امنیت اطلاعات

بخش اول

ارائه شده در مرکز آموزش عالی علوم پزشکی وارستگان

مصطفی جهانگیر

مرداد ماه ۱۳۹۲

www.mjahangir.ir

mjahangir.blogfa.com

mjahangirf@gmail.com

مقدمه

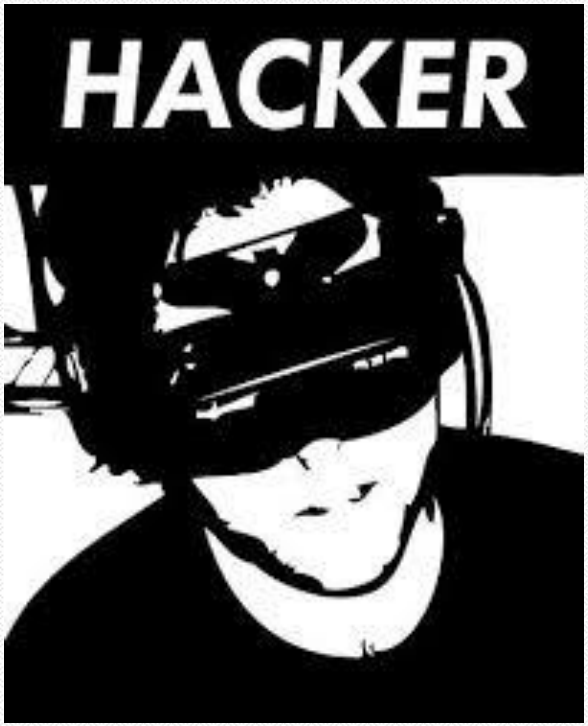
امنیت اطلاعات چیست؟

- حفاظت اطلاعات، سیستم‌های اطلاعاتی و شبکه های کامپیوتری از **فعالیت‌های غیرمجاز**:
  - دسترسی
  - افشا
  - خواندن و استفاده
  - نسخه برداری وضبط
  - خراب کردن
  - تغییر و دستکاری

امنیت اطلاعات چه ضرورتی دارد؟

- اطلاعات به عنوان یک **دارایی و سرمایه مهم و باارزش**
- اگر از سرمایه های اطلاعاتی به خوبی محافظت نشود:
  - بدون اطلاع شما به **دیگران داده شده و یا دزدیده شوند**.
  - بدون اطلاع شما **تغییر یابند** تا بی ارزش شوند و یا خسارت به بار آورند.
  - **گم شوند**، بدون این که اثری از آنها باقی بماند و یا امیدی به بازیابی آن ها باشد.
- لزوم ارائه **راهکارهای حفاظتی و امنیتی** برای حفظ آن ها

نفوذگران و تهدیدات امنیتی



انواع نفوذگران

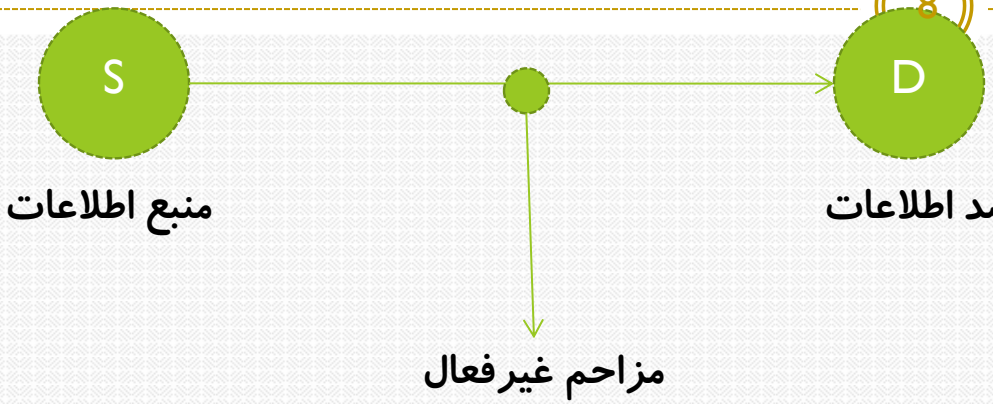
- **هکر:** نفوذ به منظور شناسایی ویژگی های و حفره های امنیتی سیستم های کامپیوتری بدون نقش تخریبی
- **کراکر:** نفوذ برای بهره برداری غیرمجاز، سرقت و یا تخریب اطلاعات در سیستم های کامپیوتری
- **واکر:** نفوذگران مزاحمی که شبیه کراکرها در پی خرابکاری یا سرقت اطلاعات نمی باشند.

