مرجع کامل رجیستری (2)

نویسنده : حمید رضایی (AHA.x92)

تاریخ : 5 دی ماه 1386

تصحیح کننده : A.R.R

منابع :

تمام اين اطلاعات با استفاده از فنون مهندسي معكوس (شرمنده ؟!!) از درون يكي از نرم افزارهاي معتبر ساخته شده توسط وطن (ايراني هاي عزيز) و تجربيات خودم در آوردم و نوشتم .

ملاحظات :

لازم به تذکر است کلیه مطالب گفته شده در این مقاله صرفا جنبه آشنایی شما عزیزان با این فنون دارد و بس . هرگونه استفاده غیرآموزشی از این مطالب بر عهده خود کاربر میباشد و بنده هیچ گونه مسئولیتی را در قبال آن عهده دار نمی باشم .
هر گونه استفاده آموزشی با ذکر منبع مجاز و تمام حقوق معنوی آن مخصوص خودم است و هیچ قانونی از آن حمایت نمیکند.

مقدمه :

رجیستری ، منبعی است که Windows و یا برنامه های دیگر از آن استفاده میکنند و اطلاعاتی را از آن میگیرند و یا در آن قرار میدهند ، پس به همین خاطر بخش مهمی از ویندوز بشمار میرود و می گویند همیشه یک Back up از رجیستری تان داشته باشید تا اگر ویروسی درون سیستم تان افتاد ویا کار دیگری شد شاید با برگرداندن Back up ، مشکلتان برطرف شود .
من به شما توصیه میکنم اگر کار با رجیستری را یاد ندارید ، آن را دستکاری نکنید .
این فایل آموزشی برای سطوح (از نظر یاد داشتن) :
» مبتدی
» متوسط
» پیشرفته
میباشد پس تمام مقاله را به خوبی بخوانید . قصد من آشنایی شما عزیزان با کارهای که یک ویروس و یا . . . میتواند درون سیستم تان بکند و راههای مبازه با آن است .
اگر مشکلی پیش آمد و یا اشتباه بود (که نیست) از طریق وبلاگ به من گزارش دهید ویا به GMail ام گزارش دهید . منتظر نظراتتان هستم .

www.godvb.coo.ir

www.godvb.blogfa.com

aha.x92@gmail.com

اگر تابحال با رجیستري کار نکرده اید ، حتما شماره 1 این مقاله را از وب سایت ام دانلود کنید .
اولین کار، به هر روش، روش خودم را فقط برای پشتیبان گیری از چند کلید توصیه می کنم و برای کل رجیستری به درد نمی خورد . چون برای اینکه بفهمید اطلاعات وارد رجیستری شده است ، باید بایستید تا پیغامی بیاید که به شما بگوید اطلاعات فایل مورد نظر بدرستی وارد رجیستری شد ولی Back up گیری از روش های دیگر برای باز گرداندنشان صدرصد دارای یک Progress Bar است که نشان میدهد چقدر این کار انجام شده است ، بهرحال از رجیستری تان یک Back UP بگیرید و بعد ادامه مطالب را بادقت بخوانید .

Internet Explorer

عوض کردن متن نوار عنوان (Title Bar Internet Explorer)

به این مسیر بروید :

HKCU\Software\Microsoft\Internet Explorer\Main

نکته :

کلمه HK مخفف HKEY است .
دوکلمه بعد آن حروف اول بخش های دیگر است همانطور که در بالا کلید های سمت چپ را که داشتم توضیح می دادم معمولا 3 بخشی بودند که هر بخش را با (_) از هم جدا میکردیم . جمله بالا مخفف HKEY_CURRENT_USER می باشد .

یک متغیر از نوع 1 باید با نام Window Title باید وجود داشته باشد متن درونش را هرچه خواستید بگذارید .

Disable Close در اینترنت اکسپلورر

به مسیر زیر بروید

HKCU \Software\Policies\Microsoft\Internet Explorer \Restrictions

و متغییری با نام NoBrowserClose از نوع 3 بسازید ومقدار درونش را صفر بدهید ، برای برگرداندن این حالات ایجادشده یا مقدار درون متغییر را صفر کنید و آن متغییر را Delete کنید .

