شهروندیار تقدیم میکند

چگونه ارتباط امن در اینترنت داشته باشیم؟!

http://www.shahrvand-yar.com

کدام ایمیل امن تر است؟

آیا می دانید یاهو "Yahoo" و هات میل "Hotmail" بر خلاف جی میل "Gmail" ، آدرس IP شما که نشان دهنده محل زندگی شماست را برای گیرنده می فرستند!

جی میل با رمز گزاری تمامی صفحات ایمیل، مانع از دسترسی به اطلاعات، در حین انتقال پیام از گیرنده به فرستنده می شود.

بنابراین از بین سه ایمیل رایج،

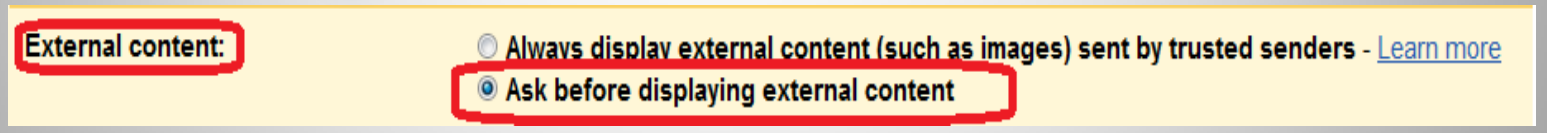
جی میل از بقیه امن تر است.

اگر از Gmailاستفاده می کنید:

" از باز شدن خودکار عکسها در Gmail جلوگیری کنید! "

برای اینکار، بعد از ورود به Gmailخود، به صفحه **" Settings "** رفته و از آنجا سربرگ General را انتخاب کنید .

حالا در قسمت **External Content**، گزینه **Ask before displaying external content**را تیک زده و سپس روی گزینه **"Save changes"** کلیک کنید.



باز شدن خودکار عکس ها در جی میل می تواند همراه با دانلود فایلهای مخرب باشد.

اگر خواستید عکس ها را ببینید " Display images below " در بالای ایمیلتان را بزنید.

کاربران Gmailبهتر است:

" صفحات Gmail را با پروتکل امنیتی SSL رمز گذاری کنند"

برای این کار بعد از ورود به Gmailخود، **Settings** را کلیک و سپس گزینه **General**را انتخاب کنید.

حال در قسمت **"Browser connection"** ، **"Always use https"** را تیک زده و سپس در پایین صفحه روی گزینه **"Save changes"** کلیک کنید.

با این کار برای همیشه همه صفحات Gmailشما رمز گزاری شده تا هیچ کس امکان دسترسی به محتوای ایمیل شما را نداشته باشد.

آیا ایمیلی با سطح امنیت بسیار بالا می خواهید؟

بسیاری از مراکز حساس برای حفظ امنیت ارتباطاتشان از این ایمیل استفاده می کنند.

از این سرویس، مجانی هم می توان استفاده کرد، اما ممکن است مدتی طول بکشد تا با درخواست شما موافقت شود.

البته اگر دو کاربر برای شما دعوتنامه بفرستند، شما می توانید عضو این سرویس دهنده ایمیل شوید.

چند نکته ساده برای امنیت حساب کاربری شما

چند ایمیل داشته باشید!

ایمیلهایی را که برای موارد خصوصی تر و امن تر بکار می گیرید، از ایمیلهای کم اهمیت جدا کنید و این ایمیل ها را در اختیار عموم نگذارید.

ایمیلهای مهم را بعد از دریافت " Delete" کرده و از " Trash" ایمیل خود نیز پاک کنید.

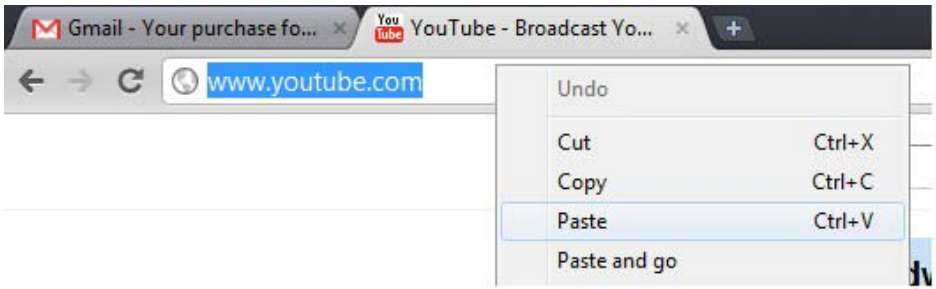
چند مرورگر (Google chrome، Internet Explorer و . .) داشته باشید و ایمیلها و صفحات خصوصی ترخود را در مرورگری جداگانه باز کنید.