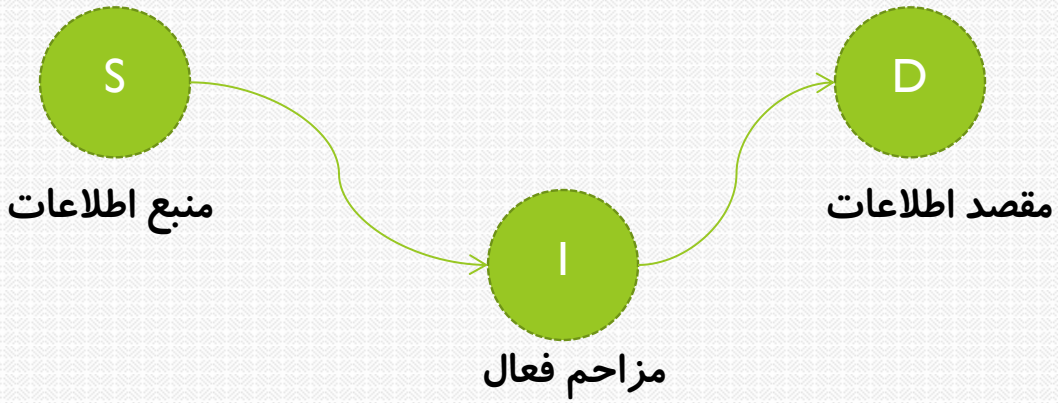
نفوذگران از حمله به اطلاعات چه اهدافی دارند؟