غیر فعال کردن Internet Option

به مسیر زیر بروید

HKCU\Software\Policies\Microsoft\Interne Explorer\Restrictions

متغییري از نوع 3 با نام NoBrowserOptions بسازید و مقدار درونش را 1 بدهید .

غیر فعال کردن Edit => view source

متغییري از نوع 3 با نام NoViewSource بسازید و مقدار درونش را 1 بدهید .

غیر فعال کردن View => Full screen

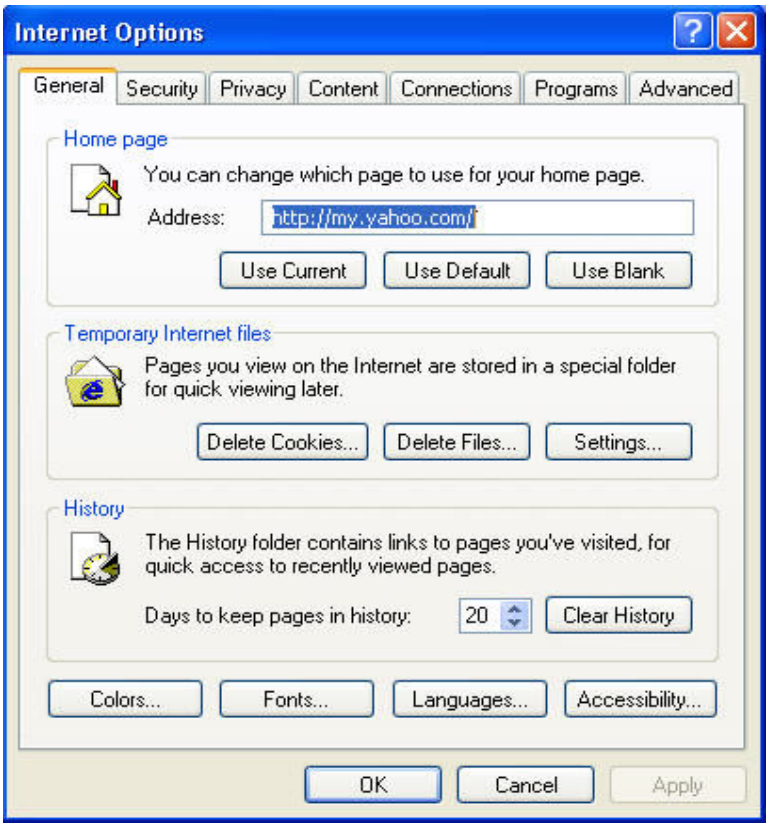
متغییري از نوع 3 با نام NoTheaterMode بسازید و مقدار درونش را 1 بدهید .

غیر فعال کردن Download

متغییري از نوع 3 با نام NoSelectDownloadDir بسازید و مقدار درونش را 1 بدهید .

Internet Option

شکل کلی Internet Option:

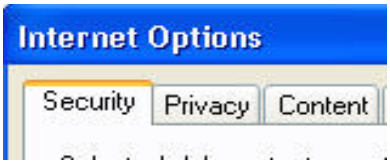


غیر فعال کردن تب General و گزینه هاي مختلف آن

به مسیر زیر بروید

HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel

متغییري از نوع 3 با نام GeneralTab بسازید ومقدار درونش را 1 بگذارید



غیر فعال کردن History

بازهم به مسیر بالا بروید متغییري از نوع 3 با نام History بسازید و مقدار درونش را 1 بگذارید . (در هر گزینه ای که مسیر ذکر نگردیده است ، مسیرش گزینه مورد نظر ، همان مسیر گزینه قبلی است .)

غیر فعال کردن دکمه Languages
بازهم به مسیر قبلي رفته و متغییري از نوع 3 با نام Languages ساخته و مقدارش را 1 بگذارید .

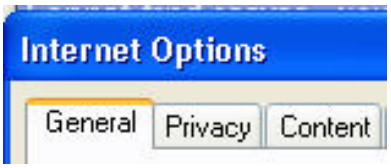
غیر فعال کردن Accessibility
متغییري با نام Accessibility از نوع 3 بسازید و مقدار درونش را 1 بگذارید .

غیر فعال کردن Temporary Internet files
متغییري از نوع 3 با نام Settings ساخته و مقدار درونش را 1 بدهید .

