

|             |       |
|-------------|-------|
| مراجعه:     |       |
| نویسنده:    |       |
| سایت منبع:  | قاصدک |
| موضوع جزئی: | 0     |
| موضوع خاص:  | 0     |

|            |          |
|------------|----------|
| موضوع کلی: | کامپیوتر |
| زیر موضوع: | 0        |
| متن سند:   |          |

### نکته امنیتی در مورد gmail

وبلاگ رسمی جی میل مطلبی را منتشر کرده با عنوان نکات امنیتی در مورد حساب های کاربری جی میل. بخاطر اهمیتی که این موضوع داره بد ندیدم این مطلب را بصورت آزاد ترجمه کرده و اینجا قرار بدم تا مورد استفاده دوستان قرار بگیره.

داشتن یک رمز عبور قوی در حفظ اطلاعات شما کمک زیادی می کند اما علاوه بر این باید چند کار دیگر انجام دهید تا خیالتان از بابت امنیت اکانت جی میلانت راحت شود :

1. حتما از ایمیل تان خارج شوید. بخصوص هنگامی که با استفاده از یک کامپیوتر عمومی به جی میل وارد می شوید (مثلا در کافی نت یا سایت دانشگاه یا محل کار) حتما پس از تمام شدن کارتان از صندوق ایمیل خود خارج شوید (sign out). کار سختی نیست، فقط بر روی لینک sign out در گوشه بالا و راست صفحه ایمیلانتان کلیک کنید. اگر می خواهید خیالتان راحت تر شود حتما پس از این کار cache ، کوکی ها و تاریخچه (history) مرورگرتان را هم پاک کنید. سپس مرورگر را بصورت کامل ببندید. در کامپیوتر خانگی تان اگر لازم است بصورت مداوم از آن دور شوید می توانید آن را با استفاده از یک اسکرین سیور رمزدار محافظت کنید تا کسی بدون اجازه و در غیاب شما به اطلاعات صندوق پستی تان دسترسی نداشته باشد.

2. مراقب ارسال اطلاعات حساس و محرمانه از طریق ایمیل باشید. هنگامی که شما یک ایمیل را فرستادید دیگر هیچ کنترلی در مورد اطلاعاتی که در آن ایمیل ارسال کرده اید ندارید. این به معنی آن است که اگر گیرندگان ایمیل بخواهند می توانند آن را برای کسان دیگری بفروشند یا اطلاعات بعضا محرمانه شما را در محیط عمومی منتشر کنند. حتی اگر به این افراد اعتماد هم داشته باشید باز هم ممکن است بخاطر سهل انگاری آنها ایمیلشان هک شود یا یک ویروس این اطلاعات را بدزدد. اطلاعات حساب های بانکی، کارت های اعتباری ، رمزهای عبور و اطلاعات حساسی از این دست به هیچ وجه نباید از طریق ایمیل و به هیچ کس دیگر منتقل شوند. گوگل هیچگاه به شما ایمیل نمی زند تا از شما رمز عبورتان را بخواهد پس هرگز فریب این حقه هکرها را نخورید !

3. فعال کردن حالت استفاده از پروتکل https. هر زمان که شما یک صفحه وب را مشاهده می کنید ، کامپیوتر شما نیاز به ارسال و دریافت اطلاعات به شبکه اینترنت دارد. https اطلاعاتی را که بین کامپیوتر و اینترنت منتقل می شود را بصورت رمز درمیآورد تا شناسایی محتوای آنها در این بین غیرممکن باشد. جی میل برای لاگین کاربران خود از این پروتکل استفاده می کند اما شما می توانید صندوق پست الکترونیکی خود را نیز با استفاده از این پروتکل مرور کنید. استفاده از https ، باعث کندتر شدن فعالیت شما در جی میل می شود اما اگر بخواهید می توانید با کلیک بر روی settings و انتخاب always use https در زبانه general جی میل را وادار کنید همیشه از این پروتکل برای ارتباط با شما استفاده کند.

