به نام خدا

عنوان همایش :

# امنیت شبکه های کامپیوتری

## ( با هدف تامین امنیت سازمانی )

کد عضویت در سایت www.edmodo.com : uhqwxt

ارائه دهنده : سید حسام الدین حسینی

# سرفصل مطالب

- آشنایی با مفاهیم امنیت
  - مثلث امنیت CIA
  - دفاع در عمق (Defense In Depth)
  - Vulnerability , Treat , Risk
  - نحوه مدیریت و روشهای کاهش ریسک
- آشنایی با انواع تهدیدات اینترنتی
  - (ویروس – کرم – فیشینگ – بات نت – مهندسی اجتماعی و ...)
- آشنایی با انواع تجهیزات مقابله با تهدیدات اینترنتی
  - (فایروال – کوزه عسل – UTM)
- آشنایی با انواع روشهای تامین امنیت شبکه سازمانها
  - تامین امنیت فیزیکی
  - تامین امنیت زیرساخت و ارتباطات
  - تامین امنیت سرویس ها و پروتکل ها
- اشتباهات متداول انسانی در نقض امنیت شبکه سازمانها

# منابع مطالعاتی مفید در زمینه امنیت شبکه :

- **ISMS , ISO 27001 , ISO 27002**
- **Pearson.CompTIA.SecurityPlus.SY0-301.Authorized .Exam.Cram.3rd. Edition .Dec.2011**
- **Microsoft , MCITP 2008 Enterprise Administrator**
- **Cisco , Top-Down Network Design , Network Security Checklist**
- **امنیت داده ها – مولف : دکتر علی ذاکرالحسینی / مهندس احسان ملکیان**

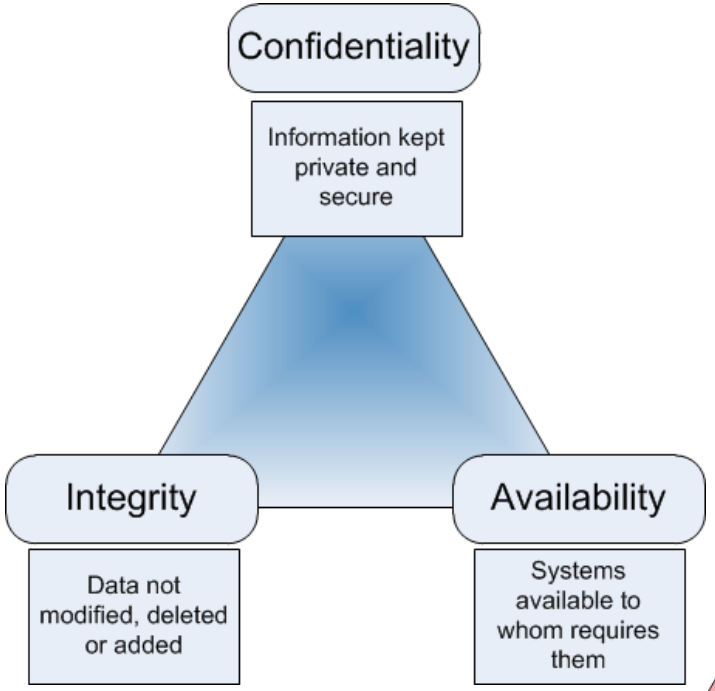
# رزومه مدرس :

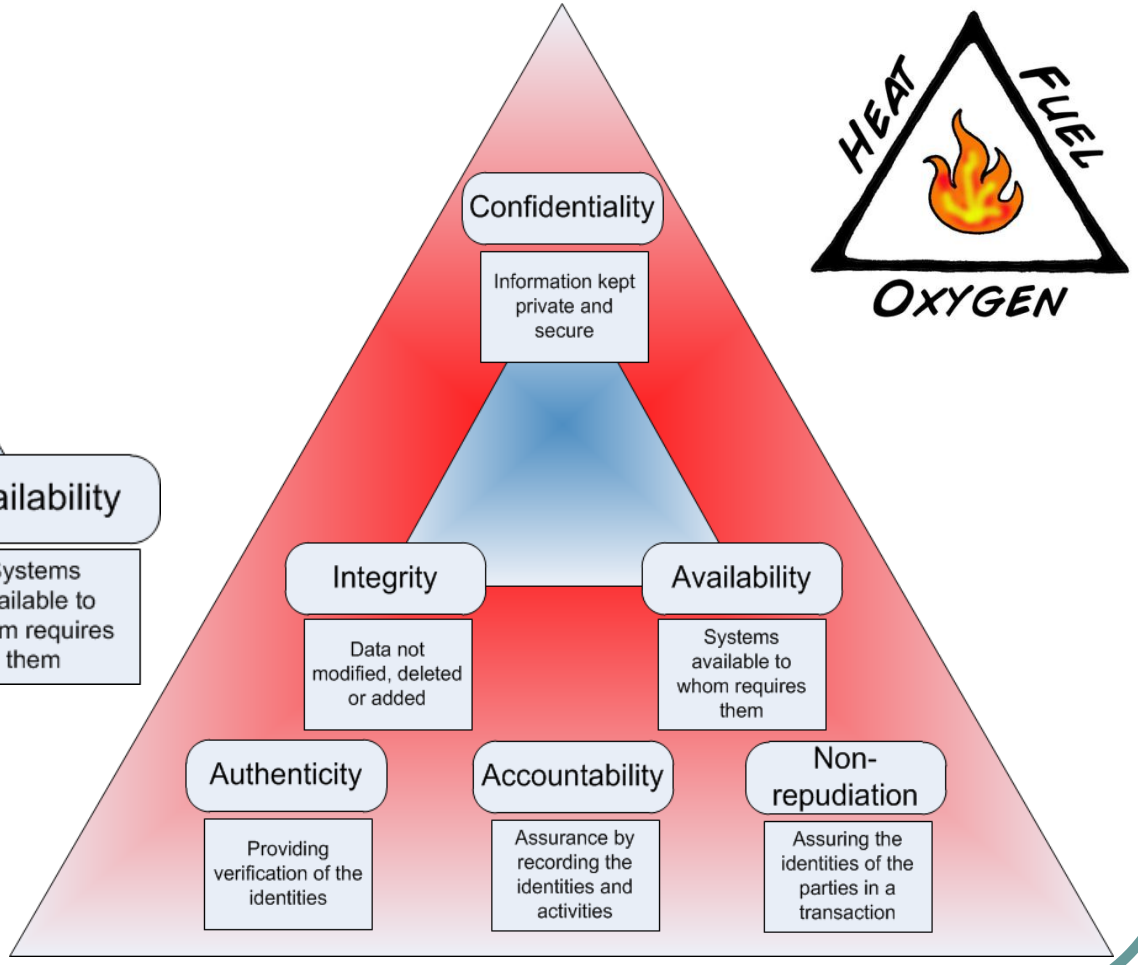
- **نام مدرس : سید حسام الدین حسینی**
  - کارشناس ارشد شبکه های کامپیوتری (دانشگاه علم و صنعت تهران )

- **رزومه :**
  - دارنده ۱۵ مدرک بین المللی در زمینه طراحی، اجرا و مشاوره شبکه های کامپیوتری
  - دارنده پروانه صلاحیت مشاوره و اجرا شبکه های کامپیوتری از نظام صنفی خراسان رضوی
  - مجری و مشاور بیش از ۱۵ سازمان دولتی در سطح استان خراسان رضوی ، شمالی و جنوبی
  - مدرس مورد تائید سازمان مخابرات ایران
  - مدرس مورد تائید سازمان فنی حرفه ای کشور

- **اطلاعات تماس :**
  - موبایل : **09155035489**
  - ایمیل : Hoseinih2@mums.ac.ir و hessam1393@gmail.com