- اهداف سیاسی
- کسب در آمد
- سرگرمی
- شناسایی حفره های امنیتی
- رقابت اقتصادی

دسته بندی تهدیدات امنیتی

- تهدیدات غیرفعال
- تهدیدات فعال



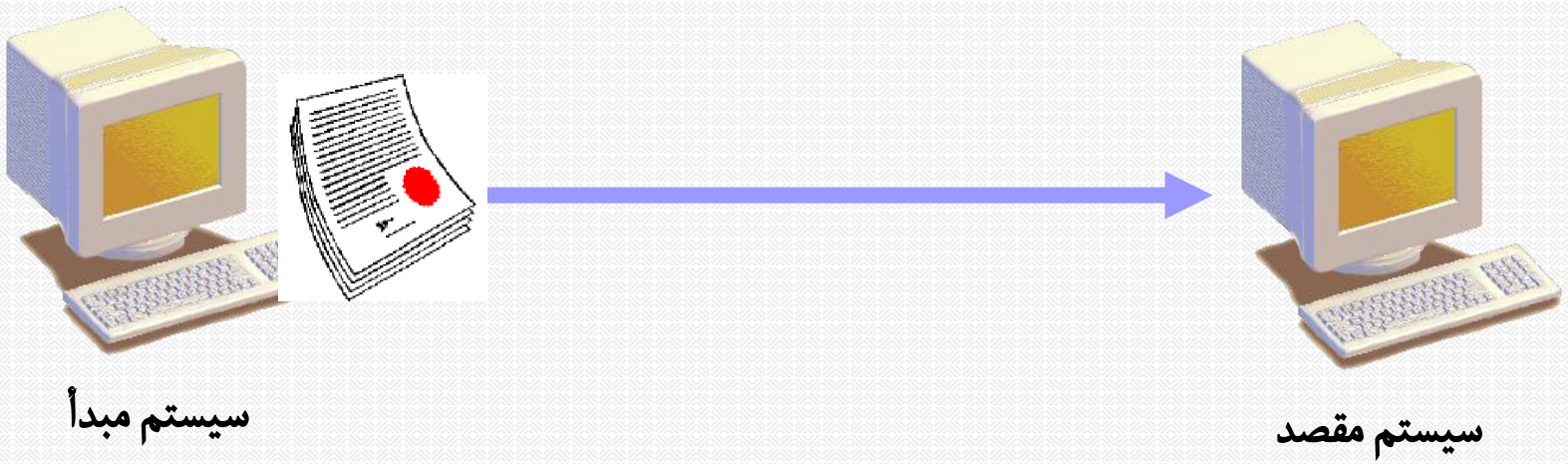


انواع تهدیدات امنیتی

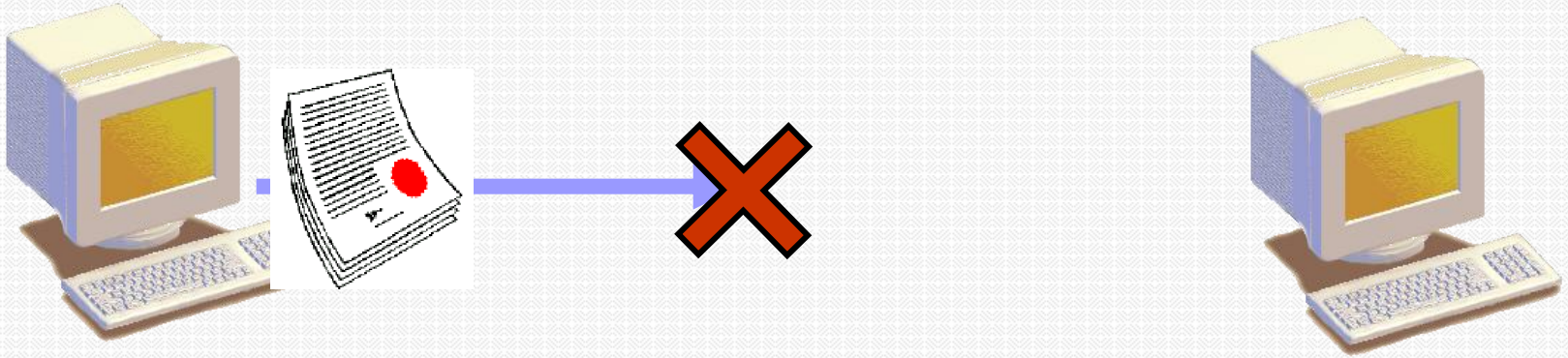
- ✓ قطع – Interruption
- ✓ شنود – Interception
- ✓ دستکاری– Modification
- ✓ فریب– Fabrication

- ✓ استراق سمع (Eavesdropping)
- ✓ تغییر قیافه (Masquerading)
- ✓ مداخله در پیام (Message Tampering)
- ✓ ارسال مجدد (Replaying)
- ✓ تحلیل ترافیک
- ✓ انکار سرویس (Denial Of service)