4. مراقب فایل های ضمیمه مشکوک باشید. برای محافظت شما از ویروس ها و نرم افزارهای مخرب دیگر جی میل تمام اتچمنت ها را هنگامی که ایمیل به صندوق شما می رسد اسکن می کند. عملیات اسکن یکبار دیگر هنگامی که ایمیل مذکور را باز می کنید تکرار می شود. فایل های ضمیمه ای که شما هم می فرستید توسط آنتی ویروس آنلاین گوگل کنترل می گردد. اما جی میل می گوید باز هم مراقب فایل های ضمیمه باشید و هر فایلی را که انتظار دریافتش را ندارید باز نکنید، حتی اگر از طرف دوست شما باشد. قبل از اینکه فایل ضمیمه ایمیل را باز کنید از فرستنده پرسید که چه چیزی را برای شما فرستاده است و وقتی از بی خطر بودنش مطمئن شدید نسبت به بازکردن آن اقدام کنید.

5. اطلاعات مربوط به بازیابی حساب کاربری خودتان را به روز نگه دارید. اطلاعات بازیابی اکانت به شما کمک می کند تا به حسابتان دسترسی پیدا کنید حتی اگر رمز عبور آن را فراموش کرده باشید یا یک نفر با دسترسی به حساب کاربری شما آن را تغییر داده باشد. در حال حاضر گوگل به سه روش می تواند به شمایی که رمزتان را فراموش کرده اید کمک کند. استفاده از آدرس ایمیل ثانوی، که با تعیین این ایمیل گوگل در هنگام فراموشی رمز توسط شما یک لینک برای ریست کردن رمز به این آدرس می فرستد. استفاده از sms که البته در همه کشورهای جهان (حتی افغانستان) فعال است بجز .... و روش سوم هم استفاده از پرسش و پاسخ امنیتی که در این روش باید سوالی را تعیین کنید که جواب دادنش برای شما آسان و برای دیگران غیرممکن باشد.

نکات ایمنی برای مقابله با هک:

- 1- از دریافت فایل های ناشناس جداً خودداری کنید.
- 2- چنانچه فایلی دریافت کردید قبل از اجرا، راست کلیک کرده و با مطالعه properties از نوع فایل مطمئن باشید فایلی اجرایی نمی باشد.
- 3- عکس های غالباً با پسوند .jpg و .gif می باشد. در صورتی که پسوند های مشکوک و یا اجرایی مانند .exe داشت با shift+delete آن را پاک کنید.



4- از voice chat بهره‌ریزید.

5- چنانچه به شخصی مشکوک هستید یا ایجاد مزاحمت می‌نماید ID شخص را به هیچ وجه Add نکرده و در صورت Add بودن Delete کنید و سپس Ignore نمایید.

چگونه ارتباطات ایمیلی امن داشته باشیم؟  
سطح بندی مطلب:

مقدماتی سرویس‌هایی مانند ایمیل برای کاربران شخصی و حتی شرکت‌ها بسیار با ارزش هستند. استفاده راحت، هزینه کم و انعطاف پذیری این سرویس‌ها باعث محبوبیت‌شان شده است. همچنین سرعت و اتصال مطمئن که در سرویس‌هایی همچون اسکایپ (سرویس انتقال صوت از طریق اینترنت) ارائه می‌گردد، از دیگر عوامل موثر در این محبوبیت هستند. اما متأسفانه چه بخواهیم و چه نخواهیم این سرویس‌های دیجیتالی هم همانند سرویس‌های قدیمی و سنتی نمی‌توانند به طور کامل از اطلاعات و ارتباطات ما محافظت کنند. سرویس‌های ایمیل، تلفن و اس ام اس همواره از لحاظ امنیتی آسیب پذیر هستند، مخصوصاً اگر توسط سرویس دهنده آن یا هکر یا و افراد فضول مورد بررسی و کنترل قرار گیرند.

تفاوت مهم سرویس‌های دیجیتال که مبتنی بر اینترنت هستند، با سرویس‌های سنتی در این است که در بسیاری از مواقع این شما هستید که سطح امنیت را در این سرویس‌ها برای خودتان تعیین می‌کنید. اگر بدون استفاده از راه‌های امن ایمیلی بفرستید، یا به صورت صوتی یا متنی با کسی صحبت (چت) کنید، به جرات می‌توان سطح امنیتی این کار شما را با یک تلفن غیر امن یا ارسال یک نامه با پست عادی مقایسه کرد.