# مثلث امنیت (CIA)



# تعاريف :

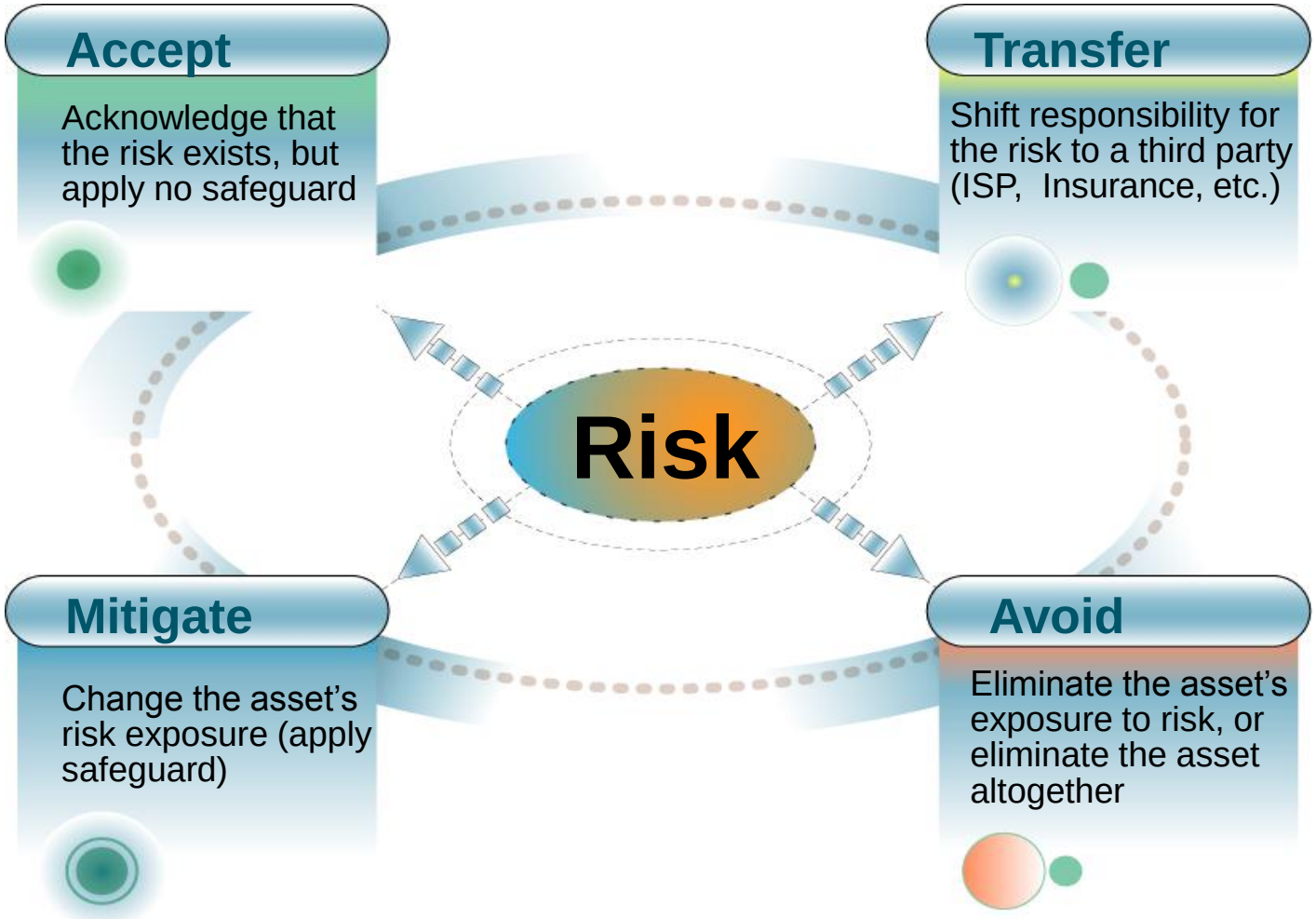
- **Asset :** People, property, and information that we're trying to protect
- **Vulnerability** : Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.
- **Threat** : Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.
- **Risk** : The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

Asset + Threat + Vulnerability = Risk

# مثال :

| Asset | Risk | Vulnerability | Treat |
|---|---|---|---|
| Notebook | خطر به سرقت رفتن | نگهداری اطلاعات حیاتی سازمان | استفاده از وسایل نقلیه عمومی |
| USB Flash | خطر جا گذاشتن – خطر سوختن فلش | نگهداری اطلاعات شخصی حیاتی (بدون پشتیبان) | اتصال فلش به سیستم های عمومی |
| User | خطر دسترسی به منابع شبکه با نام کاربری دیگران | عدم حذف نام کاربری و رمز عبور کارمندان بازنشسته | در اختیار قرار دادن نام کاربری به دیگران |
| Server | خطر دسترسی از راه دور | باز بودن پورت ۲۳ برای همه کاربران از همه جا | قرار دادن سرور در اینترنت |
| Windows OS | خطر آلوده شدن سیستم به ویروس و کرم | بروز نبودن سیستم عامل / بروز نبودن آنتی ویروس | دانلود فایل از سایتهای غیرمطمئن |

# مدیریت ریسک / کاهش ریسک :



# انواع تهدیدات امنیتی :

- **تهدیدات طبیعی :**
  - زلزله ، سیل ، رعد و برق ، آتش سوزی و .... / خارج از قدرت بشر / ارائه تمهیدات برای بازگرداندن شرایط به حالت عادی
- **تهدیدات غیر عمد:**
  - اشتباهات سهوی و ناخودآگاه عوامل انسانی ( طراحی اشتباه شبکه / عدم افزونگی در شبکه/ عدم تهیه بک آپ/ اعمال پالیسی نادرست)
- **تهدیدات عمدی :**
  - هرگونه اقدام برنامه ریزی شده جهت افشا ، نابودی یا تغییر در داده های حیاتی شبکه یا ایجاد اختلال در خدمات سرور

**حمله Attack : هر گاه یک رفتار یا یک تهدید عمدی باعث شود به دلیل وجود آسیب پذیری موجود ، ریسک شبکه از حالت بالقوه به بالفعل درآید یک حمله رخ داده است.**

**( خواه باعث خسارت شود خواه تلاش نافرجام باشد)**

# انواع حملات / تهدیدات عمدی ۴ گانه :

- **استراق سمع (Interception) :**
  - **شنود نسخه ای از داده های در حال انتقال توسط فرد غیر مجاز : نقض محرمانگی**
- **دستکاری (Modification) :**
  - **دستکاری داده های در حال انتقال توسط فرد غیرمجاز : نقض صحت اطلاعات**
- **جعل (Fabrication) : .**
  - **تولید پیامهای ساختگی توسط فرد غیرمجاز و ارسال به افراد مجاز : نقض احراز هویت**
- **وقفه (Interruption) :**
  - **وقفه انداختن در ارائه یک سرویس یا سرور : نقض Availability**

# شیوه های حمله به شبکه های کامپیوتری

- **Malware / Malicious Code Attack**
  - Virus , Worm , Trojan , Spyware , Backdoor , Logic Bomb , Botnets
- **Common Attack**
  - DoS , DDoS , Replay , Spoof , Spam , SPIM , DNS Poisoning , Vishing
- **Social Engineering Attack**
  - Phishing , Hoaxes ,
- **Wireless Attack**
  - Rogue access points, Blue jacking , Blue snarfing , War chalking
- **Application Attack**
  - Cross-site scripting , SQL injection , Buffer overflow , Zero day

