



مقدمه

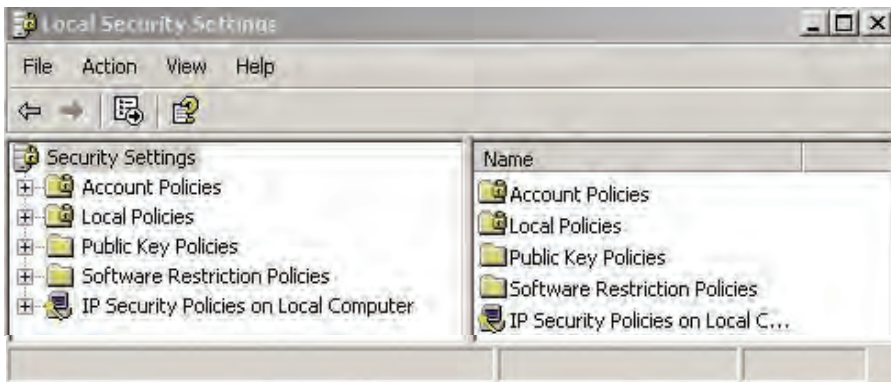
تنظیمات امنیتی (Security policy) مجموعه‌ای از تنظیمات هستند که برای کامپیوتر یا کاربر تعیین می‌شود. تنظیمات امنیتی که برای یک کامپیوتر تنظیم می‌شود روی همه‌ی کاربرانی که به آن کامپیوتر Logon می‌کنند، نیز تاثیر می‌گذارد. در صورتی که تنظیمات امنیتی (Policy) را برای یک کاربر تعیین کنیم تاثیری روی بقیه‌ی کاربران کامپیوتر ندارد و اگر این تنظیمات را برای کاربر شبکه تعریف کنیم، دیگر مهم نیست کاربر روی کدام کامپیوتر Logon کند.

۱-۶ محافظت از سیستم Security policy

Security policy در ویندوز XP بر دو نوع می‌باشد: Local Security Policy و Group Policy که ما در این بخش به نوع Local آن می‌پردازیم.

۱-۶ تنظیمات امنیتی محلی (Local security policy)

با استفاده از Security Policy، می‌توانید تعداد زیادی تنظیمات امنیتی روی یک کامپیوتر محلی از قبیل: عضویت گروه‌ها، مجوزها، الزامات کلمه عبور، تنظیمات میز کار و را پیاده کنید.

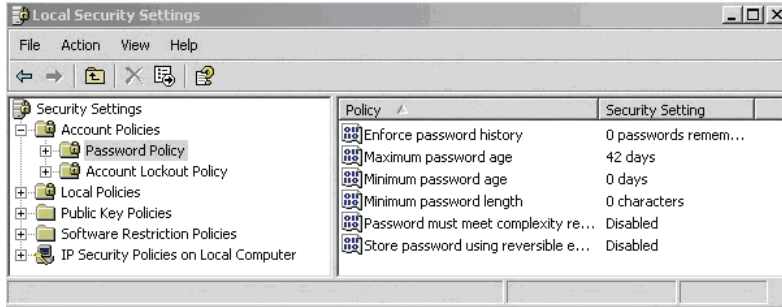


شکل ۱-۶ پنجره تنظیمات Local Security

۲-۱-۶ آشنایی با امکانات سیستم عامل ویندوز برای محافظت از سیستم

ویندوز XP، امکان پیکربندی تنظیمات امنیتی را با استفاده از Local Security Policy فراهم می‌سازد که به دو نمونه اشاره می‌کنیم:

- **Account policies:** این تنظیمات شامل سیاست‌های کلمه عبور از قبیل حداقل طول کلمه رمز و تنظیمات قفل کردن حساب می‌باشد.



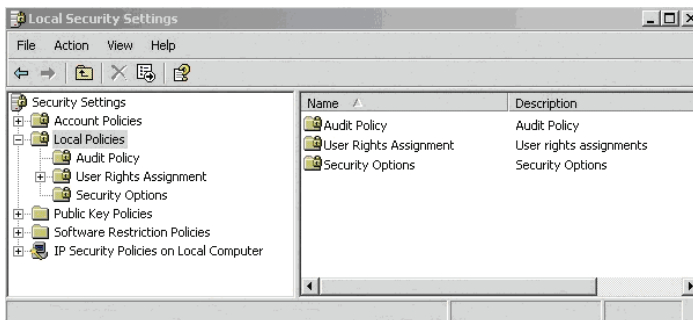
شکل ۶-۲ سیاست‌های کلمه عبور

- **Local policies:** شامل ۳ زیر گروه می‌باشد:
 - **Auditing polices:** امکان پیگیری فعالیت کاربران و دسترسی به منابع را در کامپیوتر فراهم می‌سازد، مانند رسیدگی به مدیریت حساب کاربری، رسیدگی به رویداد Logon و...
 - **User rights Assignment:** این گزینه امکان کنترل وظایف اصلی سیستم را که یک کاربر می‌تواند انجام دهد، فراهم می‌کند. مانند دسترسی به کامپیوتر از طریق شبکه، پشتیبان‌گیری از فایل‌ها و پوشه‌ها و... را فراهم می‌کند.
 - **Security options:** امکان تنظیمات امنیتی متفاوتی را در ویندوز XP فراهم می‌کند، که به آن می‌پردازیم.

۳-۱-۶ پیکربندی Security options

مراحل زیر را دنبال کنید:

- ۱- از منوی Start روی Control Panel کلیک کنید.
- ۲- در پنجره Control Panel، روی آیکن Administrative Tools کلیک کنید.
- ۳- در پنجره Administrative tools روی Local security policy دابل کلیک کنید.



شکل ۶-۳ پنجره تنظیمات Local Security



۴- در سمت راست پنجره روی علامت (+) کنار Local Policies کلیک کنید و گزینه Security Options را انتخاب نمایید (شکل ۳-۶).



شکل ۴-۶ انتخاب گزینه Security options

همان‌طور که در شکل می‌بینید نزدیک به ۶۰ گزینه امنیتی موجود است که در گروه‌های مختلف اعم از Accounts، Audit، Devices و دسته‌بندی شده‌اند (شکل ۴-۶). به‌عنوان مثال به چند نمونه اشاره می‌کنیم:

توضیح	Security option
فعال یا غیرفعال کردن حساب Guest	Accounts:guest account status
یک نام متفاوت برای حساب کاربری مدیر مشخص می‌کند. به این ترتیب تشخیص آن برای کاربران غیرمجاز مشکل می‌شود و امنیت افزایش می‌یابد.	Accounts:Rename Administrator Account
می‌توانید ویندوز را طوری پیکربندی کنید که درایوهای تأیید نشده را: ۱- اجازه نصب دهد (Silently succeed). ۲- اجازه نصب بدهد اما به کاربر هشدار دهد (Warn but allow installation). ۳- اجازه نصب ندهد (Don't allow installation).	Devices: Unsigned Drive Installation Behavior
این گزینه مشخص می‌کند که فشردن کلیدهای ترکیبی Ctrl+ Alt+ Del قبل از این که کاربر بتواند به سیستم Logon کند، الزامی است؟	Interactive logon: do not require Ctrl+ Alt+ DEL
یک پیغام برای کاربر در هنگام Logon نشان می‌دهد.	Interactive logon: message text for user attempting to logon
مشخص می‌کند که نام آخرین کاربری که به کامپیوتر وارد شده است، در کادر Logon to windows نشان داده‌شود یا خیر؟	Interactive logon: do not display last user name
تعیین می‌کند که می‌توان بدون وارد شدن به سیستم‌عامل ویندوز، کامپیوتر را خاموش کرد. فعال بودن این گزینه موجب در دسترس قرار گرفتن دستور Shut down در صفحه اول (Log on) می‌شود.	Shut down: allow system to be shut down without having to logon



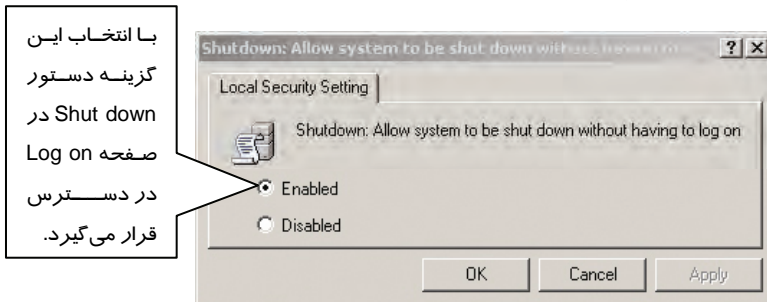
مثال ۶-۱



کامپیوتر را طوری تنظیم کنید که دستور Shut down در صفحه Log on قابل دسترس باشد.

مراحل زیر را دنبال کنید:

- ۱- از منوی Start روی Control Panel کلیک کنید.
- ۲- در پنجره Control Panel روی Administrative Tools (Administrative Tools) دابل کلیک کنید.
- ۳- در پنجره Administrative tools روی گزینه Local Security Policy دابل کلیک کنید.
- ۴- از قسمت Local Policies روی علامت (+) کلیک نمایید و گزینه Security Option را انتخاب کنید.
- ۵- در سمت راست این پنجره، روی گزینه Shut down: allow system to be shut down without having to logon در سمت راست کلیک نمایید و Properties را انتخاب کنید.
- ۶- گزینه Enabled را انتخاب کرده و روی دکمه OK کلیک کنید (شکل ۵-۶).



شکل ۵-۶ انتخاب Enabled

نکته: تنظیماتی که در ابزار Local security Settings، صورت می گیرد بلافاصله اعمال می شوند و نیازی به ذخیره تغییرات نیست. البته بیشتر تنظیمات، تأثیر خود را در Log on بعدی کاربر نشان می دهند.



۶-۲ پیکربندی دیوار آتش و Proxy

دیوار آتش (Firewall) یک نرم افزار است که شبکه را از نفوذ بیگانگان، کاربران غیرمجاز و مهاجمین حفظ می کند. یک شرکت را با ۵۰ کامپیوتر در نظر بگیرید که کاربران این شرکت هر روز باید به اینترنت دسترسی داشته باشند ولی در عین حال نمی خواهند که کاربران دیگر در اینترنت بتوانند به اطلاعات محرمانه موجود در



کامپیوترهای شرکت دست پیدا کنند. در این صورت استفاده از دیواره آتش (Firewall) سیستم را حفظ می‌کند.

دیواره‌های آتش برای کنترل و بررسی ترافیک ورودی و خروجی به روش‌های مختلفی از شبکه استفاده می‌کنند. بر اساس مقرراتی که به وسیله مدیران شبکه وضع می‌گردد بعضی از انواع ترافیک اجازه ورود به شبکه را دارند. به عبارت دیگر هر گونه اجازه ورود به شبکه خصوصی باید با نظارت دیواره آتش انجام گیرد...

نکته:



- Firewall به عنوان یک سیستم امنیتی بر روی کامپیوتر عمل می‌کند به طوری که یک دیوار ما بین کامپیوتر و شبکه یا اینترنت ایجاد می‌کند. ضمناً کامپیوتر را از ویروس‌ها، هکرها و سایر فعالیت‌های مغرضانه محافظت می‌کند.
- Firewall روی سیستم عامل ویندوز با Service pack 2 نصب می‌شود.

۱-۲-۶ فعال یا غیر فعال کردن Windows firewall

تنها کاربرانی که عضو گروه Administrators هستند می‌توانند تنظیمات Firewall را تغییر دهند. برای فعال کردن Firewall مسیر زیر را دنبال کنید:

- (۱) از منوی Start روی Control Panel کلیک کنید.
- (۲) در پنجره Control Panel روی Windows Firewall دابل کلیک کنید.
- (۳) در زبانه‌ی General، گزینه (On (Recommended) را برای فعال کردن Firewall کلیک کنید. (در صورتی که روی گزینه Off کلیک کنید، Firewall غیر فعال می‌شود.)

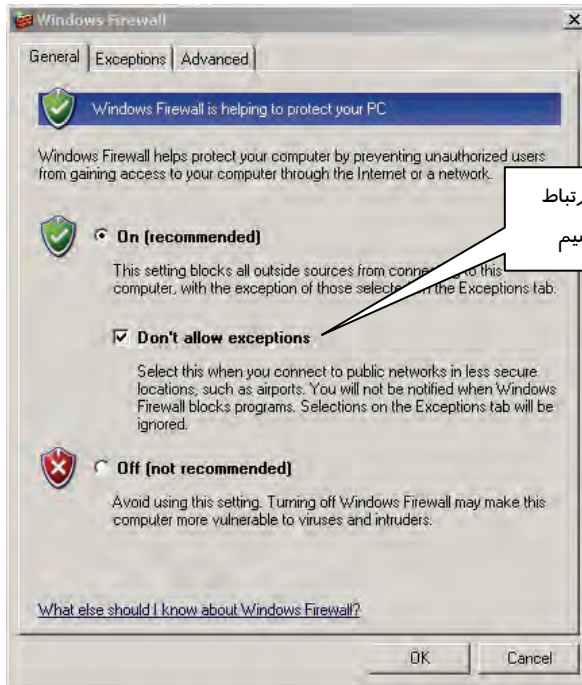


شکل ۶-۶ فعال کردن Firewall



مثال ۲-۶ در صورتی که در فضای ارتباط شبکه‌ای بی‌سیم قرار گرفته باشید، برای حفظ امنیت، Firewall را در چه وضعیتی قرار می‌دهید؟

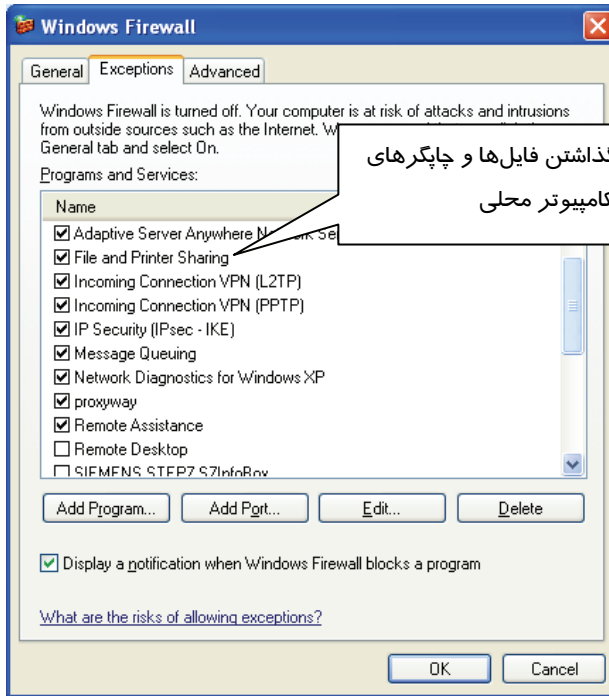
پاسخ: چون در این حالت، هیچ‌گونه نظارتی بر منابع خارجی نیست، برای این کار در زبانه General پنجره Firewall گزینه دوم Don't allow exceptions را انتخاب می‌کنیم (شکل ۶-۷).



