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 دردسر انداختن کاربران و بالا کشیدن پول آنها و خالی کردن حساب بانکی‌شان، بخش کوچی از اهداف این نامه‌های الکترونیکی هستند.

البته اکثر ایمیل‌های خطرناک و ویروسی غیر منتظره هستند و معمولا کاربران را در تشخیص دچار سردرگمی می‌کنند. اما چگونه می توان ایمیل های ویروسی و آلوده را از ایمیل های درست و واقعی تشخیص داد؛

ایمیل‌هایی با نام های اشتباهی

در دنیای واقعی آدرس اشخاص با ذکر پلاک منزل و شماره خیابان مشخص می شود. در فضای اینترنت نیز هر کامپیوتری با اعداد منحصر به فردی که بهIPمعروف است معین می‌شود که به وسیله آن راحت تر می توان 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 شماره هایIPبا یک نام مشخص می‌شود که با وارد کردن آن در مرورگر می‌توان به سایت موردنظر دسترسی پیدا کرد. مسلما بدون اینIPکامپیوتر نمی تواند آدرس را بیابد.در ایمیل های شخصی نیز افراد همزمان از اعداد و حروف استفاده می کنند.

اما گیرنده ایمیل تنها قادر به خواندن آدرس ایمیل هاست و نه خواندن شمارهIPآنها اما هکرها می توانند برنامه ایمیل های 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 می کند که از این فرد یا شرکت مذکور پیغامی دارد. لذا همواره مراقب باشید که حتی ایمیل های افرادی را که می شناسید 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 هائی 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 کاملا 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

تفاوت بین روش‌های رمزنگاری WEP، WPA و WPA2 در شبکه‌های بی سیم

امروزه با گسترش استفاده از اینترنت برای انجام فعالیت‌های خانگی و اداری و همچنین گسترش نفوذ تلفن‌های هوشمند در میان کاربران، مودم‌های بی سیم جز جدایی ناپذیر بسیاری از منازل و دفاتر در کشور شده‌اند. یکی از اولین مواردی که باید پس از نصب مودم‌های بی سیم به آنها توجه کرد، رمزگذاری روی آنها به منظور جلوگیری از سوء استفاده از سرویس اینترنت توسط کاربران ناخواسته است؛ اما حتی اگر شما به اهمیت استفاده از رمز روی مودم هم واقف باشید باز هم ممکن است بررسی تفاوت بین روش‌های مختلف رمزنگاری برایتان پیچیده بوده و خارج از حوصله شما باشد. در هر صورت به احتمال بسیار زیاد حتی اگر این تفاوت‌ها را هم ندانید با اسامی مخفی نظیر WEP، WPA و WPA2 آشنا هستید؛ اما هر کدام از این موارد به چه معنی هستند و کدام یک امنیت بیشتری را برای شبکه شما فراهم می‌کنند؟

تفاوت‌های واقعی یا ظاهری؟

اگر دستگاه مودم را از فروشنده ای با حوصله خریداری کرده باشید یا اینکه در مراحل نصب آن از افراد با تجربه کمک گرفته باشید حتما از آنها شنیده‌اید که اولین کار پس از روشن کردن مودم و در حال راه اندازی آن، در نظر گرفتن یک رمز عبور است. برای دانستن اهمیت رمزگذاری کافی است شرایطی را در نظر بگیرید که شخصی به

