
مبانی کامپیوتر
علی خان نصراصفهانی
1
1

# جلسه ششم

به کلاس درس اینجانب خوش آمدید

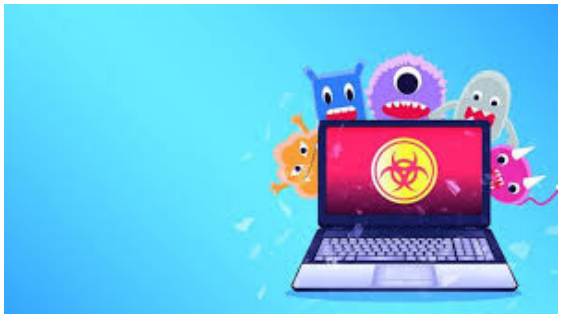
## برنامه این جلسه

- برنامه درس:
- ویروس
- حفاظت از اطلاعات

## مخاطرات احتمالی ناشی از سرقت تجهیزات

ممکن است اطلاعات تمام تماسهای حرفه‌ای و شخصی خود شامل نامها، آدرسها، تلفنها، آدرسهای پست الکترونیک را از دست بدهید. همچنین ممکن است اطلاعات با ارزشی را که در فایلها دارید از دست بدهید. بعضی از این اطلاعات ممکن است محرمانه، حساس یا بحرانی باشند. البته تمام فایلها محرمانه و مهم نیستند ولی بهرحال برای ایجاد آنها حتماً زمان قابل توجهی صرف شده است. حتی بعضی ممکن است حاوی اطلاعاتی باشند که قابل باز تولید نیستند. بهتر است یک نسخه پشتیبان از اطلاعات تماس روی موبایلهایتان، و تمام اطلاعات مهم روی PDA یا Laptop خود نگهداری کنید. همیشه هم مراقب وسائلتان باشید و هیچگاه آنها را در محلهای نا امن و در معرض دید قرار ندهید.

# ویروسهای رایانه‌ای



## ویروسهای رایانه‌ای چه هستند؟

ویروس تکه برنامه‌ای است که توسط یک برنامه‌نویس نوشته شده تا اشکالات آزاردهنده‌ای در رایانه شما بوجود آورد. مثلاً

یک ویروس ممکن است تمام مطالب روی رایانه شما را پاک کند.

## ویروسها چگونه رایانه را آلوده می‌کنند؟

یک ویروس ممکن است از راههای مختلفی رایانه شما را آلوده کند. این راهها شامل شبکه‌ها، دیسکت‌ها، پیامهای پست الکترونیک و دریافت فایل از اینترنت باشد. بدترین چیز، آن است که شما نمی‌دانید که دستگاه آلوده شده یا نه، انواع زیادی از ویروسها وجود دارد. بعضی می‌توانند سبب تخریب کامل فایلها شوند، در حالیکه برخی دیگر فقط ممکن است سبب رفتار غیرعادی رایانه شوند و پیام روی صفحه نمایش دهند. بخش بزرگی از ویروسها فقط خود را در محلهای مختلف رایانه کپی کرده و به این ترتیب فضای دیسک را اشغال می‌کنند.

## مثال هایی از عملکرد انواع ویروس های رایانه ای

در اینجا مثالهایی از انواع ویروسها و آنچه انجام می‌دهند ارائه شده است: ویروس بخش راه‌اندازی رایانه، اولین یا چند سکتور اول هارددیسک رایانه یا فلاپی دیسک را آلوده می‌کند. اگر مبتلا به این ویروس باشید، وقتی دستگاه را روشن می‌کنید، درست کار نمی‌کند. لازم است دستگاه را خاموش کرده و دیسکت راه‌انداز اضطراری برای یک راه‌اندازی سالم را استفاده نمائید.

## مثال هایی از عملکرد انواع ویروس های رایانه ای

یک ویروس همراه، خودش را در داخل فایل command.com ذخیره می‌کند و بعد خودش را به فایلهای پر مصرف مثل فایلهای اجرایی (exe) یا فایلهای (bat.) تغییر نام می دهد.

