

## توضیحات وزیر ارتباطات درباره رفع فیلتر فیس بوک

چندی پیش خبری منتشر شد مبنی بر موافقت کارگروه مصادیق جرایم رایانه‌ای درباره رفع فیلتر فیس بوک که کاربران را امیدوار کرد! وزیر ارتباطات تاکید کرد: فیلترینگ شبکه‌هایی مانند فیس بوک و توئیتر قبل از دولت یازدهم صورت گرفته و اکنون در این زمینه برخی نمایندگان دولت به طور شفاهی صحبت‌هایی را مطرح کرده‌اند.

به گزارش ایتنا از ایسنا، محمود واعظی درباره این که چندی پیش یکی از اعضای کارگروه تعیین مصادیق مجرمانه رایانه‌ای اینگونه اعلام کرده بود که این احتمال وجود دارد که با ارسال نامه درخواستی از سوی وزارت ارتباطات، شبکه اجتماعی فیس بوک رفع فیلتر شود، گفت: این صحبت‌ها از سوی یکی از اعضای این کمیته مطرح شده و به معنای نظر کلی کارگروه مربوطه نیست.

وی ادامه داد: وزارت ارتباطات زمانی وارد عمل می‌شود که بیش از ۵۰ درصد اطمینان داشته باشد که نتیجه مثبتی حاصل می‌شود. در خصوص این موضوع نیز اگرچه برخی نمایندگان دولت به طور شفاهی صحبت‌هایی را مطرح کرده‌اند اما هنوز به طور رسمی مطلبی ارسال نشده است.

واعظی با تاکید بر اینکه در این زمینه کارگروه تعیین مصادیق مجرمانه رایانه‌ای تصمیم گیرنده است و فعالیت مجدد این شبکه‌ها بستگی به تجدید نظر این کارگروه دارد، یادآور شد: این مساله تنها به وزارت ارتباطات مربوط نمی‌شود چراکه ما تنها یک عضو در این کمیته داریم. وزیر ارتباطات با اشاره به طرح فیلترینگ هوشمند متذکر شد: تلاش داریم این طرح هرچه سریع‌تر اجرایی شود و با عملیاتی شدن فیلترینگ هوشمند، شاید کارگروه تعیین مصادیق مجرمانه رایانه‌ای در این حکم تجدید نظر کند.

وی در ادامه متذکر شد: شبکه‌های اجتماعی همانطور که فوایدی به دنبال دارند ممکن است آسیب‌هایی را نیز همراه خود داشته باشند اما وظیفه دولت آن است که این فواید را براساس نیاز مردم و ارتباط آنها افزایش داده و در مقابل جلوی آسیب‌ها و تهدیدها را بگیرد. او همچنین اظهار کرد: برای این کار تلاش‌های متعددی صورت گرفته است اما در اولین گام لازم است که مردم را آگاه کنیم که بدانند بدون کمک آنها مبارزه با آسیب‌های شبکه‌های اجتماعی امری سخت و دشوار می‌شود، البته این موضوع به آن معنا نیست که ما وظایف خود را انجام ندهیم.

### آیا کلمه عبور شما واقعا از شما محافظت می‌کند؟

امروزه یکی از مهمترین نگرانی‌های کاربران، حفظ امنیت اطلاعات آنها می‌باشد که معمولا این امنیت توسط رمز گذاشتن تا حدی حفظ می‌گردد. در این اینفوگرافیک به نکاتی مهم در انتخاب رمز عبور مناسب و امن، می‌پردازیم

اینفوگرافیک | ۸

### ۷ ترفند از جیمیل Gmail

اکانت گوگل یا همان جی میل، گام صفرم برای ورود به این دنیای هیجان انگیز و اسرارآمیز است. از لحاظ مفهوم و البته کاربری، این اکانت چیزی شبیه به جمله ای است که می‌گویند افلاطون بر سر در آکادمی اش نوشته بود....

