Information
Technology
Institute

ITI

Introduction to
Computer Networks & Cyber Security

Prepared By : Mohamed AboSehly

Part 2 (Cyber Security Essentials)

Cyber Security Essentials

Part 2 (Cyber Security Essentials)

- **Session Outlines**
  - **Information Security Goals**
    - Confidentiality ,Integrity, Availability
  - **Risks & Threats**
    - Threats & Vulnerabilities
    - Attackers methodology & Methods
    - Malware Types
  - **Security Defenses**
    - Firewalls (Static & Dynamic firewalls)
    - IDS /IPS
    - VPN
    - Proxy
    - Next generation Firewalls
  - **Encryption**
    - Symmetric & Asymmetric Key Cryptography
    - Digital Signatures /Digital Certificates

Part2_ Attack Mitigation

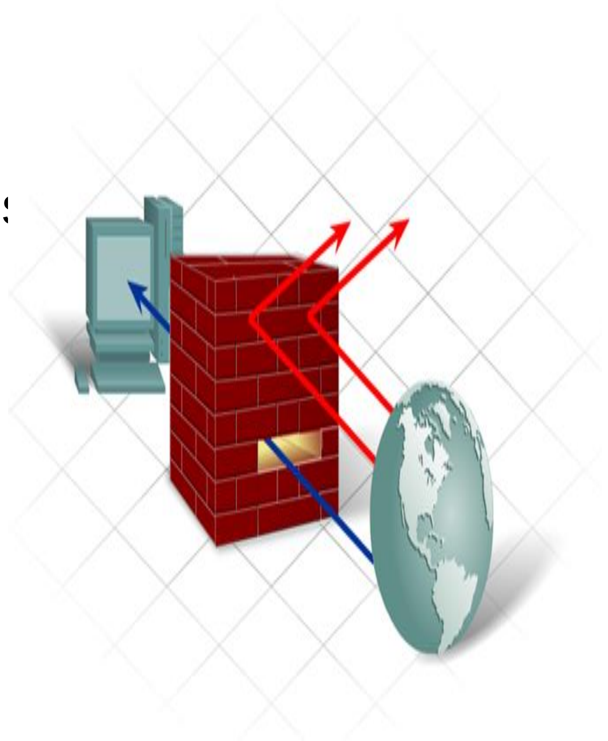
- **Hardware**
  - Firewalls
  - DMZ
  - IDS/IPS
  - NGFW
- **Software**
  - Anti-virus
  - Anti-spam
  - Anti-malware
  - Security Patches
  - User Access Control

Part 2 _ Firewall

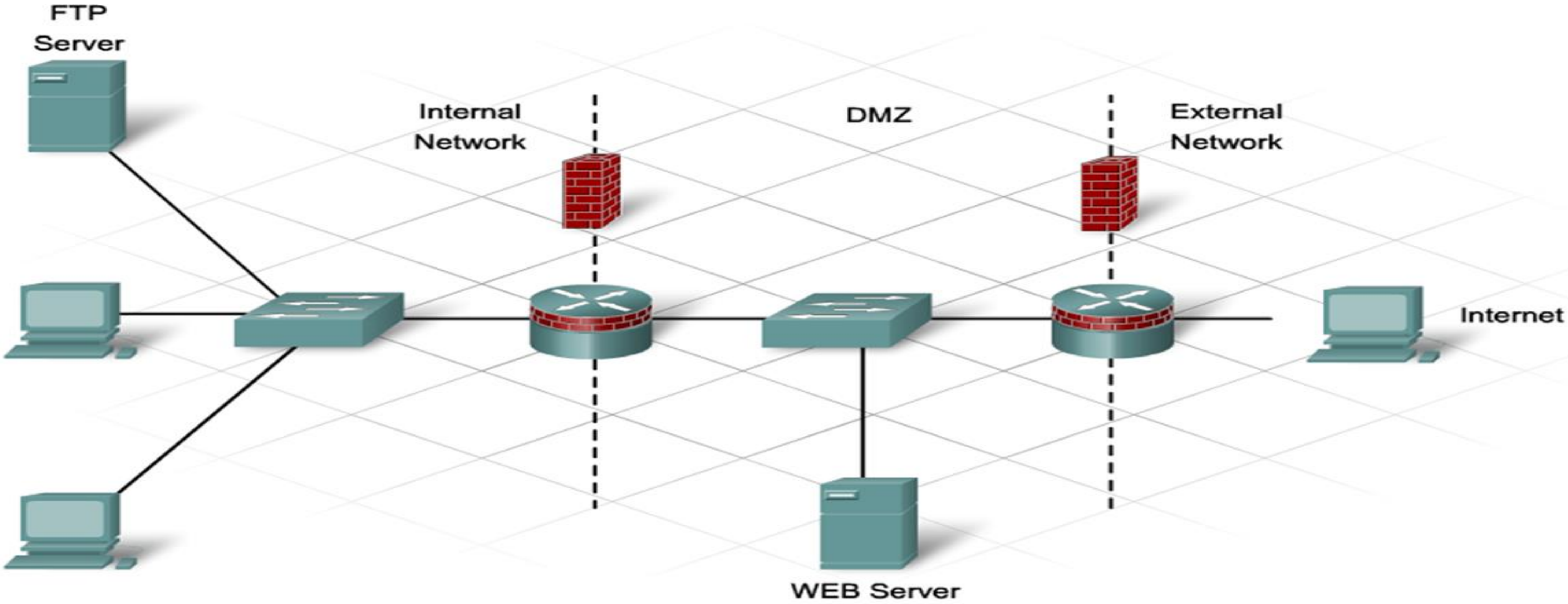
- A Firewall is one of the most effective security tools available for protecting internal network users from external threats As the first line of defense
- A firewall resides between two or more networks and controls the traffic between them as well as helps prevent unauthorized acces
- A firewall can be software-based or hardware-based