## مثال هایی از عملکرد انواع ویروس های رایانه ای

یک ویروس اجرا شونده، خودش را در داخل فایل‌های .exe ، .bat یا .com ذخیره کرده و با هر بار اجرای این فایلها خودش را تکثیر می‌کند.

## مثال هایی از عملکرد انواع ویروس های رایانه ای

ویروسهای Macro، فایلهای Word و Excel را آلوده می‌کنند. این ویروس می‌تواند فایلهای روی رایانه را تغییر داده یا حذف کند.

## مثال هایی از عملکرد انواع ویروس های رایانه ای

یک ویروس غیرساکن، خودش را در فایلهای اجرایی قرار می‌دهد، و وقتی فایل اجرا شد، فعال می‌شود. ولی ویروس ساکن در حافظه، خودش را در حافظه قرار می‌دهد مستقیماً فایلهای مشخص را آلوده می‌کند. در این موارد لازم نیست کاربر برنامه اجرایی خاصی را اجرا کند تا بقیه فایلها آلوده شوند.

## مثال هایی از عملکرد انواع ویروس های رایانه ای

ویروس‌های جایگزین شونده خودشان را بجای بخشی از یک فایل، در فایل می‌نویسند و به این ترتیب آن فایل مخدوش، غیر قابل استفاده و غیر قابل اصلاح می‌شود.

## مثال هایی از عملکرد انواع ویروس های رایانه ای

ویروسهای چند شکلی قادرند که برنامهٔ خود را مرتباً تغییر دهند و شکلهای مختلفی از خود بوجود آورند. این خاصیت شناسایی آنها را مشکل‌تر می‌کند.

## مثال هایی از عملکرد انواع ویروس های رایانه ای

ویروسهای پنهان شونده، می‌توانند ردپای خود را از بین ببرند. مثلاً وقتی فایل را آلوده کردند، کاری می‌کنند که گوئی چیزی عوض نشده است.

## مثال هایی از عملکرد انواع ویروس های رایانه ای

ویروسهای گول زننده (Hoax) معمولاً در e-mailها پیدا می‌شوند. آنها معمولاً دروغین هستند و به نظر می‌رسد که می‌خواهند کاری با رایانه بکنند ولی در عمل اتفاقی نمی‌افتد. هشدارهای با e-mail معمولاً از شما می‌خواهد که چیزی را به تمام دوستان خود بگویید یا به شرکتهای رایانه‌ای مثل میکروسافت و اینتل خبر دهید. اگر شما اینکار را بکنید و آنها هم همین کار را بکنند، این کار فقط سبب مختل شدن سیستم پست الکترونیک می‌شود.

## مثال هایی از عملکرد انواع ویروس های رایانه ای

Trojan برنامه‌ای است که در ظاهر برای تفریح است یا قرار است کار مفیدی برای رایانه شما انجام دهد ولی در زیر پوشش دوستانه‌اش می‌تواند برای فایلهای شما مخرب باشد.

## مثال هایی از عملکرد انواع ویروس های رایانه ای

نوع دیگری از ویروس می‌تواند نسخهٔ اصلی راه انداز (Master boat record) را آلوده یا دستکاری کند و معمولاً سبب از دست رفتن امکان کار با CDROM هم می‌شود.

## مقابله و علاج ویروس‌ها

### چگونه از یک ویروس جلوگیری کنیم؟

راههای زیادی برای حفاظت رایانه وجود دارد. ساده‌ترین راه، استفاده از نرم افزارهای حفاظت در برابر ویروس است که Anti-Virus نامیده می‌شوند. این نرم افزار هر فایلی که باز کپی، منتقل یا حذف می‌شود را، برای وجود اثری از ویروس در آن، بررسی می‌کند. اگر ردپایی پیدا شد، ویروس را حذف می‌کند. این راه خیلی خوبی برای حفاظت رایانه شماست و نرم افزار ضد ویروس چندان گران هم نیست. اگر هنوز نسخه‌ای از این نرم افزار تهیه نکرده‌اید، توصیه می‌شود که در این مورد اقدام کنید.