ارسال اطلاعات به صورت امن

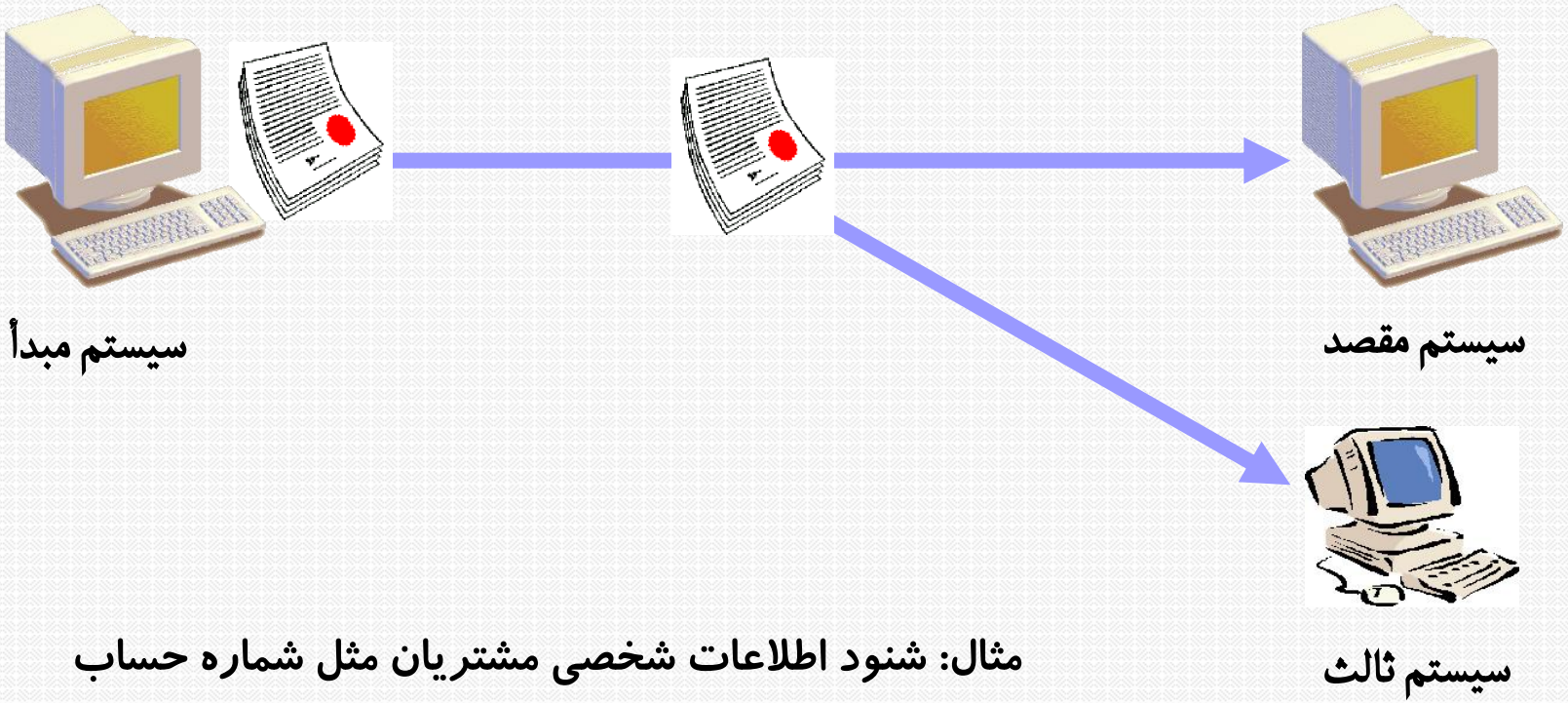


قطع (Interruption)