ایمیل ها و حسابهای کاربری مهم خود را با نام و مشخصاتی که باعث شناسایی شما نمی شود، بسازید.

اطلاعات مهم بازیابی ایمیل یا حساب کاربری خود و پسورد آن را در اختیار دوستی مطمئن قرار دهید تا در صورت شرایط اضطراری، از امکان دسترسی غیر مجاز به حساب کاربری شما جلوگیری شود

با لینک هایی که به شما ایمیل می شود، چه باید کرد؟

روی لینکهایی که به ایمیل شما فرستاده می شود، مستقیما کلیک نکنید. ابتدا آدرس لینک را کپی کرده و سپس آن را در آدرس بار وارد و صفحه را باز کنید!



دقت کنید!

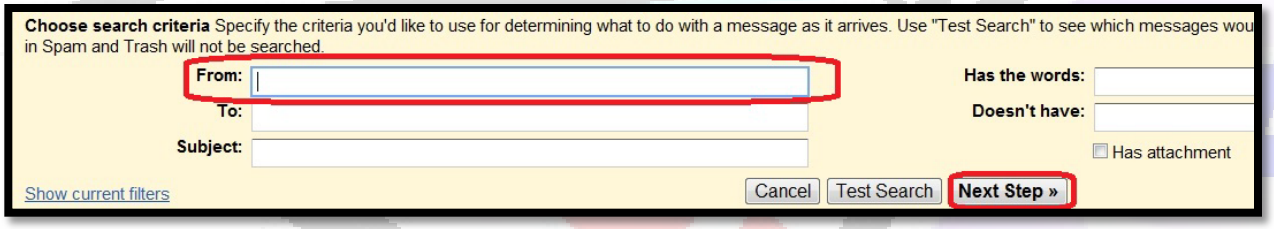
ممکن است آدرس لینکی که به شما ایمیل می شود، آدرس واقعی نباشد.

هیچگاه لینک های مشکوکی که از طرف افراد ناشناس، به شما ایمیل می شود را باز نکنید.

چگونه ایمیل های مشکوک و مزاحم را بلاک (Block) یا فیلتر کنیم؟

بعد از باز کردن جی میل، در کنار دکمه **Search the Web** در بالای صفحه روی گزینه **Create e filter**کلیک کنید.

سپس آدرس ایمیلی را که می خواهید **Filter** کنید، در قسمت **From** نوشته و **Next Step** را بزنید.



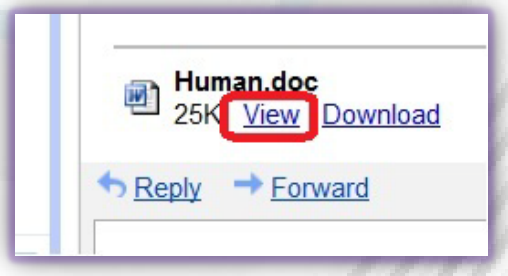
در صفحه بعد، **Delete It** را تیک زده و سپس **Create Filter** را کلیک کنید.

این ایمیل دیگر به شما فرستاده نخواهد شد.

با فایلهای ضمیمه ایمیل (Attachments) چه کنیم؟

برای امنیت بیشتر، فایلهایی را که از ایمیل خود دانلود می کنید، ویروس یابی کنید. برای اینکار پس از دانلود فایل و قبل از اینکه آن را باز کنید، روی آن کلیک راست کرده و سپس گزینه "اسکن (Scan) ویروس یاب خود" را بزنید.

برای باز کردن برخی فایلها، نیازی به دانلود آن به رایانه شما نیست، تنها کافیست در کنار فایل روی کلمه Viewکلیک کنید.