غیر فعال کردن Color
متغییري از نوع 3 با نام Colors ساخته و مقدار درونش را 1 بدهید .

غیر فعال کردن Font
متغییري از نوع 3 با نام Fonts ساخته و مقدار درونش را 1 بدهید .
دوباره به همان مسیر قبلی رفته و مقدار، متغییر links را برابر 1 کنید .

غیر فعال کردن Security Tab
متغییري از نوع 3 با نام SecurityTab ساخته و مقدار درونش را 1 بدهید .



غیر فعال کردن Level changes
متغییري از نوع 3 با نام SecChangeSettings ساخته و مقدار درونش را 1 بدهید .

غیر فعال کردن Privacy Tab
متغییري از نوع 3 با نام PrivacyTab ساخته و مقدار درونش را 1 بدهید

غیر فعال کردن Content Tab
متغییري از نوع 3 با نام ContentTab ساخته و مقدار درونش را 1 بدهید

غیر فعال کردن Profiles
متغییري از نوع 3 با نام Profiles ساخته و مقدار درونش را 1 بدهید

غیر فعال کردن Content Advisor
متغییري از نوع 3 با نام Ratings ساخته و مقدار درونش را 1 بدهید

غیر فعال کردن MS Wallet
متغییري از نوع 3 با نام Wallet ساخته و مقدار درونش را 1 بدهید

غیر فعال کردن AutoCompelet for forms
متغییري از نوع 3 با نام FormSuggest ساخته و مقدار درونش را 1 بدهید

غیر فعال کردن Autocompelet save password
متغییري از نوع 3 با نام FormSuggest Passwords ساخته و مقدار درونش را 1 بدهید

غیر فعال کردن Connections Tab
متغییري از نوع 3 با نام ConnectionsTab ساخته و مقدار درونش را 1 بدهید

غیر فعال کردن Internet Connection Wizard
متغییري از نوع 3 با نام Connwiz Admin Lock ساخته و مقدار درونش را 1 بدهید

غیر فعال کردن Dial-up setting
متغییري از نوع 3 با نام Connection Settings ساخته و مقدار درونش را 1 بدهید .

غیر فعال کردن Proxy setting
متغییري از نوع 3 با نام Proxy ساخته و مقدار درونش را 1 بدهید .

غیر فعال کردن Programs Tab
متغییري از نوع 3 با نام ProgramsTab ساخته و مقدار درونش را 1 بدهید .

غیر فعال کردن Reset Web setting
متغییري از نوع 3 با نام ResetWebSettings ساخته و مقدار درونش را 1 بدهید .

غیر فعال کردن E-mail, Newsgroups and Internet call
متغییري از نوع 3 با نام Messaging ساخته و مقدار درونش را 1 بدهید .

غیر فعال کردن Calendar/Contact list
متغییري از نوع 3 با نام CalendarContact ساخته و مقدار درونش را 1 بدهید .

غیر فعال کردن Default browser check
متغییري از نوع 3 با نام Check_If_Default ساخته و مقدار درونش را 1 بدهید .

غیر فعال کردن Advanced tab

متغییري از نوع 3 با نام AdvancedTabساخته و مقدار درونش را 1 بدهید .

غیر فعال کردن Changes

متغییري از نوع 3 با نام Advanced ساخته و مقدار درونش را 1 بدهید .

Disable Customize toolbar buttons

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری از نوع 3 با نام NoToolbarCustomize ساخته و مقدار درونش را 1 بگذارید .

Disable Configure toolbar buttons

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری از نوع 3 با نام NoBandCustomize ساخته و مقدار درونش را 1 بگذارید .

Win explorer

Disable Tools > Folder Options و همچنین کنترل پانل

برای انجام این کار به مسیر زیر از رجیستری بروید :

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

بعد در آن Value ای از نوع 3 (قبلا توضیح دادیم) بسازید و نام آن را NoFolderOptions بگذارید و مقدار درونش را 1 بگذارید .

نکته :

عدد 1 به معنی فعال بودن آن گزینه است و 0 (صفر) به معنی غیرفعال بودن آن مورد است .