ترندها | ۵

### چرا پسورد را باید دوره‌ای عوض کرد؟

رمز عبور خود را به صورت دوره‌ای تغییر دهید، حتما پیشنهاد تغییر پسورد به صورت متناوب را در اکثر سامانه‌های الکترونیک شنیده‌اید، برای مثال رمز پست الکترونیکی، کارت‌های اعتباری و سایر حساب‌های کاربری؛ اما چرا باید این کار را انجام دهیم؟ اصلا این کار مفید است؟

امنیت | ۲



## چرا پسورد را باید دوره‌ای عوض کرد؟

رمز عبور خود را به صورت دوره‌ای تغییر دهید، حتما پیشنهاد تغییر پسورد به صورت متناوب را در اکثر سامانه‌های الکترونیک شنیده‌اید، برای مثال رمز پست الکترونیکی، کارت‌های اعتباری و سایر حساب‌های کاربری؛ اما چرا باید این کار را انجام دهیم؟ اصلا این کار مفید است؟

اگر مدیر شبکه یا سامانه‌ی خاصی می‌باشید، آیا باید کاربران خود را مجبور کنید که رمزهایشان را عوض نمایند؟



## آیا تغییر متناوب پسورد مفید است؟ پاسخ کوتاه

اگر به دنبال پاسخ کوتاه هستید، بلی، در صورتی که سامانه مورد استفاده یا مدیریت شما استانداردهای امنیتی لازم را رعایت نماید، تغییر پسورد عموماً بازدارنده و مفید واقع خواهد شد و جلوی مورد سرقت و سوءاستفاده قرار گرفتن اطلاعات و... شما را خواهد گرفت.

## اجبار در تغییر رمز عبور، خوب یا بد؟

مدیران باید به یاد داشته باشند اگر کاربران را برای ادامه فعالیت مجبور به تغییر رمز عبور نمایند، ممکن است کاربر تنها با افزودن یا تغییر یک کارکتر به ادامه فعالیت خود بپردازند و یا به روش‌های خطرناک‌تری همچون یادداشت کردن رمز عبور و یا استفاده از رمزهای کوتاه، ساده و با معنی (کلمات معنی دار) روی بیاورد.

اگر جزو این دسته از کاربران هستید، رویه خطرناکی را پیش‌رو گرفته‌اید.

یکی از مزایای مجبور کردن کاربران به تغییر رمز عبور، محافظت از سیستم‌هایتان در مقابل کاربرانی است که از رمزهای یکسان برای تمام حساب‌های کاربریشان استفاده می‌نمایند، با این کار در صورتی که رمز یکسان کاربر به هر صورتی مورد سرقت قرار گیرد سیستم‌های شما امن باقی خواهند ماند.

## نظر مخالف

برخی بر این اعتقادند که تغییر پسورد نمی‌تواند مفید واقع شود فرد مهاجم که به رمز عبور دسترسی پیدا کرده است بلافاصله اقدام به استفاده از آن خواهد کرد و روزها و ماه‌ها منتظر شما نخواهد ماند تا رمز عبورتان را تغییر دهید، این



نظریه تا حدی صحیح است، اما همانطور که در ابتدا بیان شد ایجاد این تغییر زمانی مفید است که سیستم از استانداردهای امنیتی تبعیت نماید، برای مثال رمزهای عبور به صورت هش ذخیره شوند و سیستم در مقابل نصب بدافزار و درب‌های پشتی امن باشد.

موضوع دیگر مورد حملات brute-force به صورت مستقیم قرار گرفتن است، فرض کنید یک ماشین در تلاش برای حدس زدن رمز عبور شما به صورت زنده است، تضمینی وجود ندارد که رمز عبور انتخاب شده جدید شما حدس بعدی ماشین مهاجم نباشد، اما باید بپذیریم احتمال رخ داد همچین اتفاقی بسیار ناچیز است و برای مقابله با اینگونه حملات راهکارهای خاص خود وجود دارد.

### در چه شرایطی تغییر پسورد مفید واقع می‌شود؟

رمز شما به صورت هش شده نگهداری می‌شود و این هش به سرقت رفته، حال فرد مهاجم می‌تواند بدون نیاز به اتصال به سیستم اقدام به یافتن رمز اصلی شما نماید، این کار بسته به نوع الگوریتم مورد استفاده برای هش کردن پسورد عملی عموماً زمان بر خواهد بود، در صورتی که این الگوریتم به اندازه کافی قدرتمند باشد فرصت لازم را برای شما ایجاد می‌کند تا با تغییر رمز خود مهاجم را از دسترسی یافتن به حسابتان ناکام سازید.

