فصل اول

هک کردن رایانهٔ خود

یک هکر قبل از اینکه بخواهد رایانهٔ دیگران را مورد بررسی و کنکاش قرار دهد، باید از رایانهٔ خود باخبر باشد. شما بعد از مطالعهٔ این فصل، با ترفندهایی آشنا می‌شوید که باعث تعجب دوستانتان خواهد شد.

- کنترل start up
- اسکریپت برنامهٔ ویژوال‌بیسیک را غیرفعال کنید
- یک برنامهٔ کوچک برای اضافه کردن User در Windows XP
- رجیستری چیست و تهیه نسخهٔ پشتیبان از آن
- مخفی کردن یک یا چند Drive
- خروجی درگاه USB سیستم خود را قفل کنید
- افزایش سرعت اینترنت در Windows XP
- حذف گزینهٔ Setting از پنجرهٔ Display Properties
- نام کاربری خود را عوض کنید
- کنترل را در دست بگیرید
- حذف برنامه‌هایی که پاک نمی‌شوند
- از نمایش پیام‌های غیرضروری جلوگیری کنید
- فهرست برنامه‌های اجرا شده را از بین ببرید
- منوی Start را سریع‌تر کنید
- تعیین برنامه جهت اجرای CDهای صوتی
- کنترل کردن Auto Run
- افزایش سرعت برنامهٔ Internet Explorer در مرور صفحات
- عبور از کلمهٔ عبور در Windows xp
- یک Password امنیتی برای Windows XP
- عبور از کلمهٔ عبور در Windows 2000
- پیغامی برای خوش‌آمدگویی در Windows XP
- جلوگیری از دسترسی به فایل‌های مخفی

کنترل Start up

تمام برنامه‌های موجود در کامپیوتر با آنکه به طور مستقیم درون پوشهٔ Start up نیستند؛ اما به کمک Start up موجود در ویندوز راه‌اندازی می‌شوند. شما می‌توانید هرکدام از این برنامه‌ها را به دلخواه انتخاب کرده و از کار بیندازید. این کار باعث افزایش سرعت سیستم نیز می‌شود.

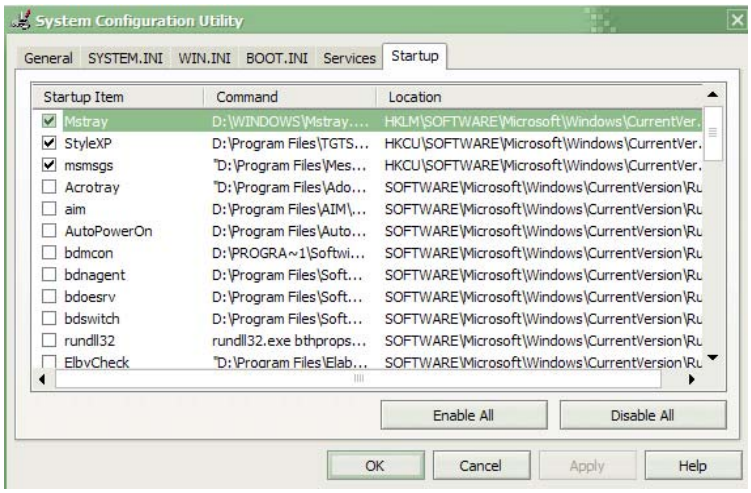
به منظور آگاه شدن و از کار انداختن برنامه‌هایی که هنگام روشن شدن کامپیوتر راه‌اندازی می‌شوند، این مراحل را دنبال کنید:

برروی Start کلیک کنید و گزینهٔ Run را انتخاب کنید. عبارت Msconfig را تایپ کرده سپس برروی Ok کلیک کنید. در این هنگام پنجره‌ای با عنوان زیر باز می‌شود:

System configuration Utitlity

بر روی زبانهٔ Start up کلیک کنید تا به لیست برنامه‌های موردنظر دسترسی پیدا کنید.

حال می‌توانید هر برنامهٔ مشکوکی را که مشاهده می‌کنید، از ادامهٔ فعالیت باز دارید.



اسکریپت برنامهٔ ویژوال‌بیسیک را غیرفعال کنید

یکی از اولین اقدامات هنگام استفاده از ویندوزهای ۹۸،۹۵ و ۲۰۰۰، از کار انداختن اسکریپت برنامهٔ ویژوال‌بیسیک است. این کار سبب می‌شود، از نفوذ ویروس‌هایی مانند Love bug جلوگیری به عمل آید.