شکل ۶-۷ انتخاب گزینه Don't allow exceptions

۲-۶ اجازه ورود برای یک سرویس یا یک برنامه (Exception)

به‌طور پیش‌فرض Firewall، تمام ترافیک‌های ناخواسته (مانند نفوذ هکرها) را مسدود می‌کند. شما می‌توانید استثنایهایی (Exception) ایجاد کنید که به نوع خاصی از ترافیک اجازه عبور از Firewall را بدهد. به‌عنوان مثال اگر می‌خواهید فایل‌ها و چاپگرهای خود را در یک کامپیوتر محلی به اشتراک بگذارید، باید گزینه File and printer sharing را در زبانه Exceptions فعال کنید (شکل ۶-۸).



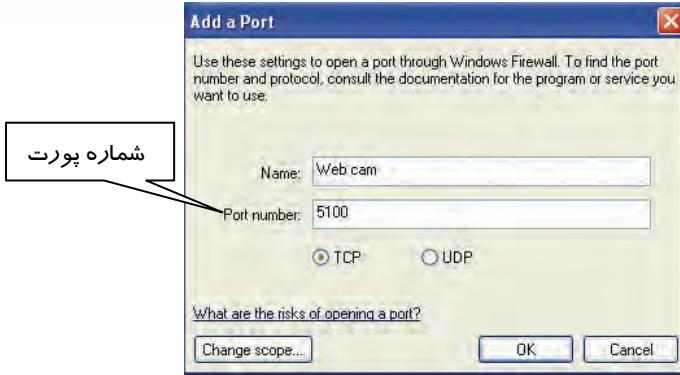
شکل ۸-۶ انتخاب برنامه‌های مورد استثناء

آیا می‌دانید که ...

اگر برنامه مورد نظر شما در قسمت Program and services از زبانه‌ی Exception وجود نداشته باشد، چه عملی انجام می‌دهید؟ با کلیک بر روی دکمه‌ی Add Program نام برنامه‌ی مورد نظر خود را از لیستی که ظاهر می‌شود، انتخاب کنید.

برخی از برنامه‌های کاربردی شامل سرویس‌های خاصی هستند که این سرویس‌ها برای ارتباط با سرویس‌دهنده‌ی خود از درگاه (پورت) های خاصی استفاده می‌کنند. مثلاً برای استفاده از Webcam در برنامه‌ی Yahoo Messenger باید پورت شماره ۵۱۰۰ از نوع TCP را روی رایانه‌ی خود باز نمایید. برای این کار مراحل زیر را دنبال کنید:

۱- در زبانه‌ی Exception از پنجره‌ی Windows Firewall، روی دکمه‌ی Add Port کلیک کنید (شکل ۸-۶).



شکل ۹-۶ باز کردن پورت

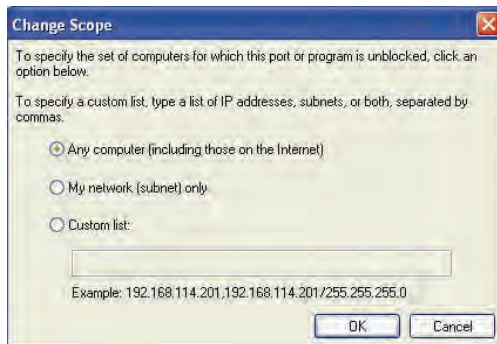
۲- در پنجره Add a Port، نام پورت و شماره آن را وارد نمایید، سپس نوع پورت را تعیین کنید و در نهایت روی دکمه OK کلیک کنید. (جهت امنیت بیشتر از حالت TCP استفاده می گردد).

آیا می دانید که ...



تفاوت TCP با UDP چیست؟ به طور خلاصه باید گفت که در ارسال اطلاعات در حالت UDP، امنیت و ارسال صحیح اطلاعات به مقصد مهم نیست. مانند ارسال یک فیلم که اگر قسمت‌هایی از آن هم به مقصد نرسد با توجه به صحنه‌های قبل و بعد آن قابل حدس زدن است. اما در TCP، امنیت و ارسال سالم اطلاعات از اهمیت برخوردار است. مانند ارسال پیام در Email.

۳- بعد از وارد کردن شماره پورت، باید میدان یا محدوده‌ای که این پورت باید در آن فعال باشد را تعیین کنید تا از دسترسی غیرمجاز به رایانه‌ی شما جلوگیری شود. روی دکمه Change Scope کلیک کنید (شکل ۹-۶).



شکل ۱۰-۶ انتخاب محدوده برای پورت

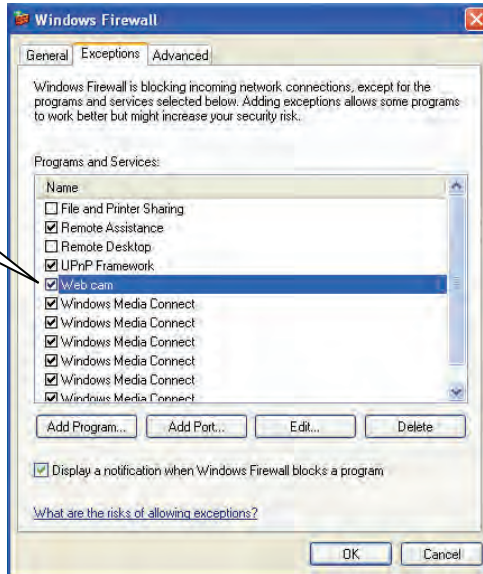
طبق شکل سه حالت برای انتخاب محدوده وجود دارد:



- **Any Computer**: تمامی رایانه‌هایی که با سیستم شما متصل در ارتباط هستند، می‌توانند از این پورت استفاده نمایند یا این پورت برای تمام رایانه‌هایی که با سیستم شما در ارتباطند باز است.
- **My Network**: فقط رایانه‌های داخل شبکه شما، که کلاس و محدوده IP آدرسشان با رایانه‌ی شما سازگار است، می‌توانند از این پورت استفاده نمایند.

- **Custom List**: می‌توان برای یک محدوده خاص از IP تعیین نمود که از این پورت استفاده نمایند.

روی دکمه OK کلیک کنید.



اضافه شدن سرویس Webcam

شکل ۱۱-۶ اضافه شدن سرویس Webcam به لیست استثناء

- ۴) همان‌طور که در شکل می‌بینید، سرویس Webcam به لیست برنامه‌های استثناء اضافه شد. روی دکمه‌ی OK کلیک کنید (شکل ۱۱-۶).

نکات مهم در باز کردن پورت:



فقط پورتهایی را باز کنید که به آنها نیاز دارید.
هرگز برنامه‌ها یا پورتهایی را که برایتان ناشناس هستند را باز نکنید.
برنامه‌ها یا پورتهایی را که برای مدت طولانی به آنها نیاز ندارید، همواره بسته نگاه دارید.



۳-۲-۶ وب پراکسی (Web proxy)

Proxy Server دسترسی به اینترنت را برای Client های موجود در شبکه فراهم می کند.

هدف استفاده از Proxy Server به شرح زیر است:

- ۱- اتصال به اینترنت را متمرکز می کند.
 - ۲- منابعی که کاربران به آن دسترسی دارند را کنترل می کند و به این ترتیب امنیت را افزایش می یابد.
 - ۳- سرعت دسترسی به اینترنت را افزایش می دهد.
- Internet Explorer دستیابی به اینترنت را از Proxy Server درخواست می کند. وقتی که Proxy Server از طرف Client به منابع اینترنت حقیقی دسترسی پیدا کرد، اطلاعات را دریافت می کند و برای Client ارسال می نماید. از مزایای وب پراکسی می توان به موارد زیر اشاره کرد:

- تعیین میزان دسترسی کاربران به اینترنت
- تهیه گزارش از سایت هایی که کاربر از آن ها بازدید کرده است.
- جلوگیری از نفوذ و دسترسی کاربران سایر شبکه ها به شبکه داخلی
- نگهداری اطلاعات وب بر روی دیسک سخت که باعث بالا بردن سرعت استفاده از اینترنت و کاهش ترافیک شبکه می شود.

۱-۳-۲-۶ پیکربندی Internet Explorer جهت استفاده از یک Proxy Server

برای تنظیم Proxy مسیر زیر را دنبال کنید:

- ۱- مرورگر وب (Internet Explorer) را باز کنید.
- ۲- از منوی Tools، گزینه Internet Option را انتخاب کنید (شکل ۱۲-۶).

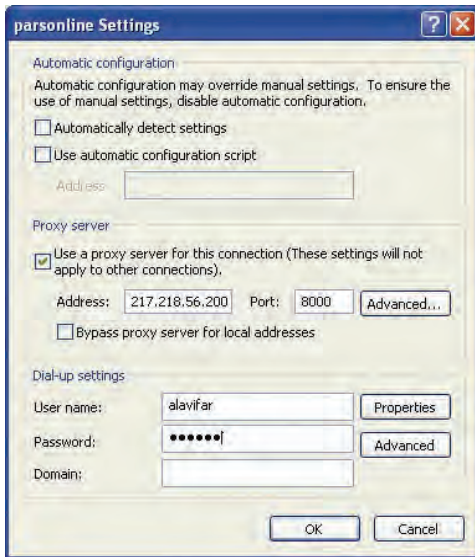


شکل ۱۲-۶ انتخاب Internet option

- ۳- روی زبانه‌ی Connection کلیک نمایید و از قسمت Dialup and virtual private network setting Connection مورد نظر را انتخاب کنید و سپس روی دکمه Setting کلیک کنید (شکل ۱۳-۶).



۴- در پنجره Setting، در قسمت Proxy Server گزینه Use a proxy server for this connection را انتخاب نمایید و آدرس IP، (به عنوان مثال 217.218.56.200) و پورت (به عنوان مثال ۸۰۰۰) را وارد کنید (شکل ۱۴-۶).



شکل ۱۴-۶ انتخاب پراکسی



شکل ۱۳-۶ انتخاب Connection

۵- تمامی پنجره‌ها را OK کنید و از آن‌ها خارج شوید. اکنون Proxy تنظیم شده است.

۳-۶ زبان تخصصی

Windows firewall

Windows firewall is turned on by default for all internet and network connections. However, some computer manufacturers and network administrators might turn it off.

Windows firewall is turn on by default, so you can not use some features of some types of programs, unless the program is listed on the exceptions tab in window firewall for example, you might not be able to send photos using an instant messaging. Program until you add the program to the exceptions list.



با توجه به متن به پرسش‌های زیر پاسخ دهید.

1. Which sentence is NOT correct?
 - a) Most of the computer manufacturers turn windows firewall on.
 - b) Some of the computer manufacturers turn windows firewall off.
 - c) You can use some features of some programs if Windows firewall is turned on.
 - d) You might not be able to send photos using an instant messaging.
2. According to the text you can use some features of some programs if...
 - a) The program isn't listed on the exceptions tab in window firewall.
 - b) The program is listed on the exceptions tab.
 - c) Both
 - d) None
3. Why can't you be able to send photos using an instant messaging program?
 - a) Because the program isn't added to the exceptions list
 - b) Because the program is added to the exceptions list.
 - c) Because Firewall is turned off.
 - d) None



- می‌توانید کاربران را قبل از این‌که بتوانند به سیستم Log On کنند، وادار به فشردن کلیدهای Alt+Ctrl+Delete کنید. این امر از برداشتن کلمه رمز توسط یک برنامه مخرب جلوگیری می‌کند.
- می‌توانید از خاموش شدن سیستم توسط کاربران غیرمجاز، به وسیله وادار کردن به Log On قبل از این‌که بتوانند کامپیوتر را خاموش کنند، جلوگیری نمایید.
- Windows firewall نرم‌افزاری است که در ویندوز XP با Service Pack 2 وجود دارد و سبب می‌شود تمام ترافیک‌های ورودی بسته شوند مگر آن‌هایی که اجازه ورود داشته باشند.
- با ایجاد یک Exception برای یک سرویس یا برنامه مجوز عبور از Firewall خواهید گرفت.
- بعضی از برنامه‌های کاربردی شامل سرویس‌های خاصی هستند که این سرویس‌ها برای ارتباط با سرویس دهنده‌ی خود از درگاه (پورت) های خاصی استفاده می‌کنند.
- Proxy server یک سرور است که به نوعی وظیفه محافظت از سیستم را به عهده دارد و قابل تنظیم است.