بسته به نوع سامانه مورد نفوذ واقع شده، مهاجم می‌تواند عملکرد متفاوتی داشته باشد. برای مثال سیستمی که قابلیت نصب Back-door را نداشته باشد را در نظر بگیرید، مثلاً یک سرویس ایمیل تحت وب، یا سیستمی که امنیت لازم برای جلوگیری از نصب Back-door در آن برقرار شده باشد، عموماً در این مواقع نفوذگر همانند یک احمق رفتار نخواهد کرد و با تغییر ندادن رمز عبور اجازه نمی‌دهد کابر متوجه نفوذ به سیستم شود و با این کار امکان دسترسی خود به سیستم مورد نفوذ در آینده را فراهم می‌سازد. در این موارد همانطور که مشخص است تغییر رمز عبورتان از اطلاعات و اکانت‌هایتان محافظت به عمل خواهد آورد و حداقل مزایای آن سخت کردن کار مهاجم و مجبور کردن آن برای تلاش دوچندان خواهد بود.

شرایط متفاوت دیگری ممکن است رخ دهد که در این موارد هم تغییر رمز عبورتان از دسترسی غیرمجاز به حساب و... شما جلوگیری به عمل خواهد آورد:

- مهاجم در ابتدا قصد تخریب نداشته باشد.
- هنوز اقدام به نصب بدافزار و درب پشتی نکرده باشد.
- دانش کافی برای پیش‌روی لازم را در اختیار نداشته باشد.
- در حال حاضر شرایط دسترسی به حسابتان را نداشته باشد.
- پس از به دست آوردن دسترسی تا مدت خاصی صبر نماید (برای اطلاعات با ارزش‌تر).

و...



## نکات مهم

در صورتی که قصد تغییر رمز عبور خود را دارید یا به اینکار مجبور می‌شوید، هرگز رمزتان را به رمز قبلی تغییر ندهید. ممکن است رمز قبلی شما به نحوی لو رفته باشد و در لیست دیکشنری مهاجم برای حملات آتی قرار داشته باشد. فرض کنید نسخه‌ی پشتیبان اطلاعات سامانه که حاوی رمز سابق شما است در دسترس فرد مهاجم قرار گیرد.

با توجه به نکته فوق مدیران سیستم باید نسخه‌ی پشتیبان اطلاعات را به صورت امن و ترجیحاً رمزنگاری شده نگهداری نمایند.

در هنگام انتخاب پسورد، نکات لازم برای ایجاد یک پسورد قوی و مناسب را رعایت نمایید، پسوردهای بسیار ساده، کوتاه و با معنی، به راحتی توسط دیکشنری یافته خواهند شد، همینطور مقدار هش شده این پسوردها بسیار سریع‌تر از هش یک رمز قوی، مهاجم را به رمز اصلی خواهد رساند.

## نتیجه گیری

با توجه به حالت‌های بررسی شده، همانطور که پیش‌تر اشاره شد، در صورتی که سیستم‌ها موارد امنیتی لازم را رعایت کرده باشند، تغییر دادن رمز عبور به صورت دوره‌ای توسط کاربران می‌تواند تا حد قابل توجه‌ای به افزایش امنیت یاری رساند. هرچند امنیت هیچگاه به طور کامل قابل تضمین نیست ولی می‌توان با افزایش سیستم‌های امنیتی و پیچیده کردن آن‌ها حداقل کار مهاجمین را سخت‌تر کرد.



## ۷ ترند از جیمیل Gmail



اکانت گوگل یا همان جی میل، گام صفرم برای ورود به این دنیای هیجان انگیز و اسرارآمیز است. از لحاظ مفهوم و البته کاربری، این اکانت چیزی شبیه به جمله ای است که می گویند افلاطون بر سر در آکادمی اش نوشته بود: "هر کس هندسه نمی داند وارد نشود". با این تفاوت که اینجا هندسه، همان جی میل است و رمز ورود به تمامی خدماتی که بعداً برایتان معرفی می کنیم، همان آی دی شماست که با Gmail.com به اتمام می رسد. پس بد نیست همین ابتدای کار و برای دستگرمی، با برخی از ویژگی های کمتر دیده و شنیده شده جی میل بیشتر آشنا شوید.

### قابلیت اول: سازماندهی جلسات و قرارها در جی میل

این ویژگی بیشتر به درد کسانی می خورد که برنامه ریزی کارهای روزمره شان را با سیستم تقویم گوگل انجام می دهند اما برای دیگران هم قابلیت بی کاربردی نیست. وقتی ایمیلی برای شخصی می فرستید و قرار می گذارید، می توانید در خود جی میل زمان و مکان این ملاقات را با کلیک روی Add Event Info سازماندهی کنید، به این ترتیب قرار به صورت خودکار وارد تقویم گوگل شما می شود. شخص دریافت کننده میل هم می تواند به سادگی قرار را وارد تقویم خود کند.