بدین‌منظور مراحل زیر را در Windows 98 دنبال کنید:

برروی دکمهٔ Start موجود در Taskbar کلیک کنید.

به مسیر Setting \ control panel بروید.

گزینهٔ Add/Remove program را انتخاب کنید.

برروی زبانهٔ windows setup کلیک کنید.

درون لیست نمایان شده، Accessories را انتخاب کنید.

برروی گزینهٔ Details کلیک کنید.

چک باکس Check box مربوط به Windows Scripting Host را غیرفعال کنید.
برروی گزینهٔ Ok، کلیک کنید.

> ***نکته:*** *شما با این کار از دسترس بسیاری از ویروس‌ها و نرم‌افزارهای هک در امان خواهید بود.*

یک برنامهٔ کوچک برای اضافه کردن User در Windows XP

با ذخیره کردن یک سری از دستورت Dos در یک فایل دسته‌ای، برنامه‌ای بنویسید که برای شما یک حساب کاربری بسازد.

۱) برنامهٔ Note Pad را باز کنید و دستورات زیر را در آن تایپ کنید:

```
Net user YourName Password /add
Net localgroup administrators YourName /add
Net Share cddrive=c
Net Share cddrive=d
```

۲) فایل را ذخیره کرده و پسوند آن را به Bat تغییر دهید.
حال با اجرای این فایل به راحتی برای خود یک User می‌سازید.

> ***نکته:*** *در قسمت YourName نام کاربر و در قسمت Password رمز عبور دلخواه خود را وارد کنید.*

رجیستری چیست؟

رجیستری فراتر از یک سری کلید است که دربارهٔ آن در مقالات و سایت‌های مختلف و حتی کتاب‌ها چیزهایی می‌خوانید. جای تأسف است Microsoft، رجیستری و تنظیمات آن را در هاله‌ای از ابهام قرار داده است و افراد زیادی با تنظیمات واقعی سیستم عامل خود بیگانه‌اند. مایکروسافت از ارائهٔ اطلاعات کافی در مورد تنظیمات صحیح خودداری کرده است و در مورد رجیستری اسرار زیادی باقی گذاشته است.

رجیستری در ویندوز، حاوی فایل‌های اطلاعاتی است که به ویندوز برای کنترل سخت‌افزار، نرم‌افزار و محیط کاربر کمک می‌کند. رجیستری شامل دو فایل در دایرکتوری ویندوز است: system.dat و user.dat. به‌وسیلهٔ فایل اجرایی Regedit.exe که در دایرکتوری ویندوز وجود دارد، می‌توان به بانک‌های اطلاعاتی رجیستری که طبق مستندات یافت شده پنج عدد هستند، دست یافت.

همچنین توصیه می‌کنم تا زمانی که با چگونگی فعالیت در رجیستری کاملاً آشنا نشده‌اید، اقدام به دستکاری متغیرها و ارزش‌های آن ننمایید، چرا که هرگونه تغییر در این محیط بدون نمایش پیغام و یا هشداری سریعاً اعمال می‌شود و از آنجا که رجیستری محیطی شلوغ و درختی است، انجام هرگونه اصلاح در آن منوط به داشتن اطلاعات جنبی در خصوص فعالیت موردنظر است.

با توجه به اهمیت رجیستری توصیه می‌کنم قبل از هر اقدامی به روش زیر، از رجیستری سیستم عامل خود یک نسخهٔ پشتیبان تهیه کنید تا در صورت نیاز آن را بازآوری نمایید.

تهیهٔ نسخهٔ پشتیبان از رجیستری

برای تهیه نسخهٔ پشتیبان و یا اصلاح رجیستری دو برنامهٔ کوچک نوشته شده که با ویندوز نصب می‌شوند: Scanregw.exe و Scanreg.exe

مشخصات برنامهٔ Scanregw.exe از این قرار است:

۱- فقط در محیط ویندوز اجرا می‌شود.
۲- از رجیستری نسخهٔ پشتیبان تهیه کرده و در فایل‌هایی با پسوند cab ذخیره می‌کند.
۳- در حالت safemode نیز اجرا می‌شود.
۴- در صورت لزوم، رجیستری را Scan کرده و خطاها را گزارش می‌کند.
۵- در صورت به وجود آمدن خطا، نمی‌تواند آن را تعمیر کند.