صورت غیر قانونی به شبکه شما دسترسی پیدا کرده و به وسیله آن، فعالیت مجرمانه ای را انجام می‌دهد. اگر بتوان این جرم را رهگیری کرد، پلیس مستقیما به منزل یا محل کار شما راهنمایی خواهد شد؛ در حالی که روح شما از اتفاقاتی که افتاده بی اطلاع است. فرضا که تصمیم بگیرید روی شبکه رمز هم بگذارید؛ اما واقعا یک اسم مخفف در کنار این رمز عبور چه تفاوتی می‌تواند ایجاد کند؟ باید بدانید روش‌های مختلف رمزنگاری در واقع سطوح و کارکردهای بسیار متفاوتی با یکدیگر دارند. در درجه اول، با گسترش دسترسی افراد مختلف به شبکه اینترنت، استانداردهای قدیمی به تدریج کاربری خود را از دست داده و در معرض خطر بیشتری قرار می‌گیرند. دانستن تفاوت بین پروتکل‌های مختلف و به کار گیری کاربردی‌ترین و پیشرفته‌ترین آنها بدون شک فرآیندی کلیدی در حفظ اطلاعات شخصی و پشتیبانی از شبکه شما به حساب می‌آید. از اواخر دهه ۹۰ میلادی، الگوریتم‌های امنیتی WiFi شاهد پیشرفت‌های چشمگیر و به روز رسانی‌های گسترده ای بوده‌اند که تقریبا تمامی آنها در ارتباط با کنار گذاشتن الگوریتم‌های قدیمی و بازنگری در راهبردهای امنیتی برای دسترسی به الگوریتم‌های پیشرفته تر و جدیدتر بوده‌اند. به همین دلیل بهترین راه برای شناخت روش‌های رمزنگاری گوناگون، بررسی تاریخچه آنهاست.

Wired Equivalent Privacy – WEP

WEP یا «امنیت مشابه با شبکه‌های با سیم» پر استفاده ترین الگوریتم امنیتی در جهان به شمار می‌رود. دلیل چنین اتفاقی قابلیت Backward Compatibility (سازگاری با شرایط قدیمی تر) و البته این نکته است که WEP اولین گزینه در فهرست روبه روی کاربران برای برقراری یک رمز است. اولین بار در سپتامبر سال ۱۹۹۹ بود که WEP به عنوان یک استاندارد امنیتی WiFi شناخته شد. اولین نسخه‌های WEP حتی در دهه ۹۰ هم آنقدرها قدرتمند نبودند، زیرا محدودیت‌های ایالات متحده روی صادرات تکنولوژی‌های مختلف رمزنگاری باعث شده بود تولید کنندگان محصولات خود را تنها به رمزگذاری‌های ۶۴ بیتی محدود کنند. پس از کنار گذاشتن این محدودیت‌ها، رمزگذاری به ۱۲۸ بیتی ارتقا پیدا کرد و در حال حاضر هم با وجود معرفی رمزگذاری WEP به صورت ۲۵۶ بیتی، باز هم مدل ۱۲۸ بیتی است که بیشترین استفاده را در بین کاربران دارد. رمزی که در حالت ۶۴ بیتی انتخاب می‌کنید، می‌تواند ۵ کاراکتر ASCII (کد استاندارد آمریکا برای تبادل اطلاعات یا آن طور که در زبان فارسی گفته می‌شود؛ اَسکی) یا ۱۰ کاراکتر هگزادسیمال (hex یا دستگاه اعداد پایه ۱۶) باشد، همچنین رمز ۱۲۸ بیتی نیز ۱۳

کاراکتر ASCII یا ۲۶ کاراکتر هگزادسیمال است. با اینکه WEP یک روش رمزگذاری به حساب می‌آید، اما شکستن آن به اندازه ای راحت است که در واقع یک شبکه با رمز WEP تفاوت خاصی با یک شبکه باز ندارد. باوجود باز نگری در این الگوریتم و معرفی حالت ۲۵۶ بیتی، نقص‌ها و ایرادات متعددی در استاندارد WEP کشف شد و بعد تر نیز با افزایش قدرت محاسباتی رایانه‌ها، عبور کردن از WEP آسان تر از قبل شد. در سال ۲۰۰۵ بود که FBI برای آگاه سازی کاربران از ضعف‌های WEP نمایشی عمومی برگزار کرد که در آن به کمک نرم افزارهای رایگان، تنها در عرض کمتر از یک دقیقه رمزهای WEP شکسته می‌شد. در حال حاضر نیز با وجود بهبودهای صورت گرفته، باز هم WEP به شدت آسیب پذیر بوده و به همین دلیل در سال ۲۰۰۴ این روش بازنشسته اعلام شد.