آزمون تئوری

گزینه‌ی صحیح را انتخاب کنید.

- ۱- انواع Security Policy عبارتند از:
- الف) Local Security Policy
ب) Group Policy
ج) Network Security
د) پاسخ های الف و ب
- ۲- زیر گروه‌های Local Policy کدامند؟
- الف) Security option, User rights, Auditing
ب) User right, Account
ج) Security Option, Auditing
د) Security Option, Account
- ۳- تنظیمات صورت گرفته در Local Security Policy چه موقع تاثیر می‌گذارند؟
- الف) بعد از ذخیره تنظیمات تاثیر می‌گذارد.
ب) بلافاصله اعمال می‌شوند و نیازی به ذخیره تغییرات نیست.
ج) در Logon بعدی کاربر تاثیر می‌گذارد.
د) پاسخ های ب و ج
- ۴- انواع حالت‌های Scope در پورت عبارتند از:
- الف) Any Computer و Custom list
ب) My Network
ج) My Computer
د) پاسخ های الف و ب
- ۵- در کدامیک از حالت‌ها ارسال صحیح اطلاعات مد نظر است؟
- الف) UDP
ب) TCP
ج) UDP & TCP
د) Email

درستی یا نادرستی عبارتهای زیر را تعیین کنید.

- ۶- Firewall به عنوان یک مرز بین کامپیوتر و شبکه اینترنت عمل می‌کند.
- ۷- Firewall روی تمام سیستم‌عامل‌های ویندوز با هر نسخه‌ای وجود دارد.
- ۸- اگر بخواهید به بعضی از برنامه‌ها، در ارتباطات شبکه‌ای اجازه عبور دهید، آن را در قسمت Exception معرفی می‌کنید.

معادل گزینه‌های سمت راست را از ستون سمت چپ انتخاب کرده و مقابل هر عبارت بنویسید.

- ۹- کامپیوتر واسط بین سیستم شبکه محلی و اینترنت
- a) Exception



- b) Security Option
- c) Internet Explorer
- d) User Right
- e) Account Policy
- f) Proxy Server

۱۰- مرورگر وب

۱۱- استثناء

۱۲- کنترل تنظیمات امنیتی متفاوت در XP

۱۳- تنظیمات حداقل طول کلمه رمز

در جای خالی عبارت مناسب بنویسید.

- ۱۴- اجازه کنترل وظایف اصلی سیستم که یک کاربر می‌تواند انجام دهد بر عهده زیر گروه می‌باشد.
- ۱۵- به مجموعه‌ای از تنظیمات که روی کامپیوتر یا یک کاربر تاثیر می‌گذارند گویند.
- ۱۶- Auditing Policy امکان پیگیری فعالیت کاربران و دسترسی به در کامپیوتر را فراهم می‌کند.

به پرسش‌های زیر پاسخ تشریحی دهید.

- ۱۷- مزایای وب پراکسی را نام ببرید.
- ۱۸- برای تنظیمات Proxy، چه اطلاعاتی لازم است؟
- ۱۹- Firewall در کدام سیستم‌عامل‌های XP وجود دارد؟

آزمون عملی

- ۱- حساب کاربری Guest را غیرفعال کنید.
- ۲- برنامه Messenger خود را جزء استثناء تعریف کنید.
- ۳- یک پیغام خوشامدگویی به دلخواه خود در هنگام Logon کاربر طراحی کنید.
- ۴- بررسی کنید که دستور Shut down قبل از ورود به سیستم عامل، در صفحه Logon وجود داشته باشد.
- ۵- روی یک سیستم خاص مثلا Client 2، یک پوشه را به اشتراک بگذارید، سپس دسترسی به آن را از روی سیستم‌های دیگر در دو حالت زیر بررسی نمایید:
الف) Firewall در حالت ON باشد و گزینه File and printer sharing در قسمت استثناء انتخاب نباشد.
ب) Firewall در حالت Off باشد.

.....

.....

.....

.....

.....

.....



فصل هفتم

هدف کلی فصل:

توانایی اعمال محدودیت در حساب کاربری

اهداف رفتاری (جزئی)

- پس از مطالعه‌ی این فصل، از فراگیر انتظار می‌رود که:
- با امکانات 'سیستم فایل' NTFS آشنا شود.
 - فایل‌ها و پوشه‌ها را رمزگذاری و فشرده نماید.
 - یک حساب کاربری با محدودیت‌های امنیتی ایجاد کند.
 - انواع مجوزهای حساب کاربری را بشناسد و به کار برد.
 - حساب کاربری را به‌عنوان عضوی از یک گروه قرار دهد.

زمان (ساعت)

تئوری	عملی
۴	۶



مقدمه

در این فصل نحوه‌ی تصمیم‌گیری راجع به استفاده از سیستم فایل FAT و NTFS، رمزگذاری و فشرده‌سازی فایل‌ها و پوشه‌ها، ایجاد یک حساب کاربری با محدودیت‌های امنیتی و تعیین عضویت حساب کاربری به یک یا چند گروه را به طور کامل فرا خواهید گرفت.

۱-۷ آشنایی با امکانات سیستم‌فایل NTFS

سیستم‌فایل اطلاعاتی است که با استفاده از آن می‌توان مکان ذخیره‌ی فایل‌ها و پوشه‌ها در یک پارتیشن و مقدار فضای آزاد دیسک را پیگیری نمود. وظیفه‌ی سیستم‌فایل به‌طور خلاصه ساماندهی اطلاعات می‌باشد. بدون یک سیستم‌فایل، ویندوز XP نمی‌تواند اطلاعات را ذخیره کند. سیستم‌های فایل عبارتند از: FAT (FAT16, FAT32) و NTFS که در فصل اول با آن آشنا شده‌اید. NTFS در ویندوزهای XP، 2000، و سرور 2003 پشتیبانی می‌شود.

نکته: با تبدیل FAT16 و FAT32 به NTFS، اطلاعات موجود بر روی درایو حفظ می‌شود ولی در تبدیل NTFS به FAT16 یا FAT32، باید درایو را فرمت کرد که این کار سبب حذف اطلاعات موجود بر روی درایو خواهد شد.

مزیت‌های NTFS به‌طور خلاصه به‌صورت زیر می‌باشد:

- NTFS به شما اجازه‌ی کنترل و دسترسی به فایل‌ها و پوشه‌ها را می‌دهد.
- NTFS می‌تواند فایل‌ها را فشرده کند تا اطلاعات بیشتری را درون یک پارتیشن نگهداری کنید.
- NTFS این امکان را می‌دهد که اطلاعات موجود در دیسک سخت را رمزگذاری کنید.
- NTFS می‌تواند از فضای بزرگ‌تر پارتیشن‌ها پشتیبانی کند. به‌عنوان مثال، برای ایجاد پارتیشن‌های بزرگ‌تر از ۳۲ گیگابایت (GB) در ویندوز XP، حتماً باید از سیستم‌فایل NTFS استفاده نمایید.
- NTFS یک یادداشت متنی از تمام فعالیت‌ها را نگهداری می‌کند، بنابراین می‌تواند پس از این که سخت‌افزاری خراب شد یا برق دستگاه قطع شد دیسک را به حالت اولیه برگرداند، در حالی که FAT تمامی داده‌ها را از دست می‌دهد.

نکته: تنها دلیل استفاده از FAT16 یا FAT32 استفاده از سیستم‌عامل دیگری در کنار ویندوز XP است که با NTFS سازگاری ندارد.

به‌عنوان مثال اگر می‌خواهید که در دیسک C سیستم‌عامل ویندوز ۹۸ نصب کنید باید قالب‌بندی دیسک C، Fat16 یا FAT32 باشد و پارتیشنی که ویندوز XP در آن نصب می‌شود با NTFS قالب‌بندی شود.



۷-۲ اصول رمز گذاری فایل‌ها (EFS) Encrypting File System

EFS به شما این اطمینان را می‌دهد که کسی نتواند فایل‌های رمز گذاری شده‌ی شما را بخواند. نام کاربری و کلمه عبور سیستم شما برای رمز گذاری فایل در نظر گرفته می‌شود بنابراین اگر کسی نام کاربری و کلمه عبور شما را بداند تمام این مزایا از بین می‌رود و ویندوز XP فایل‌های رمز گذاری شده را برای او باز خواهد کرد. بنابراین ضروری است که کسی از کلمه عبور شما آگاه نباشد.

مزیت رمز گذاری

با رمز گذاری فایل، مدیر سیستم و حساب کاربری که فایل را رمز گذاری کرده است، امکان انجام عملیات زیر را خواهد داشت:

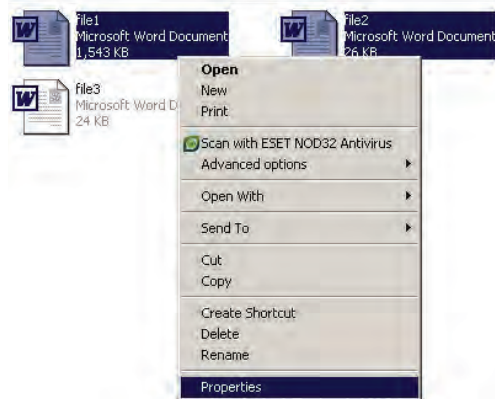
۱- محتویات فایل را مشاهده، حذف و یا تغییر دهد.

۲- نام فایل را تغییر دهد.

۳- فایل را به محل دیگر کپی کند یا انتقال دهد.

اگر کاربری با حساب کاربری دیگری Log on شود، حتی اگر Administrator هم باشد بدون داشتن رمز نمی‌تواند این فایل‌ها را باز کند، کپی کند و یا تغییر دهد. اگر کاربری اختیار کامل داشته باشد، فقط می‌تواند نام فایل را تغییر دهد.

نکته: فایل مورد نظر برای رمز گذاری باید در درایوی که سیستم‌فایل آن NTFS است، قرار داشته باشد.

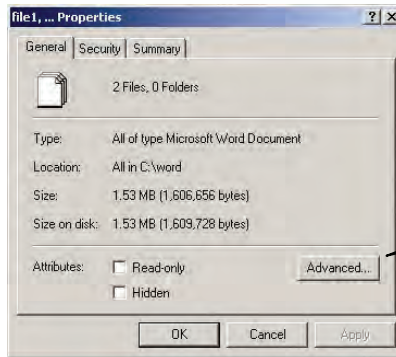


شکل ۷-۱ رمز گذاری فایل

برای رمز گذاری فایل به ترتیب زیر عمل کنید:

- ۱- بر روی فایل‌های مورد نظر (شکل ۷-۱)، راست کلیک کنید، گزینه‌ی Properties را انتخاب نمایید (در اینجا پارتیشن C دارای سیستم‌فایل NTFS است).

۲- در پنجره‌ی Properties، در زبانه‌ی General بر روی گزینه‌ی Advanced کلیک نمایید (شکل ۷-۲).



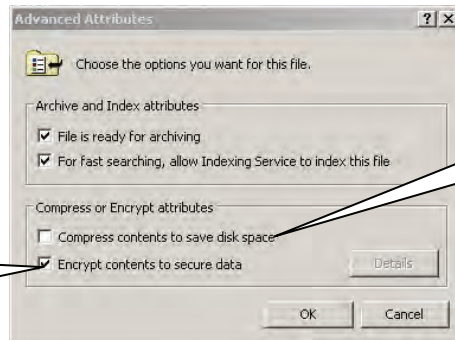
برای رمزگذاری یا فشرده سازی فایل یا پوشه بر روی این دکمه کلیک کنید.

شکل ۲-۷ پنجره Properties فایل های انتخابی

پنجره‌ی Advanced Attributes (شکل ۳-۷) ظاهر می‌گردد.

۳- در قسمت Compress or Encrypt attributes، گزینه‌ی Encrypt contents to secure data را انتخاب کنید با انتخاب این گزینه، سیستم‌عامل محتویات فایل یا پوشه را محرمانه تلقی می‌کند و آن را رمزگذاری می‌نماید.

۴- بر روی دکمه‌ی OK کلیک کنید.



فشرده سازی پوشه جهت ذخیره کردن روی دیسک

با انتخاب این گزینه، فایل یا پوشه رمزگذاری می‌گردد.

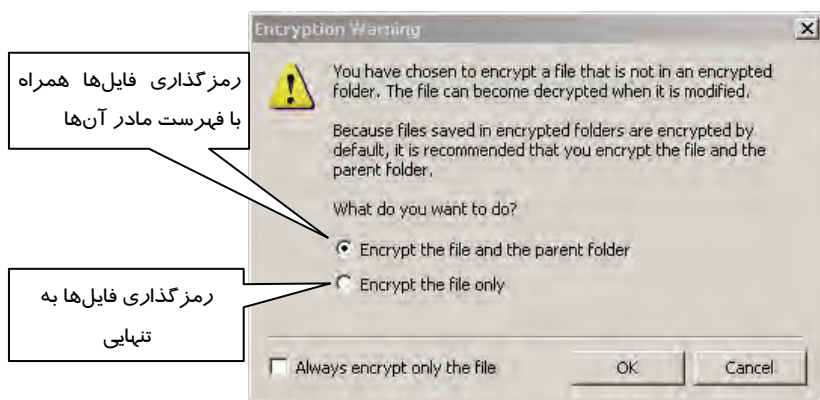
شکل ۳-۷ رمزگذاری فایل یا پوشه

چون فایل‌هایی که می‌خواهند رمزگذاری شوند درون یک پوشه قرار دارند، کادری به شکل (۴-۷) ظاهر می‌شود که شامل دو گزینه‌ی زیر می‌باشد:

- **Encrypt the file and the parent folder**: با انتخاب این گزینه فایل‌ها همراه با فهرست مادر آن‌ها (در این مثال فهرست والد، پوشه‌ی Word است) رمزگذاری می‌شوند.
- **Encrypt the file only**: اگر می‌خواهید فقط فایل‌های انتخابی رمزگذاری شوند این گزینه را انتخاب کنید.

