

سه ویژگی در گوگل کروم که معمولاً دیده نمی شود!



۱_ Other Devices

یکی از قدرتمندترین قابلیت های کروم، توانایی همگام سازی خوب آن است و -نه تنها بوکمارک ها و گذرواژه ها را شامل می شود بلکه- امکان سینک تب های باز را نیز داراست { از Setting => Advanced sync Settings می توانید این قابلیت را اضافه نمایید}.

برای مثال اگر مرورگر کروم بر روی رایانه ها، اسمارت فون ها و یا تبلت های دیگر نصب شده باشد می توانید از یک یک آن ها برای دسترسی به تب های باز روی رایانه مبدا استفاده نمایید؛ ابتدا یک تب جدید را باز و سپس بر روی منوی Other devices موجود در گوشه پائینی آن تب کلیک کنید. اکنون لیستی دسته بندی شده از تب های باز را از تمامی موارد موجود در مرورگر کروم را خواهید دید. بسیار دسترس اما غیر قابل تصور!



۲_ Recently Closed

همانطور که شاید بدانید، اگر به صورت تصادفی صفحه ای را ببندید، اگر مایل باشید می توانید سریعاً آن را با فشردن کلید های Ctrl-Shift-T پیدا نموده و اجرا کنید. با این حال، اگر موردی را بخواهید که به تازگی در آن نبوده اید یا حتی از مواردی باشد که

در این لیست به دست آمده با استفاده از فشردن این کلید ها موجود نباشد چگونه عمل می کنید؟ چیزی که شما به آن نیاز دارید، لیستی از تمامی تب های بسته شده است که کروم آن را کاملاً تحت پوشش خود دارد؛ هنگامی که در گوشه پائینی هستید به گزینه بعدی Other Devices دقت بیشتری کنید، منوی The Recently Closed همانجا قرار دارد. با کلیک بر روی آن ۱۰ تب پایانی بسته شده را مشاهده خواهید کرد.

۳_ Web Store

افرادی که جدیداً به مجموعه کروم می پیوندند، شاید از قابلیت که گوگل از کتابخانه از برنامه ها به راحتی از وب استور در اختیارشان قرار می دهد آگاه نباشند. اگر شما هم از دسته افرادی هستید که با آن برخورد نداشته اید، می توانید از همان گوشه درست در گزینه کنار آخرین تب ها بسته شده آن را مشاهده نمایید. سپس اگر بر روی Web Store کلیک کنید، مسیر اپ ها در تبی جدید بازخواهد شد. اکنون می توانید به جستجوی مواردی که برای نصب شدن نیاز دارید بپردازید.

چه ایمیل هایی رو هرگز باز نکنیم ؟



روزانه میلیون ها ایمیل خطرناک و ویروسی در شبکه جهانی رد و بدل می شود و هدف همه آنها یک چیز است. به دزدان انداختن کاربران و بالا کشیدن پول آنها و خالی کردن حساب بانکی شان، بخش کوچکی از اهداف این نامه های الکترونیکی هستند.

البته اکثر ایمیل های خطرناک و ویروسی غیر منتظره هستند و معمولاً

کاربران را در تشخیص دچار سردرگمی می‌کنند. اما چگونه می‌توان ایمیل‌های ویروسی و آلوده را از ایمیل‌های درست و واقعی تشخیص داد؟



ایمیل‌هایی با نام‌های اشتباهی

در دنیای واقعی آدرس اشخاص با ذکر پلاک منزل و شماره خیابان مشخص می‌شود. در فضای اینترنت نیز هر کامپیوتری با اعداد منحصر به فردی که به IP معروف است معین می‌شود که به وسیله آن راحت‌تر می‌توان کاربر را پیدا کرد.

همانند دفتر تلفن که نام هر شخص با شماره مخصوصی تعیین شده و معین است، اما برای سهولت در کار این شماره‌های IP با یک نام مشخص می‌شود که با وارد کردن آن در مرورگر می‌توان به سایت موردنظر دسترسی پیدا کرد. مسلماً بدون این IP کامپیوتر نمی‌تواند آدرس را بیابد. در ایمیل‌های شخصی نیز افراد همزمان از اعداد و حروف استفاده می‌کنند.

اما گیرنده ایمیل تنها قادر به خواندن آدرس ایمیل‌هاست و نه خواندن شماره IP آنها اما هکرها می‌توانند برنامه‌ای که شما را طوری تغییر دهند که آدرس ایمیل شما با آدرس ایمیل فرد دیگر یا شرکتی مشهور یکسان شود، فرد گیرنده نیز به محض دریافت این ایمیل گمان می‌کند که از این فرد یا شرکت مذکور پیغامی دارد. لذا همواره مراقب باشید که حتی ایمیل‌های افرادی را که می‌شناسید را نیز با احتیاط باز کنید و قبل از آن از ارسال چنین ایمیلی از طرف آن فرد اطمینان حاصل کنید.