### قابلیت دوم: دسته بندی اتوماتیک ایمیل ها

اگر می خواهید ایمیل هایی که از افراد، سایت ها یا گروه هایی خاص به شما می رسد لابلای باقی نامه های Inbox تان گم و گور نشود، می توانید پوشه ای ویژه برایشان درست کنید. برای اینکار در ساب منوهای آیکون چرخ مانند بالای صفحه، روی Settings کلیک و در صفحه باز شده روی تب Filters کلیک کنید.

Create a new Filter را در قسمت پایین انتخاب کنید و در قسمت From، آدرس ایمیل فرستنده را بنویسید. روی Create Filter with this search کلیک و پیغام نمایش داده شده را OK کنید. Apply the label را تیک بزنید و با انتخاب New Label یک لیبل جدید بسازید که در واقع پوشه ای است که ایمیل های دریافتی از این آدرس وارد آن می شود. می توانید اسمش را همان اسم نشریه یا آدم مورد نظرتان بگذارید. بعد روی Create Filter کلیک کنید. از الان در منوی سمت چپ جی میل، آن لیبل را می بینید.



## قابلیت سوم: انتقال ایمیل سرویس های دیگر به جی میل

اگر در عهد دقیانوس در سرویس هایی مثل یاهو، هات میل یا ... ایمیلی باز کرده اید و هنوز خیلی ها به همان آدرس شما ایمیل می دهند، نیازی نیست که هر روز چند ایمیل متفاوت را چک کنید. جی میل همه آنها را یکجا به شما نشان می دهد.

کافی است به منوی **Setting** و سربرگ **Accounts** بروید. روی **mail account you own Add a POP** کلیک کنید و آدرس ایمیل و پسورد سرویس دیگران را در کادر مربوطه وارد کنید. با زدن **Continue**، یک صفحه جدید باز می شود که آنجا هم چند تنظیم کوچک را انجام می دهید و این سرویس برای شما فعال می شود. برای غیرفعال کردن این امکان هم می توانید به همین بخش برگردید و گزینه **Stop** را انتخاب کنید.

## قابلیت چهارم: بازبینی فایل های ضمیمه در Google Docs

فرض کنید میلی برای شما فرستاده شده که حاوی یک فایل **Word** یا **Excel** است اما شما برنامه **Word** یا **Excel** را به هر علت در سیستماتان ندارید. در چنین شرایطی، نگرانی به دل خودراه ندهید و بی خیال نشوید.

بلکه به راحتی و با کلیک ساده روی **Open as a Google Docs Spreadsheets** در پایین فایل های پیوست شده، می توانید فایل ها را با استفاده از سرویس آنلاین گوگل ببینید و حتی آنها را ویرایش کنید! می توانید فایل **Word** را با فرمت **HTML** بخوانید یا فایل پاورپوینت را به صورت یک اسلایدشوی فلش تماشا کنید. کلا با گوگل میل کارها دشوار نیست!

## قابلیت پنجم: برچسب گذاری ایمیل ها

ایمیل های یک موضوع یا آدم خاص را می توانید با برچسب های رنگی و تگ مشخص کنید. با این کار را به راحتی این ایمیل ها را لابلای انبوه ایمیل هایتان پیدا می کنید. برای ساختن برچسب یا **Label**، می توانید به **Settings** و سربرگ **Labels** بروید.

آنجا یک برچسب بسازد و اسم مورد نظرتان را در آن وارد کنید. حتی می توانید برای هر کدام از لیبل ها رنگ تعیین کنید. برای دسته بندی ایمیل ها می توانید در نوار ابزار بالای ایمیل، روی **Labels** کلیک و برچسب مورد نظرتان را مشخص کنید تا ایمیلتان صاف به پوشه مربوطه برود.



## قابلیت ششم: افزودن آدرس های دیگر در مبدأ جی میل

تصور کنید شما ایمیل اکانت های دیگری هم دارید که متعلق به دانشگاه محل تحصیل یا شرکت محل کارتان است که مسئولان شرکت و دانشگاه، فقط با همان میل با شما در ارتباط هستند. در عین حال نمی خواهید برای فرستادن میل به صورت مرتب، وارد دیگر حساب های میل خودتان بشوید.