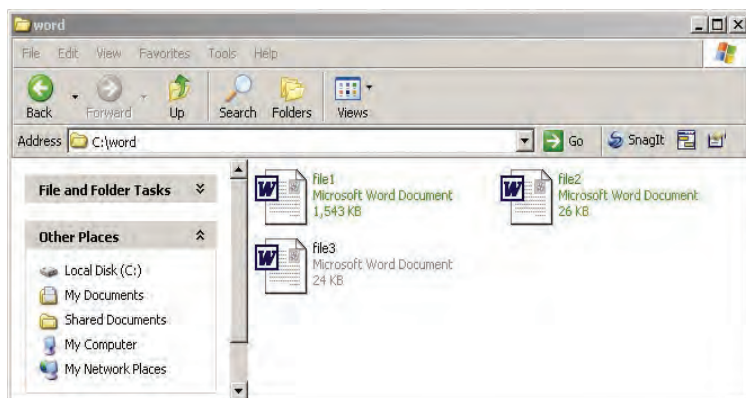


۶- گزینه‌ی اول را انتخاب و بر روی دکمه‌ی OK کلیک نمایید (در این مثال با انتخاب گزینه‌ی اول، پوشه‌ی Word نیز رنگی نمایش داده می‌شود ولی این پوشه نمی‌تواند به طور کامل رمزگذاری شود، چون پوشه‌ی Word شامل یک فایل رمزگذاری نشده است).



شکل ۴-۷ انتخاب نوع رمزگذاری

مشاهده می‌کنید که فایل‌های رمزگذاری شده به رنگ سبز نمایش داده می‌شوند (شکل ۵-۷).



شکل ۵-۷ فایل‌های رمزگذاری شده به رنگ سبز نمایش داده می‌شوند

• نکاتی در مورد رمزگذاری فایل‌ها

- ۱- هنگامی که فهرستی رمزگذاری شد، همه‌ی زیرفهرست‌ها و فایل‌های موجود در آن فهرست نیز رمزگذاری می‌شوند.
- ۲- کپی یک فایل یا پوشه فاقد رمز به پوشه‌ای که رمزگذاری شده، آن فایل یا پوشه را رمزگذاری می‌کند.
- ۳- امکان رمزگذاری فایل‌های سیستمی وجود ندارد



- ۴- پوشه My Document را رمز گذاری نکنید چون اگر مجبور شوید به دلیل برخی مشکلات، ویندوز را دوباره بارگذاری کنید، اسناد شما غیر قابل استفاده خواهد شد.
- ۵- یک پوشه بسازید و سپس هر فایل یا فهرستی که مایل هستید از آن پشتیبانی کنید، داخل این پوشه قرار دهید سپس آن را رمز گذاری کنید.
- ۶- اگر فایلی فشرده شود رمز گذاری نمی‌شود همچنین اگر فایلی را رمز گذاری نمایید دیگر نمی‌توانید آن را فشرده کنید.
- ۷- اگر فایل یا فهرستی که رمز گذاری شده است را به دراپوی با سیستم فایل FAT کپی کنید، از حالت رمز گذاری خارج می‌شود.

۳-۷ فشرده‌سازی فایل‌ها با استفاده از NTFS Compression

NTFS Compression یکی از عملیات سیستم‌فایل NTFS است و تنها در پارتیشن‌هایی که با NTFS قالب‌بندی شده‌است، موجود می‌باشد. فایل‌های فشرده‌ی NTFS می‌توانند بدون نیاز به آنکه به وسیله‌ی برنامه‌ی دیگری از حالت فشرده خارج شوند، به وسیله‌ی برنامه‌های تحت ویندوز خوانده یا نوشته شوند. زمانی‌که یک برنامه یا یک سیستم‌عامل درخواست دسترسی به فایل فشرده را داشته باشد، NTFS به صورت خودکار فایل را از حالت فشرده خارج و در اختیار درخواست‌کننده قرار می‌دهد و هر زمان که فایل را می‌بندید یا ذخیره می‌کنید، NTFS دوباره آن را فشرده می‌کند.

۱-۳-۷ روش فشرده سازی یک فایل یا پوشه

- برای فشرده کردن یک فایل یا پوشه به ترتیب زیر عمل کنید:
- ۱- بر روی فایل یا پوشه‌ی مورد نظر راست کلیک نمایید و گزینه‌ی Properties را انتخاب کنید.
 - ۲- بر روی دکمه‌ی Advanced کلیک کنید (طبق شکل ۲-۷).
 - ۳- در کادر Advanced Attributes گزینه Compress Contents To Save Disk Space را انتخاب و روی دکمه OK کلیک کنید (شکل ۳-۷).
 - ۴- در کادر Properties بر روی Apply کلیک کنید (طبق شکل ۲-۷).

تکته: فشرده‌سازی و رمز گذاری NTFS با یکدیگر سازگار نیستند. به همین دلیل اگر گزینه Encrypt Contents to secure Data را انتخاب کنید نمی‌توانید فایل یا پوشه را فشرده کنید.





وضعیت فشرده بودن یک پوشه تأثیری بر فایل‌ها و زیرپوشه‌های درون آن نمی‌گذارد. یک پوشه می‌تواند فشرده باشد اما فایل‌های درون آن می‌توانند به حالت غیرفشرده باشند. به این ترتیب یک پوشه فشرده نشده نیز می‌تواند حاوی فایل‌های فشرده باشد.

۵- زمانی که شما پوشه‌ای را که دارای یک یا چند فایل و پوشه است فشرده می‌کنید، ویندوز XP کادر Confirm Attribute Changes را نمایش می‌دهد (شکل ۶-۷) که شامل دو گزینه‌ی زیر می‌باشد:



با انتخاب این گزینه، فقط این پوشه فشرده می‌گردد.

با انتخاب این گزینه، این پوشه و زیر پوشه‌ها و فایل‌های درون آن فشرده می‌شود.

شکل ۶-۷ انتخاب نوع فشرده‌سازی

- **Apply changes to this folder only** : با انتخاب این گزینه فقط فایل‌های درون پوشه‌ای که انتخاب کرده‌اید، فشرده می‌شوند.
 - **Apply changes to this folder, subfolders and files** : با انتخاب این گزینه، این پوشه و فایل‌ها و پوشه‌های درون آن فشرده می‌شوند همچنین فایل‌ها و پوشه‌هایی که از این به بعد اضافه شوند نیز فشرده می‌گردد.
- ۵- گزینه‌ی دوم را انتخاب کرده و بر روی دکمه‌ی OK کلیک نمایید.
- ملاحظه می‌کنید که فایل‌هایی که فشرده شده‌اند به رنگ آبی نمایش داده می‌شوند.

۲-۳-۷ نکاتی پیرامون کپی و انتقال فایل‌ها و پوشه‌های فشرده

• کپی یک فایل داخل همان پارتیشن با فرمت NTFS

زمانی که شما یک فایل را به محلی جدید درون یک پارتیشن NTFS کپی می‌کنید فایل، وضعیت فشرده‌بودن را از پوشه‌ی مقصد به ارث می‌برد. به عنوان مثال اگر پوشه‌ی فشرده را به پوشه‌ی عادی کپی کنید، از حالت فشرده خارج می‌شود.

• انتقال یک فایل یا پوشه داخل همان پارتیشن با فرمت NTFS

زمانی که شما یک فایل را درون یک پارتیشن NTFS منتقل می‌کنید، فایل یا پوشه وضعیت فشرده‌بودن اصلی خود را نگه می‌دارد. برای مثال اگر شما یک فایل فشرده را به یک پوشه عادی منتقل کنید فایل همچنان فشرده



باقی می‌ماند. در این حالت جابه‌جایی واقعی صورت نمی‌گیرد و فقط آدرس‌ها به‌طور منطقی در جدول تخصیص فایل تغییر می‌کنند.

• کپی یک فایل یا پوشه به یک پارتیشن NTFS دیگر

زمانی که شما یک فایل یا پوشه را درون یک پارتیشن NTFS دیگر کپی می‌کنید، فایل یا پوشه وضعیت فشرده بودن را از پوشه مقصد به ارث می‌برد.

• انتقال یک فایل یا پوشه به یک پارتیشن NTFS دیگر

زمانی که شما یک فایل را درون یک پارتیشن NTFS دیگر منتقل می‌کنید، فایل یا پوشه، وضعیت فشرده بودن را از مقصد به ارث می‌برد. زیرا ویندوز در این حالت ابتدا پوشه را در مقصد کپی می‌کند و سپس از مبدأ حذف می‌کند.

• انتقال یا کپی یک فایل در یک پارتیشن با فرمت FAT

فشرده‌سازی فایل‌ها تنها در NTFS پشتیبانی می‌شود. بنابراین زمانی که شما یک فایل یا پوشه‌ای را که فشرده شده است، در یک پارتیشن FAT کپی یا منتقل می‌کنید، ویندوز XP به‌صورت خودکار فایل یا پوشه را از حالت فشرده خارج می‌کند.

• انتقال یا کپی یک فایل یا پوشه‌ی فشرده در یک دیسک فلاپی

زمانی که یک فایل یا پوشه فشرده شده را به فلاپی دیسک منتقل می‌کنید از حالت فشرده خارج می‌شود.

۳-۷ توصیه‌هایی برای فشرده‌سازی در NTFS

- فایل‌هایی که فشرده شده‌اند را در یک پوشه‌ی فشرده‌شده ذخیره نکنید. ویندوز XP سعی می‌کند فایل‌ها را فشرده کند که این کار، باعث صرف زمان بیهوده شده و فضای اشغال شده روی دیسک را کاهش نمی‌دهد.
- اطلاعات با ارزشی که به ندرت مورد استفاده قرار می‌گیرد، فشرده کنید. زیرا ویندوز XP در هنگام استفاده از فایل‌ها مجبور به غیر فشرده و فشرده کردن مجدد آن‌ها می‌شود و این امر باعث کاهش کارایی سیستم می‌شود.
- فشرده‌سازی NTFS می‌تواند زمانی که فایل‌ها کپی و منتقل می‌شوند، باعث کاهش کارایی سیستم شود. وقتی یک فایل فشرده شده کپی می‌شود ابتدا از حالت فشرده خارج شده، عمل کپی انجام گرفته و سپس فایل جدید مجدد فشرده می‌شود. بنابراین اطلاعاتی را فشرده کنید که مرتب کپی یا منتقل نمی‌شوند.

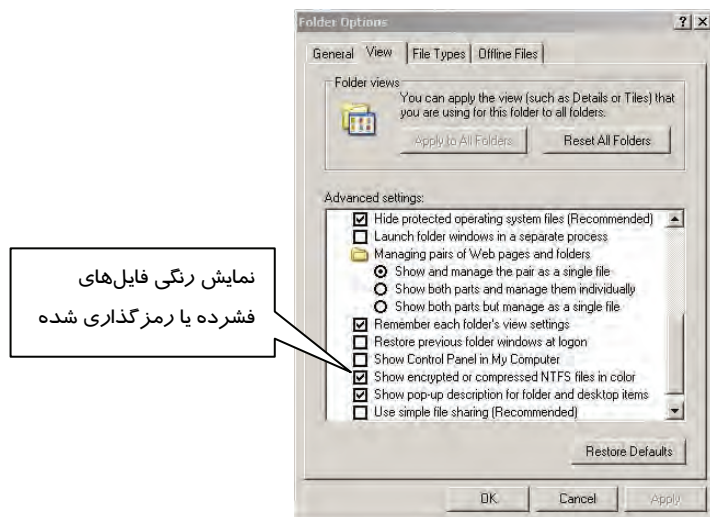
مثال ۱-۷



به روش زیر می‌توان تشخیص داد چه فایل‌ها و فهرست‌هایی در سیستم، رمزگذاری و یا فشرده شده‌اند. با نمایش رنگی فایل‌ها و فهرست‌های رمزگذاری شده و فشرده می‌توان به‌وجود آن‌ها در سیستم پی‌برد.



در پنجره‌ی Folder Options، بر روی زبانه‌ی View کلیک کنید. برای نمایش رنگی فایل‌های رمزدار و فشرده، گزینه‌ی Show encrypted or compressed NTFS files in color را انتخاب نمایید (شکل ۷-۷). در این صورت فایل‌ها یا پوشه‌هایی که رمزگذاری شده‌اند به رنگ سبز و فایل‌ها یا پوشه‌های فشرده به رنگ آبی نمایش می‌یابند.



شکل ۷-۷ برای نمایش رنگی فایل‌های فشرده یا رمزگذاری شده، گزینه اشاره شده را انتخاب کنید.

۴-۷ حفاظت داده و اعمال مجوزهای کاربری

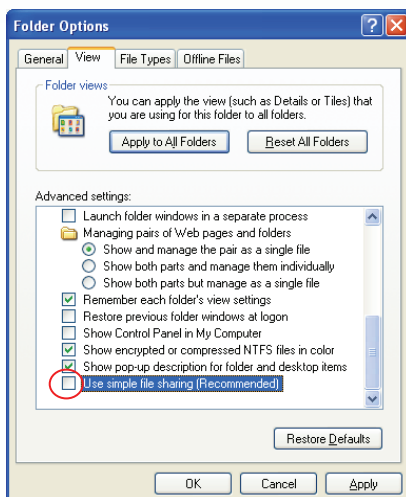
قابلیت محدود کردن دسترسی به داده، از امکانات مهم ویندوز XP حرفه‌ای می‌باشد. با تنظیم مجوزها و استفاده از کلمات عبور، می‌توان امنیت داده‌ها را افزایش داد. حتی اگر کسی وارد سیستم شود با استفاده از مجوزها می‌توان دسترسی به فایل‌ها و پوشه‌ها را محدود کرد.