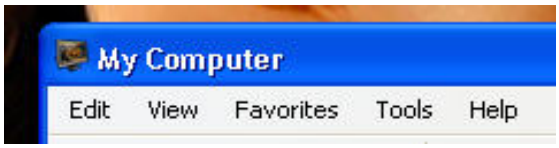
Hidden Device Manager

به مسیر زیر بروید
HKEY_USERS\.DEFAULT\Software\Windows\CurrentVersion\Policies\System
متغییری از نوع 3 با نام NoDevMgrPage ساخته ومقدار درونش را 1 بدهید.

غیر فعال کردن منوی File (internet explorer & win explorer)

به مسیر زیر بروید
HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

و متغییری از نوع 3 با نام NoFileMenu بسازید و مقدار درونش 1 بگذارید . برای غیر فعال کردن هرکدام از حالات انجام شده می توانید مقدار درون متغییر دستکاری شده را 0 و یا آن را حذف کنید که را اول یعنی 0 کردن مقدار بهتر است .



غیر فعال کردن تب های سخت افزاری در کنترل پانل و Properties my computer

به همان مسیر بالایی بروید و متغییری از نوع 3 با نام NoHardwareTab بسازید و مقدار درونش را 1 بگذارید .البته برای دیدن این کار احتیاج به Restart اصلی می باشد .

غیر فعال کردن Recycle Bin

به مسیر زیر بروید
HKCU \Software\Microsoft \Windows \Current Version \Policies\Explorer

متغییری از نوع 3 با نام NoRecycleFiles بسازید و مقدار درونش را 1 بگذارید .

غیر فعال کردن Security tab

متغییری از نوع 3 با نام NoSecurityTab بسازید و مقدار درونش را 1 بگذارید

تغییر مقدار رم مجازی (Virtual Memory)

برای این کار به مسیر زیر بروید

HKLM \SYSTEM\ ControlSet002\Control\Session Manager\Memory Management

متغییری از نوع 1 با نام Paging Files ساخته و مقدار درونش را براین اساس بدهید

" C:\pagefile.sys 800 1700 " عددهای 800 و 1700 را باید تغییر دهید .

و متغییر های PagedPoolSize و NonePagedPoolSize را اصلاح کنید .

غیر فعال کردن Manage

متغییري از نوع 3 با نام NoManageMyComputerVerb بسازید و مقدار درونش را 1 بگذارید

پاك كردن Shared Documents از My Computer

متغییري از نوع 3 با نام NoSharedDocuments بسازید و مقدار درونش را 1 بگذارید

افزودن گزینه Copy to folder . . . به منوي كليك راست

به مسیر زیر رفته

HKCR\AllFilesystemObjects \shellex \ContextMenuHandlers \Copy to

در متغییر Default آن این مقدار را وارد کنید

{C2FBB630-2971-11D1-A18C-00C04FD75D13}

براي برگرداندن به حالت اولیه ، مقدار آن را پاك كنيد (برابر Null كنيد) .

افزودن گزینه Move To . . . به منوي كليك راست

به مسیر زیر بروید

HKCR\AllFilesystemObjects \shellex \ContextMenuHandlers \Move to

و مقدار زیر را در متغییر Default آن بگذارید :

{C2FBB631-2971-11D1-A18C-00C04FD75D13}

براي برگردان ، مقدار را پاك كنيد (برابر Null كنيد) .

این دو مورد بالا درست است که به درد ویروس نمی خورد ، اما به درد خودتان که می خورد .

پنهان و قفل کردن درایوها در My Computer

به مسیر زیر بروید

HKLM\SOFTWARE\MicrosoftWindows\CurrentVersion\policie\Explorer

براي پنهان كردن متغيير No Drives مي باشد و براي قفل كردن درايو NoViewOnDrive مي باشد كه نوع هر دو متغيير از نوع 3 مي باشد .

ردیف	نام درایو	مقدار(Dec)	ردیف	نام درایو	مقدار(Dec)
1	A	1	8	H	128
2	B	2	9	I	256
3	C	4	10	J	512
4	D	8	11	K	1024
5	E	16	12	L	2048
6	F	32	13	M	4096
7	G	64	14	N	8192

* براي كل درايوها مقدار دهدهي (Decimal) 67108863 را قرار مي دهيم .

اگر می خواهید این اعمال بر روی چند درایو انجام گیرد،مقدار درایوهای مورد نظرتان را باهم جمع کنید (A + B = 3) و مقدار بدست آمده را در درون متغییر قرار دهید .