تجارت کثیف با ایجاد وحشت، طمع و جلب اعتماد

در بسیاری از مواقع جنایتکاران با ارسال ایمیل‌هایی با نام مقامات سیاسی و عنوان «احضاریه پلیس» و نامه‌ای که در آن اتهاماتی در خصوص کالاهای تقلبی مطرح شده از دریافت کننده ایمیل درخواست می کنند که با کلیک بر روی لینک ذکر شده از جزئیات اتهام آگاه شوند. کاربری که روی لینک معرفی شده کلیک کند کامپیوتر خود را با بدافزارها آلوده کرده است. همچنین ایمیل های با عناوینی چون «شما برنده شده اید» یا «حساب بانکی تان مسدود شده است» و یا «اخطاریه» نیز حاوی لینک هایی با کدهای اشتباهی و پیوست های آلوده هستند.

برای خوشبینی بیش از اندازه باید بهای سنگینی بپردازید

کاربران هیچگاه نباید به سرعت روی لینک خاصی کلیک کنند و یا پیوست های آن را باز کنند. هر قدر هم عنوان ایمیل وسوسه کننده و وحشت برانگیز باشد زیرا بانک ها، مراجع دولتی و رسمی و شرکت های مطرح هیچگاه از طریق ایمیل اطلاعات حساس همانند رمز کارت اعتباری و یا اطلاعاتی در خصوص حساب بانکی و یا رمز عبور شما را درخواست نمیکنند.

پس از هک شدن حساب های شخصی چه باید کرد؟



بسیاری تصور می کنند هک سیستم های رایانه ای و سرقت اطلاعات تنها به شرکت ها و سرویس های بزرگ محدود می شود و اشخاص حقیقی نیاز مبرمی برای حفاظت از رایانه یا دستگاه های دیجتالی خود در مقابله با نفوذ هکرها احساس نمی کنند اما باید گفت در مواردی اشخاص

حقیقی نسبت به شرکت های بزرگ، از هک سیستم های رایانه ای و حساب های خود آسیب بیشتری می بینند.



وجود یک حفره امنیتی در نرم افزارهای نصب شده روی رایانه یا تلفن همراه، وجود برنامه های Keylogger و انواع و اقسام روش های دیگر می تواند به نفوذ هکرها به حریم خصوصی کاربران و به خطر افتادن تمامی حساب های شخصی از جمله حساب های بانکی منتهی شود.

با رعایت تمام اصول امنیتی، احتمال نفوذ هکرها کمتر خواهد شد اما هرگز از بین نمی رود. از سوی دیگر، پروسه حفاظت از حساب های شخصی تنها به کاربران محدود نمی شود و تا به امروز بارها خبرهایی از افشا شدن اطلاعات و کلمه های عبور کاربران سرویس های بزرگ با هک شدن سرورهای آنها شنیده ایم. با این وجود در صورت هک شدن حساب های شخصی چه باید کرد و راه های جلوگیری از تبعات آن چیست؟

واکنش سریع با استفاده از پست الکترونیکی

اگر برخی از حساب های اینترنتی شما هک شده و با تغییر کلمه عبور توسط هکر، امکان ورود به آنها وجود ندارد، امید خود را از دست ندهید؛ زیرا در صورت واکنش سریع احتمال بازگرداندن حساب های از دست رفته همچنان وجود دارد.

در هنگام ثبت نام در سرویس های اینترنتی، آدرس پست الکترونیکی خود را ثبت کرده اید و در صورتی که این آدرس از دسترس هکرها در آمان مانده باشد، می توان از آن برای بازگرداندن کلمه عبور استفاده کرد.

این اقدام نخستین گام در مقابله با نفوذ هکرها و بازیابی حساب های از دست رفته محسوب شده و توصیه می شود هر چه زودتر به استفاده از آن اقدام کنید.

در زمان ثبت نام سرویس های ایمیل نیز از شما درخواست می شود به شکل دلخواه آدرس دیگری را به عنوان پست الکترونیکی پشتیبانی معرفی کنید. همواره از این پیشنهاد برای مقابله با هک شدن ایمیل خود و بازیابی کلمه عبور در آینده، بهره بگیرید.