البته چون کامپیوترهای کمی وجود دارند که توانایی جستجو و ردیابی موردی خاص از بین انبوهی از اطلاعات (عبارات مورد نظر، فرستنده، گیرنده و ...) را داشته باشند، دلیل نمی‌شود که امنیت را دست کم بگیریم؛ باید بدانیم در صورت لزوم نیروی لازم برای تجسس در آن حجم از اطلاعات هم همانند سرویس‌های سنتی فراهم می‌شود و ارتباط امنی نخواهیم داشت. با این حال با رعایت برخی نکات احتیاطی، می‌توان تا حد زیادی از بروز مشکل و ناامنی جلوگیری کرد. هرکدام ممکن است هر جایی در میان ارتباطات اینترنتی شما در کمین باشند تا از کارهای شما سر در بیاورند. بنابراین همیشه باید مراقب امنیت ارتباطات خود باشید. در این مطلب نگاهی خواهیم داشت که چگونه از حداقل امنیت برای ارسال و دریافت ایمیل هنگام استفاده از سرویس‌های Webmail برخوردار شوید.

امنیت ارتباطات ایمیلی وقتی که از Webmail استفاده می‌کنید

درکل تنها چند قدم ساده اما مهم برای افزایش امنیت ارتباطات ایمیلی وجود دارد که انجام آنها اکیدا توصیه می‌شود.

به یاد داشته باشید که راه‌های امنیت ایمیلی که در این مقاله می‌آموزید، جلوی نرم افزارها و فعالیت‌های جاسوسی احتمالی در سیستم شما را نمی‌گیرد. برای جلوگیری از نفوذ بدافزارها و هکرها می‌توانید به این مطالب مراجعه کنید:

- ۱- چگونه یک رمز عبور مطمئن بسازیم و از آن نگهداری کنیم - بخش اول
- ۲- چگونه یک رمز عبور مطمئن بسازیم و از آن نگهداری کنیم - بخش دوم
- ۳- چگونه از کامپیوترمان در مقابل بد افزارها و هکرها محافظت کنیم - بخش اول: ویروس‌ها
- ۴- چگونه محافظت از کامپیوتر در برابر خطرات - بخش دوم: جاسوس افزارها
- ۵- چگونه محافظت از کامپیوتر در برابر خطرات- بخش سوم: دیواره آتش و نرم افزارهای متن باز

چگونه ایمیل مان را محرمانه نگه داریم:

درواقع اینترنت از شبکه‌ها پیوسته‌ای از اطلاعات تشکیل شده است. آن هم اطلاعاتی قابل خواندن که دائماً در حال جابجایی هستند. اگر ایمیلی معمولی که در راه رسیدن به گیرنده است در میانه راه دزدیده یا باز شود، به راحتی می‌توان اطلاعات و نوشته‌های آن را بازخوانی کرد. اینترنت شبکه‌ای عظیم و جهانی است که اتصال واسط بین این همه کامپیوتر و دستگاه‌های مختلف را برقرار کرده و در هر لحظه



افراد زیادی هم در حال جا به جا کردن پیام بین هم هستند که این پیام ها باید از واسط های مختلفی عبور کنند تا به مقصد برسند؛ پس ممکن است افراد زیادی هم در میان این همه تقاطع و اتصال بعضی از این تبادل ها را زیر نظر بگیرند.

اولین دریافت کننده ایمیل شما، همان ISP یا سرویس دهنده اینترنت شما است و مسلماً سرویس دهنده ی اینترنتی گیرنده ی اصلی پیام هم یکی دیگر از نقاط توقف ایمیل است؛ که البته آخرین توقف گاه، قبل از گیرنده واقعی است. باید بدانید که پیام های شما می توانند در این ایستگاه های اجتناب ناپذیر و سایر ایستگاه های احتمالی توسط هر کسی خوانده شوند و این در صورتی اتفاق می افتد که شما از حریم ایمیلی خود محافظت نکنید.

پدرام: من قبلاً با یکی از همکاران مان در این مورد صحبت کرده ام، او گفت که او و هم دانشکده ای هایش پیام های مهم را در پوشه Draft ایمیل خود ذخیره می کنند و همه آنها یک رمز عبور مشترک دارند. اما این کار امن و منطقی به نظر نمی رسد، آیا این کار درستی است؟

کاوه: هر وقت که تو یک ایمیل را در کامپیوتر خود می خوانی این ایمیل از طریق اینترنت برای کامپیوتر تو ارسال می شود، درست است؟ حال اگر کسی تو را زیر نظر داشته باشد، فقط ایمیل های تو را نمی خواند، بلکه تمامی اطلاعات قابل خواندن ورودی و خروجی به کامپیوتر تو را کنترل می کند. پس بهترین کار این است که از یک ارتباط امن و کدگذاری شده برای دسترسی به این ایمیل استفاده کنند. خب، وقتی که یک ارتباط امن و مطمئن برای خودشان راه اندازی کنند، آنگاه دیگر نگران خوانده شدن ایمیل ها در میان راه نخواهند بود.