۱-۴-۷ انواع مجوزها در NTFS

مجوزها کنترل می‌کنند که یک کاربر یا گروهی از کاربران با یک فایل، پوشه و غیره چه اعمالی را مجازند که انجام دهند. ویندوز زمانی از مجوزها پشتیبانی می‌کند که گزینه‌ی Use Simple File Sharing غیرفعال باشد و فایل‌ها و پوشه‌های شما در درایو NTFS باشند.

برای غیرفعال کردن گزینه‌ی Use Simple File Sharing مراحل زیر را اجرا کنید:

- ۱- در پنجره‌ی My Computer، از منوی Tools گزینه‌ی Folder Option را انتخاب کنید.
- ۲- زبانه View را انتخاب کنید، در انتهای کادر گزینه Use Simple File Sharing را غیر فعال کنید (شکل ۷-۸).



شکل ۸-۷ فعال کردن زبان Security

نکته:



با غیرفعال کردن گزینه Use Simple File Sharing ، زبان Security به کادر محاوره‌ای Properties پوشه‌ها اضافه می‌شود.

جدول ۱-۷ مجوزهای مخصوص پوشه‌ها و جدول ۲-۷ مجوزهای مخصوص فایل‌ها را نشان می‌دهد.

جدول ۱-۷ مجوز مخصوص پوشه‌ها

مجوز پوشه	اجازه انجام این عملکرد را می‌دهد یا از انجام آن جلوگیری می‌کند
Change Permission	تغییر مجوز پوشه‌ها
Create File	ایجاد فایل‌های جدید در پوشه
Create Folder	ایجاد زیرپوشه‌هایی در درون پوشه
Delete	حذف پوشه
Delete Subfolder and Files	حذف پوشه‌ها و فایل‌های موجود در پوشه، حتی اگر شما مجوزی برای فایل‌ها و زیرپوشه‌های مستقل نداشته باشید.
List Folder	نمایش اسامی فایل‌ها و پوشه‌هایی که در پوشه وجود دارد.
Read Attributes	نمایش صفات پوشه
Read Permission	خواندن مجوز پوشه
Take Ownership	گرفتن مالکیت از مالک جاری آن



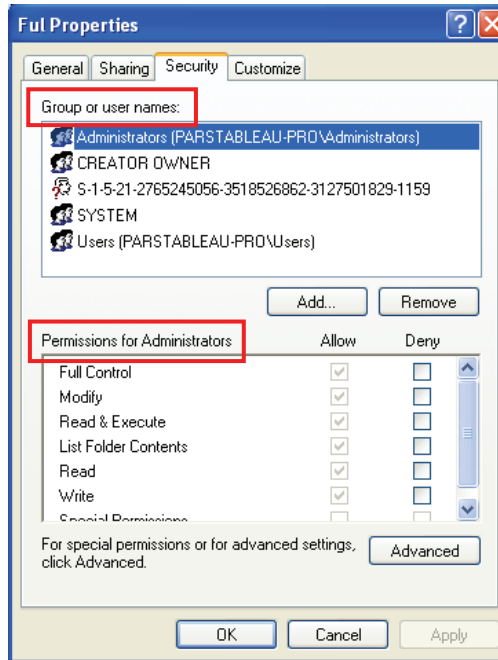
مجوز پوشه	اجازه انجام این عملکرد را می‌دهد یا از انجام آن جلوگیری می‌کند
Traverse Folder	باز کردن پوشه به منظور دسترسی به زیرپوشه‌ها و یا پوشه‌ی والد آن
Write Attribute	تغییر صفات پوشه

جدول ۲-۷ مجوز مخصوص فایل‌ها

مجوز فایل	اجازه انجام این عملکرد را می‌دهد یا از انجام آن جلوگیری می‌کند
Append Data	افزودن اطلاعات به انتهای فایل، بدون این که اطلاعات موجود تغییر کند.
Change Permission	تغییر مجوزهای فایل
Delete	حذف فایل
Execute File	اجرای برنامه‌ی موجود در فایل
Read Attributes	نمایش صفات فایل
Write Attribute	تغییر صفات فایل
Read data	نمایش محتویات فایل
Read Permission	خواندن مجوزهای فایل
Take Ownership	گرفتن مالکیت از مالک جاری آن
Write Data	تغییر محتویات فایل

برای مشاهده مجوزهای یک فایل یا پوشه (فایل یا پوشه در پارتیشنی است که دارای سیستم فایل NTFS می‌باشد) مراحل صفحه بعد را اجرا کنید:

- ۱- روی فایل یا پوشه مورد نظر کلیک راست کنید و گزینه Properties را از منو انتخاب کنید.
- ۲- از کادری که باز می‌شود، زبانه Security را انتخاب نمایید (شکل ۹-۷).



شکل ۹-۷ زبانه Security

کادر محاوره‌ای شامل دو بخش است:

- **Group or user names:** در این بخش می‌توان مشاهده کرد که چه حساب کاربری یا گروهی مجوز کار با فایل را دارد.
- **Permissions for Administrators:** در این قسمت نوع مجوزهای مربوط به گروه یا حساب کاربری که در کادر بالا انتخاب شده است را نمایش می‌دهد.
در کادر Permissions for Administrators دو گزینه به شرح زیر موجود می‌باشد:
 - **Deny:** برای لغو یک مجوز بر روی گزینه‌ی Deny کلیک کنید.
 - **Allow:** برای تخصیص یک مجوز بر روی گزینه‌ی Allow کلیک کنید.اگر گزینه‌ای کم‌رنگ باشد یعنی اجازه‌ی تغییر مجوز نخواهید داشت.
مجوزهای حساب کاربری به صورت جدول ۳-۷ می‌باشند.



جدول ۳-۷ مجوزهای نشان داده شده در کادرهای محاوره‌ای File Properties و Folder properties

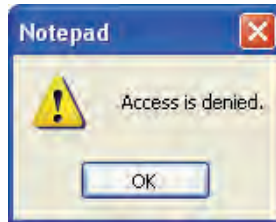
مجوز	مجوز برای پوشه‌ها	مجوز برای فایل‌ها
Full Control	تمامی عملکردها	تمامی عملکردها
Modify	Traverse Folder	Append Data
	List Folder	Read data
	Read Attributes	Write data
	Write Attribute	Write Attribute
	Create File	Read Attributes
	Create Folder	Read Permission
	Delete	Delete
	Read Permission	Execute File
Read & Excute	Traverse Folder	Read Permission
	List Folder	Read Attributes
	Read Attributes	Read data
	Read Permission	Execute File
Read	List Folder	Read Permission
	Read Attributes	Read Attributes
	Read Attributes	Read data
Write	Create File	Append Data
	Create Folder	Write data
	Write Attribute	Write Attribute
	Read Permission	Read Permission
List Folder Contents	Traverse Folder	
	List Folder	
	Read Attributes	
	Read Permission	

مثال ۲-۷



یک فایل متنی با نام Student ایجاد کنید و مجوز آن را طوری تنظیم کنید که امکان مشاهده متن درون آن نباشد. به هنگام باز کردن فایل چه پیغام خطایی مشاهده می‌کنید؟
روش اجرا به شرح زیر است:

- ۱- یک فایل متنی به نام Student در درایوی که سیستم فایل NTFS دارد، ایجاد کنید.
 - ۲- روی نام فایل کلیک راست کنید و گزینه‌ی Properties را انتخاب کنید.
 - ۳- زبانه‌ی Security را انتخاب کنید.
 - ۴- در بخش Permissions for روی مجوز Read گزینه‌ی Deny را علامت‌دار کنید و سپس OK را انتخاب کنید.
 - ۵- کادری مبنی بر تأیید ظاهر می‌شود که شما باید روی OK کلیک کنید.
- از این لحظه امکان خواندن فایل وجود ندارد. در صورت باز کردن فایل با پیغام خطای زیر مواجه می‌شوید.

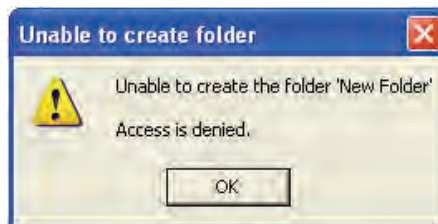


شکل ۱۰-۷ پیغام خطای دسترسی به فایل

مثال ۳-۷



- یک پوشه به نام CLASS ایجاد کنید و مجوز آن را طوری تنظیم کنید که نتوان پوشه‌ی جدید، درون آن ایجاد کرد. به هنگام ساختن پوشه جدید چه پیغام خطایی مشاهده می‌کنید؟
روش اجرا به شرح زیر است:
- ۶- یک پوشه به نام CLASS در درایوی که سیستم‌فایل NTFS دارد، ایجاد کنید.
 - ۷- روی نام پوشه کلیک راست کنید و گزینه Properties را انتخاب نمایید.
 - ۸- زبانه Security را انتخاب کنید.
 - ۹- در بخش Permissions for روی مجوز write گزینه Deny را علامت‌دار کنید و سپس OK را انتخاب کنید.
 - ۱۰- کادری مبنی بر تأیید ظاهر می‌شود که شما باید روی OK کلیک کنید.
- از این لحظه امکان ایجاد زیر پوشه وجود ندارد. در صورت ایجاد زیر پوشه با پیغام خطای زیر مواجه می‌شوید.



شکل ۱۱-۷ پیغام خطای دسترسی به پوشه

مثال ۴-۷



- یک پوشه به نام K1 ایجاد کنید به طوری که شامل یک فایل دلخواه باشد و مجوز آن را طوری تنظیم کنید که نتوان پوشه را حذف کرد. به هنگام حذف پوشه چه پیغام خطایی مشاهده می‌کنید؟
روش اجرا به شرح زیر است:
- ۱- یک پوشه به نام K1 در درایوی که سیستم‌فایل NTFS دارد، ایجاد کنید.
 - ۲- روی نام پوشه کلیک راست کنید و گزینه Properties را انتخاب کنید.
 - ۳- زبانه Security را انتخاب کنید.



- ۴- در بخش Permission for Modify روی مجوز Modify گزینه Deny را علامت‌دار کنید و سپس OK را انتخاب کنید.
- ۵- کادری مبنی بر تأیید ظاهر می‌شود که شما باید روی OK کلیک کنید.
- از این لحظه امکان حذف پوشه وجود ندارد. در صورت حذف پوشه با پیغام خطای زیر مواجه می‌شوید.



شکل ۱۲-۷ پیغام خطای دسترسی

نکته: در صورتی که پوشه خالی باشد، با وجود لغو مجوز Modify، پوشه قابل حذف است.



نکته: امنیت داده شامل حفاظت از کلمات عبور کاربران و اعطای صحیح مجوزها می‌باشد. زمانی می‌توان امنیت پوشه و فایل را برقرار نمود که فایل و پوشه در درایوی که دارای سیستم‌فایل NTFS است، قرار داشته باشند.



۵-۷ آشنایی با اعمال مجوز به حساب کاربری

- همان‌طور که می‌دانید ویندوز XP، حساب‌های کاربری (User Account) را برای حفظ امنیت در هنگام کار با سیستم‌عامل، تعریف کرده است. با استفاده از User Account می‌توان به هر نفر نوع حساب کاربری Computer Administrator یا Limited را بر حسب سطح استفاده از سیستم اختصاص داد. می‌توانید غیر از روشی که تاکنون به کار می‌بردید، یک حساب کاربری با محدودیت‌های امنیتی ایجاد کنید.
- انواع حساب‌های کاربری در ویندوز XP حرفه‌ای به صورت زیر می‌باشد:
- کاربران (Users): یک User. یک حساب کاربری بر مبنای نام کاربر و کلمه عبور می‌باشد.
 - گروه‌ها (Groups): یک گروه شامل حساب‌های کاربری می‌باشد و از آنجایی که این حساب‌های کاربری چون همگی عضو یک گروه می‌باشند، ویژگی‌های گروه را به ارث می‌برند.



مثال ۵-۷



یک حساب کاربری به نام Student ایجاد کنید.

برای ایجاد و مدیریت یک حساب کاربری، به ترتیب زیر عمل کنید:

۱- در پنجره‌ی Control Panel، بر روی آیکن Administrative Tools دابل کلیک کنید.

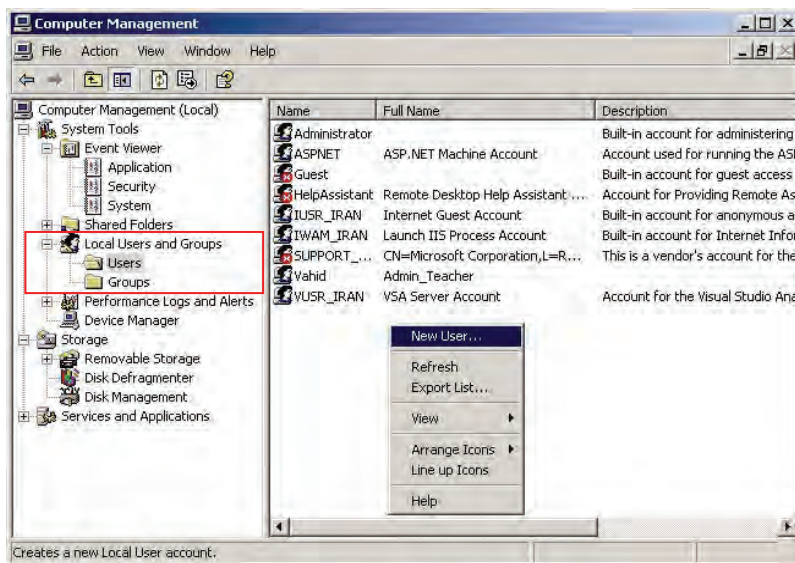


۲- گزینه‌ی Computer Management را انتخاب نمایید.