Desktop

مخفي كردن تمام آيتم هاي روي دسكتاپ

به مسیر زیر بروید

HKCU \Software Microsoft\Windows \ Current Version \Police\Explorer

متغييري از نوع 3 با نام No Desktop ساخته و مقدار درونش را برابر با 1 قرار دهيد .

تغییر تصویر زمینه در Safe Mode

به مسیر زیر بروید

HKCU \Software \Microsoft \Internet \Explorer \Desktop \Safe Mode \General

یک داده رشته ای با نام Wallpaper ساخته و مقدار درونش را مسیر فایل مورد نظر رات قرار دهید.

ازبین بردن Switch کردن بین برنامه ها

به مسیر زیر بروید

HKCU \ Control Panel \Desktop

متغییری از نوع 1 با نام Cool Switch ساخته و مقدار درونش را 0 قرار دهید .

غیرفعال کردن کادر کلیک راست بر روی دسکتاپ

حتی اگر کلید ترکیبی Alt + Enter را هم بیگیرید این کادر نمایش داده نمی شود ، به مسیرزیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری از نوع 3 با نام NoViewContextMenu ساخته و مقدار درونش را 1 بدهید .

پنهان کردن My Document از دسکتاپ

به این مسیر بروید

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktopIcons\NewStartPanel

متغییري از نوع 3 با نام {D8FBA-AD25-11D0-98A8-0800361B1103450} و مقدار درونش را 1 بگذارید .

تغیر عکس Background

به مسیرزیر بروید :

HKLM \Software \Microsoft \Windows \Current Version

مقدار درون متغییر WallPaperDir را مسیر عکس مورد نظر قرار دهید.

پاك کردن My Computer

باز هم به مسیر قبلي رفته . متغییري از نوع 3 با نام

{D04FE0-3AEA-1069-A2D8-08002B30309D20} ساخته و مقدار درونش را 1 بگذارید .

Lock desktop toolbars

به این مسیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییري از نوع 3 با نام NoCloseDragDropBands ساخته و مقدار درونش را 1 بگذارید .

Don't save settings on exit

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییري از نوع 3 با نام NoSaveSettings ساخته و مقدار درونش را برابر 1 بگذارید .

Disable all item properties

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop

متغییري از نوع 3 با نام No Components سا خته و مقدار درونش را برابر 1 قرار دهید .

Disable Active Desktop

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییري از نوع 3 با نام NoActiveDesktop ساخته و مقدار درونش را برابر با 1 قرار دهید .

نشان دادن پیغامی قبل از ورود به ویندوز

میتوانید پیغامی قبل ورود به ویندوز نشان هید (من که از این کارهای بچه گانه نمی کنم) ، به مسیر زیر بروید

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

دو متغییر از نوع1 با نام های LegalNoticeCaption و LegalNoticeText بسازید ، Title Bar را در متغییر اول و پیام را در متغییر دوم تایپ نمایید .

Start Menu

Remove My Documents

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version Policies\Explorer

متغییري از نوع 3 با نام NoSMMyDocs ساخته و مقدار درونش را برابر 1 قرار دهید

Remove my picture

به همان مسير قبلي رفته و متغييري از نوع 3 با نام NoSMMyPictures ساخته و مقدار درونش را برابر با 1 قراردهيد .

Remove My Network Places (Windows XP Professional only)

به مسير زير رفته

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغييري از نوع 3 با نام NoStartMenuNetworkPlaces ساخته و مقدار درونش را برابر با 1 بگذاريد.

پاك كردن My Computer

به مسير زير برويد

HKCU\Software\Microsoft\Windows\Current Version\Explorer\Advanced

متغييري با نام Start_ShowMyComputer از نوع 3 ساخته و مقدار درونش را 0 بدهيد.

پاك كردن گزينه پرينتر و فاكس

به مسير زير برويد

HKCU\Software\Microsoft\Windows\Current Version\Explorer\Advanced

متغييري از نوع 3 با نام Start_ShowPrinters ساخته و مقدار درونش را 0 بدهيد .

پاك كردن گزينه Run

به مسير زير برويد

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغييري از نوع 3 با نام NoRun ساخته و مقدار درونش را برابر با 1 قرار دهيد .