البته امکان برقراری اینگونه ارتباطات امن مدت های مدیدی است که ایجاد گردیده است. اغلب اوقات در زمان وارد کردن رمز عبور یا اطلاعات کارت اعتباری، رد و بدل اطلاعات بصورتی امن انجام می شود. تکنولوژی مورد استفاده در این مواقع، SSL Encryption (Secure Sockets Layer – لایه رمزگذاری شده امن) نام دارد. معمولاً همه شما با این سایت ها و صفحات برخورد کرده اید و می توانید رد پای این سطح امنیتی را در محل آدرس بار در مرورگر خود مشاهده کنید.

همه آدرس های معمولی مانند شکل زیر با HTTP شروع می شوند:

و وقتی که شما با آدرسی شبیه زیر روبرو می شوید که با HTTPS شروع شده است، درواقع از شیوه رمزگذاری SSL استفاده می کنید.

این "S" اضافه شده به انتهای HTTP، نشان دهنده اتصال امن از نوع SSL Encryption است. همچنین ممکن است شما شکل یک قفل را هم در بالا یا پایین مرورگر خود مشاهده کنید. این قفل هم نشانه دهنده آن است که در واقع هیچ کس به جز شما و سایت هدف، اطلاعات صفحه مورد نظر را بازبینی و یا مشاهده نمی کند.

برای اطلاعات بیشتر در مورد SSL می توانید این مطلب نخبان را مطالعه کنید:

SSL چیست و چرا توجه به آن بسیار مهم است؟



این شیوه علاوه اینکه برای ارتباط امن هنگام کار با رمزهای عبور و اطلاعات مالی به کار می رود، در بعضی سرویس های ایمیل هم استفاده می گردد، که تا حد زیادی هم موثر و کارآمد است. به هر ترتیب متأسفانه بسیاری از سرویس دهنده های ایمیل برای دسترسی امن کاربران به ایمیل شان اهمیتی قائل نیستند، اما بعضی هم با بصورت پیش فرض و یا بصورت سفارشی، امکان استفاده از این قابلیت را برای کاربران خود فراهم می کنند.

در هر صورت شما باید هنگام وارد کردن رمز عبور و همچنین باز کردن، خواندن و ارسال ایمیل، از امنیت اتصال به سرویس ایمیل خود اطمینان حاصل کنید.

همچنین در زمان ورود باید مراقب اخطارهای احتمالی مرورگر، در خصوص صفحات امن نامعتبر هم باشید. چرا که ممکن است کسی با مداخله در ارتباط کامپیوتر شما و سرور مربوطه، قصد نفوذ به سیستم و دسترسی به پیام های شما را داشته باشد. شدیداً توصیه می کنیم که اگر اطلاعات مهم و حساسی را با ایمیل مبادله می کنید، از سرویس های امن استفاده کنید. همچنین استفاده از مرورگر فایرفاکس به همراه افزونه های امنیتی آن هم توصیه می شود.

وبگردی امن با فایرفاکس

پدرام: یکی از دوستان من که با ما همکاری هم می کند، از سرویس ایمیل یاهو استفاده می کند، اما به هیچ وجه در محل کارش ایمیل اش را باز نمی کند. ضمن اینکه تا آنجا که به یاد دارم، یک همکار دیگرم هم از سرویس هات میل استفاده می کند. اگر من برای این همکاری ایمیلی بفرستم، امکان دارد کسی آنها را ببیند؟  
کاوه: احتمالاً. یاهو، هات میل و بسیاری از سرویس دهنده های ایمیل، سایت هایی نا امن دارند که احتمال از دست رفتن اطلاعات شخصی کاربران و پیامهایشان در این سرویس ها زیاد است.