اسکن کامل رایانه

دومین گام، جلوگیری از دسترسی های بعدی و نفوذ مجدد هکرها به اطلاعات شخصی خواهد بود که برای انجام این کار ابتدا باید حرفه امنیتی یا راه نفوذ هکرها را پیدا کنید. برای انجام این کار باید از یک نرم افزار آنتی ویروس و ضد بدافزار برای اسکن کامل رایانه یا تلفن همراه استفاده کنید.

در این مرحله باید از ضد بدافزار و آنتی ویروس هایی کمک بگیرید که مورد تایید کارشناسان بوده و از اعتبار و قدرت کافی در زمینه کاری خود برخوردار باشند. ورود یک تروجان یا نصب Keylogger روی رایانه می تواند به ثبت اطلاعات ورودی و ارسال آنها به هکرها منجر شود و آنتی ویروس های قدرتمند قادر به تشخیص بدافزارها و حذف آنها خواهند بود.

اطلاع از مسیر بدافزارها و ویروس های پیدا شده می تواند به یافتن

ریشه آلودگی و رفع آن نیز کمک کند. یک فایل دانلود شده، داده های آپلود شده توسط سایت یا نرم افزارهای بی نام و نشان، همه به نوبه خود می توانند منشأ آلودگی و راه نفوذ هکرها باشند.



نفوذ هکرها به منبع اطلاعات

همان طور که گفته شد، نفوذ هکرها به حساب های شخصی افراد تنها به بی احتیاطی اشخاص حقیقی و کاربران اینترنت مربوط نمی شود. در مواردی هکرها به سرورهای سرویس های بزرگ نظیر یاهو یا جی میل نفوذ می کنند و حجم انبوهی از اطلاعات محرمانه و شخصی افراد را به سرقت می برند.

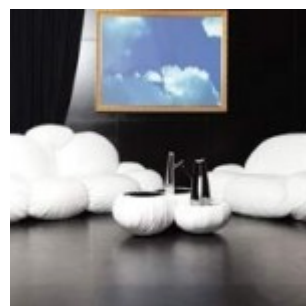
حتی اگر تمام نکات امنیتی را رعایت کنید، ممکن است سرویس مورد استفاده شما در ابعاد بزرگ مورد دستبرد هکرها قرار بگیرد و در این حالت هیچ کاری از دست کاربران معمولی برنخواهد آمد. برای اطلاع از این گونه اتفاقات باید روی اینترنت نام سرویس خود را با عبارت Password Leak جستجو کنید و با پیگیری اخبار مرتبط مطلع شوید آیا واقعا سرویس مورد استفاده شما با سرقت اطلاعات محرمانه توسط هکرها مواجه شده است یا خیر.

برای نمونه در جولای سال ۲۰۱۲ سرویس پست الکترونیکی یاهو، هک و میلیون ها کلمه عبور کاربران این سرویس جهانی در فضای اینترنت پخش شد. با این اتفاق سایر حساب های افراد مانند حساب فیس بوک یا توییتر آنها نیز با خطر مواجه شد و مقابله با این مشکل کاملاً خارج از قدرت کاربران بود.

اوضاع زمانی بدتر می شود که از یک کلمه عبور یکسان برای تمامی حساب های خود استفاده کرده باشید و با فاش شدن آن، تمامی حساب های تان به راحتی در دسترس هکرها قرار بگیرند. برای مقابله با این مشکل توصیه می شود از کلمه های عبور مختلف برای حساب های اینترنتی متفاوت خود بهره بگیرید و به منظور مقابله با فراموش کردن آنها از برنامه های مدیریت کلمه عبور استفاده کنید.

منبع: هفته نامه عصر ارتباط

فضای ابری چه کاربردی دارد؟



به گزارش ایتنا از مرکز ماهر، داریوش زندی اظهار کرد: تعداد کثیری از شرکت های مختلف به این فضای ابری علاقه نشان داده اند و مقدار محدودی از این فضا را در اختیار کاربران به صورت رایگان قرار می دهند.

وی افزود: این فضا دقیقاً شبیه هارد درایو شما روی سیستم است

منتها برای دسترسی به آن باید از اینترنت استفاده کنید در ضمن این فضا بر روی هارد درایو شما قرار ندارد و بر روی سرورهای قدرتمندی در کشورهای توسعه یافته قرار دارد.

این کارشناس ارشد هوش مصنوعی بیان کرد: برای دسترسی به این فضا هر کاربری نیاز به یک حساب کاربری دارد. کاربر با وارد شدن به حساب کاربری خود در هر مکانی و روی هر سیستمی می‌تواند به فضای ابری خود دسترسی داشته باشد.