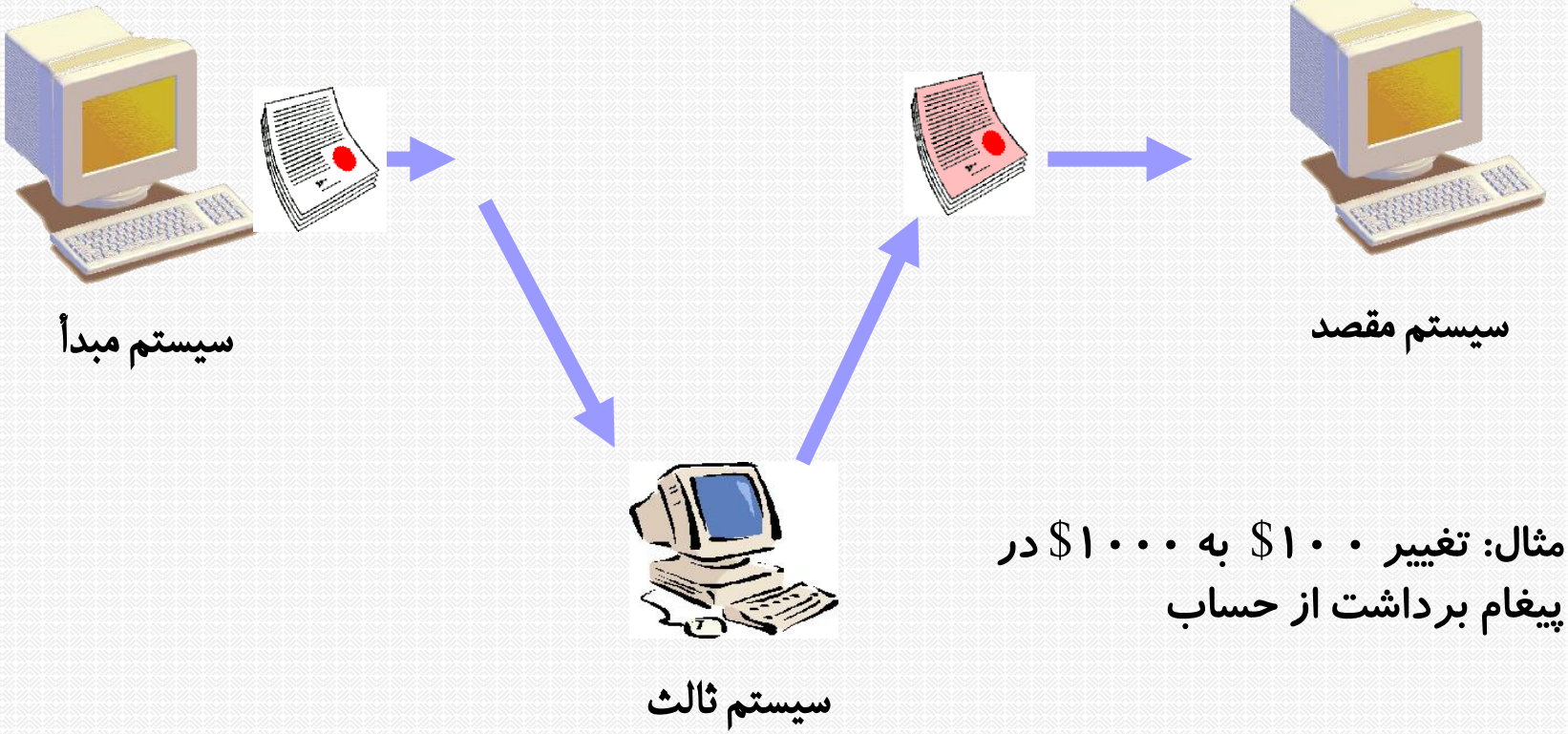
مثال: از کارانداختن یک سرویس اشتراکی در شبکه (چاپگر)

شنود (Interception)



مثال: شنود اطلاعات شخصی مشتریان مثل شماره حساب

دستکاری (Modification)



مثال: تغییر ۱۰۰$ به ۱۰۰۰$ در پیغام برداشت از حساب

فریب (Fabrication)

سیستم مبدأ

سیستم مقصد

سیستم ثالث

مثال: خود را بجای کسی جازدن و برداشت از حساب وی

سرویس های امنیت اطلاعات

سرویس های امنیت اطلاعات

- محرمانگی (Confidentiality)
  - اطمینان از این که اطلاعات فقط در دسترس افراد مجاز قرار دارد.
  - جلوگیری از افشای اطلاعات برای افراد غیر مجاز
  - مثال: رمز نگاری اطلاعات کارت بانکی در هنگام خرید اینترنتی
- صحت یا یکپارچگی (Integrity)
  - تامین صحت، دقت و کامل بودن اطلاعات
  - جلوگیری از تغییر داده‌ها به طور غیرمجاز و تشخیص تغییر در صورت دستکاری غیر مجاز اطلاعات

سرویس های امنیت اطلاعات

- دسترس پذیری (Accessibility)
  - اطمینان از این که کاربران مجاز در صورت نیاز به اطلاعات به آن ها به درستی و بدون اختلال دسترسی دارند.
  - مثال: در دسترس بودن سامانه اعلام نتایج یا انتخاب رشته کنکور
- اصل بودن یا احراز هویت (Authenticity)
  - اطمینان از اصل بودن و درست بودن اطلاعات ارسالی و نیز فرستنده و گیرنده اطلاعات
- قابلیت عدم انکار (Non-repudiation)
  - فرستنده یا گیرنده نتواند ارسال یا دریافت پیامی را انکار کند.