- **Static Packet Filtering (stateless firewall)**
  - - Prevents or allows access based on IP or MAC addresses.

- **Dynamic Packet Filtering (state full firewall)**
  - Incoming packets must be legitimate responses to requests from internal hosts. filter out specific types of attacks such as DoS

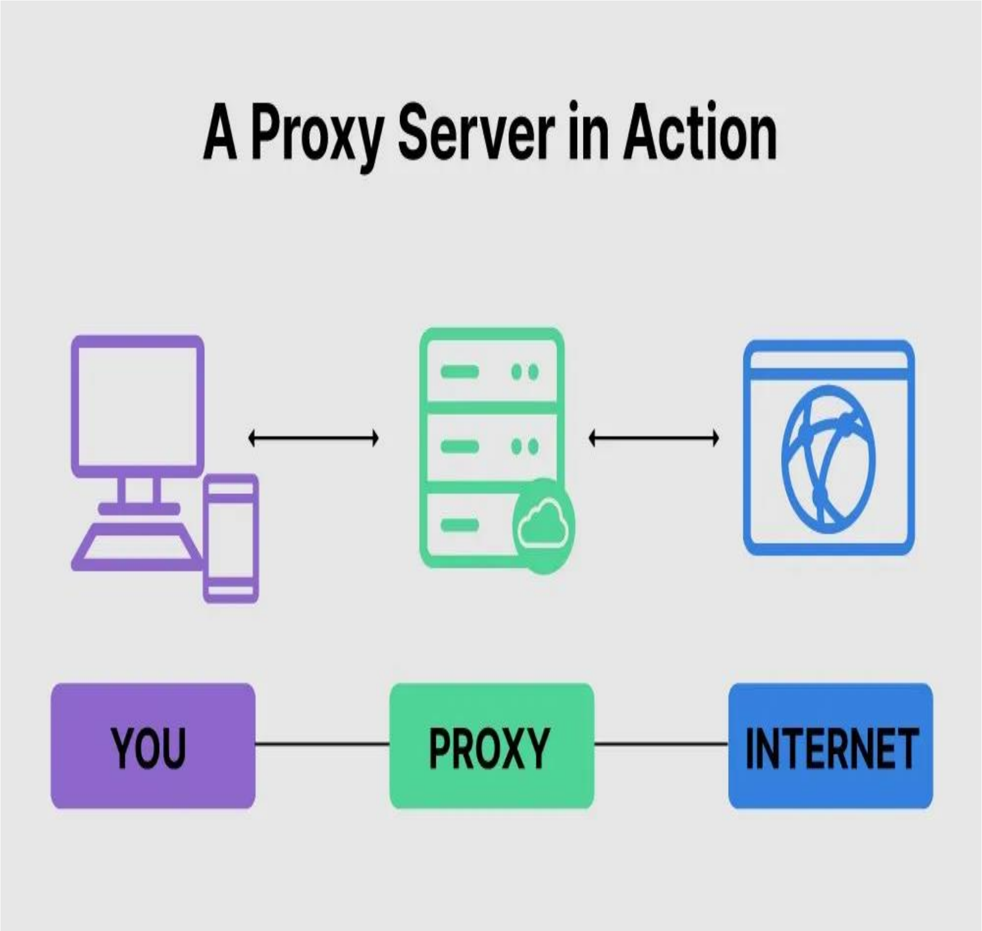