وی عنوان کرد: از مهم‌ترین شرکت‌هایی که در این حوزه فعالیت دارد دراپ باکس است. با وارد شدن به سایت دراپ باکس و ساخت یک حساب کاربری در آن از دو گیگابایت فضای مجانی آن استفاده کنید. اگر به فضای بیشتری نیاز داشته باشید باید در عوض پولی بپردازید که برای کاربران ایرانی مشکلاتی را به همراه دارد.

وی اعلام کرد: مزیت دراپ باکس وجود نرم‌افزار لازم در تمام سیستم‌عامل‌های موجود و همچنین داشتن اپلیکیشن موبایل نیز است.

زندی تصریح کرد: از این به بعد اگر می‌خواهید به اطلاعاتتان در هرجایی و بر روی هر کامپیوتری و حتی روی گوشی‌تان دسترسی داشته باشید با ساخت یک اکانت در دراپ باکس از این امکان لذت ببرید.

وی ادامه داد: فرض کنید روی یک فایل متنی در منزل در حال کار هستید، شما می‌توانید آن را در فضای ابری خود قرار دهید و در محل کار آن را ویرایش کنید در واقع می‌توانید روی لپ‌تاپتان یک سند خلق کنید و آن را روی تلفن همراهتان ببینید و حتی بعداً روی سیستم‌تان در محل کار آن را ویرایش کنید.

این کارشناس ارشد هوش مصنوعی خاطرنشان کرد: همچنین در دراپ باکس این امکان مهیا شده است که می‌توانید به یک فایل خاص در فضای ابری خودتان لینک بدهید و آن را با دیگران به اشتراک بگذارید.

منبع: <http://www.ostovarit.com/single/article/2561> فضای ۱۲۰٪ بری ۲۰٪ چه ۲۰٪ کاربردی ۲۰٪ دارد؟

چگونه ایمیل اسپم را متوقف کنیم؟



این مقاله به شما مختصراً در مورد نحوه متوقف کردن ایمیل های اسپم توضیح می دهد. ایمیل های اسپم (هرزنامه) نه تنها مقدار قابل توجهی از فضای جهان مجازی را به خود اختصاص داده اند ، همچنین می توانند وسیله ای برای سرقت های امنیتی باشند. برای اطلاعات بیشتر در مورد تهدیدات ناشی از ایمیل های اسپم ، لطفاً این مقاله را مطالعه نمایید.

آیا می دانید در کشورهای پیشرفته فردی که ایمیل اسپم (هرزنامه) برای شما ارسال می کند مجرم بوده و علاوه بر بلوک شدن وب سایتش باید جریمه نقدی زیادی هم برای هر ایمیلی که برای شما می فرستد پرداخت نماید ؟

ما در این مقاله قصد داریم برخی از روش های موثر در مورد چگونگی متوقف کردن ایمیل های اسپم را به شما ارائه دهیم.

چرا ایمیل های اسپم یک تهدید به حساب می آیند؟

ایمیل های اسپم گاهی ممکن است ابزار خوبی برای سرقت هویت شما توسط هکرها باشند. شما با کلیک بر روی لینک موجود در این گونه

ایمیل ها ، ممکن است به طور ناخواسته برای فرستنده ی ایمیل ، این امکان را فراهم کنید که به بسیاری از اطلاعات مهم موجود در کامپیوتر شما دسترسی پیدا کند. مانند شماره Social Security، پسورد، مشخصات حساب و فایل های شخصی و غیره ، یعنی همه ی اطلاعات محرمانه ای که از آن ها استفاده می نمایید ، با استفاده از این روش تمام اطلاعات شما توسط فرد دیگری که این ایمیل را برایتان فرستاده است سرقت (سرقت هویت) می شود.

مشکل دیگر این ایمیل های اسپم این است که بعضا حاوی نرم افزارهای مخرب ، نرم افزارها جاسوس و غیره می باشند.

شما تنها با یک کلیک ساده روی هر یک از لینک های ایمیل اسپم ممکن است داندلود برخی از نرم افزارهای مخرب را در کامپیوتر خود آغاز نمایید.

بنابراین شما باید اطلاعات بیشتری در مورد حفاظت از سیستم تان در مقابل ابزارهای تبلیغاتی مزاحم و نرم افزارهای جاسوسی بدست آورید. با استفاده از این اطلاعات، ما به شما می گوئیم که در مورد این واقعیت کاملا مطمئن باشید که بسیاری از ایمیل های اسپم تهدیدی برای حریم خصوصی شما می باشند.