# Malware Attack :

Trojan Horse

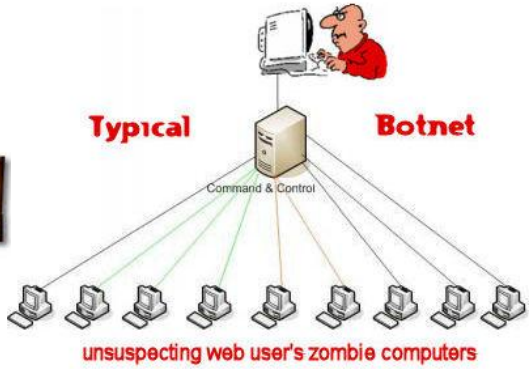
Virus


Worm

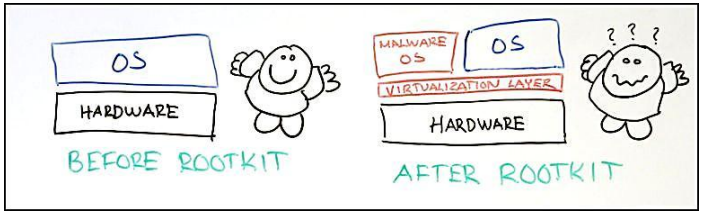
Spyware

Backdoor


**Adware**



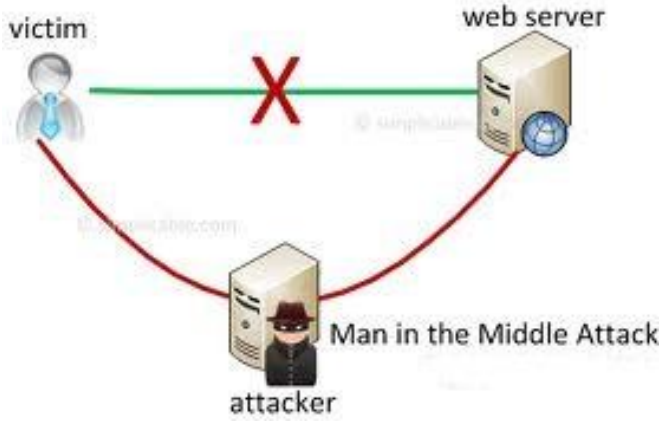

Botnets

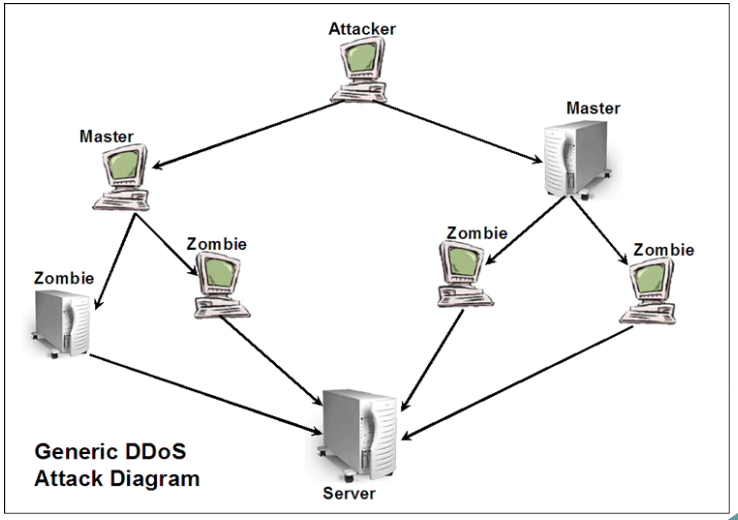



Rootkit

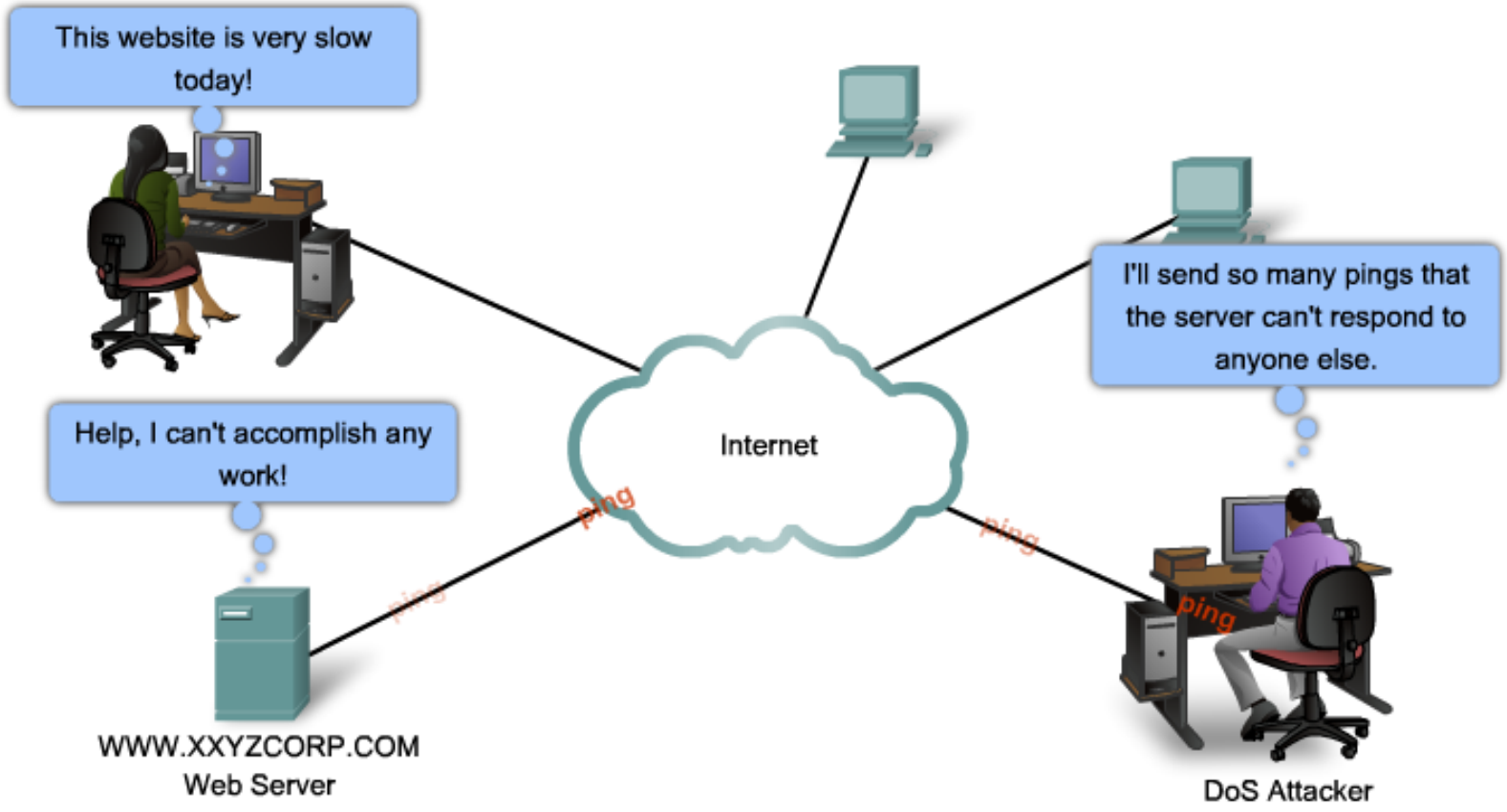
# Common Attacks :

- Man In the Middle
- DoS / DDoS
  - Smurf Attack
  - SYN Flood
  - Xmas attack
- Replay
- IP Spoofing
- Spam
- SPIM
- Privilege escalation
- Malicious insider threat
- DNS poisoning
- ARP poisoning
- Transitive access
- Client-side attacks