اتچمنتهای مشکوک، از طرف افراد ناشناس را باز نکنید. مخصوصا اگر پسوند آن **Exe**باشد.

اتچمنتهایی با پسوندهایی نظیر bif، vbs، scr و bat که غالبا برای برنامه نویسی ویروس ها، مورد استفاده قرار می گیرد، را **ابدا باز نکنید.**

شما در جی میل می توانید این پسوندها را فیلتر کرده تا هرگز به شما فرستاده نشوند.

قبل از دانلود هر فایلی از روی اینترنت، آنرا ویروس یابی کنید.

کافیست: لینک فایلی را که می خواهید دانلود کنید، در قسمت "**submit a URL**"سایت www.virustotal.com وارد کرده و سپس **Enter** کنید.

این سایت لینک فایل شما را با دهها برنامه ویروس یاب کنترل کرده و نتیجه را می گوید.

اگر در رایانه خود فایل مشکوکی داشته باشید که می خواهید امنیت آنرا بررسی کنید، کافیست فایل را به آدرس scan@virustotal.com ایمیل کنید.

یک آنتی ویروس یا نرم افزار امنیتی خوب چه ویژگی هایی دارد؟

آنتی ویروس شما باید متعلق به یک شرکت معتبر مانند Norton، McAfee و . . . باشد.

قابلیت بروز رسانی (Update) داشته و توسط شما مدام بروز شود.

در زمان اتصال به اینترنت همیشه روشن (ON) باشد.

هر چند وقت یکبار و بنا به ضرورت، کل رایانه شما را ویروس یابی (Full system Scan) کند.

دقت کنید، استفاده از برنامه های امنیتی مجانی با قابلیت بروز رسانی (مانند Avast و . . . ،) بهتر از ویروس یاب های قفل شکسته یا کرک شده است.

آیا برنامه امنیتی شما کامل است؟

تنها برنامه ویروس یاب برای امنیت رایانه شما کافی نیست. شما باید برنامه های فایروال (firewall) و ضد جاسوس افزار (SpyWare) نیز روی رایانه خود داشته باشید.

برخی نرم افزارهای امنیتی با امکانات کامل (Full Options)، همه این گزینه ها را دارند!

چگونه یک پسورد (رمز عبور) امن و قوی بسازیم؟

رمز عبورهایی قوی هستند که پیچیده و ترکیبی از اعداد، حروف بزرگ، حروف کوچک و علایمی نظیر (؟ ! @ + - * / > < . = : #) باشند.

یک رمز عبور قوی نباید کوتاه باشد و یا از حروف مشابه یا پشت سرهم تشکیل شود.

تاریخ تولد، نام پدر، نام شهر و یا اطلاعاتی که هکرها و یا دوستان شما بتوانند آنها را از منابع مختلف بدست آورند، رمز عبور قوی به شمار نمی رود!

رمز عبور خود را بصورت دوره ای تغییر دهید.

آیا می دانید اگر رمز عبور ساده داشته باشید، برخی نرم افزارها می توانند در کمتر از چند دقیقه آنرا بیابند!

چگونه رمز عبور خود را بازیابی کنیم؟

اگر رمز عبور خود را فراموش کرده یا هک شدید، می توانید با پاسخ صحیح به پرسشهایی که در زمان ساخت ایمیل یا هر حساب کاربری داده اید، رمز عبور جدیدی را دریافت و دوباره حساب کاربری خود را بدست آورید.

بنابراین همیشه این سوال و جواب ها را به یاد داشته باشید.

دقت کنید!

همیشه بازیابی حساب کاربری شما بصورت پرسش و پاسخ نیست، ممکن است ایمیل یا شماره تلفنی را برای بازیابی ایمیل خود داده باشید.

در اینصورت رمز عبور جدید به شما ایمیل یا اس ام اس خواهد شد.

روی رایانه خود رمز بگذارید!