چگونه ایمیل های ناخواسته را متوقف کنیم ؟

بسیاری از ارائه دهندگان سرویس ایمیل (یاهو ، گوگل و ...) تا حد زیادی اقدامات لازم برای مسدود کردن ایمیل های اسپم را می دانند. بله ، شما باید متوجه پوشه اسپم ، در حساب ایمیل خود باشید. جایی که بسیاری از ایمیل های اسپم به صورت خودکار به آنجا منحرف می شوند. اما باز هم شما برخی از ایمیل های اسپم را در حساب اصلی خود دریافت می نمایید. شما می توانید اقدامات زیر را انجام دهید که می تواند به شما در متوقف کردن ایمیل های اسپم کمک کند.

هرگز پاسخ ایمیل اسپم را ندهید

مسلما شما آن قدر باهوش هستید که هرگز به یک ایمیل اسپم پاسخ

ندهید و یا روی لینک موجود در این ایمیل های ناخواسته کلیک نکنید . من به شخصه هیچ عنوان بر روی ایمیل های ناشناس کلیک نمی کنم و به سرعت آنها را Delete خواهم کرد . اما با این حال ممکن است گاهی تحت شرایطی ، این کار را انجام دهید مانند پاسخ دادن به یک ایمیل اسپم احساسی یا جواب دادن به یک سوال در ایمیل هرزنامه ای که برایتان ارسال شده است. کلیک روی ایمیل های اسپم تنها راهی است که شما به کسی که ایمیل اسپم را برایتان ارسال کرده اجازه می دهید به سیستم تان نفوذ کند ، باید بدانید که این ایمیل ها همیشه فعال هستند. فرستندگان ایمیل اسپم همیشه حواسشان هست که آدرس ایمیلی فعال باشد تا او را طعمه قرار دهند.

مورد دیگر اینکه گاهی حتی با کلیک کردن بر روی یک دکمه مانند قبول 'اشتراک' در ایمیل نیز راه برای فرستنده ایمیل اسپم باز خواهد شد تا شما را پیدا کند و بداند که آدرس ایمیل شما فعال است. پس تحت هیچ شرایطی روی ایمیل های ناشناس و مشکوک کلیک نکنید تا فرستنده ایمیل اسپم، ایمیل شما را غیر فعال تلقی نماید.



استفاده از ایمیل های مختلف برای شناسه ها

با استفاده از آدرس های ایمیل مختلف ، برای مقاصد مختلف، ایده ی هوشمندانه ای است. اگر شما کسی هستید که استفاده از سیستم خرید آنلاین را دوست دارید ، استفاده از یک آدرس ایمیل دیگر برای همه معاملاتی که از طریق اینترنت انجام می دهید روش خوبی خواهد بود. یعنی آدرس ایمیلی را که برای کسب و کار و یا استفاده شخصی تان استفاده می کنید ، برای انجام معاملات اینترنتی مورد استفاده قرار ندهید. در این شرایط شما می توانید هر زمان که خرید آنلاین انجام

میدهید، بدون نگرانی آدرس پست الکترونیکی خود را به فروشنده بدهید.

استفاده از فیلترهای هرزنامه

استفاده از فیلترهای اسپم ارائه شده توسط ارائه دهندگان خدمات پست الکترونیکی، یکی دیگر از راه های موثر برای کاهش دریافت ایمیل های اسپم هستند. اگر چه این فیلترهای هرزنامه به طور خودکار حذف می شوند و گاهی باز هم برخی از این گونه ایمیل های اسپم را دریافت می کنید، ولی شما می توانید ابتکار عمل به خرج داده و با مارک کردن این گونه ایمیل ها کاری کنید که بازهم این گونه ایمیل ها به عنوان اسپم به صندوق پستی بروند. کافی است که ایمیل خاصی را انتخاب کنید و آن را به عنوان اسپم علامت گذاری نمایید. به این روش شما می توانید دریافت ایمیل های اسپم را فیلتر نمایید.

این ها اطلاعات کمی در مورد نحوه متوقف کردن ایمیل های اسپم بود.

در ایالات متحده آمریکا قانون CAN – SPAM وجود دارد، این قانون چیزی است که حاکم بر تمام دادرسی هایی مربوط به سازمان های اسپم است. به امید روزی که در کشور ما نیز این قانون جزئی از قوانین حاکم بر این صنعت شود هر چند با توجه به رشد روز افزون تجارت آنلاین در ایران این روز زیاد دیر نیست.

منبع: <http://www.amoozesh-computer.ir/computer-traning-pro/how-to-stop-email-spam>