نرم افزارهای امنیتی (آنتی ویروس، فایروال و ...)

آنتی ویروس معتبر

- رشد روز افزون تهدیدات سایبری و لزوم نصب و استفاده از یک نرم افزار آنتی ویروس معتبر و اصلی بر روی کامپیوتر، گوشی موبایل و تبلت
- انتخاب و خرید آنتی ویروس معتبر و خوب که نیازهای ما را به خوبی پاسخ دهد.
- وجود نسخه های تقلبی و جعلی (FAKE AV) در بین آنتی ویروس ها
- تهدید بودن آنتی ویروس های جعلی و تقلبی

لایسنس آنتی ویروس

- آنتی ویروس باید قابلیت ثبت (رجیستر) و آپدیت (بروزرسانی) مستقیم در ایران را داشته باشد و کاربر هیچگونه دخالتی در آن نداشته باشد.
- ثبت و رجیستر آنتی ویروس باید آنلاین باشد و از شرکت تولید کننده آنتی ویروس ایمیلی مبنی بر معتبر بودن لایسنس برای شما ارسال شود.
- در حال حاضر آنتی ویروس های شرکت های AVG , PC-Tools , Avast و McAfee و Kaspersky قابلیت ثبت و آپدیت در ایران ندارند.

آپدیت آنتی ویروس

- عدم استفاده از آپدیت های آفلاین
- آپدیت و بروزرسانی آنتی ویروس باید بدون دخالت هرگونه عامل انسانی و به صورت کاملا خودکار صورت بگیرد .
- امروزه بیشتر آنتی ویروس ها برخی ویروس ها را بر اساس تکنولوژی کلود شناسایی می کنند و آپدیتی برای آن ارائه نمی شود.

اعتبار گارانتی و شرکت پشتیبانی کننده آنتی ویروس در ایران

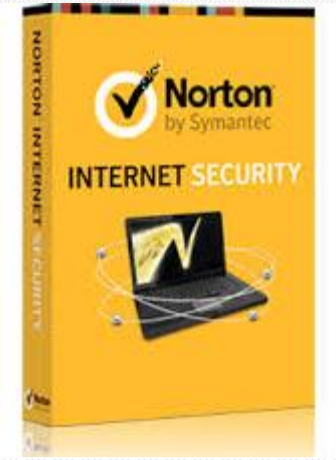
- اهمیت **اعتبار واردکننده و پشتیبانی کننده** آنتی ویروس در ایران
- خرید محصول از **مراکز غیر معتبر** و یا **گارانتی های غیر معتبر** باعث می شود:
  - محصول جعلی و تقلبی به دست شما برسد.
  - شرکت گارانتی کننده قادر به پاسخگویی و ارائه پشتیبانی به شما نباشد.
  - لایسنس آنتی ویروس پس از مدتی بلاک شود.
- آنتی ویروس های به ظاهر معتبر ولی با گارانتی های غیر معتبر:
  - ESET Nod 32
  - Kaspersky

اعتبار گارانتی و شرکت پشتیبانی کننده آنتی ویروس در ایران

- **نشانه های نامعتبر بودن گارانتی آنتی ویروس:**
  - سرقت از زمان لایسنس ها
  - مسدود کردن اشتباهی لایسنس ها
  - توزیع عمدی لایسنس جعلی به فروشندگان و توزیع کنندگان
  - عدم ارائه پشتیبانی وقتی نرم افزار با مشکلی مواجه می شود.