WiFi Protected Access – WPA

دسترسی حفاظت شده به WiFi یا همان WPA یک سال پیش از بازنشستگی WEP و برای جایگزینی آن ارائه شد. پر کاربردترین ساختار استفاده از WPA را می توان WPA-PSK نامید که توسط آن می توان بین ۸ تا ۶۳ کاراکتر ASCII را به عنوان رمز در نظر گرفت. کلیدهای استفاده شده توسط WPA به صورت ۲۵۶ بیتی بوده که پیشرفت چشمگیری نسبت به حالت‌های ۶۴ و ۱۲۸ بیتی WEP به حساب می‌آیند. برخی از مهم‌ترین تغییرات صورت گرفته توسط WPA عبارتند از بررسی یکپارچگی پیام برای مشخص کردن اینکه آیا مهاجمی توانسته بسته‌های اطلاعاتی رد و بدل شده بین access point و client را تصاحب کند یا خیر و پروتکل یکپارچگی کلیدهای موقت (TKIP). البته بعدتر TKIP با استاندارد رمزنگاری پیشرفته یا AES جایگزین شد. با وجود اینکه WPA برای راحت کردن خیال کاربران و خلاص شدن از WEP طراحی شده بود، اما به دلیل اینکه به وسیله به‌روزرسانی‌های firmware روی دستگاه‌های دارای WEP ارائه می‌شد، باید عناصر مشخصی از آن را تغییر می‌داد که همین موارد در نهایت باعث آسیب پذیری آن می‌شدند. پس از مدتی WPA هم به سرنوشت WEP دچار شد و نمایشی عمومی برای اثبات آسیب پذیری آن اجرا شد.

WiFi Protected Access II – WPA2

در سال ۲۰۰۶ بود که WPA با WPA2 جایگزین شد. یکی از بزرگ ترین تغییرات صورت گرفته در این جایگزینی، استفاده اجباری از الگوریتم‌های AES و همچنین معرفی CCMP (حالت ضد رمز به همراه

پروتکل کد اعتبارسنجی پیام تغییر بلوک) به عنوان جایگزینی برای TKIP بود. در حال حاضر استفاده از WPA2 برای کاربران خانگی تقریبا بدون نقطه ضعف بزرگ بوده و عمده نگرانی‌های پیرامون آن به امنیت بخش‌های تجاری مربوط می‌شود. متاسفانه بزرگ ترین نگرانی‌های موجود در WPA همچنان در WPA2 هم حاضرند و با وجود اینکه شکستن دیوار ایجاد شده توسط WPA2 به زمانی بین ۲ تا ۱۲ ساعت کار مداوم در یک رایانه حرفه ای نیاز دارد، اما باز هم ضرورت بازنگری و برطرف کردن حفره‌های امنیتی در آن احساس می‌شود.

کدام را انتخاب کنیم؟

حالا که با اسامی مختلف این روش‌های رمزگذاری آشنا شدیم باید به این پرسش پاسخ دهیم که در یک شبکه خانگی باید از کدام یک از آنها استفاده کرد؟ اگر بخواهیم خیلی ساده به این سوال پاسخ دهیم، می توان روش‌های رمزگذاری را بر حسب میزان نفوذناپذیری آنها به این صورت در نظر گرفت: قوی‌ترین و امن‌ترین حالت در شبکه‌های خانگی توسط WPA2+AES حاصل خواهد شد. پس از آن به ترتیب می توان WPA+AES، سپس WPA+TKIP/AES، بعد از آن WPA+TKIP، پس از آن WEP و در نهایت شبکه باز و بدون رمزگذاری را نام برد. البته برای استفاده از این روش‌ها باید یک نکته را در نظر داشت و آن، پشتیبانی تجهیزات شبکه شما از روش‌های مختلف رمزگذاری است. برای مثال اگر از یک مودم قدیمی استفاده می‌کنید ممکن است شرایط به کار گرفتن روش‌های WPA یا WPA2 در آن موجود نباشد و به همین دلیل مجبور شوید از تنظیمات نا امن WEP استفاده کنید. به همین دلیل اگر از این نوع مودم‌ها استفاده می‌کنید حتما به‌روزرسانی‌های امنیتی آن را در وب سایت تولید کننده دنبال کنید و همچنین پیش از خرید یک مودم جدید مطمئن شوید دستگاهی که انتخاب می‌کنید قابلیت به کار گیری روش‌های رمزگذاری جدید را دارد.