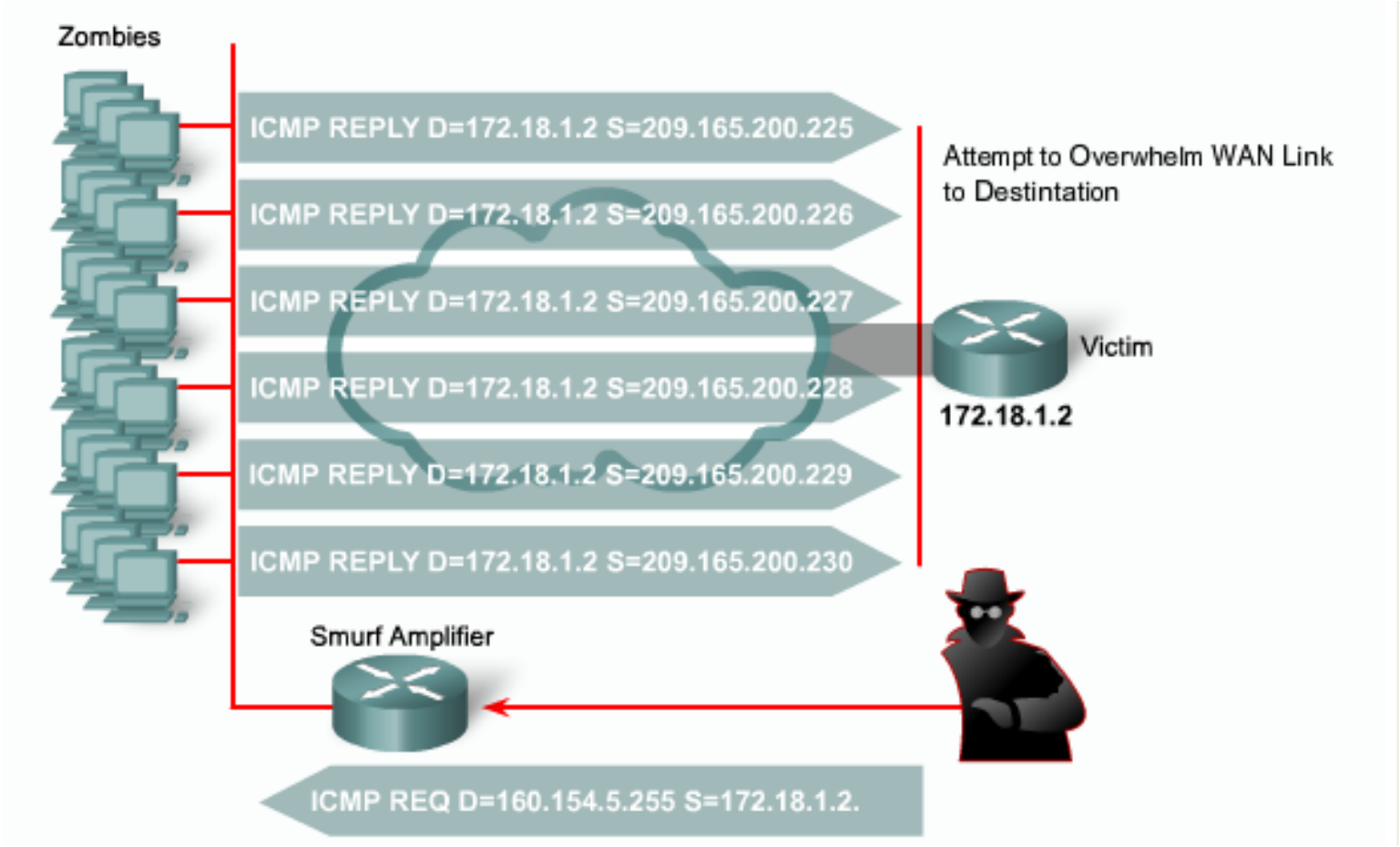


# مثال : کندی سایت سازمان به دلیل حمله DoS



# مثال : حمله Smurf برای ایجاد سربارترافیک وایرلس

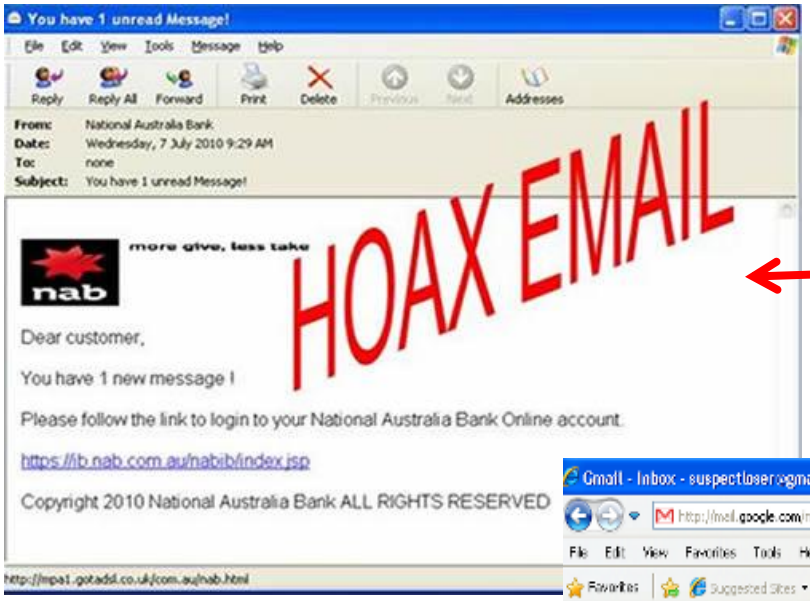


# Social Engineering Attacks

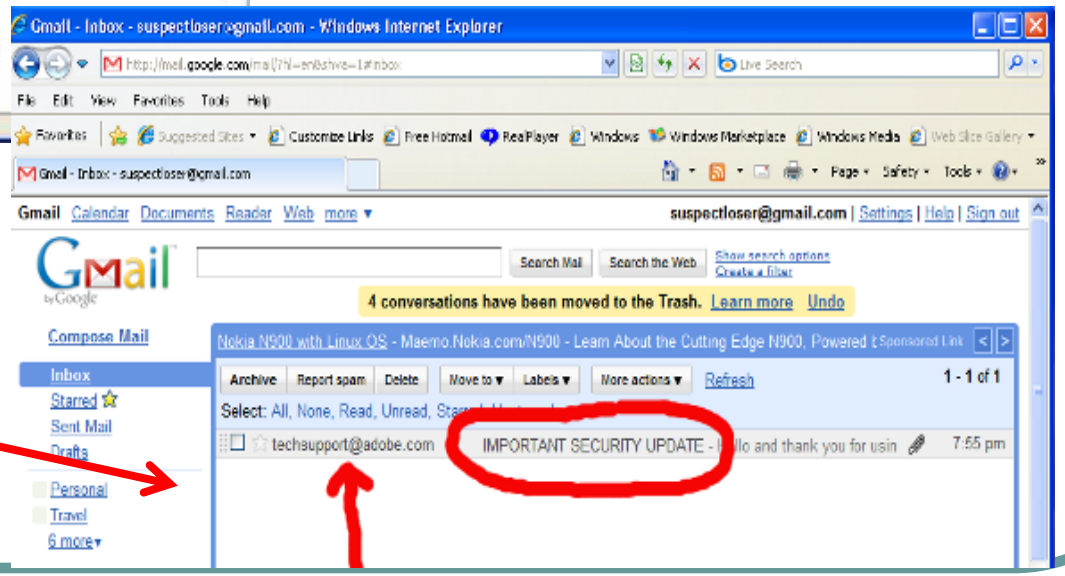
- Shoulder surfing
- Dumpster diving
- Tailgating
- Impersonation
- Hoaxes
- Whaling
- Vishing
- Phishing
- Spear phishing
- Pharming



# مثال : ایمیل جعلی و فریبنده (Hoax Email)




لاگین به حساب بانکی از طریق یک
لینک ارسال شده در ایمیل جعلی




ضمیمه فایل آپدیت امنیتی مهم
از طریق ارسال ایمیل جعلی

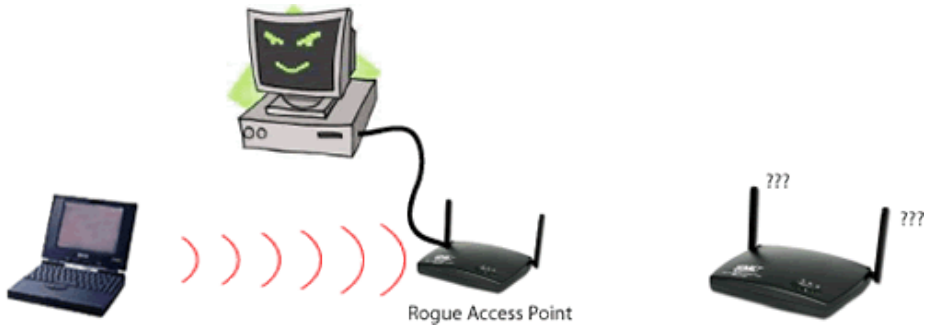
# مثال : حمله مهندسی اجتماعی برای ورود به اتاق سرور

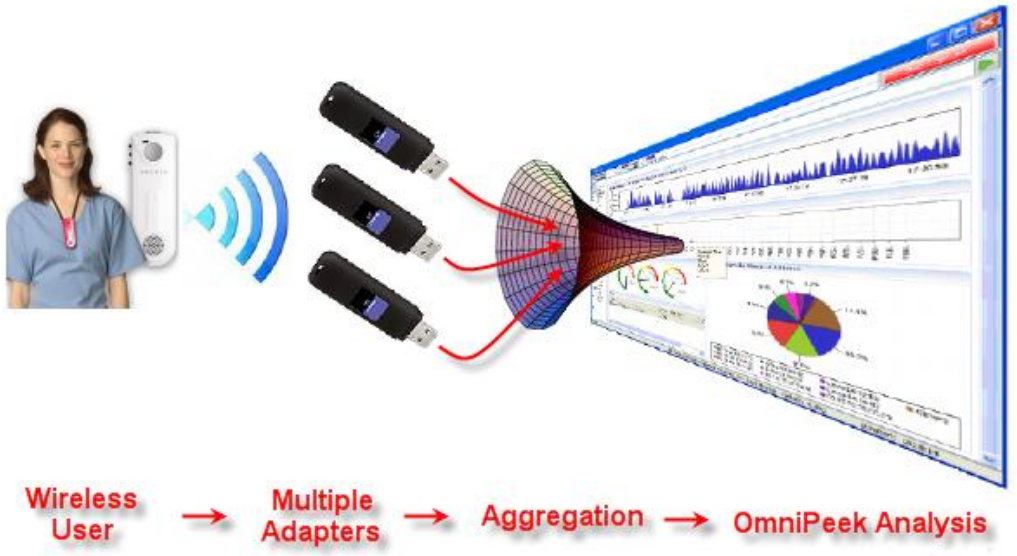

درخواست ورود به اتاق سرور از طریق هویت فرد دیگر

نکات مهم امنیت دسترسی فیزیکی

# Wireless Attacks :

- Rogue access points
- Interference
- Evil twin
- War driving
- Blue jacking
- Blue snarfing
- War chalking
- IV attack
- Packet sniffing