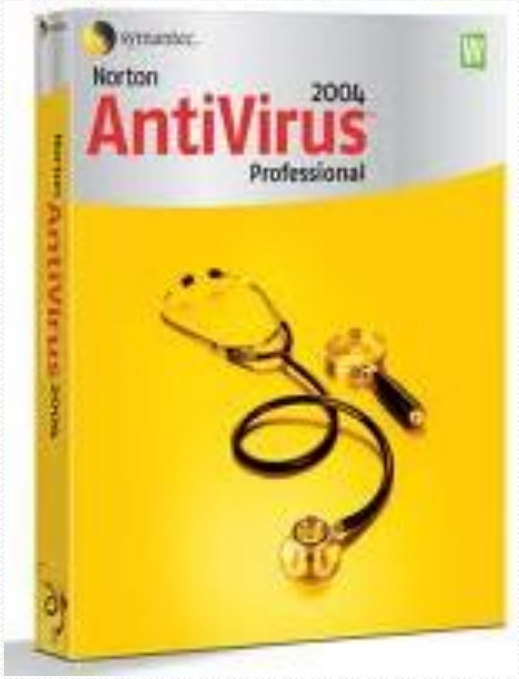
کلاس های آنتی ویروس ها

- آنتی ویروس هایی که **فقط ضد ویروس** هستند تا آنتی ویروس هایی که دارای **ویژگی های بسیار بیشتری** هستند.
  - قابلیت بهینه سازی ویندوز
  - کنترل والدین بر فرزندان
  - مدیریت پسوردها
  - قابلیت نصب بر روی کامپیوترهای ویندوزی ، مکینتاش و تبلت و گوشی های هوشمند
  - حفاظت در برابر ایمیل های آلوده
  - حفاظت در برابر صفحات وب آلوده
  - فضای پشتیبان گیری کلود و آنلاین



کلاس های آنتی ویروس ها

- محصولات کامل آنتی ویروس:
  - Internet security
  - Maximum Security
  - Total Security
  - Global Protection



فایروال (Firewall)

- امنیت در برابر حملات هک و نفوذ
- با خرید اینترنت سکیوریتی ها هم از آنتی ویروس و هم از فایروال بهره مند می شویم.

حفاظت از مرورگرها (Protect Browsers)

- افزایش تعداد وب سایتهای آلوده، به شکلی که حتی برخی وب سایت های به ظاهر معتبر هم آلوده به بدافزارها و ویروس ها می باشند.
- نرم افزارهای اینترنت سکیوریتی، ویژگی حفاظت از مرورگرها را به صورت خودکار به ما ارائه می دهند.
- حفاظت در مقابل آلوده شدن به ویروس ها از طریق صفحات و وب سایت های آلوده و یا کدهای مخرب درون وب سایت ها
- حفاظت از اسپم ها و ایمیل های آلوده

امنیت پسوردها

اهمیت امنیت پسوردها

- روشی به منظور تایید کاربران بوده و تنها حفاظ موجود بین کاربر و اطلاعات
- مهاجمان با بکارگیری برنامه های متعدد نرم افزاری، قادر به حدس رمزهای عبور (کرک) آنان می باشند.
- لزوم انتخاب مناسب و نگهداری ایمن رمزهای عبور

انتخاب پسورد مناسب

- استفاده از حداقل ۸ کاراکتر
- استفاده از هم کلمات بزرگ و هم کوچک
- استفاده از عدد، سمبل ها و نشانه ها
- تایپ نادرست برخی کلمات نظیر daytt در مقابل استفاده از date
- استفاده از روشی خاص به منظور بخاطرسپردن پسوردهای پیچیده
- استفاده از رمزهای عبور متفاوت برای سیستم های متفاوت

گزینه های نامناسب پسورد

- مبتنی بر اطلاعات شخصی باشد نظیر: تاریخ تولد، شماره شناسنامه، شماره تلفن، شماره دانشجویی، شماره پرسنلی و ...
- از کلمات موجود در دیکشنری باشد.
- عدم استفاده از یک پسورد برای کلیه سیستم ها (کلید جادویی)

حفاظت از پسوردها

- اجتناب از دادن رمز عبور خود به سایر افراد
- اجتناب از نوشتن رمز عبور بر روی کاغذ و گذاشتن آن بر روی میز یا کامپیوتر
- رمزنگاری پسوردها (public key encryption)
- Logout در هنگام استفاده از کامپیوتر عمومی

نرم افزار مدیریت پسوردها (Password Manager)