منبع:سخت افزار مگ

خرید اینترنتی: چرا، کجا، کی و چگونه؟

بسیاری از دارندگان وب سایت های فروشگاهی برای توجیه شروع فعالیت اقتصادی خود، یک یا حداکثر دو دلیل موجه دارند. برخی تعداد زیاد درخواست یک محصول را دلیل راه اندازی می دانند، برخی اطلاعات خوبی از سن و جنسیت مشتریان بالقوه خود دارند و تصور می کنند می توانند بر اساس آن اطلاعات پیشنهادهای خوبی به مشتری بدهند و … ولی هیچکدام اطلاعات و آمار دقیق برای راه اندازی فروشگاه اینترنتی ندارند.

به گزارش **پایگاه خبری فناوری اطلاعات استوار به نقل از برسام**، یک فروشگاه اینترنتی باید بتواند اطلاعات درست و کاملی داشته باشد. باید بداند یک خریدار دوست دارد چرا، کجا، کی و چگونه خرید کند. اگر حتی یکی از این موارد را برای خود به طور کامل و دقیق نتوانید جواب دهید پیشنهاد می کنیم اصلا منتظر نتیجه نباشید!

مانند گذشته ها نیست که به راحتی محصول خوش قیمتی پیدا کنید و با هزینه کم، فروشگاهی راه اندازی کنید و در نهایت هم رقیب جدی نداشته باشید. امروزه هر کس اراده ای برای خرید می کند، بلافاصله روش های مختلف برای خرید پیش روی خود می بیند. در محل کار، در حال پیاده روی، در فروشگاه های بزرگ، در اینترنت و بوسیله موبایل، کامپیوتر، ایکس باکس و … بدون کمترین دغدغه بهترین مکان برای خرید محصول خود را انتخاب می کند. رقابت در این تجارت هر روز بیشتر و پیچیده تر می شود و البته در صورت برداشتن قدم های درست، جذابیت و نتایج بسیار مطلوب تری نسبت به گذشته دارد.

یک از اشتباه هایی که فروشنده ها می کنند این است که هیچوقت خود را جای خریدار نمی گذارند. اصلا نمی دانند مشتری چه مراحلی را برای خرید از فروشگاه اینترنتی طی می کند تا به نتیجه نهایی برسد. باید به عنوان مدیر یک فروشگاه اینترنتی در هر لحظه از فعالیت و بروز رسانی سایت، بداند که مشتری نسبت به آن تغییرات چه واکنشی خواهد داشت. باید بدانید که مشتری در هنگام خرید در کدام بخش ها فرود می آید، به چه موانع و انتخاب هایی می رسد و شما اگر جای او بودید در هر کدام از این مراحل چه تصمیمی می گرفتید.

مشتری شما کیست؟

حتما این اطلاعات را از مشتری خود با ترفند های مناسب بدست آورید:

- سن
- جنسیت
- وضعیت تاهل
- میزان یا درجه درآمد
- میزان تحصیلات
- محل زندگی
- شغل

بسیاری از این اطلاعات در مراحل اولیه خرید می تواند بدست آید. برای تکمیل پروفایل مشتری خود می توانید با او تماس بگیرید و به سادگی از وی کسب اطلاع کنید.

زمانی که با وی تماس گرفته می شود اگر افراد آموزش دیده ای داشته باشید، مشتری با رضایت کامل این اطلاعات را نیز در اختیار شما می گذارد:

- فعالیت فعلی
- علاقمندی ها

مشتری چه چیزی نیاز دارد از محصول بداند؟

مشتری ها یک سری اطلاعات پایه از محصول باید بدانند. اتفاقا اگر به دنبال خرید اینترنتی است، شاید اطلاعات جزئی تر و دقیقتری نیاز دارد. در حقیقت او به دنبال آن است که کمبود مشاهده مستقیم محصول را با موارد دیگر تا حد امکان پر نماید. این موارد حتما به بهترین وجه ممکن به او باید داده شود:

- ظاهر آن چگونه است
- چگونه کار می کند
- ابعاد آن چیست
- چه رنگ هایی دارد
- امکانات آن چیست
- قیمت آن چقدر است
- آیا گارانتی دارد
- مدت زمان مصرف آن چقدر است
- مشخصات آن چیست

البته این سوالات برای محصولات مختلف تغییراتی نیز دارد. به هر حال شما باید سعی کنید تمام پرسش های ممکن مشتری در مورد محصول را حدس زده و جواب آنها را بدهید.