مشخصات برنامهٔ Scanreg.exe بدین قرار است:

۱- فقط در محیط Dos اجرا می‌شود.
۲- از رجیستری نسخهٔ پشتیبان تهیه کرده و در فایل‌هایی با پسوند cab ذخیره می‌کند.
۳- در صورت لزوم رجیستری را Scan کرده و خطاها را گزارش می‌کند.
۴- در صورت به وجود آمدن خطا می‌تواند آن را تعمیر کند.
۵- تنظیمات رجیستری را به حالت قبل از تغییر، برمی‌گرداند.
۶- هر بار که ویندوز بوت می‌شود، به طور خودکار یک نسخهٔ پشتیبان از رجیستری تهیه کرده و آنها را در فایل‌های مخفی با پسوند cab در مسیر مخفی C:\Windows\sysbackup ذخیره می‌کند.

مخفی کردن Drive موردنظر

وارد رجیستری Windows شوید و به این آدرس رجوع کنید:

Heky_ Current_ User / Software/Microsoft/ Windows/ Current Version/ Policies/ Explorer

روی آیکون Explorer رفته و روی آن کلیک راست کنید. گزینهٔ New و سپس DWORD value را بزنید. در قسمت رو به رو، یک ارزش جدید باز می‌شود که باید نام آن را NoDrives بگذارید. باید توجه داشته باشید که حروف N و D را بزرگ تایپ کنید.

حالا شما یک آیکون با نام NoDrives دارید. روی آن دوبار کلیک کنید. در قسمت Base گزینهٔ Hexadecimal را انتخاب کنید و سپس در قسمت Value data دقیقاً نوشتهٔ FFFFFF3 را تایپ کنید. حروف F را بزرگ تایپ کرده و سپس کلید OK را بزنید. حالا کلید F5 را بزنید تا سیستم شما دوباره جان بگیرد.

رایانه را یکبار restart کنید و پس از ورود به سیستم عامل به سراغ My Computer بروید. با تعجب خواهید دید که هیچ یک از درایوها دیده نمی‌شود.

برای برگرداندن Driveها، دوباره همهٔ مراحل فوق را طی کنید و ارزش جدیدی را که ایجاد کرده‌اید پاک کرده و دوباره سیستم عامل را restart کنید.

نکته: *اگر تصمیم دارید یک درایو خاص را محو کنید، پس از درست کردن فایل NoDrives در قسمت Value data اعداد زیر را بنویسید:*

A	*1*	*I*	*256*	*Q*	*65536*	*Y*	*16777216*
B	*2*	*J*	*512*	*R*	*131072*	*Z*	*33554432*
C	*4*	*K*	*1024*	*S*	*262144*		
D	*8*	*L*	*2048*	*T*	*524288*		
E	*16*	*M*	*4096*	*U*	*1048574*		
F	*32*	*N*	*8192*	*V*	*20907152*		
G	*64*	*O*	*16384*	*W*	*4194304*		
H	*128*	*P*	*32768*	*X*	*8388608*		

اگر قصد داشتید چند درایو را همزمان مخفی کنید، باید مقادیر Decimal آنها را با هم جمع کرده و نتیجه را وارد کنید. به عنوان نمونه برای مخفی کردن درایوهای D، E و F باید مقادیر ۸، ۱۶ و ۳۲ را جمع کرده و مقدار ۵۶ را وارد نماییم.

برای ناپدید کردن تمام درایوها می‌توانید عدد دسیمال ۶۷۱۰۸۸۶۳ را به متغیر NoDrives بدهید.

خروجی درگاه usb سیستم خود را قفل کنید

یک هکر باید مواظب باشد تا اطلاعات وی به دست کسی نیفتد. از آنجا که در حال حاضر Flash Memoryها به لوازم شخصی افراد تبدیل شده‌اند، باید به گونه‌ای عمل کرد تا در نبود ما کسی اطلاعات ما را نرباید. برای این منظور کافیست تنظیمات زیر را اعمال کنید تا Flash Memory رفتاری مانند یک CD Drive فقط خواندنی داشته باشد و قابلیت کپی کردن بر روی آن غیرفعال شود.

۱ـ وارد رجیستری شوید.

۲ـ کلید زیر در رجیستری را پیدا و مشخص کنید:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Contro l\StorageDevicePolicies

ممکن است کلید StorageDevicePolicies وجود نداشته باشد، به راحتی با استفاده از دستور New Key، این کلید را به وجود آورید.