مهاجرت به یک سرویس ایمیل امن تر

وب میل های کمی هستند که برای سرویس ایمیل شان از پروتکل امنیتی SSL استفاده می کنند. به عنوان مثال یاهو و هات میل فقط در پنجره ورودی از SSL استفاده می کنند، که برای حفظ امنیت رمز ورود شما است؛ اما این دو سرویس دهنده برای ارسال و دریافت ایمیل های شما از این تکنولوژی استفاده نمی کنند. ضمن اینکه یاهو و هات میل حتی آدرس IP کامپیوتری را که از آن برای ارسال ایمیل استفاده کرده اید نیز ضمیمه ایمیل می کنند. بنابراین این دو سرویس برای کسانی که به دنبال ایمیل امن هستند واقعاً مناسب نیستند.

سرویس جیمیل، از اتصال امن برای دسترسی کاربران به ایمیل هایشان استفاده می کند. البته در حالت پیش فرض فقط هنگام ورود به جیمیل آدرس صفحه را اینگونه (<https://www.mail.google.com>) و با HTTPS می بینید و این آدرس بعد از ورود به ایمیل به HTTP بر می گردد. شما می توانید از طریق بخش تنظیمات جیمیل استفاده از آن را به طور دائمی بر روی HTTPS و تحت یک اتصال امن قرار دهید.

بنابراین تا وقتی که این تنظیم را روی جیمیل فعال نکرده باشید جیمیل هم مانند یاهو و هات میل یک سرویس غیرامن محسوب می شود.

برای این کار در جیمیل روی Settings کلیک کنید و در قسمت General روی بخش Browser connection گزینه Always use https را فعال کنید. و دکمه Save را بزنید. حالا یک بار از جیمیل خارج شوید و دوباره وارد اکانت ایمیل خود بشوید. از این به بعد جیمیل همیشه روی حالت https باز خواهد شد و تمام ایمیل های شما در مسیر به صورت رمزنگاری منتقل می شود.

همچنین برخلاف یاهو و هات میل، در جیمیل آدرس IP شما ضمیمه ایمیل های ارسالی تان نمی شود. بنابراین امکان ردیابی شما وجود



خواهد داشت. البته همین موارد نباید منجر به اعتماد کامل شما به گوگل و ارسال ایمیل های حساس و محرمانه توسط جیمیل شود. جیمیل مطالب کاربران را اسکن و ذخیره می کند و در صورت انجام تخلفات اینترنتی توسط یک کاربر، اطلاعات ایمیل او را پس از طی مراحل قانونی به دولت مربوطه تحویل می دهد.

## راه حل دوم استفاده از سرویس RiseUp

در صورتیکه بتوانید از سرویس ایمیل RiseUp بهره مند شوید، یک وب میل امن دارید که به بهترین نحوه و با بهترین سیستم های رمزگذاری از ایمیل های شما محافظت می کند. این سرویس دهنده از بهترین و امن ترین راه های ایمن سازی ایمیل استفاده می کند. بر خلاف سیاست گوگل در ارائه اطلاعات ایمیل افراد بخاطر مسائل امنیتی کشورها، RiseUp از سیاست امنیت مطلق برای کاربران استفاده می کند. (استفاده از این سرویس علیرغم رایگان بودن نیازمند پاسخ این سرویس دهنده به شما از طریق ارسال درخواست در سایت آن است. همچنین از طریق دعوت کاربران این سرویس -با دریافت دعوتنامه از طرف دو کاربر- می توان به عضویت آن در آمد. بنابراین متأسفانه دریافت حساب ایمیل در این سرویس کار آسانی نیست.

آدرس سایت: <https://mail.riseup.net>

به هر شکل سریعترین و بهترین راه برای دسترسی به این سرویس رایگان، پیدا کردن دو کاربر و درخواست دعوت نامه از طرف آنها است.

جیمیل، RiseUp و بسیاری از سرویس های ایمیل، از برنامه های (کلاینت) دریافت ایمیلی هم که بر روی کامپیوتر کاربر نصب می شود، پشتیبانی می کنند. یکی از این برنامه ها Mozilla Thunderbird است که بسیاری از تکنیک ها و سیستم های امنیت ایمیلی را پشتیبانی می کند. تضمین رمزگذاری اتصال اینترنتی برای یک کلاینت همانند دسترسی به سرویس ایمیل در وب از طریق HTTPS، از اهمیت ویژه ای برخوردار است. در صورتی که شما به صورت مستقیم از وب میل خودتان استفاده نمی کنید و از یک کلاینت واسط مانند تاندربرد برای دریافت و ارسال ایمیل استفاده می کنید باید قبل از کار با آن، از برقرار بودن اتصال تحت SSL، مطمئن باشید.