Part 2 _Firewall



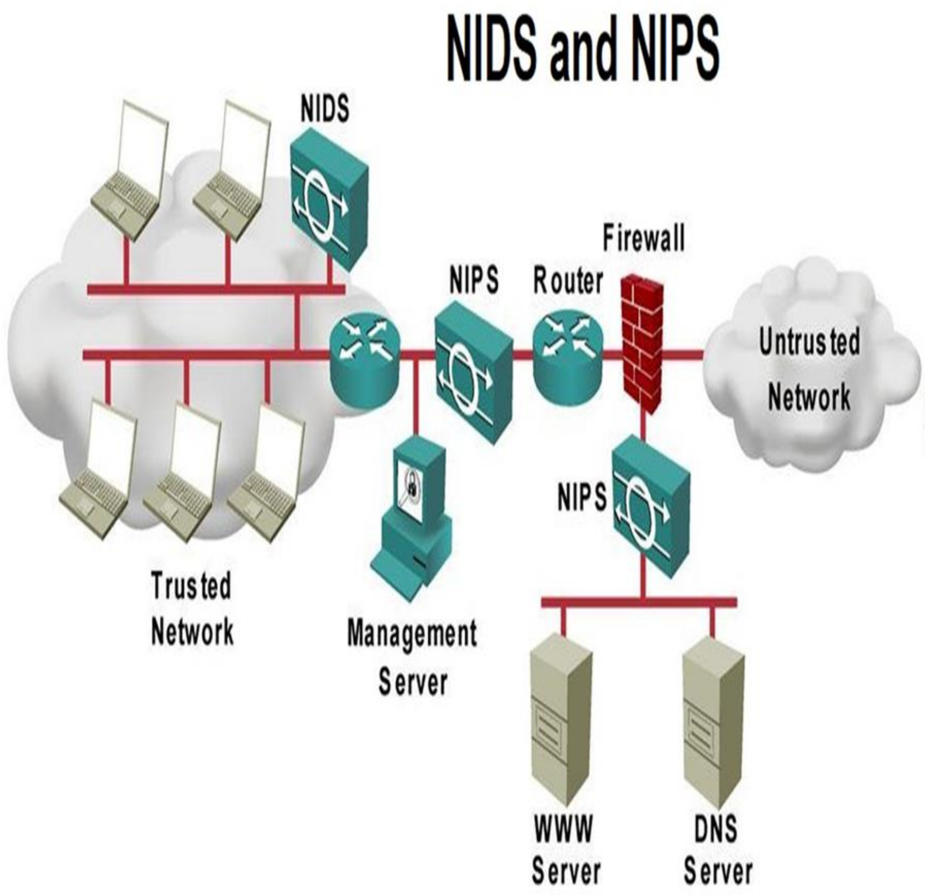
Part 2 _ Proxy Server

- A **computer system** (or an application program) that intercepts internal user requests and then processes that request on behalf of the user
- Goal is to **hide the IP address** of client systems inside the secure network