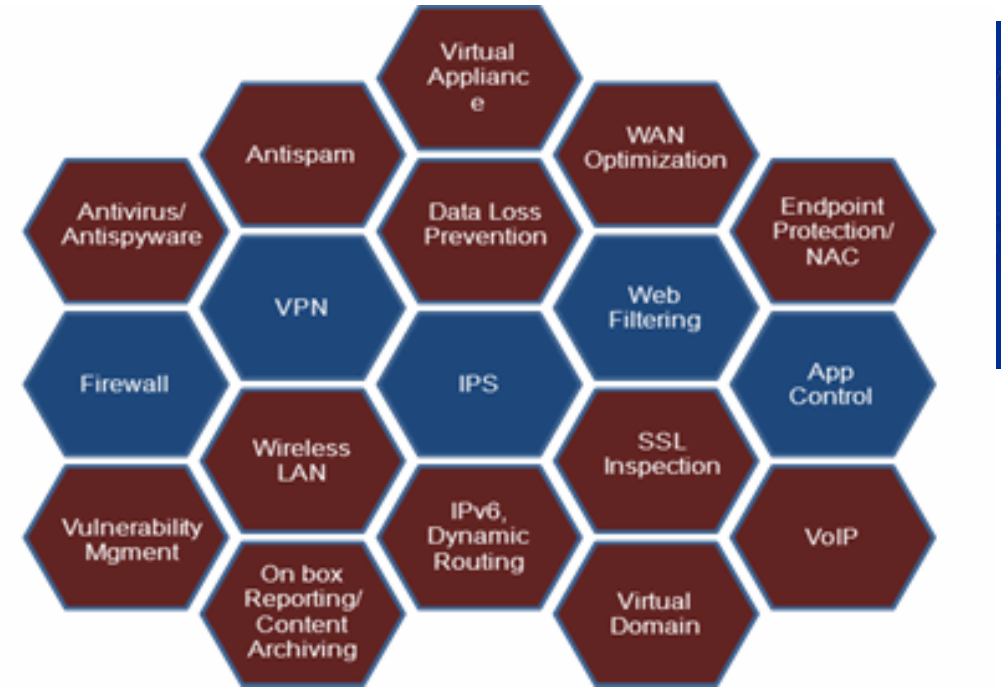



# Application Attacks :

- Cross-site scripting
- SQL injection
- LDAP injection
- XML injection
- command injection
- Buffer overflow
- Zero day
- Cookies and attachments
- Malicious add-ons
- Session hijacking
- Header manipulation



# انواع تجهیزات مقابله با تهدیدات امنیتی :




UTM
(Unified Treat Management )