با طی کردن مراحل زیر در ویندوز XP، می توانید روی رایانه خود رمز بگذارید:

Start >Control panel >User Account> Your User Name> create a password

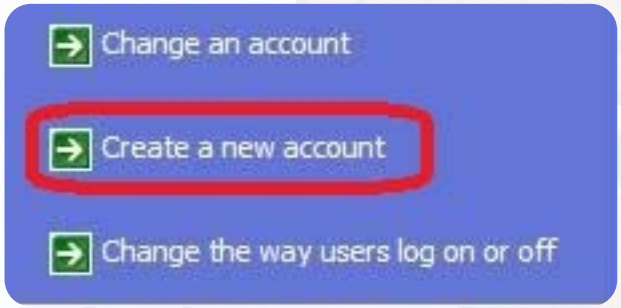
با این رمزگزاری، کسی بدون داشتن رمز، نمی تواند به رایانه شما دسترسی داشته باشد.
این رمزگزاری مانند اسکرین سرورهای رمز دار عمل کرده و اگر مدتی با رایانه خود کار نکنید، بطور اتوماتیک قفل می شود.

شما می توانید رایانه خود را با نگه داشتن همزمان دکمه ی "ویندوز" و" L " قفل کنید.

برای رایانه خود چند یوزر (شناسه کاربری) تعریف کنید!

اگر احتمالا چند نفر با رایانه شما کار می کنند، برای آنها چند شناسه کاربری با میزان دسترسی محدود درست کنید.

مانند اسلاید قبلی با پیمودن مراحل زیر برای رایانه خود یک یا چند شناسه کاربری تعریف کنید:



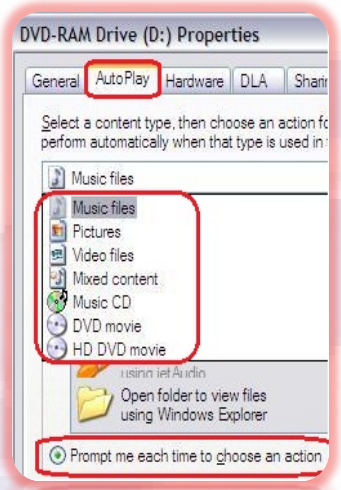
START > CONTROL PANEL > USER ACCOUNTS > YOUR USER NAME

قابلیت اتوران (Auto Run) رایانه خود را خاموش کنید!

قبل از استفاده از هر نوع حافظه جانبی مانند: سی دی ها، فلش مموری ها و رم های دوربین و موبایل، قابلیت Auto Run رایانه را خاموش کنید.

برای خاموش کردن قابلیت اتوران در ویندوز XP

در قسمت My Computer روی درایو CD ROMراست کلیک کرده و منوی Propertiesرا انتخاب کنید.



حال روی تب Auto play کلیک کنید و تک تک لیست کرکره ای (Music files، Picutures و . . .) را انتخاب و گزینه prompt me each time to choose an action را انتخاب و OK کنید.

دقت کنید!

هنگام استفاده از حافظه های جانبی، آنتی ویروس شما به روز (Update) و روشن باشد.

نرم افزارهای خود را به روز (Up date) کنید.

بروز رسانی، یعنی نصب آخرین تغییرات نرم افزار ها از روی وب سایت سازنده آن

با به روز کردن نرم افزارها، حفره های نا امن برنامه مسدود می شود.

به روز کردن ویندوز یا سیستم عامل و کلا مرورگرهای اینترنتی مانند Internet explorer، Google chrome

و...بیش از سایر برنامه ها ضروری است

بروز رسانی، صرفا به معنی ارتقا نسخه نرم افزار نیست. نسخه های قدیمی نیز بروز می شوند.