۳- در کادر سمت چپ پنجره‌ی (شکل ۱۳-۷)، گزینه‌ی local users and groups را باز کنید و گزینه‌ی Users را انتخاب نمایید. در کادر سمت راست، لیستی از حساب‌های کاربری نمایش می‌یابد.

۴- در قسمت خالی کادر سمت راست، راست کلیک کرده و گزینه‌ی New User را انتخاب نمایید.



شکل ۱۳-۷ لیست حساب‌های کاربری

۵- کادر محاوره‌ی New User باز می‌شود (شکل ۱۴-۷)، که گزینه‌های آن به شرح زیر می‌باشد:

- **User name**: نام حساب کاربری جدید را وارد کنید.
- **Full name**: نام کامل شخص را وارد نمایید.
- **Description**: در صورت تمایل توضیحی وارد کنید.
- **Password**: کلمه‌ی عبور را تایپ نمایید.
- **Confirm password**: برای اثبات درستی کلمه عبور، آن را دوباره تایپ کنید.



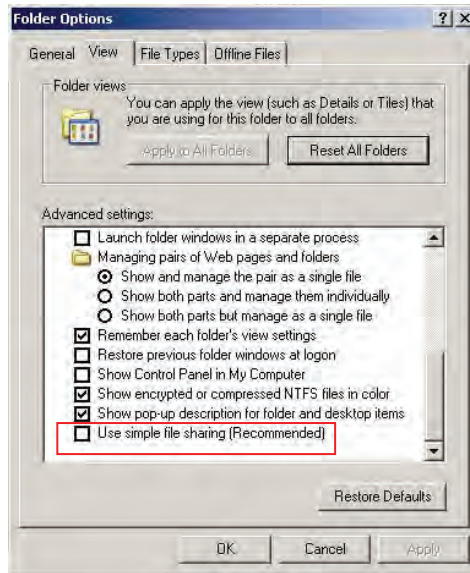
- Log on : با انتخاب این گزینه، باید کاربر در اولین User must change password at next log on شدن، کلمه عبور را تغییر دهد که این به مفهوم امنیت بالاتر می‌باشد که فقط آن کاربر کلمه عبور را خواهد داشت.
 - User cannot change password : کاربر قدرت تغییر کلمه عبور خودش را نداشته باشد.
 - Password never expires : این کلمه عبور دائمی باشد و محدود به زمان خاصی نباشد و هرگز با گذشت زمان به طور خودکار از بین نرود.
 - Account is disabled : حساب کاربری غیرفعال شود. زمانی این گزینه مفید است که به طور موقت بخواهید مجوزهای فایل‌ها و پوشه‌هایی را که این کاربر استفاده می‌کند، تغییر دهید.
- ۶- بر روی دکمه‌ی Create کلیک کنید (شکل ۱۴-۷) و سپس بر روی دکمه‌ی Close کلیک نمایید.

شکل ۱۴-۷ ایجاد حساب کاربری

پس از ایجاد حساب کاربری می‌توان مجوزهای دسترسی به منابع را برای آن تعیین کرد.

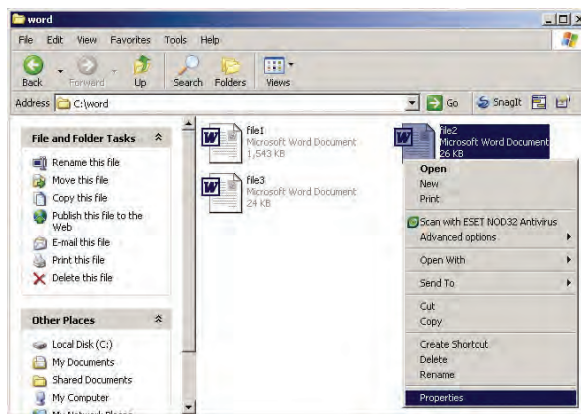
مثال ۶-۷

- مجوزی برای حساب کاربری student تعیین نمایید به طوری که فایل file2 واقع در شکل (۱۷-۷)، توسط حساب کاربری Student خوانده و اجرا شود ولی تغییر نکند.
- برای مشاهده‌ی مجوزهای یک فایل (یا پوشه) به ترتیب زیر عمل کنید:
- ۱- ابتدا باید فایل مورد نظر، در درایوی که سیستم فایل آن NTFS است قرار داشته باشد.
 - ۲- بر روی آیکن Folder Options واقع در پنجره‌ی Control Panel دابل کلیک کنید.
 - ۳- در زبانه‌ی View، گزینه‌ی Use simple file sharing را غیرفعال کنید و بر روی دکمه‌ی OK کلیک نمایید (شکل ۱۵-۷).



شکل ۱۵-۷ کادر محاوره‌ای Folder Option

۳- روی فایل مورد نظر (file2)، کلیک راست کرده و گزینه‌ی Properties را انتخاب نمایید (شکل ۱۶-۷).



شکل ۱۶-۷ نحوه فعال کردن کادر مکالمه Properties یک فایل

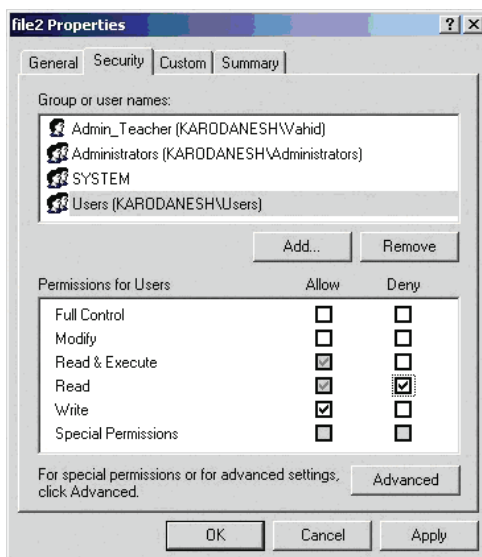
کادر مکالمه‌ی file2 Properties ظاهر می‌شود (شکل ۱۷-۷).

۴- روی زبانه‌ی Security کلیک کنید. دو قسمت به شرح زیر مشاهده می‌کنید:

- **Group or user names:** در این قسمت می‌توان تعیین کرد که چه حساب کاربری یا گروهی اجازه‌ی کار با فایل را دارد.

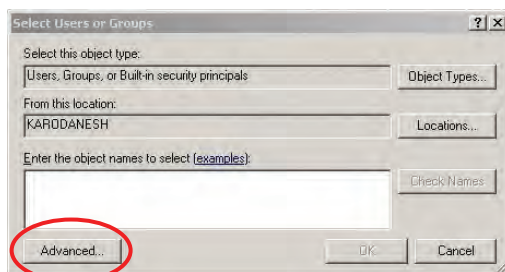


- (نام گروه یا حساب کاربری انتخاب شده) Permissions for: در این قسمت نوع مجوزهای مربوط به گروه یا حساب کاربری که در کادر بالا انتخاب شده است را نمایش می‌دهد.
- ۵- برای انتخاب حساب کاربری student، بر روی دکمه‌ی Add کلیک کنید (شکل ۱۷-۷).



شکل ۱۷-۷ کادر مکالمه‌ی Properties یک فایل

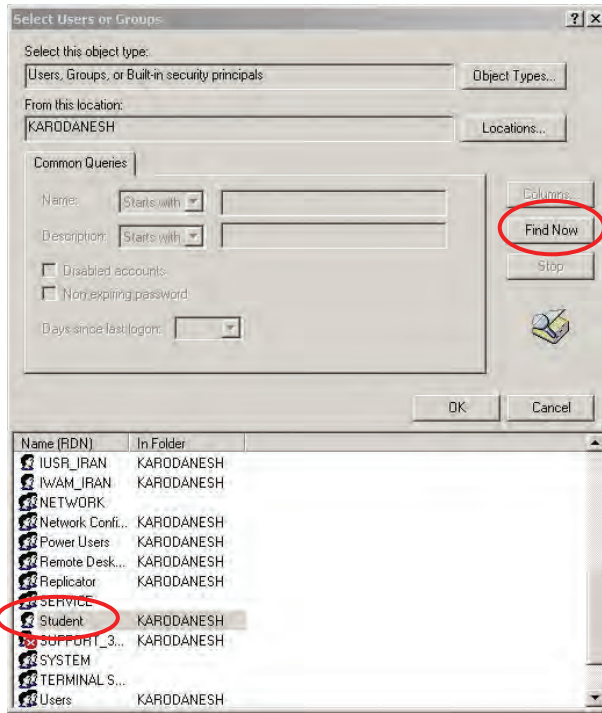
- ۶- در کادر محاوره‌ای Select Users or Groups، بر روی دکمه‌ی Advanced کلیک کنید (شکل ۱۸-۷).



شکل ۱۸-۷ کادر محاوره‌ی Select Users or Groups

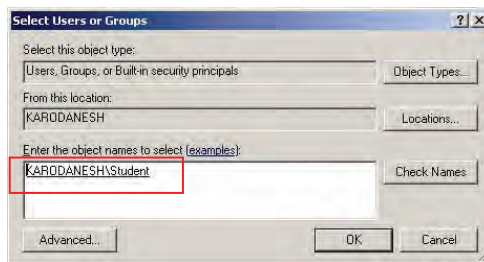
- ۷- در شکل (۱۹-۷)، بر روی دکمه‌ی Find Now کلیک کنید تا لیست حساب‌های کاربری و گروه‌ها را در کادر پایین مشاهده نمایید.

- ۸- از کادر پایین، حساب کاربری Student را انتخاب نمایید و بر روی دکمه‌ی OK کلیک کنید.



شکل ۱۹-۷ انتخاب حساب کاربری Student

۹- در کادر محاوره‌ای Select Users or Groups، نام حساب کاربری که انتخاب کرده بودید، دیده می‌شود بر روی دکمه‌ی OK کلیک کنید.

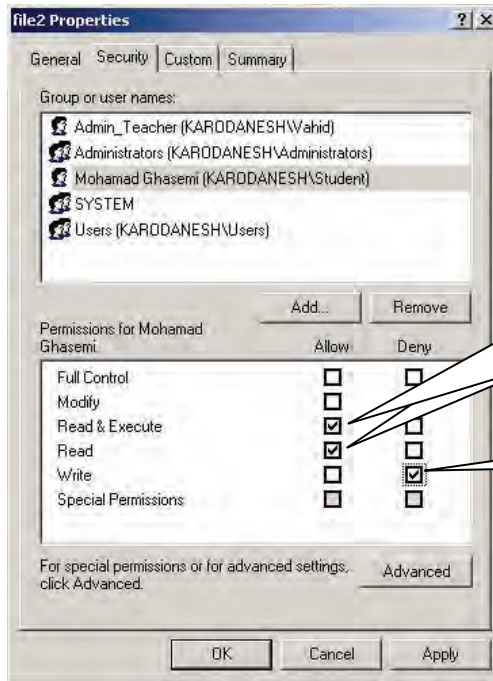


شکل ۲۰-۷

۱۰- در کادر محاوره‌ای Properties، در قسمت Group or user names نام حساب کاربری Student را انتخاب کنید تا در قسمت Permissions for student، مجوزهای آن را مشاهده نمایید.

۱۱- طبق شکل (۲۱-۷)، مجوز Read & Execute را Allow و مجوز Write را Deny کنید.

۱۲- در پایان بر روی دکمه‌ی OK کلیک کنید.



با تخصیص یک مجوز
زیر مجموعه‌های
آن نیز تخصیص
می‌یابند.

لغو یک مجوز

شکل ۲۱-۷ با انتخاب گزینه‌ی Allow مربوط به مجوز Read & Execute چون مجوز Read نیز زیر مجموعه‌ی آن می‌باشد، انتخاب می‌گردد.

بنابراین فایل file2 می‌تواند به وسیله‌ی کاربر Student، خوانده شود و اجرا گردد ولی تغییر نکند.

۶-۷ آشنایی با ارث‌بری مجوزها

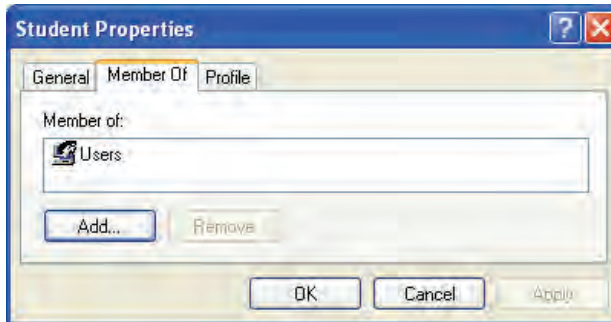
اگر حساب کاربری شما، عضو گروهی در نظر گرفته شود، مجوزهای آن گروه را به ارث خواهد برد.

مثال ۷-۷

حساب کاربری Student را عضو گروه Administrator قرار دهید.