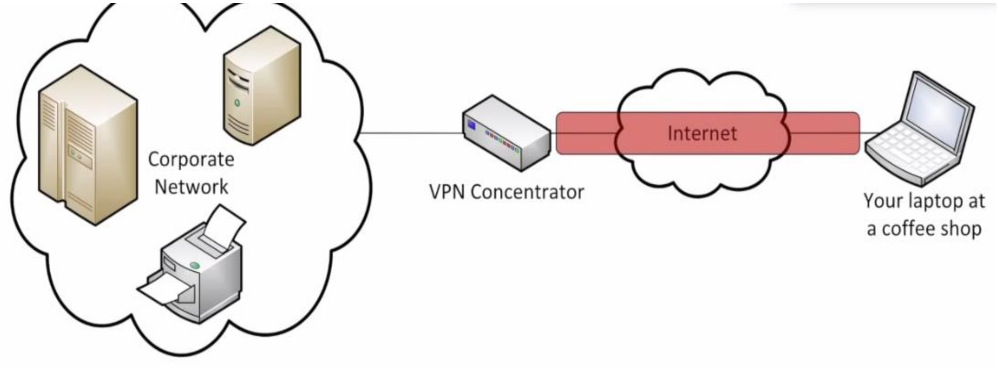
Part 2_ IDS/IPS

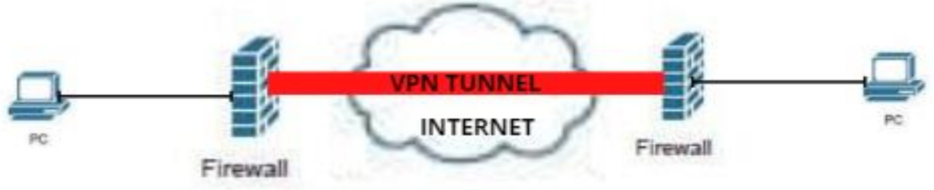
- Network Intrusion Detection System (NIDS):
  - **Watch** the Network Traffic and if there **is Intrusion it Detects** that there is Bad traffic Flow.
  - it **send alarms and logs**
- Network Intrusion prevention System (NIPS):
  - **Stops** the traffic if it **detects that there is intrusion**
- Types of IDS&IPS
  - **Signature-based:** look for the perfect match
  - **Anomaly-based:** Built a based line of what is normal
  - **Behavior-based: observe and report**



VPN

- It Tunnel the traffic between the Two Sides of Network
- Types:
  - Remote Access VPN
  - Site to Site VPN

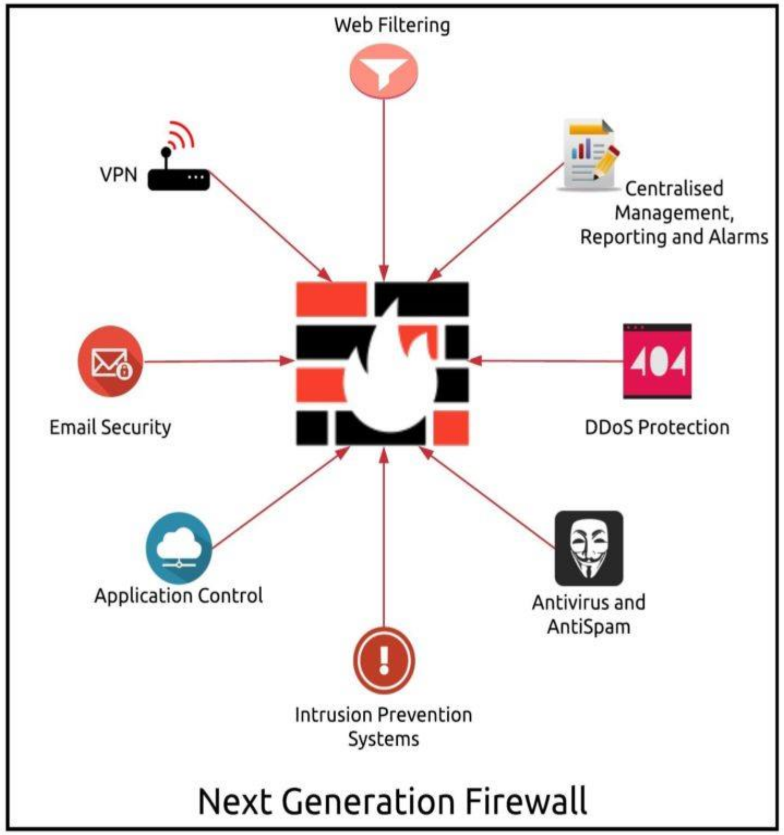




SIte-to-Site VPN

Part 2 _ Next generation Firewall (NGFW)

- **Next generation Firewall (NGFW)**
  - a "deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall."



Part 2 _Wireless Security

- Open Access
  - SSID
  - No encryption
  - Basic authentication
  - Not a security handle
- WEP
  - No strong authentication
  - Static, breakable keys
  - Not scalable
- WPA
  - Improved encryption
  - Strong, user-based authentication
- WPA2
  - AES Encryption
  - Authentication