### در صورت آلوده شدن، چه باید کرد ؟

اگر یک نرم افزار ضد ویروس داشته باشید و ویروس تشخیص داده شده باشد، برنامه سعی می‌کند که فایلهای آلوده را حذف یا علاج کند. احتمالاً گزارشی به شما ارائه می‌شود که نام ویروس، فایلهای آلوده شده و آدرس آنها و عملیاتی که برای رفع مشکل انجام شده را در آن خواهید دید. اگر شما آلوده شدید و به شبکه وصل هستید، توصیه می‌شود کابل ارتباطی شبکه را از رایانه‌تان جدا کنید. این از انتشار بیشتر ویروس، آلوده شدن سایر کاربران و حتی سرور جلوگیری می‌کند. چنانکه گفته شد، ویروسها بیشتر با e-mail منتشر می‌شوند. آدرسهای موجود روی دستگاه شما، برای انتشار ویروس از طریق پست الکترونیک، مورد استفادهٔ ویروس قرار می‌گیرد.

نکته مهمی که باید در مورد نرم افزارهای ضد ویروس بدانید، آن است که ویروسهای جدید بطور روزانه شناسایی می‌شوند و هر سطح از حفاظت که شما امروز داشته باشید، ممکن است فردا مؤثر و کارا نباشد. لذا خوبست که نرم‌افزار ضد ویروس خود را مرتباً به روز کنید.

وقتی نرم افزار ضد ویروس را اجرا می‌کنید، برنامه تمام فضاهای رایانه شما را بدنبال ویروس جستجو می‌کند. خیلی برنامه‌ها فایلها را با حذف ویروس یا غیرقابل اجرا کردن فایل، پاک یا غیر مضر می کنند. روش استفاده از ضدعفونی کننده‌های خانگی برای مبارزه با میکروب‌ها را در نظر بگیرید. برنامه‌های ضد ویروس هم تقریباً همان کار را با رایانه شما می‌کنند.

## انتخاب روشهای مناسب در مقابله با آلودگی

وقتی از اینترنت اطلاعات دریافت می‌کنید باید بیشتر مراقب باشید. گاهی از شما خواسته می‌شود که برای دریافت فایل از یک سایت مشخص، ok را کلیک کنید. شما می‌توانید یک سایت قابل اطمینان را برای استفاده‌های آتی انتخاب کنید. قبل از باز کردن هر ضمیمه یک e-mail مطمئن شوید که فرستنده را می‌شناسید. اگر از افرادی که نمی‌شناسید پیامی دریافت کردید، حتی اگر ضمیمه هم نداشت.با نهایت احتیاط رفتار کنید. اگر به هر دلیلی شک دارید، پیام را بدون بازکردن پاک کنید. اگر برنامهٔ ضد ویروس دارید، هر پیامی با احتمال وجود ویروس در آن شناسایی شده و به شما اطلاع داده می‌شود. به یاد داشته باشید: ویروسها همیشه در دل فایلهای به ظاهر پاک پنهان می‌شوند.

حق کپی و قوانین

# حق کپی نرم افزار

## موضوعات مرتبط با حق کپی نرم افزار

هر نرم افزاری که شما تهیه می‌کنید با قانون حق کپی حفاظت شده است. هر نرم افزار که شما می‌خرید باید یک صفحهٔ مجوز داشته باشد که در آن شرایط مجاز استفاده از نرم افزار قید شده باشد. اگر شما نرم افزار را کپی کرده، بفروشید یا به دوستانتان بدهید، شما ممکن است قانون شکنی کرده باشید و ممکن است متهم شوید. بسیاری از مردم یک بازی را می‌خرند و بعد یک کپی از آن را به دوستان یا بستگان خود می‌دهند. این عمل هم قانونمند نیست و ممکن است منجر به اتهام شود. سازمانهای متعدد، مثل FAST : (Federation Against Software Theft) یا BSA : (British Software Alliance) می‌توانند در مواردی که شما شک دارید، شما را راهنمایی کنند.

