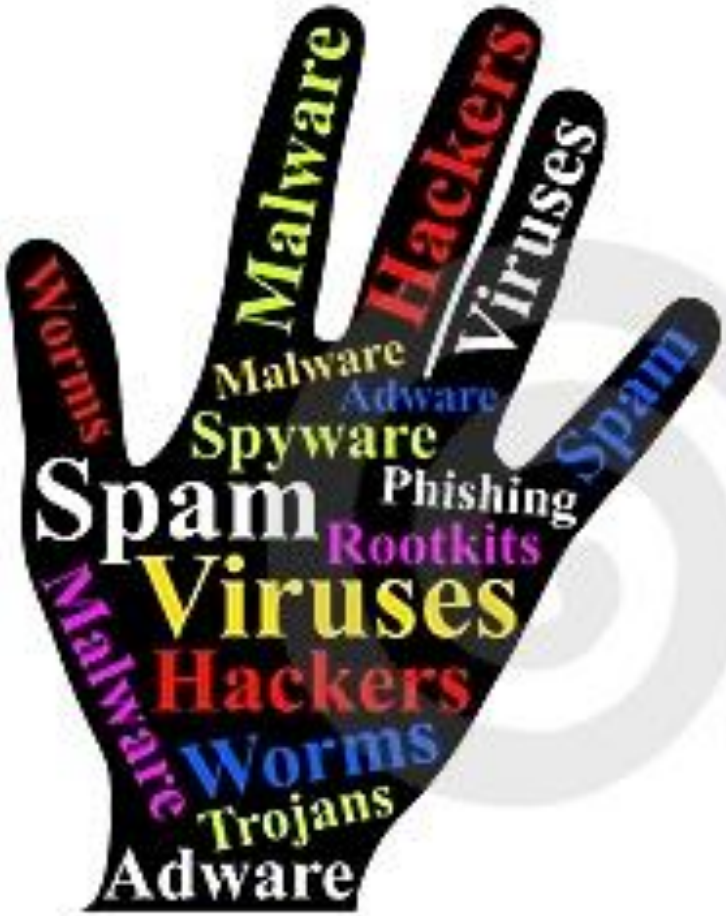
Types of firewalls

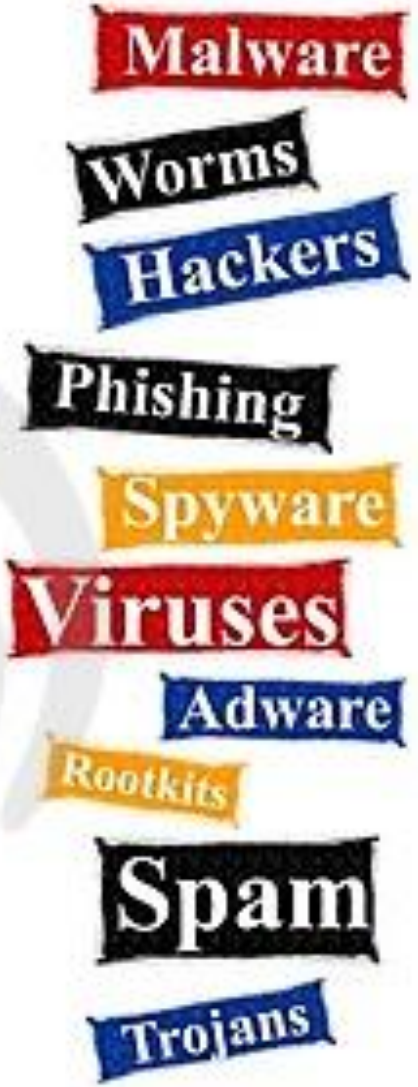
- **Packet filters**
- **Circuit-level gateways**
- **Application-level gateways**