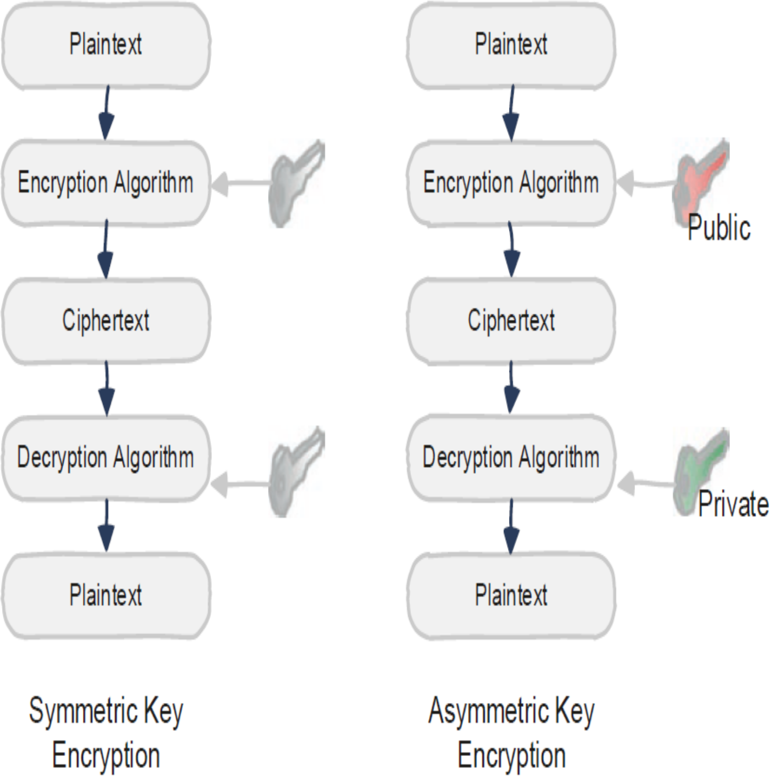
Part 2_Controlling Wireless LAN Access

- SSID broadcasts from access points are off
- MAC Address filtering is enabled
- WPA2 / WPA3 Security implemented

Part 2_ Encryption

Encryption

- encryption is the process of **encoding information.** This process converts the original representation of the information, known as **plaintext**, into an alternative form known as **ciphertext.**
- Unencrypted data, called plaintext, is sent through an encryption algorithm to generate a ciphertext. **A key** is used for encryption.
- in **a symmetric encryption** algorithm, the **same key** is also **used for decryption**. (Not secure) needs to be a secure way for the two sides to have the same key



Part 2 (Digital Signatures & Certificates)

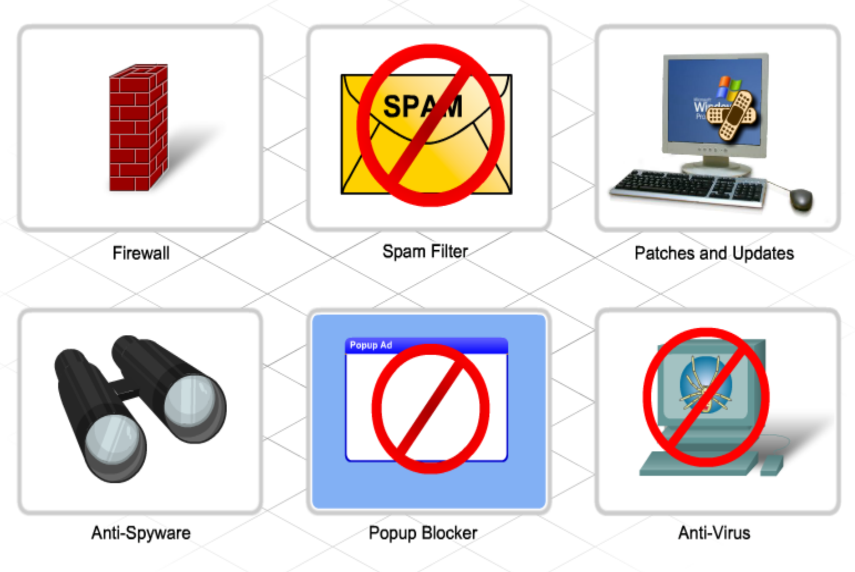
- **Digital Signatures**
  - A digital signature is done by hashing a document and then encrypting the hash with a private key.
  - Any entity (like a bank) that has the public key can verify that the document is signed by the owner of the private key.
  - digital signatures do not provide confidentiality but only provide nonrepudiation and integrity.
- **Digital Certificates** (public-key certificate)
  - electronic file that contains identification information about the holder, including the person's public key (used for encrypting and decrypting messages), along with the authority's digital signature,
  - the recipient can verify with the authority that the certificate is authentic.
  - Digital certificates are issued by certification authorities.
  - Websites usually also have digital certificates, to enable a person intending to buy its products to confirm that it is an authenticated site. Such certificates serve as the security basis for HTTPS

Part2 lab Practices

- How to use your local firewall to block a port and stop DOS attack from a zombie device

Best Practices

- ✓ Define security policies
- ✓ Physically secure servers and network equipment
- ✓ Set login and file access permissions
- ✓ Update OS and applications
- ✓ Change permissive default settings
- ✓ Run anti-virus and anti-spyware
- ✓ Update antivirus software files
- ✓ Activate browser tools –
- ✓ Popup stoppers, anti-phishing, plug-in monitors
- ✓ Use a firewall



Thank You