### تکلیف نرم افزارهای روی اینترنت چیست؟

اکثر نرم افزارهای دریافتی از اینترنت اشتراکی یا رایگان هستند. البته برخی سایتهای اینترنتی هم هستند که نرم افزارهای فروشی را بدون مجوز در اختیار می‌گذارند. اگر شما یکی از این برنامه‌ها را دریافت کنید، شما هم قانون را نقض کرده‌اید. اگر متن، تصویر، فایلهای صدا یا فیلم از وب سایتی دریافت کردید و استفاده شخصی کرده و آن را توزیع نکردید ( به هیچ صورت )، در این صورت شما ناقض قانون حق کپی نیستید. همیشه، حتماً وجود حق کپی و رعایت آن در مورد هر فایل را کنترل کنید.

## چگونه قانون حق کپی Copyright در استفاده و توزیع مدرک اثر می‌گذارد؟

اگر خواستید فایلهای تصویر، صدا و صوت را بر روی تجهیزات جانبی مثل دیسکت یا zip دیسک یا CD توزیع نمائید، اول باید مطمئن شوید که اجازهٔ چنین کاری را دارید. بعضی فایلهای صوتی با این قانون حفاظت شده‌اند و برای کپی و توزیع آنها باید هزینه‌ای را به صاحب حق کپی آنها بپردازید ولی اگر این کار را نکنید و این کشف شود، عواقب آن خیلی گران خواهد بود. بهتر است که اول این را کنترل کرده و اقدامات لازم را انجام دهید. اگر به هر دلیل شک کردید، با شرکت یا شخصی که آن محتوا را از او دریافت کرده‌اید تماس بگیرید تا ببینید چه کسی صاحب حق کپی است و شما حق استفاده از آن را دارید و اگر دارید چگونه؟

## *کنترل شماره‌های شناسایی محصول و درک محتوای مجوزهای استفاده*

وقتی نرم افزاری می‌خرید، روی بستهٔ آن یک شماره شناسایی یا شمارهٔ مجوز وجود دارد. بعضی محصولات شرکت میکروسافت معمولاً یک شماره شناسایی CD دارند که پشت بستهٔ آنها چاپ شده است. وقتی نرم افزار را نصب می‌کنید این شماره از شما پرسیده می‌شود. وقتی نرم افزار نصب شد، از گزینه About از منوی Help نرم افزار، این شماره را خواهید دید. کادری که در آنجا باز شده، نام محصول، شماره نسخه، کاربر ثبت نام کرده، نام شرکت در صورت کاربرد و شمارهٔ شناسایی محصول را هم نشان می‌دهد. توجه کنید که در آنجا پیام هشداری وجود دارد و آن این است که محصول تحت حفاظت قانون حق کپی است.

### Freewareچیست ؟

Freeware لفظی است که برای نامیدن نرم افزارهای رایگان استفاده می‌شود. نرم افزارهایی که Freeware هستند، باید رایگان باشند و هیچ وجهی نباید برای آنها پرداخت شود. سایتهای بی‌شماری روی اینترنت هستند که نرم افزارهای رایگان مثل بازی‌ها، واژه‌پردازها و برنامه‌های کمکی را ارائه می‌کنند.

### Shareware چیست؟

Shareware حالتی است که شما نرم افزاری را قبل از خرید آزمایش می‌کنید. معمولاً تا ۳۰ روز به شما این اجازه داده می‌شود و بعد از آن از شما خواسته می‌شود که برای ادامه استفاده، ثبت نام کنید. این روش خوبی است، چون می‌توانید اول ببینید آیا نرم افزار دقیقاً همان که می‌خواهید را انجام می‌دهد و اگر مفید بود، آن را تهیه کنید.

گواهی استفاده کاربر از نرم افزار، شرایط استفاده از نرم افزار را تعریف می‌کند. این شرایط از نظر قانونی توافقهایی هستند که خریدار نرم افزار، آنها را پذیرفته و مشخص می‌کند که خریدار چه کارهایی می‌تواند بکند و چه کارهایی نمی‌تواند انجام دهد. وقتی شما نرم افزاری می‌خرید، صاحب آن نیستید، بلکه مجوزی برای استفاده از آن می‌خرید.