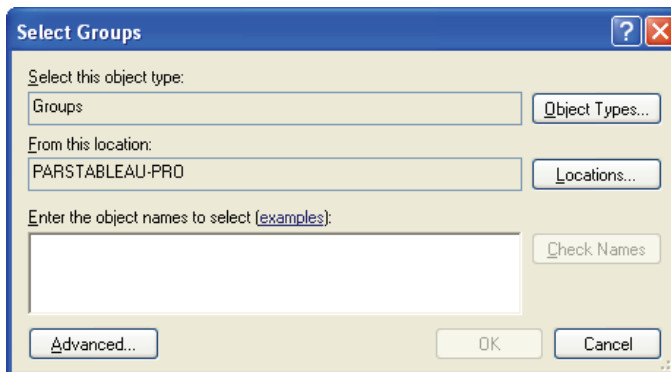
برای انجام این کار، به ترتیب زیر عمل کنید:

- ۱- در کادر سمت چپ پنجره Computer Management، گزینه‌ی Users را انتخاب نمایید.
در سمت راست لیست کاربران (حساب‌های کاربری) نمایش داده می‌شود.
- ۲- روی حساب کاربری Student دابل کلیک کنید. پنجره‌ی Student Properties ظاهر می‌شود (شکل ۲۲-۷).
- ۳- روی زبانه‌ی Member Of کلیک کنید.



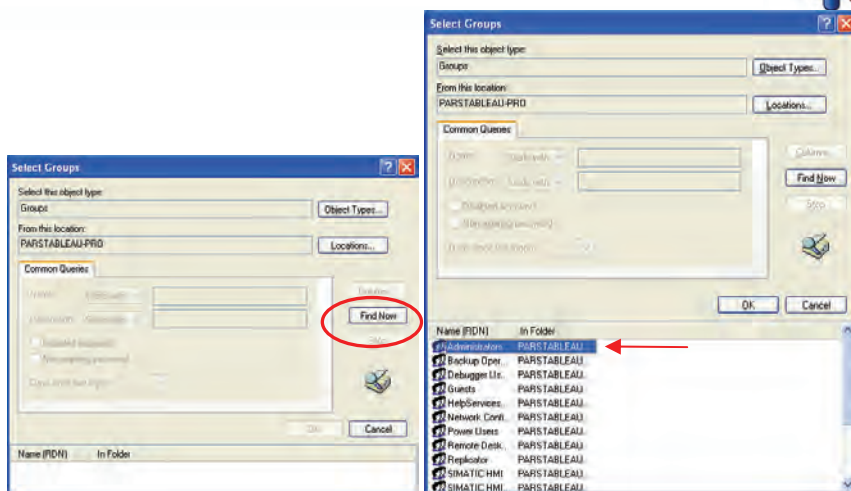
شکل ۷-۲۲ کاربر student عضو گروه users می‌باشد

- درون کادر Member of، گروه Users را مشاهده می‌نمایید. همیشه حساب‌های کاربری که ایجاد می‌شوند، به صورت پیش فرض، عضو گروه users (کاربران) می‌باشند که اختیارات کمتری از Administrators دارند. ۴- برای انتخاب گروه Administrators، روی دکمه‌ی Add کلیک نمایید (شکل ۷-۲۲).



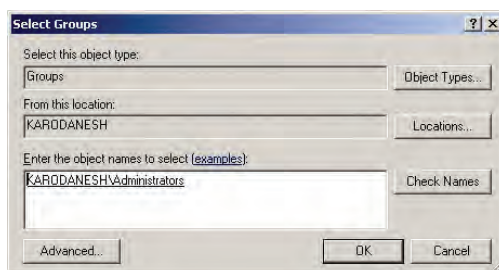
شکل ۷-۲۳ منوی Add

- ۵- در پنجره‌ی Select Groups روی دکمه‌ی Advanced کلیک نمایید (شکل ۷-۲۳).
۶- در کادری که ظاهر می‌شود (شکل ۷-۲۴)، بر روی دکمه‌ی Find Now کلیک کنید، گروه Administrators را انتخاب نمایید و بر روی دکمه‌ی OK کلیک کنید.



شکل ۷-۲۴ انتخاب گروه Administrators

۷-۲۴ در کادر محاوره‌ای Select Groups، بر روی دکمه‌ی OK کلیک نمایید (شکل ۷-۲۵).



شکل ۷-۲۵ پنجره Select Groups

نکته: در سیستم‌فایل NTFS اگر حساب کاربری، عضو چندین گروه باشد مجوز این کاربر اشتراک مجوز گروه‌هایی است که کاربر عضو آن‌ها می‌باشد.

۸- در کادر Student Properties، مشاهده می‌نمایید که کاربر Student عضو گروه‌های Administrator و Users می‌باشد. بنابراین مجوز کاربر Student، اشتراک مجوزهای دو گروه می‌شود. بدین معنی که در واقع کاربر Student، فقط خواص گروه Users را دارا می‌باشد.

۹- اگر مایل هستید کاربر Student، عضو گروه Administrators باشد باید گروه Users را حذف کنید. برای حذف گروه Users، آن را انتخاب کنید و بر روی دکمه‌ی Remove کلیک نمایید.

۱۰- روی دکمه‌ی OK کلیک کنید (شکل ۷-۲۶).



شکل ۲۲-۷

بنابراین حساب کاربری Student، عضو گروه Administrators می‌شود و مجوزهای گروه Administrator را به ارث خواهد برد.

مثال ۸-۷ ✓

اگر student عضو دو گروه باشد، یک گروه مجوز Read و گروه دیگر مجوز Read & Execute داشته باشند، کاربر student چه مجوزی خواهد داشت؟

مجاز کاربر student، اشتراک دو مجوز دیگر خواهد شد. یعنی Student مجوز Read را خواهد داشت.

مثال ۹-۷ ✓

اگر Student عضو دو گروه باشد، یک گروه مجوز Read را Allow و گروه دیگر مجوز Read را Deny کرده باشد، کاربر Student چه مجوزی خواهد داشت؟

نکته: اگر یک مجوز از طرف گروهی Allow و همان مجوز از طرف گروه دیگر Deny باشد، برای کاربر Student، آن مجوز Deny می‌باشد چون در NTFS برای امنیت بیشتر مجوز Deny بر Allow اولویت دارد.

۷-۸ زبان تخصصی

When the option "Encrypt contents to secure data" is selected:

It Specifies that the contents of this file or folder be encrypted. Only the user who encrypts the file or folder can access the content.



If multiple files are selected, a check mark means that all the files have the encryption attribute set. A filled box means that some files have the attribute set and some don't. Encrypted files and folders cannot be compressed.

با توجه به متن به پرسش‌های زیر پاسخ دهید.

1. Who can access the encrypted files and folders?

- a) Every user who uses the computer.
- b) The user who didn't encrypt the files and folders.
- c) The user who encrypted the files and folders.
- d) None

2. How can you find that a file is encrypted?

- a) The file will be high lighted.
- b) The file will be check marked
- c) The file will be deleted.
- d) A and b

3. Which sentence is FALSE about the text?

- a) Only the user who encrypts the file or folder can access them.
- b) The files and folders that are check marked have encryption attribute set.
- c) Users can compress encrypted files and folders.
- d) "Encrypt contents to secure data" specifies that the contents of the file or folder be encrypted.



- این فصل نحوه‌ی استفاده از FAT و مزایای NTFS را بیان می‌کند. در سیستم‌فایل NTFS می‌توان فایل‌ها و پوشه‌ها را رمزگذاری یا فشرده نمود و تنظیماتی در پنجره‌ی Folder Options انجام داد تا فایل‌های رمزگذاری و فشرده در سیستم به‌صورت رنگی نمایش داده شوند. می‌توانید اطمینان حاصل کنید که فایل‌های رمزگذاری شده‌ی شما هیچ‌گاه توسط شخص دیگری خوانده نمی‌شود.



- می‌توان یک حساب کاربری در پنجره‌ی Computer Management ایجاد کرد و آن را عضو گروه دلخواه قرار داد که در این صورت مجوزهای گروه را به ارث می‌برد.
- اگر کاربری عضو چند گروه باشد، مجوز کاربر، اشتراک مجوزهای گروه خواهد بود.

واژه نامه

Account	حساب
Advanced	پیشرفته
Allocation	تخصیص
Attribute	ویژگی
Compress	فشرده کردن
Content	محتوا
Depend on	وابسته بودن
Disable	از کار انداختن، غیر فعال
Decrypt	کشف رمز کردن
Description	توضیح
Encryption	رمزدار کردن
Execute	اجرا
Expire	به پایان رسیدن، منقضی شدن
Filled box	کادر علامت دار
Find	یافتن
Member of	عضو
Multiple	متعدد، چندتایی
Parent folder	پوشه والد
Permission	مجوز، اجازه
Security	امنیت
Sharing	اشتراک
Simple	ساده
Specify	مشخص کردن



آزمون تئوری

گزینه‌ی صحیح را انتخاب کنید.

- ۱- اگر کاربری عضو چند گروه باشد، مجوز کاربر در NTFS به چه صورت خواهد بود؟
 - الف) اشتراک مجوز گروه‌ها
 - ب) اجتماع مجوز گروه‌ها
 - ج) مجوز آخرین گروه
 - د) بستگی به مجوزهای گروه‌ها دارد.
- ۱- کدام یک از عبارتهای زیر صحیح می‌باشند.
 - الف- فایل‌های فشرده به رنگ سبز نمایش داده می‌شوند.
 - ب- کپی یک فایل به پوشه‌ای که رمز گذاری شده است، آن فایل را رمز گذاری نمی‌کند.
 - ج- اگر فایل یا فهرستی را در پوشه‌های فشرده کپی کنید، فشرده می‌شوند.
 - د- اگر فایل رمز گذاری شده را به درایوی با سیستم فایل FAT کپی کنید، از حالت رمز گذاری خارج نمی‌شود.

گزینه‌ی صحیح را از سمت چپ انتخاب کنید و در سمت راست قرار دهید.

- ۳- سیستم فایل‌های و NTFS را برای ویندوز XP و 2000 قابل استفاده است.
 - ۴- رمز گذاری فایل‌ها و پوشه‌ها از مزیت سیستم‌فایل می‌باشد.
 - ۵- برای لغو یک مجوز فرمان به کار می‌رود.
 - ۶- ویندوز XP، برای حفظ امنیت در هنگام کار با سیستم‌عامل، تعریف کرده است.
- User account
- NTFS
- FAT32
- Deny

در جای خالی عبارت مناسب قرار دهید.

- ۷- اگر فایل یا فهرستی را که رمز گذاری شده است روی درایوی با سیستم‌فایل کپی کنید از حالت رمز گذاری خارج می‌شود.
- ۸- با تبدیل FAT به NTFS، اطلاعات موجود بر روی درایو
- ۹- زمانی می‌توان امنیت پوشه و فایل را برقرار کرد که فایل و پوشه در درایوی باشد که دارای سیستم‌فایل است.
- ۱۰- فایل‌ها و فهرست‌های نمی‌توانند رمز گذاری شوند.



فصل هشتم

هدف کلی فصل:

توانایی کار با Network and Internet connection , Network connection

اهداف رفتاری (جزئی)

پس از مطالعه این فصل، از فراگیر انتظار می‌رود که:

- اتصال به اینترنت ایجاد کند.
- وضعیت اتصال را فعال یا غیرفعال کند.
- مشکلات مربوط به اینترنت را رفع کند.
- اتصال به شبکه ایجاد کند.
- کامپیوترهای عضو یک گروه کاری خاص را ببیند و از اطلاعات و منابع آن‌ها استفاده کند.

زمان (ساعت)

تئوری	عملی
۲	۴



مقدمه


اینترنت نقش عظیمی در فعالیت‌های روزانه بسیاری از افراد و سازمان‌ها دارد، هدف کاربران تجاری و خانگی از یک ارتباط Online، جستجوی اطلاعات، گفتگو با دوستان و انجمن‌ها، خرید و برداشت نرم‌افزار است. قبل از این که بتوان از مزایای اینترنت برخوردار شد نیاز به برقراری ارتباط است که معمول‌ترین راه برای اتصال به اینترنت از طریق یک مودم Dial - Up است.


۸-۱ آشنایی با روش اتصال به اینترنت

۸-۱-۱ ایجاد اتصال به اینترنت

برای ایجاد یک اتصال اینترنتی مسیر زیر را دنبال کنید:

۱- Control Panel را از Start انتخاب کنید.

۲- روی برنامه Network Connections  دابل کلیک کنید.

۳- در پنجره Network connection، از قسمت سمت چپ (Network tasks) روی گزینه Create a new Connection  کلیک کنید.

۴- در کادر خوشامدگویی، روی دکمه Next کلیک کنید.

۵- گزینه‌ی Connect to the Internet را که برای متصل شدن به اینترنت است، انتخاب کنید سپس روی دکمه Next کلیک نمایید (شکل ۸-۱).

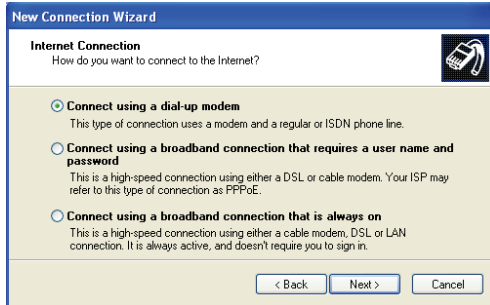


شکل ۸-۱ New connection wizard

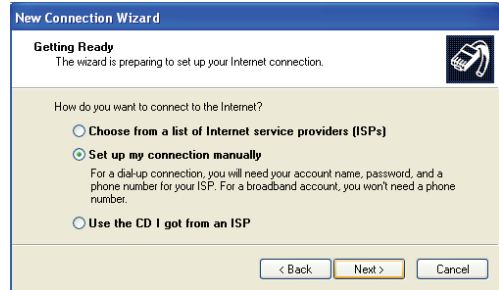
۶- در صفحه Getting Ready، گزینه‌ی Set up my connection manually که برای تنظیم اتصال به صورت دستی است را انتخاب کنید و روی دکمه‌ی Next کلیک نمایید (شکل ۸-۲).