جی میل چنین کاری را برای شما ممکن می کند. برای این کار باید در گوشه شمال شرقی (!) صفحه میل، روی Setting کلیک کرده و Accounts را باز کنید. حالا نام و آدرس میل دیگران را بنویسید. روی Next Step کلیک کنید. جی میل برای اینکه تشخیص دهد این آدرس ایمیل جدید، واقعا متعلق به شماست یک میل تاییدی می فرستد. شما باید آن میل را باز و روی لینکش کلیک کنید تا این مرحله هم انجام شود.

به این ترتیب می توانید وقتی در جی میل هستید ایمیل هایی با آدرس میل های دیگران هم بفرستید. در این حالت شخص دریافت کننده چنین پیغامی را به عنوان آدرس فرستنده می بیند:

From [customaddress] @ [domain].com on behalf of [yourusername] @gmail.com

## قابلیت هفتم: ایجاد ایمیل های نامحدود با یک حساب

با لحاظ کردن چند ترفند ساده می توانید با استفاده از یک اکانت جی میل، آدرس ایمیل های متعددی داشته باشید. نکته اول این است که نقطه در آدرس جی میل تاثیری ندارد و توسط خود گوگل نادیده گرفته می شود. یعنی najiraji@gmail.com با naji.raj.i@gmail.com فرقی نمی کند.

علامت مثبت هم در آدرس های جی میل بی تاثیر است؛ یعنی اگر آدرس ایمیل شما najiraji@gmail.com باشد و شما به آخر ایمیل خود، یک علامت مثبت و یک کلمه اضافه کنید و مثلا بشود naji raji mohammad@gmail.com، تمام ایمیل های ارسال شده به همان آدرس قدیمی شما فرستاده می شود. با این ترفند می توانید چند اکانت مختلف برای خودتان بسازد. البته اگر آدرس ایمیل مشابهی در دیتابیس جی میل موجود نباشد.



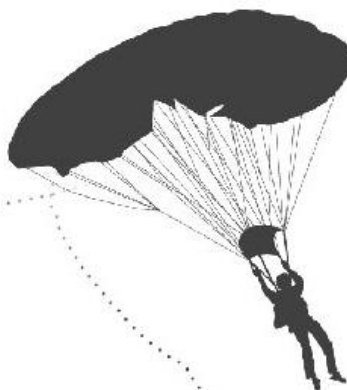
## آیا کلمه عبور شما واقعا از شما محافظت می کند؟

پسوردها به عنوان استراتژی نظامی پدیدار شدند



قبل از کامپیوترها، پسوردها توسط سربازان در جنگ جهانی دوم استفاده می شدند.

جنگ جهانی آمریکا از پسوردها و ضد پسوردها به عنوان روشی برای شناسایی در نبرد نرمادی در سال ۱۹۹۴ استفاده کردند.



ضد پسورد به صورت پرسش و پاسخ استفاده می شد. (مثال: فرمانده میگفت برق و سربازان باید میگفتند رعد.)



در طول جنگ جهانی پسوردها و ضد پسوردها هر ۳ روز تغییر می کردند.







ابداع شره پوسینه  
رایرت هورس

پسوردها به آن شکل که ما امروز  
آنها را می شناسیم تا سال ۱۹۷۲  
ابداع نشده بودند و تا سال ۱۹۷۴  
به کار گرفته نشدند.

## حریم خصوصی شما به شدت بر محافظت با استفاده از کلمات عبور وابسته است



- رمز خودپرداز بانک
- رمز سیم کارت تلفن همراه
- دسترسی به کامپیوتر
- حساب ایمیل
- بانکداری الکترونیکی
- پسورد شبکه WiFi
- حساب شبکه‌های اجتماعی
- رمز سیستم امنیتی
- تمامی وب سایت‌های محافظت شده با پسورد

## استفاده از پسردهای مختلف یک الزام است

یک فرد معمولی به طور متوسط ۲۵ وب سایت محافظت شده با پسرود را مشاهده می کند ولی تنها از ۶ پسرود متفاوت استفاده می کند

۳۳%

از مردم از یک پسرود برای هر وب سائتی استفاده می کنند

۷۳%

از مردم از پسرود مشابه برای سایت های مختلف استفاده می کنند

۶۲%

از صاحبان گوشی های هوشمند از رمز عبور برای محافظت از گوشی خود استفاده نمی کنند

۳۲%

از مردم پسرود و سایر اطلاعات ورود به حساب های کاربری را در گوشی همراه خود ذخیره می کنند

## اغلب مردم از پسوردهای ضعیف استفاده می کنند

کلمات عبور پیچیده کلید امنیت هستند  
و بسیار سخت تر شکسته می شوند



یک هکر حرفه‌ای می‌تواند  
پسوردهای معمولی را در  
کمتر از ۳ دقیقه بشکند.