Firewall

Honeypot

# مثال ) روشهای معمول مقابله با تهدیدات امنیتی :

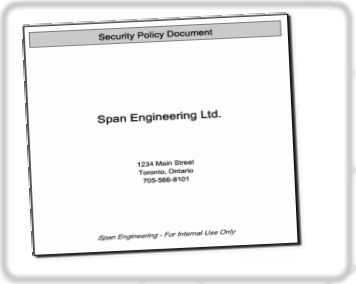
Patches and Updates

Control physical access

Password protection

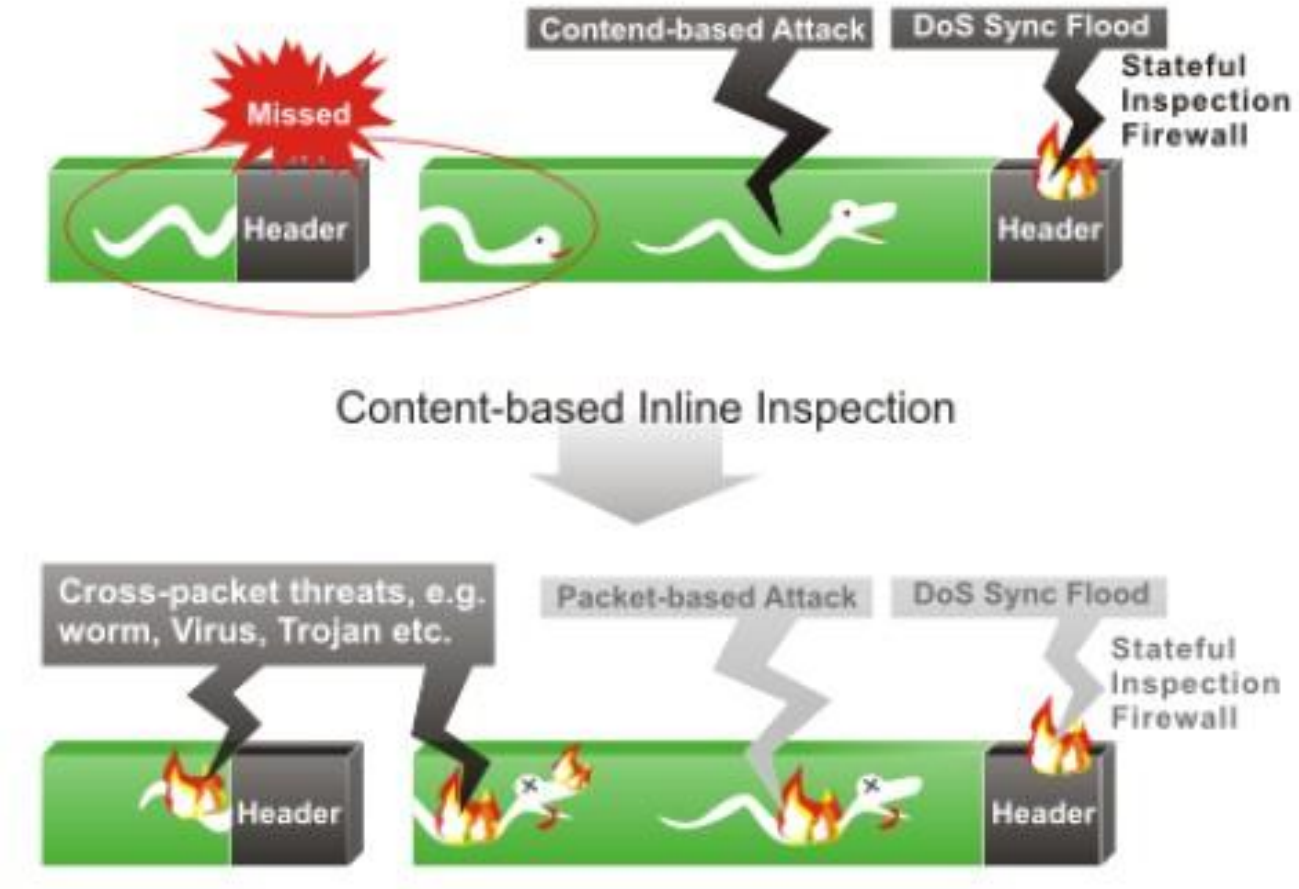
Anti-Virus

Firewall

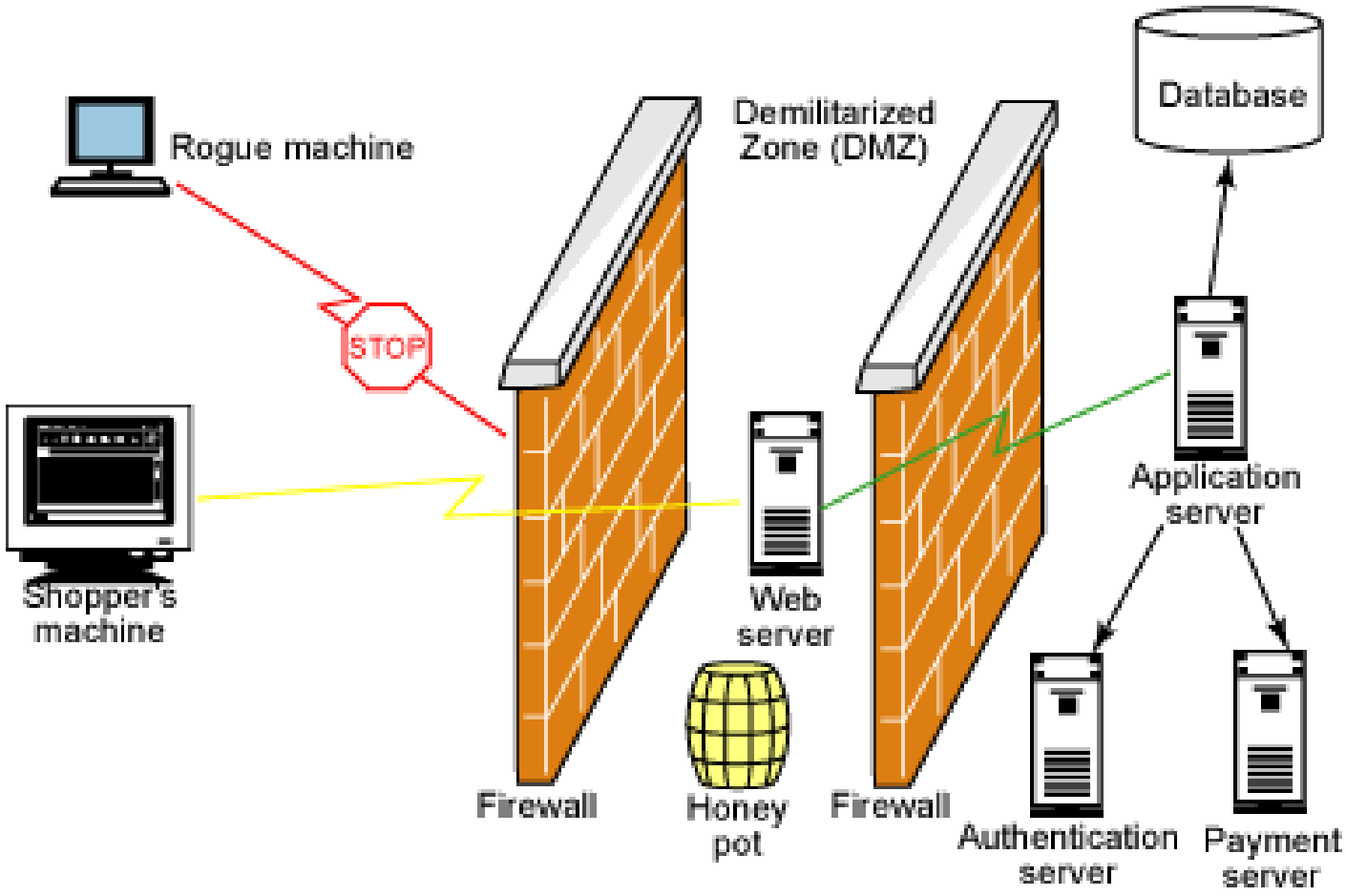



Develop a Security Policy

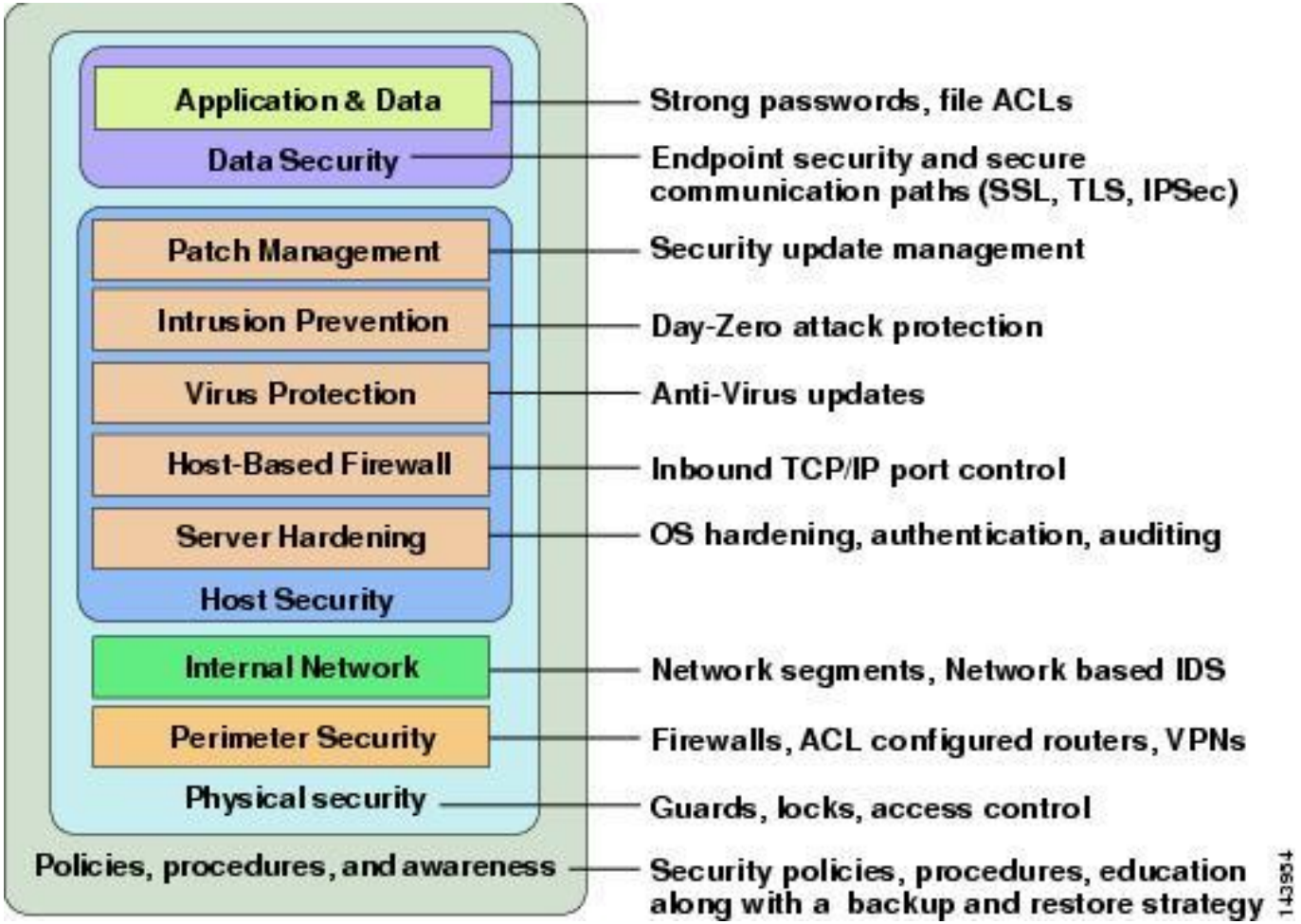
# مثال : فایروال های با قابلیت تشخیص Content Based



# مثال : طراحی و پیاده سازی یک  شبکه امن



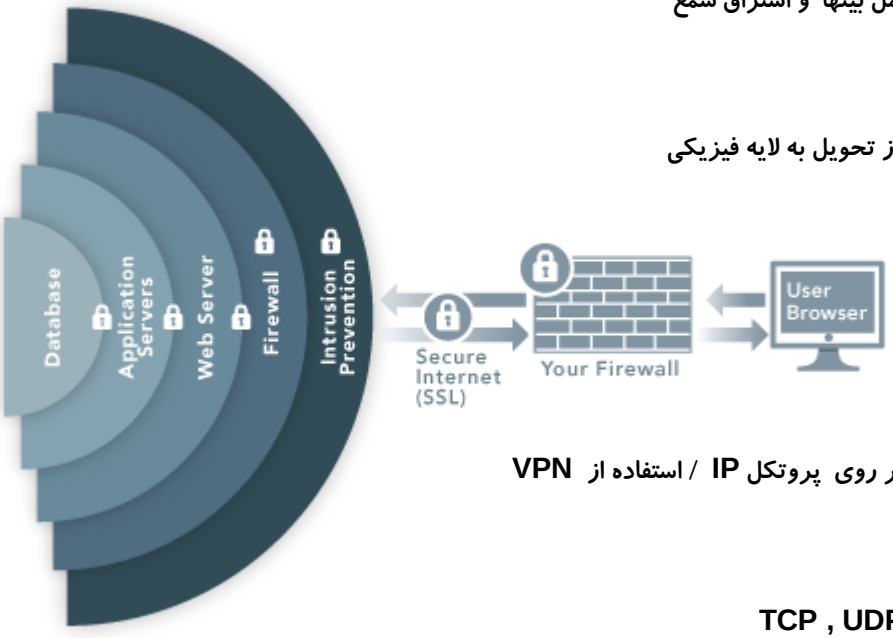
# دفاع در عمق / امن سازی شبکه در ۷ لایه OSI



# تامین امنیت در ۷ لایه OSI

- **امنیت در لایه فیزیکی :**
  - حراست فیزیکی از کانال / تغییر مداوم فرکانس سیگنال حامل
  - تامین روشهایی برای جلوگیری از گرفتن انشعاب از سیم حامل بیتها و استراق سمع

- **امنیت در لایه پیوند داده :**
  - رمزنگاری هر فریم به کمک روشهای رمزنگاری متقارن قبل از تحویل به لایه فیزیکی

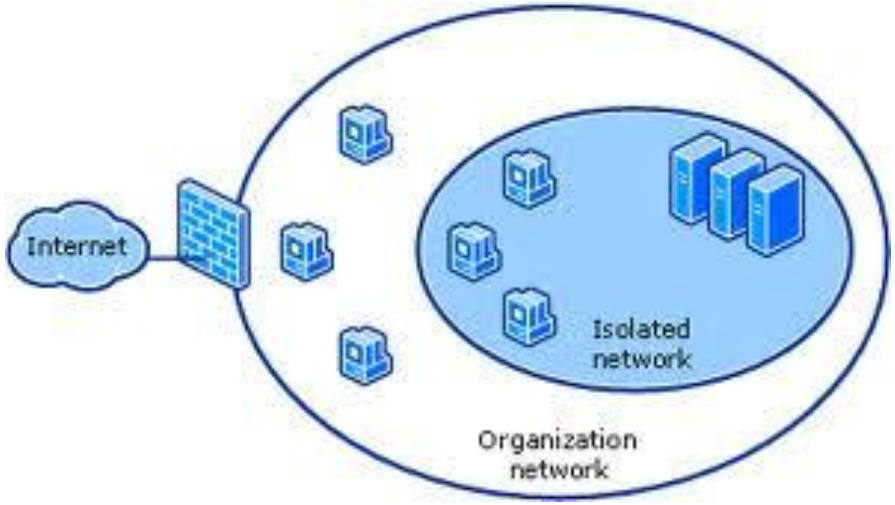



- **امنیت در لایه شبکه :**
  - استفاده از IDS و فایروال / استفاده از پروتکل IPSec بر روی پروتکل IP / استفاده از VPN