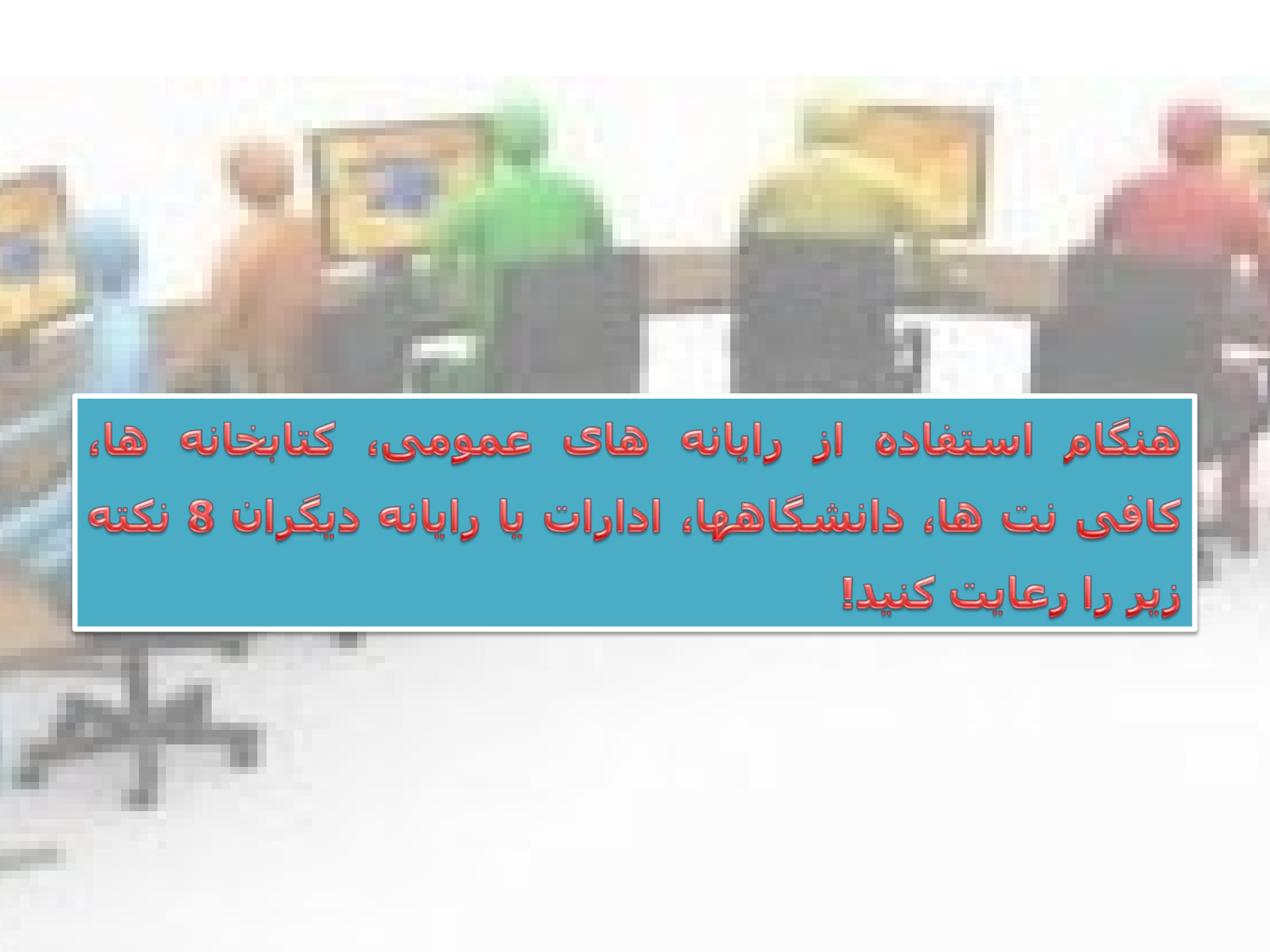
از پاک کردن (Remove) دقیق نرم افزارهایی که نمی خواهید، مطمئن شوید!

برای پاک کردن نرم افزارها، Deleteکردن فایل اجرایی آن اشتباه بزرگی است .

برای پاک کردن نرم افزارها، قابلیت Remove یا Uninstall کردن ویندوز نیز کافی نیست.

شما برای اینکار می توانید از نرم افزارهایی مانند " Revo Uninstaller" استفاده کنید.

به این ترتیب مطمئن خواهید شد، همه ردپاهای برنامه هایی که دیگر به آن نیاز ندارید، پاک شده است.



هنگام استفاده از رایانه های عمومی، کتابخانه ها، کافی نت ها، دانشگاهها، ادارات یا رایانه دیگران 8 نکته زیر را رعایت کنید!

1. از نرم افزارهای پرتابل(روی دیسکت یا فلش مموری) خود استفاده کنید!