از ۲۰ پسورد متداول  
برتر، اسامی کوچک است



از مردم عبارت password  
را به عنوان کلمه عبور  
خود استفاده می‌کنند



میانگین طول پسوردها  
۶ حرف است که همگی  
حروف کوچک هستند

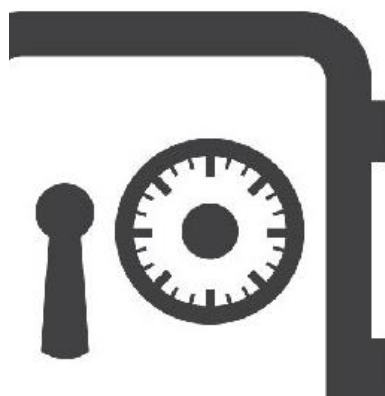


از زنان نام شریک زندگی  
خود را در کلمات عبور  
استفاده می‌کنند



از مردان نام شریک زندگی  
خود را در کلمات عبور  
استفاده می‌کنند

## ۱۰ پسورد ضعیف سال ۲۰۱۴



- |               |             |
|---------------|-------------|
| ۱۲۳۴۵۶۷۸۹۰ .۶ | ۱۲۳۴۵۶ .۱   |
| ۱۲۳۴ .۷       | password .۲ |
| baseball .۸   | ۱۲۳۴۵ .۳    |
| dragon .۹     | ۱۲۳۴۵۶۷۸ .۴ |
| football .۱۰  | qwerty .۵   |



## بایدها و نبایدها در ساختن یک کلمه عبور

### بایدها

\*\*\*\*\*

طول کلمه عبور خود را ۸ حرف و یا بیشتر کنید

هر طولی کمتر از این ضعیف تلقی می‌شود

ABC abc 123 @\$&

از ترکیبی از تمام ۴ نوع حروف استفاده کنید

حروف کوچک، حروف بزرگ، اعداد و کاراکترهای خاص

مثلا: ToBeMan&\$Bedehkari

پسوردی انتخاب کنید که به خاطر می‌سپارید

پسورد مستحکمی که اغلب فراموش می‌کنید به کار شما نمی‌آید

خیلی مستحکم ★★★★★

پسورد خود را تست کنید

سایت‌های ایمن زیادی هستند که استحکام پسورد شما را بررسی می‌کنند

و پیشنهادهایی به شما می‌دهند تا پسورد خود را قوی‌تر کنید

۰۹۳۵۲۲۲۳۳۴۴

یک روش بازیابی کلمه عبور تنظیم کنید

روش بازیابی با موبایل مناسب است چرا که گوشی تلفن همراه

شما به صورت فیزیکی در اختیار شما قرار دارد

سال/۲ بار

کلمه عبور خود را ۲ بار در سال تغییر دهید



## نبایدها



### استفاده از اطلاعات عمومی

نام شما، تاریخ تولد، نام فرزندان، نام همسر و غیره  
به صورت عمومی در دسترس هستند  
و هکرها از آنها برای حدس زدن پسوندد شما استفاده می کنند

### استفاده از کلمات کامل

پسوندهایی که از کلمات کامل استفاده می کنند، به شکل قابل ملاحظه ای راحت تر شکسته می شوند

### نوشتن پسوندد در جایی

از نوشتن پسوندد خود روی کاغذ خودداری کنید. مخصوصا بر روی کاغذ یادداشت های چسبان  
اگر مجبور شدید پسوندد خود را بنویسید به جای پسوندد یک یادآوری بنویسید

### استفاده از یک پسوندد برای چندین حساب

این کار باعث می شود همه چیز یکجا برای مجرمان اینترنتی فراهم شود

### لاگین کردن به حساب های شخصی از کامپیوترهای عمومی

اطلاعات شما ممکن است ثبت شوند و یا فراموش کنید از حسابان خارج شوید

### گفتن پسوندد خود به کسی

شما و فقط شما تنها کسی هستید که باید پسونددتان را بداند