- **امنیت در لایه انتقال :**
  - استفاده از پروتکل های SSL و TLS در کنار پروتکل TCP , UDP

- **امنیت در لایه کاربردی / نمایش / جلسه :**
  - استفاده از پروتکل PGP / استفاده از استاندارد SET / استفاده از Smart Card

# تامین امنیت شبکه سازمانها



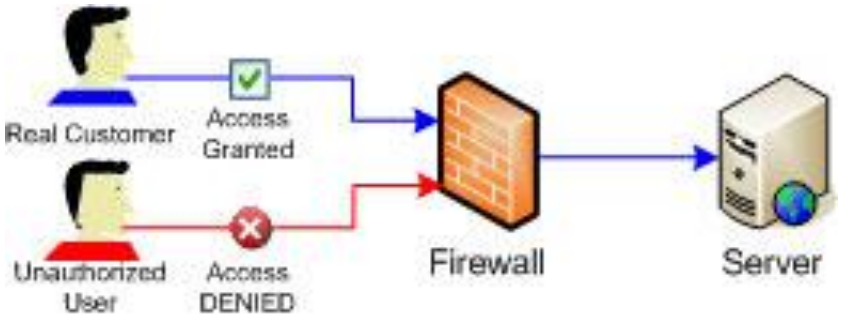

- امنیت فیزیکی شبکه
- امنیت زیرساخت شبکه
- امنیت پروتکل های ارتباطی شبکه
- امنیت سیستم عامل و نرم افزارها
- امنیت کاربران نهایی
- مانیتورینگ / ممیزی/ مدیریت متمرکز
- پشتیبان گیری
- مستند سازی / تهیه خط مشی ها و دستورالعملهای امنیتی
- آموزش کاربران / آموزش مدیران شبکه
-

# تامین امنیت شبکه سازمانها

- **امنیت فیزیکی شبکه :**
  - **تامین امنیت ارتباط فیزیکی بستر ارتباطی (فیبرنوری ، کابل ، امواج رادیویی )**
  - **مکانیزم ثبت ورود و خروج / استفاده از دوربین مدار بسته /**
  - **عدم دسترسی افراد بیگانه به اتاق سرور و یا به سیستم های شخصی**
  - **عدم دسترسی افراد بیگانه به تجهیزات سوییچینگ، روتینگ و فایروال شبکه**
  - **بستن پورتهای غیر ضروری بر روی سرور و یا کلاینتها**
  - **عدم اتصال فلش و یا تجهیزات ناشناخته به سرور و یا سیستم شخصی**
  - **لحاظ نمودن چک لیست الزامات اتاق سرورها ( UPS ، ارت ، Cooling ، .... )**

# تامین امنیت شبکه سازمانها

- **تامین امنیت زیرساخت شبکه :**
  - **جدا سازی نواحی مختلف شبکه و استفاده از شبکه DMZ**
  - **استفاده از فایروال، UTM ، IDS/IPS و سایرتجهیزات امنیتی در لبه شبکه**
  - **پیکربندی استاندارد و امن تجهیزات زیر ساخت شبکه**
    - **طبق چک لیستهای امنیتی شرکت سازنده**
  - **پیاده سازی قابلیتهای امنیتی در ساختار سوییچینگ ، روتینگ و ارتباطات سیمی**
    - **VLAN , Port Security , ACL , 802.1X , NAC , ....**
  - **استفاده از الگوریتم های رمزنگاری و Hashing در ارتباطات وایرلس**




# تامین امنیت شبکه سازمانها

- **تامین امنیت پروتکل های ارتباطی شبکه :**
  - **پیش بینی تامین امنیت در ۷ لایه OSI ( دفاع در عمق )**
  - **طراحی و پیاده سازی مکانیزم AAA مناسب برای دسترسی به منابع شبکه**
  - **لحاظ نمودن چک لیست دسترسی های کاربران**
  - **طراحی و پیاده سازی مکانیزم Auditing و Logging مناسب**
  - **اطمینان از پیکربندی استاندارد و امن سرویسهای زیر ساخت شبکه و پروتکل های ارتباطی**
    - **طبق چک لیستهای امنیتی شرکت سازنده (Best Practice)**
  - **امن کردن پروتکل ها و سرویسهایی که به خودی خود مکانیزم امنیتی ندارند**
    - **مانند Telnet , RDP , IP**


# تامین امنیت شبکه سازمانها

- امنیت سیستم عامل و نرم افزارها
  - نصب سیستم عامل مناسب
    - تائید شده توسط مشاور امنیتی سازمان / عدم استفاده از کرک
  - نصب آخرین آپدیت ها و Patch ها
    - ( وصله های امنیتی ) روی سیستم عامل / استفاده از سرویس WSUS
  - Hardening سیستم عامل و سرویس های زیر ساخت
  - استفاده از آنتی ویروس و فایروال مناسب بر روی سرورها و کلاینتها
  - نصب نرم افزارهای مورد نیاز
    - با تائید واحد IT / حذف نرم افزارهای اضافی / عدم استفاده از کرک
  - اعمال پالیسی های ضروری در سازمان
    - ( محدودیت دسترسی / سیاست نام کاربری و رمزعبور ترکیبی / الزام تغییر پسورد دوره ای .... )

# تامین امنیت شبکه سازمانها

- **آموزش کاربران / آموزش مدیران شبکه :**
  - آموزش کاربران در خصوص تهدیدات رایج/چگونگی تشخیص سایتهای جعلی(fake)
  - آموزش کاربران در خصوص عدم استفاده از پسورد ساده و قابل حدس
  - آموزش کاربران در خصوص عدم ارائه اطلاعات شخصی /سازمانی در اینترنت و یا در تلفن
  - آموزش کاربران در خصوص عدم اشتراک گذاری فایل ها بدون لحاظ نمودن امنیت
  - آموزش کاربران در خصوص تهیه بک آپ از اطلاعات حیاتی سازمان و شخصی
  - آموزش کاربران در خصوص عدم نگهداری اطلاعات شخصی /سازمانی بر روی نوت بوک و یا فلش
  - آموزش مباحث تخصصی شبکه به مدیر شبکه و کارمندان واحد IT
  - پیاده سازی استانداردهای امنیتی در سازمان : ISMS (ISO 27001 , 27002)

# تامین امنیت شبکه سازمانها

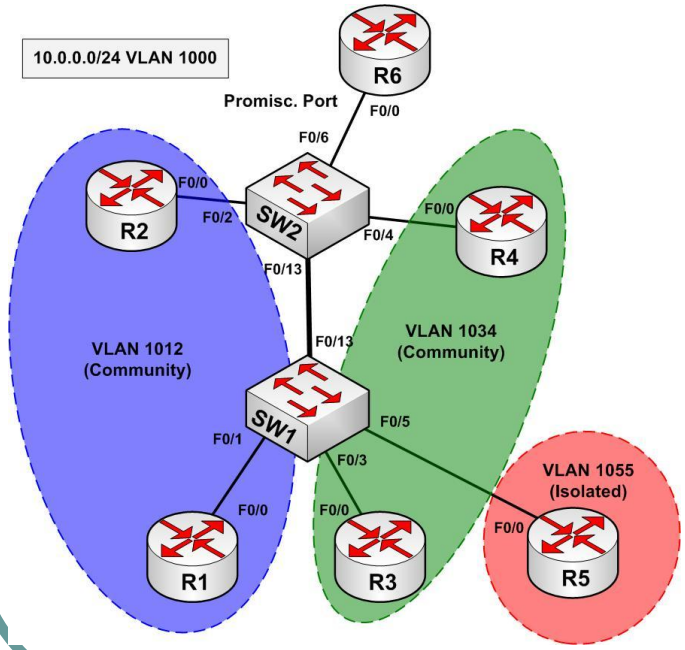
- مانیتورینگ / ممیزی:/ مدیریت متمرکز :
  - استفاده از نرم افزارهای مانیتورینگ آنلاین ( .. .. , Solawinds Orion NPM)
  - استفاده از نرم افزارهای مدیریت متمرکز شبکه ( ... , Microsoft SCCM)
  - استفاده از نرم افزار های اسکنر شبکه (Solarwinds Engineering Tools)
  - استفاده از نرم افزارهای مانیتورینگ لاگها ، خطاها و تلاشهای ناموفق (GFI Event Viewer )
  - استفاده از نرم افزارهای تست نفوذ جهت مشخص شدن نقاط آسیب پذیر شبکه
    - ( , Acunetix , GFI LAN Guard)
  - پایش و بازنگری خدمات شرکتهای طرف قرارداد
  - استفاده از تجربیات افراد متخصص جهت ارائه مشاوره و بازبینی طرح امنیتی شبکه