هنگام استفاده از برنامه هایی مانند Yahoo messenger، Google chromeو . . . ردپای فعالیت شما برروی رایانه میزبان ثبت می شود.
زمانیکه شما نسخه پرتابل (قابل حمل) این برنامه ها را روی فلش مموری خود نصب کنید، اطلاعات شما بر روی رایانه میزبان باقی نخواهد ماند.

نرم افزارهای پرتابل، نرم افزارهایی هستند که بدون نیاز به نصب (Setupیا) Install، بر روی هر رایانه ای اجرا می شوند.

برنامه های "پرتابل مرورگرها و مسنجرها" از اهمیت بیشتری برخوردار هستند.

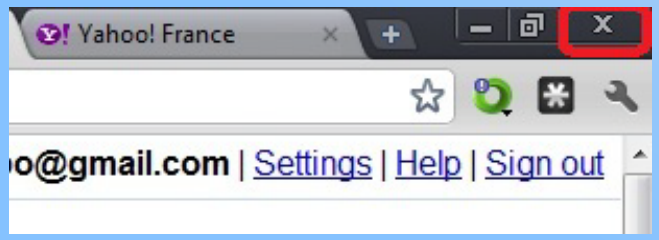
پس، هنگام استفاده از رایانه دیگران، فلش مموری حاوی نرم افزارهای پرتابل را همراه داشته باشید.

2؛ در هنگام ورود به ایمیل یا حساب کاربری خود، دقت کنید تیک مربوط به Saveپسورد را برداشته باشید!

اگر تیک save پسورد زده شده باشد، نفر بعدی که از رایانه شما استفاده می کند، براحتی وارد ایمیل یا حساب کاربری شما شده و تمام اطلاعات رد و بدل شده را مشاهده می کند!

3؛ قبل از پایان کار با رایانه، حتما از تمام حساب های کاربری خود خارج (sign out) شوید.

دقت کنید هیچگاه برای خروج از حساب کاربری خود قبل از Sign Out، آیکن ضربدر در گوشه راست بالای هر برنامه ای را نزنید.



4؛ حدالمقدور از رایانه دیگران استفاده نکنید، ممکن است کامپیوتر دیگران آلوده به نرم افزار جاسوسی (Spyware)باشد و اطلاعات شما را به سرقت برد.

رایانه خود را نیز به همین دلیل در اختیار کسی قرار ندهید.

5؛ قبل از ترک "رایانه ی که از مرورگر آن استفاده کرده اید"، اطلاعات ذخیره شده روی آن از جمله History، Temporary Internet files، کوکی ها، کش مرورگر و رمزهای عبور را پاک کنید.

به عنوان نمونه در Google chrome می توانید با کلیک روی علامت آچار در گوشه سمت راست مرورگر، گزینه Options را انتخاب و سپس روی گزینه Under the Hood کلیک کنید.

حال Clear browsing data را انتخاب و پس از تیک زدن همه گزینه ها Clear browsing data را بزنید.

6؛ بعد از اتمام کار با رایانه، فایلهایی را که با آنها کار کردید، Deleteکنید. سپس آشغالی خود (Recycle Bin) را نیز خالی کنید.

7؛ از کافی نت ها و رایانه های عمومی نا امن استفاده نکنید.

از کافی نت ها یا مراکز عمومی که امکان ریست کردن، پاک کردن هیستوری، خالی کردن آشغالی و . . . را بسته اند، استفاده نکنید. این کافی نت ها نا امن هستند.

8؛ با کیبورد مجازی رمز عبور خود را وارد کنید.

با فشار دادن همزمان کلید ویندوز و U، کیبورد مجازی ظاهر می شود، حال با موس روی دکمه های کیبورد مجازی کلیک و رمز عبور خود را در محل مورد نظر وارد کنید.

ممکن است نرم افزارهای جاسوسی یا Spyware ها در کمین نشسته تا با زدن کلیدهای کیبورد، رمز عبور شما را بدست آورند.