Malicious software and antivirus

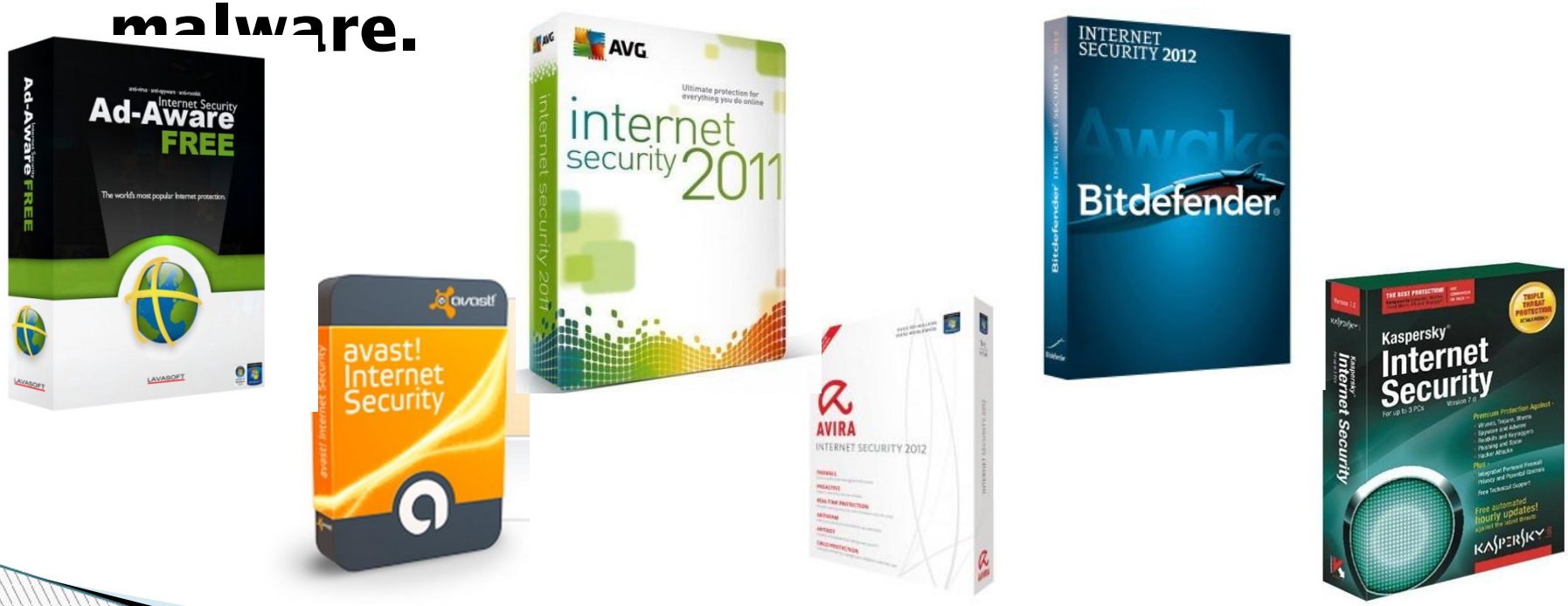
- Malware
- Viruses
- Trojan horse
- Spyware
- Worms
- Botnet





Antivirus

Antivirus programs and Internet security programs are useful in protecting a computer or programmable device from malware.

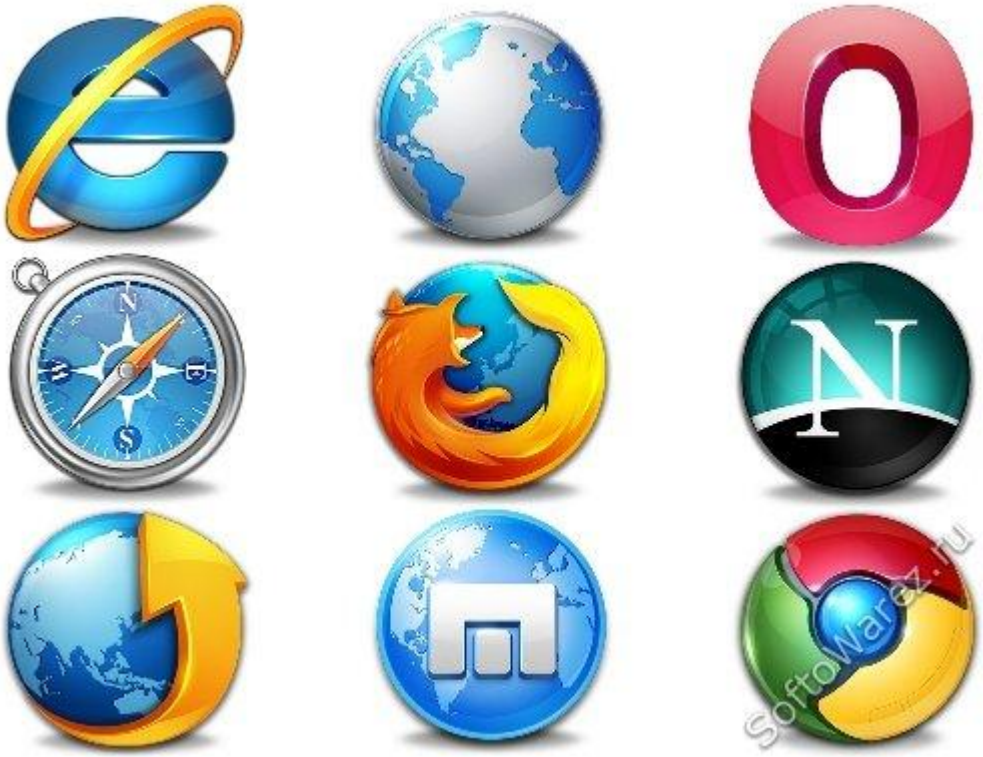


Denial of service attack

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

Browser choice

Web browser statistics tend to affect the amount a Web browser is exploited.



Buffer overflow attacks

A buffer overflow is an attack that could be used by a cracker to get full system access through various methods by essentially cracking a computer using brute force. Most security applications and suites are incapable of adequate defense against these kinds of attacks.

The End


Thank you for your attention
Verification Status:
SECURED & AUTHENTIC
SSL Provider:
VeriSign