No Logoff

به مسير زير برويد و متغيير هايي از نوع 3 با نام No Logoff و StartMenuLogOff ساخته و مقدار درونش را برابر با 1 قرار دهيد .

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

Remove Turn off Computer button

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری از نوع 3 با نام No Close ساخته و مقدار درونش را برابر با 1 قرار دهید .

Remove Undock PC button (portables only)

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری از نوع 3 با نام NoStartMenuEjectPC ساخته ومقدار درونش را برابر با 1 قرار دهید.

Remove user name

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری از نوع3 با نام NoUserNameInStartMenu ساخته و مقدار درونش را برابر با 1 قرار دهید .

Clear history on exit

به مسیر زیر بروید .

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری از نوع 3 با نام ClearRecentDocsOnExit ساخته و مقدار درونش را برابر با 1 قرار دهید.

Disable Drag-and-drop

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری از نوع 3 با نام NoChangeStartMenu ساخته و مقدار درونش را برابر با 1 قرار دهید .

Remove All Programs

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری از نوع 3 با نام NoStartMenuMorePrograms ساخته و م قدار درونش را برابر با 1 قرار دهید .

Lock Taskbar and Start menu settings

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری از نوع 3 با نام NoSetTaskbar ساخته و مقدار درونش را 1 قرار دهید .

Lock Taskbar

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری با نام Lock Taskbar از نوع 3 ساخته و مقدار درونش را برابر 1 قرار دهید .

افزودن متن به ساعت سیستم

به این مسیر بروید

HKCU \Control Panel \ International

متغییری از نوع 1 بانام S1159 و S2359 را ساخته و مقدار درونش را هرچه خواستید بگذارید .

Remove & Disable Toolbars from Taskbar

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری از نوع 3 با نام NoToolbarsOnTaskbar ساخته و مقدار درونش را برابر 1 قرار دهید .

Remove Clock

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییري از نوع 3 با نام Hide Clock ساخته و مقدار درونش را برابر با 1 قرار دهید .

Hide notification area

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییري با نام NoTrayItemsDisplay ازنوع 3 ساخته و مقدار درونش را برابر با 1 قرار دهید .

Control Panel

Disable Control Panel access

براي انجام اين كار به مسير زير برويد

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغييري از نوع 3 با نام NoControlPanel ساخته و مقدار درونش را برابر با 1 قرار دهيد .

مشاهده اطلاعاتی در مورد Bios

به مسير زير برويد

HKLM \HARDWARE \DESCRIPTION \SYSTEM

تمام کلید های موجود در این قسمت مربوط به Bios میباشد . که بعد ها به دردتان می خورد .

مدیریت اولویت عملیات در CPU

به مسير زير برويد

HKLM \ System \CurrentControlSet \Services \VxD\ Bios

داده ای از نوع 3 با نام CPUPriority ایجاد کنید و مقدار درونش را 0 وارد کنید که عملیات پیش زمینه بلادرنگ انجام شود که این حالت امکان قفل کردن دیگر برنامه ها و خود کامپیوتر را زیاد می کند.

حذف امکان افزودن چاپگر جدید

به این مسیر بروید

HKCU \Software \Microsoft \Windows \Current Version \Policies \Explorer

مقداری از نوع 3 با نام NoAddPrinter ساخته و مقدار درونش را 1بدهید .

Restrict Add/Remove Programs

براي انجام اين كار به مسير زير برويد

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall

متغييري از نوع 3 با نام NoAddRemovePrograms ساخته و مقدار درونش را برابر با 1 قرار دهيد

Hide Change/Remove button

براي اين كار به مسير زير برويد

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall

متغييري از نوع 3 با نام NoRemovePage ساخته و مقدار درونش را 1 بگذاريد .

Disable Display

براي انجام اين كار به مسير زير برويد

HKCU\Software\Microsoft\Windows\Current Version\Policies\System

متغييري از نوع 3 با نام NoDispCPL ساخته ومقدار درونش را برابر با 1 قرار دهيد .