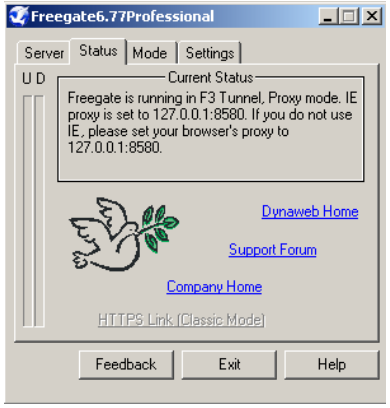
رعایت این 8 نکته روی هر رایانه ای، امنیت شما را افزایش می دهد.

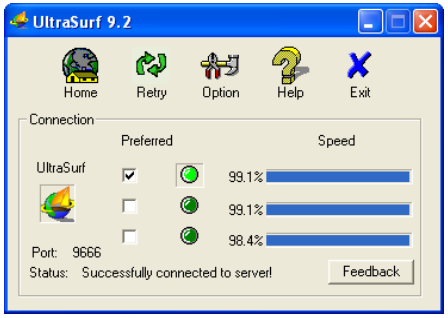
از وی پی ان (VPN) های معتبر، استفاده کنید.

VPNها، آدرس آی پی شما که "نشان دهنده محل استفاده شما از اینترنت" است را بوسیله یک سرور خارجی تغییر و غیر قابل شناسایی می کنند.

VPNها، ضمن عبور شما از فیلتر با رمز گزاری بروی اطلاعات، آنها را برای هکرها و آی اس پی ها غیر قابل خواندن می کنند.

نرم افزارهایی مانند Ultrasurf و Freegateکارهایی مشابه را برای شما انجام می دهند.





در هنگام استفاده از رایانه های عمومی، VPNها را می توانید روی فلش مموری خود همراه داشته باشید.

اشتراک فایل ها در اینترنت را غیر فعال کنید.

روشن بودن این گزینه امکان دسترسی هکرها، به محتویات رایانه شما را آسان تر می کند.

برای خاموش کردن اشتراک فایل ها، بعد از ورود به Control Panel و انتخاب Folder Options، گزینه Viewرا انتخاب کنید.

سپس با برداشتن تیک Use simple file sharing روی دکمه Okکلیک کنید.

مراقب صفحات مشابه جعلی یا Spoofing ها باشید.

در این حملات، هکرها با ساختن صفحاتی با آدرس هایی مشابه که دارای شکل و شمایلی یکسان با سایتهای مهم هستند، می کوشند تا خود را به عنوان سایت اصلی جا بزنند.

قربانی spoofing ها، با تصور اینکه به سایت اصلی رفته، رمز عبور و شناسه کاربری خود را وارد می کند. اما با اینکار در واقع آنرا در اختیار هکرها قرار داده است.

برای جلوگیری از این حملات، همیشه آدرس دقیق سایتها را کنترل کنید.

برای نمونه این آدرس، مشابه فیس بوک است: www.fasebook.com

اما آدرس دقیق فیس بوک این است : www.facebook.com

اگر اتفاقات زیر برای شما افتاد، به احتمال قوی هک شده اید.

ایمیلتان بدون دخالت شما، خوانده شده یا پاسخ داده شود.

بدون دخالت شما، ایمیلهایی برای دیگران فرستاده شود.

دیگر نمی توانید با رمز عبور صحیح، وارد ایمیل، فیس بوک و . . . شوید.

بخاطر ایمیلهای تبلیغاتی زیاد که شما نفرستاده اید (اسپم ها)، از شما شکایت شده باشد.

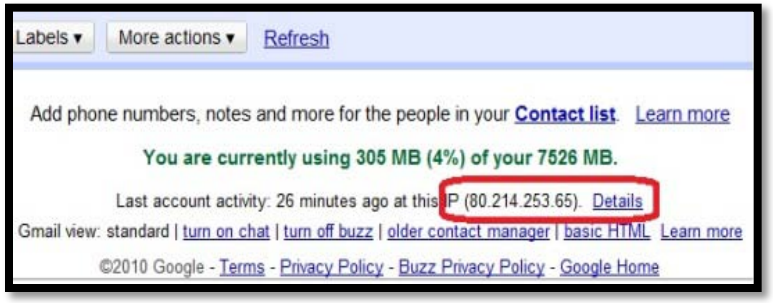
در اینصورت رمز عبور خود را عوض و رایانه خود را از لحاظ امنیتی بررسی کنید.