### مجوز سایت‌های رایانه‌ای چیست؟

شرکتهای بزرگ معمولاً نرم افزارهای مورد نیاز خود را از فروشگاه و بصورت تک تک تهیه نمی‌کنند. بلکه مجوز استفادهٔ انبوه، به تعداد مورد نیاز. از نرم افزار را تهیه می‌کنند.

### مجوزهای آموزشی یا دانشجویی چیست؟

اکثر شرکتهای رایانه‌ای مثل میکروسافت، تخفیف‌هایی برای مجوزهای استفاده از نرم افزارهایشان توسط دانشجویان و مؤسسات آموزشی در نظر می‌گیرند.

بیاد داشته باشید که عدم رعایت حق کپی، یک جرم و قانون شکنی است. تهیه کپی‌های غیرمجاز از نرم افزار مجاز نیست. همواره مجوزهای استفاده از نرم افزار خود و دیسک‌های نرم افزار خود را در محل مناسب نگهدارید. ممکن است گاهی لازم شود که آنها را به بازرسانی از مؤسسات مرتبط ارائه نمائید.

## قوانین حفاظت از داده‌ها

مسائل مربوط به حفاظت داده‌ها و حریم خصوصی

اگر روی رایانه‌تان اطلاعات افراد را ذخیره کرده‌اید، آنگاه شما قانوناً و اخلاقاً موظف به مراقب از این داده‌ها، با دقت کافی هستید. مثلاً اگر رایانه یک پزشک رها شده و کسی اطلاعات شما را در آنجا بخواند، این آغاز خدشه‌دار شدن اعتماد است.

دولتها – پلیس – مؤسسات اعتباری – بانکها و سایر مؤسساتی که اطلاعات زیادی در مورد عموم مردم نگهداری می‌کنند، که تمام این اطلاعات محرمانه و خصوصی است، این الزام از سال ۱۹۸۴ مطرح شده و فقط در مورد اطلاعات افراد زنده اعمال می شود. از نظر قانونی موظفند که عدم دسترسی منابع غیرمجاز به این اطلاعات را تأمین نمایند.

## حفاظت عملی از داده‌ها

در این بخش قواعد اصلی حفاظت عملی از داده‌ها در کشور انگلستان مورد اشاره قرار می‌گیرند. بدیهی است موارد اشاره شده در اینجا صرفاً جنبه نمونه داشته و در صورت نیاز به اصل و شرح موارد، باید به اصل قانون مراجعه شود.

## ➢ حفاظت عملی از داده‌ها

- اطلاعات افراد باید منصفانه و قانونمند بررسی و پردازش شود.
- اطلاعات فردی باید برای مقاصد مشخص گردآوری شده و فقط برای همان مقاصد پردازش و استفاده شوند.
- اطلاعات فردی برای هر منظور باید کافی و مرتبط بوده و نباید بیشتر از مقدار لازم برای منظوری که مورد نظر بوده است گردآوری و پردازش شود. اطلاعات افراد باید دقیق بوده و هر زمان که لازم است، به روز شود.