و اینک بهترین کاری که میتوان در کنترل پانل انجام داد ، پنهان کردن بخش های مختلف آن است پس ادامه را بخوانید :

برای این کار اول از همه به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explorer

متغییری از نوع 3 با نام DisallowCpl بسازید و مقدار درونش را 1بدهید تا مجوز پنهان کردن صادر شود . حالا به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\Explore\ DisallowCpl

به تعداد گزینهای که می خواهید پنهان شود، متغییر از نوع 1 بسازید و نام هایشان را از 1 تا آخر (8 یا 10 و . . .) یعنی متغییر اول نامش را یک قرار دهید ، متغییر دوم نامش را دو قرارد دهیدوالآخر.
و هر گزینه ای را که می خواهید پنهان شود از ستون آیتم مورد نظر پیدا کنید و مقدار نسبت داده شده آ ن را در درون متغییر وارد کنید ، در هر متغییر فقط یک گزینه را قرار دهید .

ردیف	آیتم مورد نظر	مقدار نسبت داده شده
1	Fire Wall	firewall.cpl
2	Sounds and Audio Devices	mmsys.cpl
3	Phone and Modem Option	telephon.cpl
4	Date and Time	timedate.cpl
5	Power Option	powercfg.cpl
6	Internet Option	Inetcpl.cpl
7	User Account	nusrmgr.cpl

Ncpa.cpl	Network Connection	8

غیر فعال کردن فایروال

به مسیر زیر بروید

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile

متغییری از نوع 3 با نام Enable Firewall بسازید و مقدار آن را 0 بدهید .

Change Color quality

به همان مسیر قبلی بروید و متغییری از نوع 3 با نام DefaultSettings.BitsPerPel ساخته و مقدرش را در حالت دسیمال بدهید . حالا یا 16 یا 32 یا 64 بدهید .

جابجا شدن کلید چپ و راست ماوس

باید به مسیرزیر بروید

HKCU\Control Panel\Mouse

متغییری از نوع 1 یا نام SwapMouseButtons بسازید و مقدار درونش را 1 بدهید .

تعیین سرعت ماوس

به همان مسیر قبلی بروید و متغییری از 1 با نام Mouse Sensitivity بسازید .
کمترین سرعت عدد 1 و بیشترین سرعت عدد 20 است .

تعیین سرعت دابل کلیک

به همان مسیر قبلی رفته و متغییری از نوع 1 با نام DoubleClickSpeed بسازید .
کمترین سرعت عدد 200 و بیشترین سرعت عدد 900 است .

و حالا اصلی ترین کارهای یک ویروس برای غیر فعال نشدنش :

بهترین پیشنهادی که من می توانم به شما بدهم اینست که کاری بکنید ویروس تان طوری بسازید که بعد عوض کردن ویندوز بازهم ویروستان اجرا بشود (همه تان این را خوب میدانید) و برای این کار عمومی ترین راه اینست که یک فایل Auto Run برایش بسازید .
برای ساخت این فایل Notepad را باز کنید و در درونش این تکه کد را تایپ بکنید :

[auto run]
نام فایل مورد نظر =OPEN

و سپس آن با اسم دلخواه و با پسوند inf ذخیره کنید و هرگاه ویروس را در جایی کپی می کنید حتما فایل Auto Run را همراهش کپی کنید (ویروس و فایل Auto Run همیشه در کنار هم باشند) .

یک اسم کوتاه به ویروس تان بدهید که اگه شخص قربانی (Victim) خواست ویروس تان را از درون Task Manager ازبین ببرد اشتباه کند و گمراه شود و فکر کند که یکی از برنامه های در حال اجرای خود ویندوز هست (مثلا اسمی به نام csmm) .

برای اینکه خودکار اجرا شود هیچ وقت آن را درون پوشه Startup کپی نکنید ، و یا در رجیستری در بخش مربوط به Msconfig برایش مقداری نسازید . چرا ؟
چون تمام این کار ها باعث نشان دادن آن در بخش تنظیمات Startup از پنجره Msconfig (System Configuration Utility) می شود و درصد از بین بردن آن بیشتر میشود . پس چکار کنید ؟
به مسیر زیر در رجیستری رفته

HKLM \Software \Microsoft \WindowsNT \Current Version \Win logon

متغییری از نوع string به نام Shell دارد ، شما میتوانید آدرس ویروس را بعد از متن درونش (explorer.exe) با یک کاراکتر فاصله بنویسید تا قبل از بقیه برنامه اجرا شود .
و یا می توانید در فایل System.ini جای دهید .