پدرام: پس در این صورت بهتر است که من از RiseUp استفاده کنم. یا کار با جیمیل را با اعمال تغییر در تنظیمات جیمیل برای استفاده از HTTPS ادامه دهم؟

کاوه: تصمیم با تو است، اما نکته هایی ظریف وجود داد که باید قبل از این تغییر بدانی. اول اینکه اگر تو فقط به یک ارتباط امن نیاز داری، جیمیل این قابلیت را دارد و می توانی از آن استفاده کنی. دوم اینکه آیا امنیت کامل ایمیل های تو برایت خیلی مهم است و دوست نداری تحت هیچ شرایطی به دست هیچ کس بیافتد؟ خب در این صورت بهتر است که از دومی استفاده کنی، البته اگر بتوانی یک حساب ایمیل در آن بدست بیاوری. اما داشتن جیمیل نیازی به درخواست دادن یا دعوت نامه ندارد.

با توجه به اهمیت تصمیم گیری در انتخاب یک سرویس ایمیل، به یاد داشته باشید که هر پیامی یک فرستنده و یک یا چند گیرنده دارد. حتی اگر شما در امن ترین حالت به ایمیل خود دسترسی داشته باشید، ممکن است گیرنده ایمیل در زمان دریافت، باز کردن، خواندن و یا حتی ارسال آن به دیگری بی دقتی کند. توجه داشته باشید که اگر می خواهید از امنیت ایمیل های ارسالی خود مطمئن باشید، باید ابتدا از وضعیت امنیتی دوستان و همکارانی که با آنها تبادل ایمیل دارید مطمئن شوید.

ضمناً باید به نکات دیگری هم توجه داشته باشید چرا که امکان دارد شما از جاهای دیگری که بسیار ساده هم به نظر می رسند، لطمه بخورید. مواردی مانند یک Keylogger\* مخفی که روی سیستم شما نصب شده است، یا فردی که ممکن است از طریق یک دوربین مخفی رمز عبور شما را هنگام تایپ کردن ببیند و یا عدم رعایت اصول اولیه ایمنی از طرف فردی که با وی مکاتبه می کنید. یک راه خوب برای حل مشکلات امنیتی طرف مقابلتان این است که نگاهیان را به او معرفی کنید تا بخواند!



یکی از برنامه های جاسوسی است که کلیدهای فشرده شده توسط کاربر را مانیتور و ذخیره کرده، برای شخص ثالثی می \*Keylogger فرستد. این برنامه ها عموماً برای یافتن نام کاربری و رمز عبور حساب های اینترنتی و ایمیل ها بکار برده می شوند.

نکات تکمیلی برای بالا بردن سطح امنیت ایمیل

همیشه در زمان باز کردن ایمیل های ناشناس و حاوی فایل ضمیمه، به اخطارهای احتمالی مرورگر و یا نرم افزار ایمیل خود توجه کنید و - ۱ بدانید که کامپیوتر شما باید مجهز به یک آنتی ویروس قوی و به روز باشد

برای مخفی کردن هویت استفاده کنید، TOR (<http://www.torproject.org>) از نرم افزارهایی مانند - ۲

در زمانی که شما در یک سایت مانند تالار اینترنتی یا شبکه اجتماعی و غیره ثبت نام می کنید، که ممکن است بعداً از طریق سرویس ایمیل - ۳، خود پیامی را برای این سایت ها ارسال کنید، توجه داشته باشید که بهتر است از نام واقعی خود و نام هایی که شناسایی شما را آسان می کنند استفاده نکنید. مخصوصاً در سرویس های ایمیلی مانند یاهو و هات میل که آی پی شما را هم برای گیرنده به نمایش می گذارند، رعایت این نکته بسیار مهم است

سیستم خود Temporary در صورتی که افراد دیگری هم از کامپیوتر شما استفاده می کنند، باید در دوره های زمانی مشخص فایل های - ۴ برای این کار استفاده کنید CCleaner را پاک کنید. توصیه می کنیم از نرم افزار

پاک کنیم؟ CCleaner چگونه ردها ها را با

را بر روی مرورگرتان NoScript به هیچ عنوان روی لینک هایی که توسط ایمیل برای شما ارسال شده اند کلیک نکنید و حتماً افزونه - ۵ نصب کنید

افزونه ای برای وبگردی ای امن NoScript