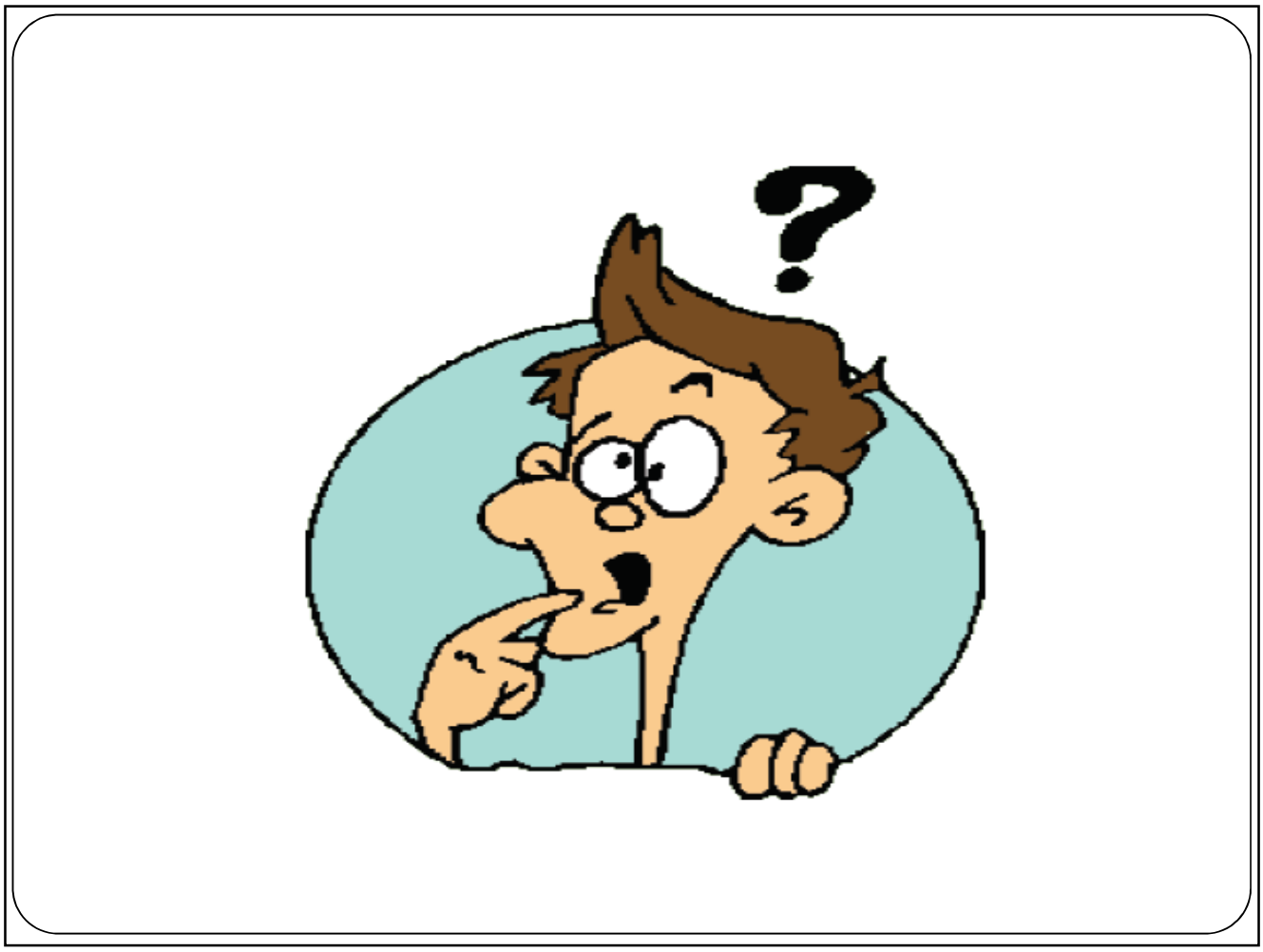
## ➢ حفاظت عملی از داده‌ها

- اطلاعات فردی، برای هر منظور پردازش می‌شوند، نباید بیش از مدت لازم برای آن منظور نگهداری شوند.
- اطلاعات فردی باید با توجه به حقوقی که در مورد داده‌ها در این دستورالعمل آمده، پردازش شده و مورد استفاده قرار گیرند.
- برای مقابله با دسترسی غیرمجاز – از دست رفتن تصادفی – تخریب و آسیب رسیدن به اطلاعات فردی، باید اقدامات مناسب فنی و سازمانی انجام شود.

مناسب فنی و سازمانی انجام شود.

## حفاظت عملی از داده‌ها

- اطلاعات فردی نباید در اختیار کشورها یا حاکمیت‌های خارج از اتحادیه اروپا قرار گیرد، مگر آنکه آن کشور یا حاکمیت، سطح قابل قبولی از حفاظت اطلاعات فردی از نظر حقوقی و محتوای اطلاعات در مقابل پردازش را تضمین نموده باشد.



# پایدار باشید