Disable CMD

برای انجام این کار به مسیر زیر بروید

HKCU\Software\Policies\Microsoft\Windows\System

متغییری از نوع 3 با نام DisableCMD ساخته و مقدار درونش را برابر با 2 (دو) قرار دهید .

Disable registry editing tools

خداییش این کار خیلی باحاله ، امتحان کن تا " فکت بیفته " (تیکه کلام خودم) .
به مسیر زیر بروید

HKCU\SOFTWARE\Microsoft\Windows\Current Version\Policies\System

متغییری از نوع 3 با نام DisableRegistryTools ساخته و مقدار درونش را 1 بدهید .

Disable System Restore

به مسیر زیر بروید

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\System Restore

متغییری از نوع 3 با نام DisableConfig بسازید ومقدار درونش را 1 بدهید .

Disable Task Manager

به مسیر زیر بروید

HKCU\Software\Microsoft\Windows\Current Version\Policies\System

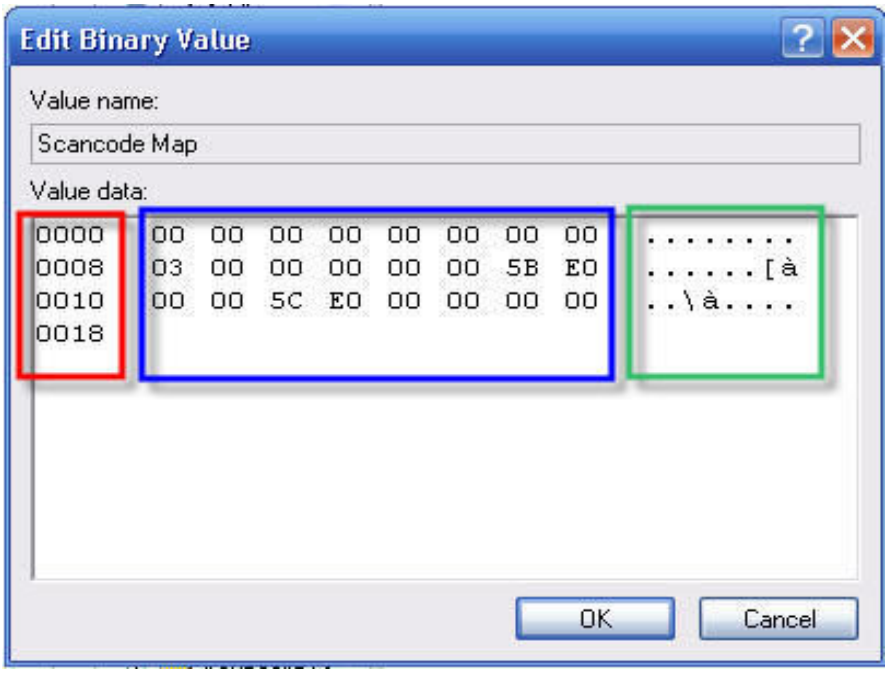
متغییری از نوع 3 با نام DisableTaskMgr بسازید ومقدار درونش را 1 بدهید .

Disable Win Key

به مسیرزیر بروید

HKLM\SYSTEM\CurrentControlSet\Control\Keyboard Layout

متغییری از نوع 2 با نام Scan code Map ساخته و مقدار درونش را براساس شکل زیر تنظیم کنید .



نکته :
شکل بالا دارای 3 ناحیه مشخص شده می باشد که مهمترین آن ناحیه آبی است ، ناحیه های قرمز و سیز به صورت خودکار در حین انجام کارتان درج می شود ، وارد کردن مقادیر به صورت بالا زیاد سخت نیست (نترسید !!) ، اگر شما خط اول را کامل کنید (شانزده بار عدد صفر را وارد کنید) نشانگر ماوس بصورت خودکار به خط پایین میرود ، و اگر شما در خط دوم کادر آبی ، عبارت 5B E0 را وارد کنید عبارت ([a) خودکار در کادر سبز درج میشود . و ادامه کار هم براین اساس است .

امیدوارم استفاده کامل را برده باشید ، اگردر مقاله مشکلاتی بود من را ببخشید .

پایان