۳ـ یک رشته از نوع DWORD که در واقع دارای ارزش کلید است به نام WriteProtect ایجاد کنید و مقدار عددی آن را به عدد ۱ تغییر دهید.

۴ ـ سیستم را یکبار راه‌اندازی کنید تا تغییرات ایجاد شده اعمال شود.

افزایش سرعت اینترنت در Windows XP

از منوی Start گزینهٔ Run را انتخاب و عبارت Regedit را تایپ نمایید و کلید Enter را فشار دهید تا وارد رجیستری شوید. پس از ورود به آدرس زیر بروید:

HKEY_CURRENT_USER\software\Microsoft\Windows\Curre nt Version\internt setting

حالا در پنجرهٔ سمت راست، دنبال عبارت‌های زیر بگردید:

۱- MaxConnections PerServer

۲- Oserver _MaxConnectionPerl

اگر این گزینه را مشاهده نمی‌کنید، در طرف راست پنجره، راست کلیک کرده و سپس New\DWORD را انتخاب کنید.

حال عبارات MaxConnections PerServer و Oserver _MaxConnectionPerl را بنویسید. به این ترتیب شما دو ارزش DWORD با نام‌های موردنظر ساخته‌اید.

> ***نکته:*** *در نام‌گذاری ارزش‌ها به حروف بزرگ و کوچک دقت کنید.*

سپس روی عبارت‌های ساخته شده، دوبار کلیک کنید و در قسمت Dtata Value برای گزینهٔ اول، مقدار ۸ و برای گزینهٔ دوم، حرف a را وارد کنید. سیستم را Restart نمایید.

فعال کردن ویژگی‌های مربوط به DVD در Media player

همان‌طور که می‌دانید، به صورت پیش‌فرض فایل‌های DVD در Media player باز نمی‌شود.

تغییرات زیر باعث می‌شود در Media player، DVD نمایش داده شود، ابتدا کلید زیر را پیدا کنید:

HKEY_CURRENT_USER\Software\Microsoft\Medial\Player\settings

یک متغیر جدید از نوع string با نام Enable DVDUI ایجاد کنید و مقدار آن را جهت فعال شدن Yes قرار دهید.

حذف گزینهٔ setting از پنجرهٔ Display propertice

گاهی اوقات مدیر سیستم تصمیم می‌گیرد تنظیماتی را به زور به کاربران القا کند، شما با استفاده از مراحل زیر می‌توانید تنظیمات تصویر پس‌زمینه، screensaver و اندازهٔ نمایش صفحات را قفل کنید.

HKEY_CURRENT_USER\Software\Microsoft\windows\currentersion\policies\system

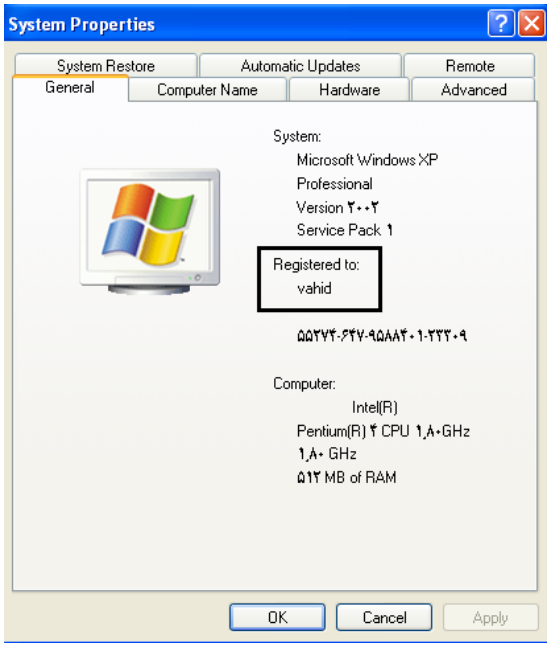
متغیری ایجاد و نام آن را NodispSettingspage قرار داده و مقدار آن را : ۰۱ ۰۰ ۰۰ ۰۰ قرار دهید و سیستم را از نو بوت کنید.