۷- گزینه Connect using a dial-up modem برای اتصال به اینترنت از طریق مودم است، آن را انتخاب و دکمه‌ی Next را کلیک کنید (شکل ۳-۸).



شکل ۳-۸ انتخاب اتصال به اینترنت از طریق مودم



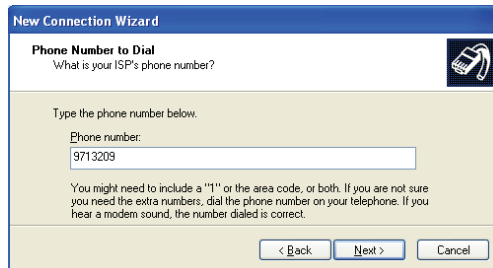
شکل ۳-۸ تنظیم اتصال به اینترنت

۸- در کادر Connection Name نام ISP مورد نظر خود را (Internet Service Provider) را که مایل هستید به کمک آن به اینترنت متصل شوید را وارد کنید (شکل ۴-۸) سپس روی دکمه Next کلیک نمایید (به عنوان مثال Tebyan).



شکل ۴-۸ تعیین نام برای اتصال

۹- در پنجره Dial to Phone Number، شماره اتصال به شبکه را که ISP در اختیار شما گذاشته است (این شماره روی کارت اینترنت نیز وجود دارد) وارد کنید (شکل ۸-۸) سپس روی دکمه Next کلیک کنید (به عنوان مثال ۹۷۱۳۲۰۹).



شکل ۸-۵ وارد کردن شماره تلفن جهت اتصال به شبکه



۱۰- در صفحه‌ی Internet account information نام کاربری و کلمه‌ی رمزی را که ISP در اختیار شما گذاشته است وارد کنید، روی دکمه Next کلیک نمایید.



شکل ۶-۱ وارد کردن نام کاربری و کلمه رمز

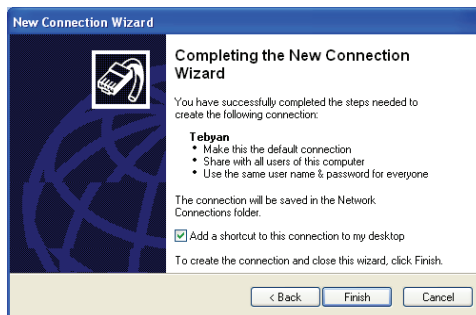
در این صفحه به ترتیب دو گزینه نیز وجود دارد، می‌توان آن‌ها را انتخاب کرده و یا از حالت انتخاب خارج کرد. این گزینه‌ها به ترتیب به شرح زیر می‌باشند:

- از این نام کاربری و کلمه رمز برای اتصال سایر کاربران این سیستم به اینترنت نیز استفاده شود.
- این اتصال را به عنوان اتصال پیش‌فرض در نظر بگیرید.

نکته: New Connection wizard به صورت خودکار، Windows firewall را برای همه اتصالات جدید فعال می‌کند (رجوع کنید به فصل ۶).



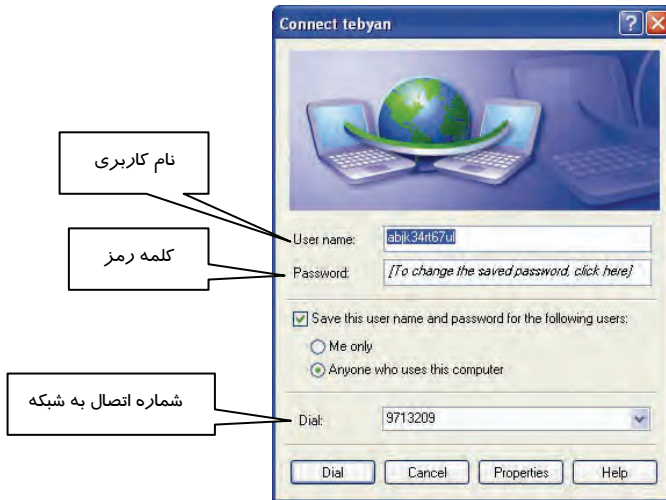
۱۱- برای داشتن یک میان‌بر روی میز کار ویندوز از اتصالی که ایجاد کرده‌اید (شکل ۷-۸)، گزینه Add a shortcut to this connection to my desktop را انتخاب و، روی دکمه Finish کلیک کنید.



شکل ۷-۸ پنجره پایانی




۱۲- کار ایجاد اتصال به اتمام رسیده و پنجره اتصال به اینترنت ظاهر شده است (شکل ۸-۸) در صورتی که نیاز به استفاده از اینترنت دارید روی دکمه Dial و در غیر این صورت روی دکمه Cancel کلیک کنید.

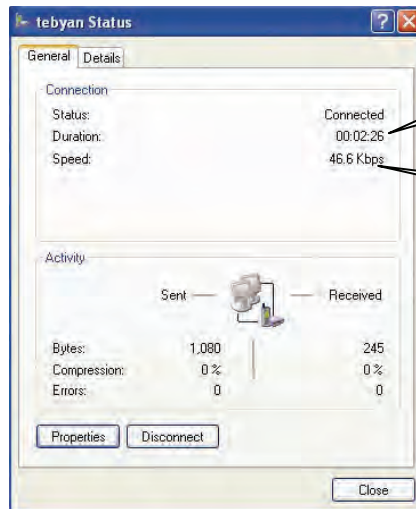


شکل ۸-۸ اتصال به اینترنت

۸-۱-۲ بررسی وضعیت اتصال

زمانی که از طریق اتصال ایجاد شده به اینترنت متصل شدید، یعنی اتصال شما فعال است و آیکن آن در Notification area در نوار Taskbar دیده می شود و کامپیوترهای آیکن اصلی در پنجره Network connection به رنگ آبی دیده می شود (به حالت کامپیوترهای روشن). () راه دیگر این است که روی اتصال راست کلیک کنید و گزینه‌ی Status را انتخاب نمایید.

همان طور که در شکل ۸-۹ مشاهده می کنید پیام Connected در قسمت Connection و حجم اطلاعات ارسال شده از سیستم به اینترنت (Send) و دریافت شده از اینترنت به سیستم (Received) در قسمت Activity دیده می شود.



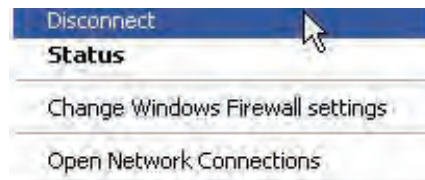
زمان سپری شده از اتصال

سرعت ارتباط

شکل ۹-۸ اتصال در حالت Connected

برای قطع اتصال اینترنت مسیر زیر را دنبال کنید:

- ۱- روی آیکن موجود در قسمت Notification area و Task bar در نوار Task bar، کلیک راست کنید.
- ۲- گزینه Disconnect را انتخاب کنید.



شکل ۱۰-۸ Disconnect

تمرین ۸-۱

با توجه به شکل ۹-۸ پاسخ دهید:

- ۱- وضعیت اتصال در حالت فعال یا غیرفعال است؟
- ۲- چند ثانیه از زمان اتصال به اینترنت سپری شده است؟
- ۳- سرعت انتقال اطلاعات چند کیلو بایت در ثانیه است؟
- ۴- چه حجمی از اطلاعات ارسال (Send) شده است؟
- ۵- چه حجمی از اطلاعات، (Received) دریافت شده است؟




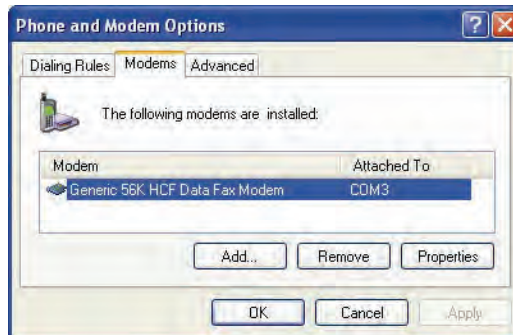
۳-۱-۸ رفع مشکلات اتصال به اینترنت

اگر در اتصال به اینترنت دچار مشکل شدید می‌توانید آن را رفع کنید که در بسیاری از مواقع به راحتی هم رفع می‌گردد. مشکلات اتصال به اینترنت همیشه دلیل واضح و روشنی ندارد، می‌تواند از مودم باشد یا ناشی از تنظیمات ویندوز XP یا تداخل خط تلفن یا هر چیزی در بیرون کامپیوتر باشد که در ادامه به چند مورد اشاره می‌شود.

۱-۳-۸ کنترل خط تلفن

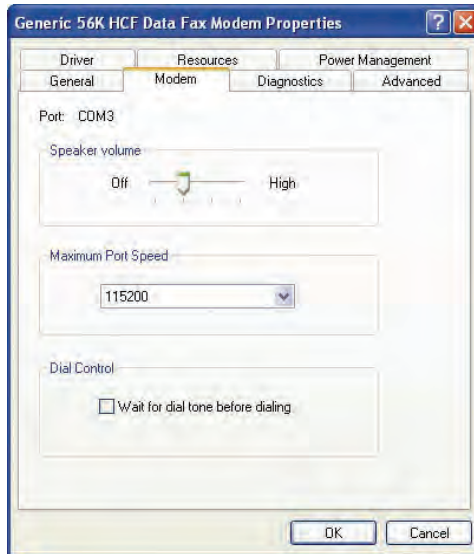
- ۱- آیا از شماره گیری Tone (شماره گیری به شکل صدای بوق) استفاده می‌کنید؟
- ۲- تمام اتصالات را چک کنید. آیا خط تلفن به پورت مناسبی از مودم وصل شده است؟ اگر مودم خارجی دارید از سالم بودن اتصالات کابلی مودم و کامپیوتر اطمینان حاصل کنید.
- اگر صدایی همانند زمانی که پیام از پست صوتی در حالت انتظار است، می‌شنوید این به معنی درست عمل نکردن اتصال شماست. مسیر زیر را دنبال کنید:

- ۱) در Control panel روی برنامه Phone and modem options  دابل کلیک کنید.
- ۲) در پنجره Phone and modem options پس از انتخاب زبانه Modem ، روی دکمه Properties کلیک کنید(شکل ۸-۱۱).



شکل ۸-۱۱ زبانه Modems

- ۳) روی زبانه Modem کلیک کنید(شکل ۸-۱۲).



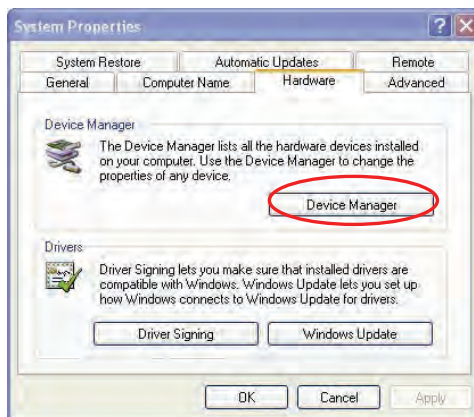
شکل ۱۲-۸ زبانه Modem

۴) گزینه‌ی Wait for dial tone before dialing را از حالت انتخاب خارج کنید.

۲-۳-۱-۸ بررسی صحت نصب مودم

اطمینان حاصل کنید که مودم به طور صحیح نصب شده است و می‌تواند با ویندوز ارتباط برقرار کند. مسیر زیر را دنبال کنید:

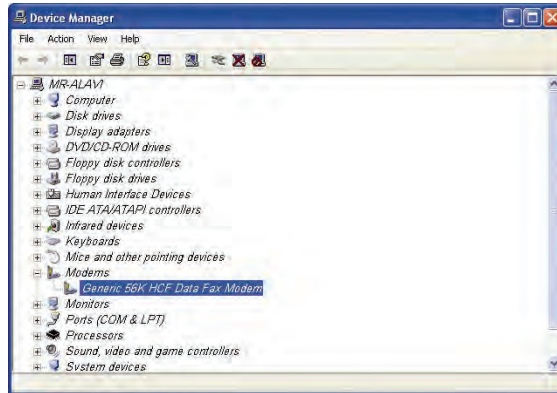
- ۱) روی My Computer کلیک راست نمایید و گزینه‌ی Properties را انتخاب کنید.
- ۲) در زبانه Hardware، روی دکمه Device manager کلیک کنید.



شکل ۱۳-۸ زبانه Hardware



۳) در پنجره‌ای که باز می‌شود، روی مودم دابل کلیک کنید (شکل ۸-۱۴). اگر علامت دایره زرد یا قرمز در کنار مودم دیدید به پیام خطای موجود در زیر قسمت Device status در نوار General توجه کنید.




شکل ۸-۱۴ بررسی صحت نصب مودم

- در این شکل مودم درست نصب شده است.

۳-۳-۱-۸ بررسی ارتباط صحیح مودم با ویندوز

مسیر زیر را دنبال کنید:

۱) Control Panel را از Start انتخاب کنید.

۲) روی برنامه‌ی Phone and modem options () دابل کلیک کنید.

۳) در زبانه‌ی Modems از پنجره Phone and modem options روی دکمه‌ی Properties کلیک کنید (شکل ۸-۱۳).

۴) در زبانه‌ی Diagnostics روی دکمه Query modem کلیک کنید (شکل ۸-۱۵).

۵) کمی تامل کنید تا ویندوز XP با مودم ارتباط برقرار کند.

اگر ارتباط برقرار شد به گزارش گزینه‌های Command و Response در پایین پنجره دقت کنید. همان‌طور که در شکل ۸-۱۶ مشاهده می‌کنید، پیام‌ها بر این دلالت دارند که ویندوز و مودم به درستی با هم ارتباط برقرار کرده‌اند (اگر هیچ گونه مطلبی در قسمت Response نبود، احتمالاً درایور مودم شما درست نصب نشده است).