- ذخیره شدن پسوردهای ما در یک فضای امن
- لازم نبودن حفظ همه پسوردهای خود
- عدم لزوم استفاده از کیبورد برای ورود به حساب های کاربری خود
- امکان انتخاب پسوردهای بسیار مشکلتر و طولانی تر
- تهیه نسخه های پشتیبان امن از پسوردهای خود
- نرم افزارهای Direct Pass و Identity Protection

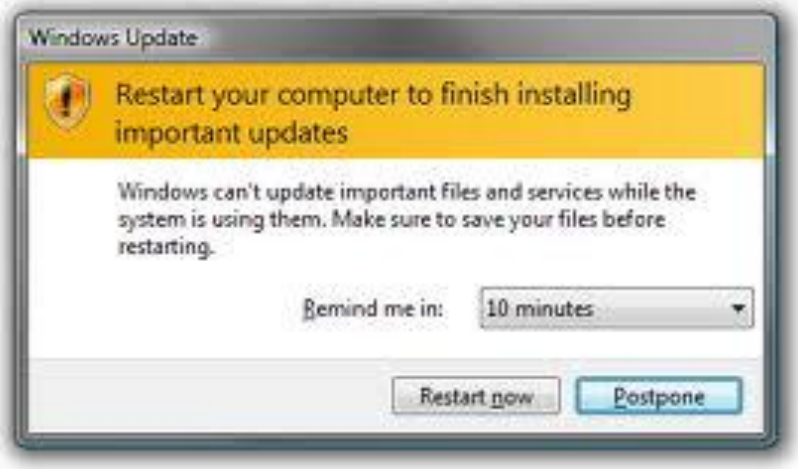
امنیت فیزیکی کامپیوتر و لپ تاپ

بهینه سازی سیستم (System Tune)

- پاک کردن اطلاعات اضافی بر روی هارد دیسک مانند کوکی ها و فایلهای اضافه اینترنتی
- اینترنت سکیوریتی ها ویژگی System Tune را ارائه داده و نیاز به نصب نرم افزارهای جداگانه نیست.
- در صورتی که نیاز به نصب نرم افزار جداگانه: برنامه CClearn پیشنهاد می شود.

آپدیت و بروزرسانی مستمر (Update)

- آپدیت و بروزرسانی مستمر برای بهبود عملکرد کامپیوتر و پوشش دادن نقص های امنیتی
  - سیستم عامل (ویندوز)
  - برنامه های کاربردی مانند آدوب ، فلش ، جاوا و ...
  - مرورگر اینترنت
  - نرم افزارهای امنیتی و آنتی ویروس ها



اقدامات در زمان بلا استفاده بودن کامپیوتر و اینترنت

- قفل نمودن کامپیوتر زمانی که از آن دور هستیم، حتی برای چند دقیقه
- قطع ارتباط با اینترنت زمانی که از آن استفاده نمی گردد.

دقت در نصب نرم افزارها

- زمانی که یک برنامه را جهت اجراء انتخاب می نمائید، در واقع این تصمیم را گرفته اید که کنترل کامپیوتر خود را به آن واگذار نمائید.
- یک برنامه پس از فراهم شدن شرایط لازم جهت اجراء، قادر به انجام هر کاری می باشد.
- حتی می تواند محدودیت هایی را به منظور استفاده از سیستم برای شما ایجاد نماید.

حفاظت فیزیکی از کامپیوتر

- در صورتی که فردی بتواند به طور فیزیکی به کامپیوتر شما دستیابی داشته باشند، می توانند کنترل کامپیوتر شما را بطور کامل دراختیار گرفته و هر کاری را که دوست دارند انجام دهد.
  - تغییر داده
  - سرقت اطلاعات
  - سرقت سخت افزار
  - ایجاد اشکال فیزیکی در کامپیوتر

منابع

- پایگاه اطلاع رسانی امنیت اطلاعات ایران (دیسنا)، www.disna.ir
- وب سایت ویکی پدیا، www.wikipedia.org/fa
- وب سایت سخاروش، www.srco.ir