نام کاربری خود را عوض کنید

در هنگام نصب سیستم عامل، به نصاب اجازه داده می‌شود تا اطلاعات خود را وارد کند و تا مرگ سیستم عامل، شما قادر به تغییر در این نام نیستید؛ اما اگر لازم شد شما با دنبال کردن مراحل زیر این تغییرات را اعمال کنید:

HKEY_LOCAL_MACHINE\Software\Microsoft\windowsNT\current version

حال متغیرهای registered owner و registered organization را پیدا کرده و مقدار آنها را به نام‌های موردنظرتان تغییر دهید.



کنترل را در دست خود بگیرید

شما می‌توانید با کمی تغییر در رجیستری مجوز دسترسی به بعضی امکانات را از کاربران سیستم بگیرید.

به عنوان مثال، برای حذف کردن تابع search از منوی start متغیری از نوع DWORD را در مسیر زیر بسازید و نام آن را NOFind بگذارید و مقدار آن را ۱ قرار دهید. به این ترتیب تابع Search از منوی start محو خواهد شد:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

یک مورد دیگر حذف کردن تابع Run می‌باشد. برای این کار نیز متغیر دیگری از نوع DWORD بسازید و اسم آن را NORun گذاشته و مقدار آن را ۱ قرار دهید.

برای قفل کردن نوار وظیفه می‌توانید متغیر دیگری تعریف کرده و اسم آن را NosetTaskbar بگذارید و مقدار ۱ به آن دهید.

حذف کردن برنامه‌هایی که پاک نمی‌شوند

حتماً تا حالا به برنامه‌هایی که به دلایل نامشخص از روی سیستم پاک نشده‌اند برخورد کرده‌اید و ناچاراً با پاک کردن فایل‌ها و پوشهٔ آن نام آنها را از جلوی چشمانتان حذف کرده‌اید؛ اما متأسفانه نام

آنها برای همیشه در Add\Remove Program باقی خواهند ماند، برای آنکه فهرست این برنامه‌ها را از بین ببریم، باید از رجیستری استفاده کنیم:
ابتدا به کلید زیر بروید:

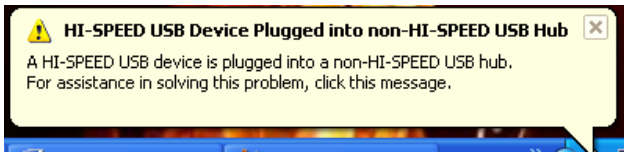
HKEY_LOCAL_MACHINE\\Microsoft\windows\current version\uninstall

و سپس کلید متناظر با این کلید را باز کنید. حالا برنامه‌هایی را که نمی‌توانستید پاک کنید، از این جا حذف کنید تا برای همیشه از بین بروند.

از نمایش پیام‌های غیرضروری جلوگیری کنید

از آنجا که سیستم عامل ویندوز علاقهٔ زیادی به راهنمایی کاربران خود دارد، گاه و بی‌گاه با نمایش پنجره‌هایی در پایین صفحه، اعصاب کاربرانش را به هم می‌ریزد؛ شما با اعمال تغییرات زیر از دست این پیام‌ها راحت خواهید شد.

HKEY_current_user\Software\Microsoft\windows\current version\Explorer\Advanced



اکنون متغیری از نوع DWORD بسازید و نام آن را enablebaloontips بگذارید و مقدارآن را ۰ قرار دهید.

فهرست برنامه‌های اخیر اجرا شده را از بین ببرید

اگر نمی‌خواهید کسی بداند شما اخیراً از چه برنامه‌هایی استفاده کرده‌اید به آدرس زیر در رجیستری رجوع کنید:

HEKY_CURRENT_USER > Software > Microsoft > Windows > CurrentVersion > Policies > Explorer

در این قسمت یک ارزش از نوع Binary بسازید. نام آن را NoRecentDocsMenu گذاشته و مقدار آن را ۰۰ ۰۰ ۰۰ ۰۱ قرار دهید.

منوی start را سریع‌تر کنید

به صورت پیش‌فرض در منوی start زیرمنوها پس از ۴۰۰ میلی‌ثانیه ظاهر می‌شود. شاید برای شما این زمان زیاد باشد. برای کم کردن آن مراحل زیر را دنبال کنید:

HKEY_CURRENT_USER\ \CONTROL PANEL\DESKTOP

در اینجا MENU SHOW DELAY را پیدا کنید. مقدار این متغیر طول تأخیر منو را برحسب میلی‌ثانیه از ۰ تا ۹۹۹ نشان می‌دهد که می‌توانید با دادن مقدار ۱۰ به آن، سرعت آن را بسیار زیاد کنید.