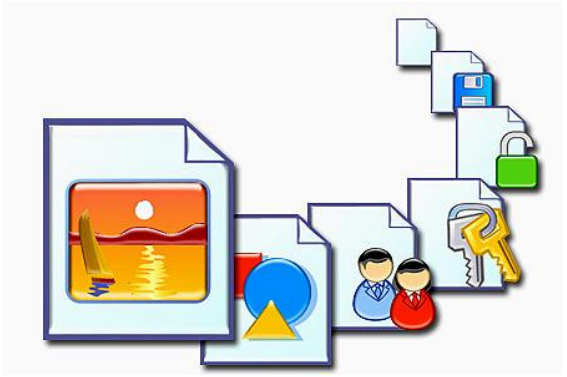
# تامین امنیت شبکه سازمانها

- **پشتیبان گیری :**
  - تهیه پلان بک آپ از سرورها ، پیکربندی ها ، نقشه ها و اطلاعات حیاتی سازمان
  - تهیه پشتیبان از پیکربندی های سوییچینگ ، روتینگ و قوانین فایروال
  - پیش بینی **Redundancy** در زیرساخت فیزیکی شبکه
  - پیش بینی **Redundancy** در زیرساخت منطقی ( سرویس های ) شبکه
  - استفاده از تجهیزات ذخیره سازی آنلاین (**SAN , NAS**)
  - استفاده از تجهیزات ذخیره سازی آفلاین (**Tape**)

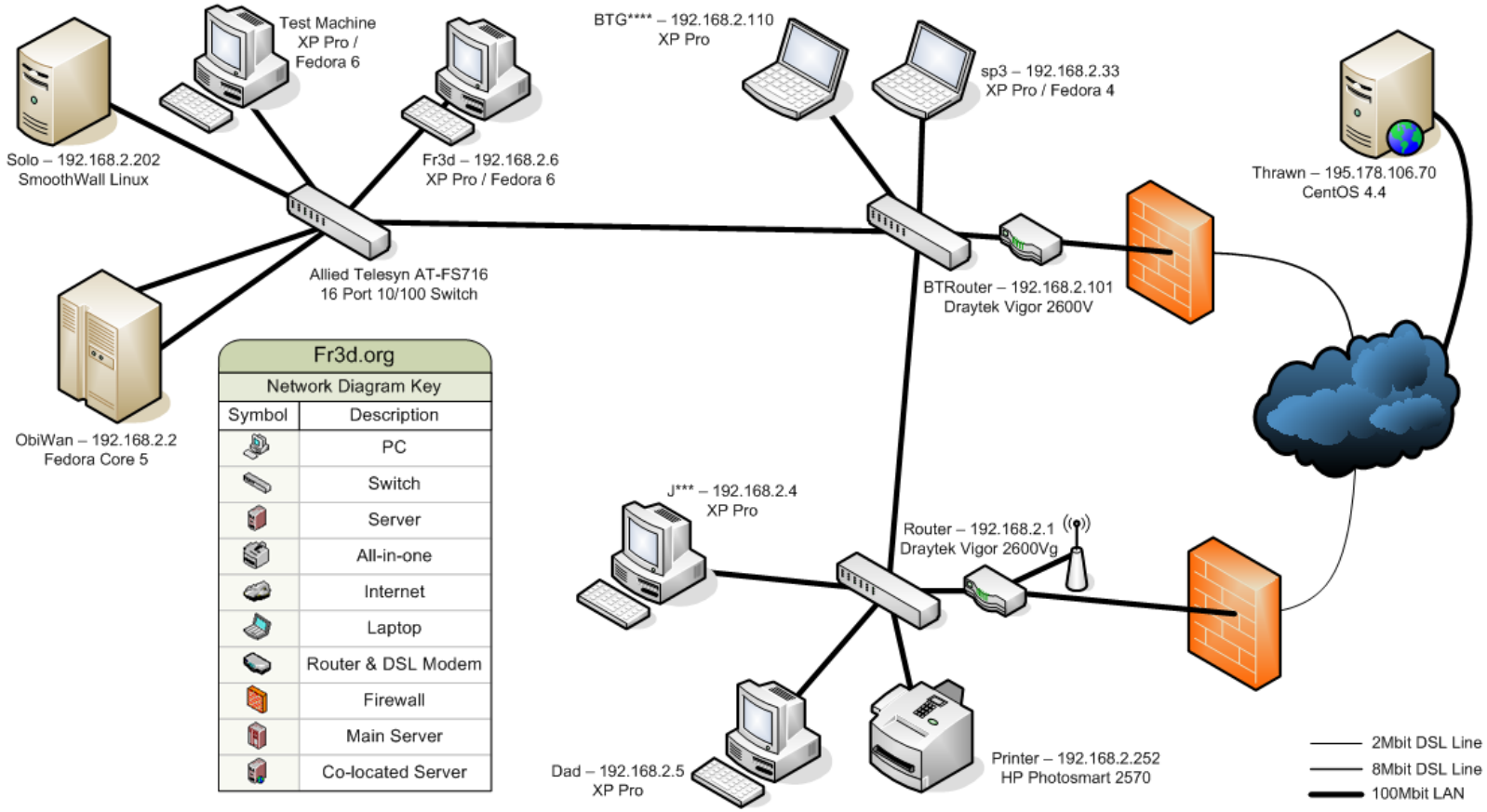
# تامین امنیت شبکه سازمانها

- مستند سازی / تهیه خط مشی ها و دستورالعملهای امنیتی :
  - تهیه نقشه فیزیکی شبکه
    - جانمایی سرورها – سوییچ ها – روترها – فایروال ها
    - جانمایی ارتباطات وایرلس – ارتباطات اینترنت – ارتباطات اینترانت
  - تهیه نقشه منطقی شبکه
    - تهیه ساختار معماری آدرسهای IP
    - تهیه نقشه VLAN بندی های شبکه
  - مستندسازی سیاستهای سازمانی اعمال شده
    - Cisco ACL , Microsoft GPO ,



# مثال ) نقشه فیزیکی شبکه



# تامین امنیت شبکه سازمانها

- **اشتباهات متداول مدیران سازمانها :**
  - **استخدام کارشناسان IT آموزش ندیده و غیرخبره**
  - **فقدان آگاهی لازم در رابطه با تاثیر یک ضعف امنیتی بر عملکرد سازمان**
    - **باور مدیر سازمان : " این مسئله برای ما اتفاق نخواهد افتاد "**
  - **عدم تخصیص بودجه مناسب برای پرداختن به امنیت اطلاعات**
    - **باور مدیر سازمان : " صرف هزینه در زمینه امنیت ، هزینه اضافی خواهد بود"**
  - **اتکاء کامل به ابزارها و محصولات تجاری**
    - **باور مدیر سازمان : " امنیت فقط یعنی یک فایروال و آنتی ویروس خارجی"**
  - **یک مرتبه سرمایه گذاری در ارتباط با امنیت**
    - **باور مدیر سازمان : " چندمرتبه باید هزینه کرد ؟ همین پارسال بود که ..... "**

# نقش عوامل انسانی در امنیت شبکه های کامپیوتری

- **اشتباهات متداول مدیران شبکه :**

- عدم آشنایی با مفاهیم امنیتی / عدم آشنایی با تهدیدات رایج و راه های مقابله
- عدم آشنایی با راه حل های طراحی و پیاده سازی امن شبکه
- عدم مطالعه پیوسته و به روز نبودن دانش فنی/ عدم عضویت در خبرنامه ها
- عدم وجود یک سیاست امنیتی مشخص در سازمان
- اتصال تجهیزات ، سرورها و کلاینتهای فاقد پیکربندی مناسب به اینترنت
- اعتماد بیش از اندازه به ابزارها
- عدم بررسی لاگ ها (Logs) / عدم مانیتورینگ شبکه / عدم ممیزی شبکه
- اعطای دسترسی اضافی به کاربران
- و .....

# نقش عوامل انسانی در امنیت شبکه های کامپیوتری

- **اشتباهات متداول کاربران معمولی**
  - تخطی از سیاست های امنیتی سازمان
  - انتقال داده های سازمان بر روی کامپیوتر شخصی ، نوت بوک و یا فلش
  - یاداشت نمودن داده های حساس و ذخیره غیرایمن آن
  - دریافت فایل از سایت های غیر مطمئن
  - عدم رعایت امنیت فیزیکی

# پایان