اگر نمی توانید وارد حساب کاربری خود شوید، باید ایمیل یا حساب کاربری خود را با اطلاعاتی که در زمان ثبت آن داده اید، بازیابی کنید.

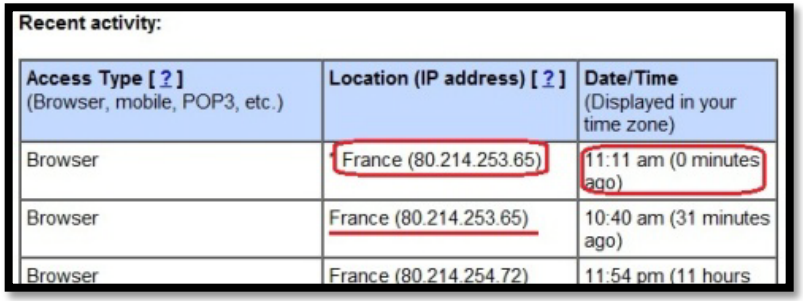
اگر آدرس Gmail دارید و فکر می کنید، هک شده اید!

آخرین آی پی آدرس هایی که ایمیل شما با آن باز شده است را کنترل کنید.

برای اینکار در زیر صفحه ایمیل خود، روی لینک Details کلیک کرده تا 10 آدرس آی پی (IP address) آخری که با آن ایمیل شما باز شده است را ببینید!



اگر این آی پی آدرس ها و زمانهایی که به ایملتان وارد شده اید، متعلق به شماست، نگران نباشید!



Recent activity:

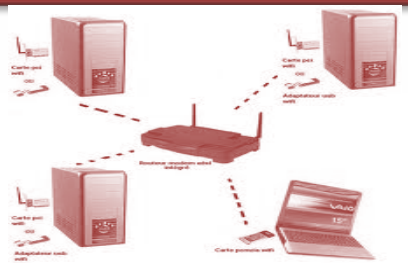
Access Type [?] (Browser, mobile, POP3, etc.)	**Location (IP address) [?]**	**Date/Time** (Displayed in your time zone)
Browser	France (80.214.253.65)	11:11 am (0 minutes ago)
Browser	France (80.214.253.65)	10:40 am (31 minutes ago)
Browser	France (80.214.254.72)	11:54 pm (11 hours

دقت کنید:

تغییر چند شماره آخر آی پی های شما، بسته به نوع اتصال شما به اینترنت عادی است.

اگر از برنامه هایی مانند Ultrasurf و Freegate برای عبور از فیلتر یا تغییر آدرس آی پی خود استفاده می کنید، تغییر کلی آدرس آی پی شما نیز عادی است. کافیست که زمان ورود به ایمیل خود را کنترل کنید.

در صورت استفاده از مودم های وی فی (WI FI)، رمز عبور اولیه را تغییر دهید.



برای جلوگیری از دسترسی دیگران به ارتباطات وی فی (یا بی سیم)، بعد از خرید این مودمها (MODEM) حتما نام کاربری و رمز عبور خود را تغییر دهید.

عموما مودم های شرکتهای مختلف، بصورت پیش فرض رمز عبور یکسانی دارند که حدس آن برای هکرها آسان است.

برای تغییر رمز عبور و احتمالا حساب کاربری خود، در بخش تنظیمات مودم به دنبال کلمه هایی مانند: Administration یا Administrator Setting باشید، سپس رمز عبور و شناسه کاربری خود را تغییر دهید.

در صورت استفاده از مودم های وی فی، ارتباطات خود را رمز گزاری کنید.

برای اینکار کافیست در تنظیمات مودم، به دنبال کلمه WPA2بوده و آنرا انتخاب یا فعال کنید، با این کار یکی از قوی ترین رمز گزاری ها روی ارتباطات بی سیم شما انجام می شود.

در صورتیکه WPA2 روی تنظیمات مودم شما یافت نشد به دنبال کلمه WPA باشید که ارتباط نسبتا امنی را برای شما فراهم می کند.

شهروندیار

همیار شهروندان

www.shahrvand-yar.com