تعیین برنامه جهت اجرای سی‌دی‌های صوتی قرار داده شده در CD ROM

کلید زیر را پیدا کنید:

HKEY_CLASSESt_ROOT\AudioCD\Shell\play\command

یک متغیر به نام default در اینجا موجود است که معمولاً توسط خود ویندوز به Media player ست شده است. حال اگر قصد تغییر آن را دارید، به صورت زیر عمل کنید:

تنظیم برای win amp :

" c:\program File Win amp3\ Winamp3 . exe " CD : ٪۱

یا اگر از برنامهٔ دیگری استفاده می‌کنید، آدرس آن را وارد کنید.

حال جهت فعال شدن، سیستم را reset کنید.

کنترل کردن Auto run

از لحاظ امنیتی اجرای خود به خود CD می‌تواند مشکلاتی به همراه داشته باشد، لذا پیشنهاد می‌شود که قابلیت Auto Run را غیرفعال کنید.

HKEY_local_machine\ currentcontrolset\ services\CDROM

یک متغیر از نوع DWORD و با نام AUTORUN ایجاد کنید و برای اینکه AUTORUN سی‌دی‌ها را از کار بیندازید، به آن مقدار صفر و برای فعال کردن آن مقدار یک بدهید.

افزایش سرعت برنامهٔ Internet Explorer در مرور صفحات

۱- وارد محیط Registry شوید: Start \ Run \ regedit

۲- به شاخهٔ زیر در رجیستری بروید:

HKEY _ LOCAL _ MACHINE \ Software\ Microsoft \ windows \ CurrentVersion \ Explorer \ Remotecomputer \ NameSpace

۳- حالا به دنبال این زیرشاخه بگردید.

{D6277990 – 4C6A – 11CF – 8D87 – 00AA0060F5BF}

۴- با فشردن کلید Delete پوشهٔ بالا را حذف کنید.

۵- جهت تازه‌سازی Registry کلید F5 را فشار دهید.

عبور از کلمهٔ عبور در Windows xp

در صورت انجام مراحل زیر از کلمهٔ عبور Windows xp خواهید گذشت.

الف) در صفحه‌ای که از شما کلمهٔ عبور و رمز عبور سؤال می‌شود (Swich User) دکمه‌های Alt+Ctrl+Del را دوبار فشار دهید.

ب) حال در کادر پدیدار شده در قسمت User Name عبارت روبرو را بنویسید: Administrator و در قسمت Password هیچ عبارتی وارد نکنید.

پ) Ok را انتخاب کنید تا وارد Windows xp شوید.

نکته: *اگر در هنگام انتخاب گزینهٔ OK با پیغام خطا مواجه شدید، در کادر User name عبارت ADMINISTRATOR را وارد کنید و کلید Enter را بفشارید. اگر باز با پیغام خطایی مواجه شدید، به این معناست که برای سیستم عامل یک مدیر تعریف شده و شما نمی‌توانید وارد آن بشوید.*

Password امنیتی برای Windows XP

در ویندوز XP می‌توانید قبل از فعال شدن هر حساب کاربری (USER)ها پسورد دیگری قبل از همهٔ اینها قرار دهید. انتخاب این پسورد سبب خواهد شد تا دیگران قبل از ورود به ویندوز از دو سپر امنیتی عبور کنند. برای اضافه نمودن این پسورد به ویندوز مراحل زیر را دنبال کنید:

۱- از منوی Start گزینهٔ RUN را انتخاب و عبارت Syskey را تایپ کرده، سپس OK کنید.

۲- در پنجرهٔ ظاهر شده با سربرگ Securing the Windows XP Account Database روی گزینهٔ Update کلیک کنید.

۳- حال در قسمت Password Startup پسورد دلخواه خود را وارد و پنجره را با OK ببندید.

۴- در صورت لزوم می‌توانید در قسمت System Generated Password پسورد را بر روی Floppy Disk ذخیره نمایید تا فقط با استفاده از آن قادر به عبور باشید. از این پس زمانی که سیستم روشن و یا ریبوت شود، پسورد امنیتی قبل از ورود به حساب‌های کاربری ظاهر می‌شود و برای ورود، از شما پسورد درخواست می‌کند.

توجه: *اگر پسورد را سه مرتبه اشتباه وارد کنید، سیستم ریبوت می‌شود.*