چرا باید از شما خرید کند؟

این شاید اصلی ترین سوالی باشد که باید حتما از خودتان سوال کنید. خیلی از مواقع انتظار داریم مشتری با دیدن بنر و اسلایدر زیبای شما در سایت، با خود فکر کند که چقدر این محصول خوب است و چرا من آنرا ندارم و اتفاقا چقدر پولدار هستم که بدون فکر و مکث، خیلی سریع روی آن کلیک کرده و سریع پرداخت می کنم!

تا زمانی که نتوانید به جای مشتری نشسته و دلیل خرید محصول را بیابید نمی توانید موفق شوید. اتفاقا جای تعجب دارد که چرا مدیران وب سایت های اینترنتی بدون بررسی هیچکدام از این موارد، نظریات خود را کاملا حرفه ای دانسته و شکی نمی کند که شاید مشتری نظری متفاوت با او داشته باشد و در نهایت شکست می خورد و باز هم همان روند را تکرار می کنند!

چرا باید مشتری محصول شما را بخرد:

- نیاز آنی و فوری مشتری را برآورده می کنید
- نیاز دائمی و متناوب مشتری را برآورده می کنید
- نماینده انحصار محصول یا برند خاصی هستید
- محصولی است کاملا جذاب و جالب
- کمترین قیمتی است که مشتری جستجو کرده است
- هزینه های اضافی مانند پست و مالیات ندارد
- ویژگی های برگشت محصول منحصر به فردی دارد
- کیفیت محصولات در بالاترین سطح قرار دارد

و چیزهایی از این قبیل… یک مدیر فروش حتما باید وجه تمایز خود با دیگر فروشگاه ها را حداقل در یکی از موارد ذکر شده بیابد تا مطمئن شود، محصول او برای قشری خاص حداقل فروش را خواهد داشت.

در مورد محصول چطور تحقیق می کند؟

تا ۱۵ سال پیش برای بررسی چیزی که قصد خرید داشتید حتما باید به فروشگاه می رفتید و یا از روی مجله ها یا روزنامه ها آنها را دیده و در مورد آنها می خواندید. امروزه روش های بررسی و تحقیق در مورد یک محصول بسیار متنوع تر شده است. می توانید در اتوبوس، روی تخت خواب یا داخل وب سایت ها همه کارها را انجام دهید.

با شنیدن اولین کلمه، سریعا به سراغ گوگل می روید یا برای خرید بدون دردسر به آمازون سر می زنید.

خیلی ها از طریق ایمیل خود با یک محصول آشنا می شوند و پس از خواندن در مورد آن محصول، باز به سراغ اینترنت رفته و گوگل و آمازون را باز می کند.

بسیاری دوست دارند از زبان دیگران بشنوند. به سراغ فروم ها رفته و نظر دیگران را در مورد آن محصول می شنوند. البته همیشه نمی توان این کار را انجام داد. اگر وسط خیابان هستید و باید بین دو مارک از یک محصول سریعا یک مورد را انتخاب کنید، نمی توانید وارد فروم شده و با خیال راحت به صحبت های ضد و نقیض دیگران گوش کنید!

همه اینها را به این خاطر گفتیم که بدانید هر قشری، در هر مکان و شرایطی روش های خود را برای مطالعه و بررسی محصول مورد نظر خود بر می گزیند. شما به عنوان فروشنده باید اینها را بدانید.

- جستجو بر اساس تصویر محصول یا نگاه کردن به مشخصات و امکانات آن
- مطالعه وبلاگ ها، سایت های مقایسه محصول و شبکه های اجتماعی
- مطالعه بررسی ها یا سوال کرد از دوستان و اطرافیان
- جستجو در برند ها و محصولات مشابه
- جستجو در مورد قیمت آن در وب سایت ها، منابع مختلف و حراجی ها

باید سعی کنید در همه این مکان ها یافت شوید! باید بر طبق اولویت های خود و هزینه ها، سعی کنید به مرور در تمامی این بخش ها فعالیت داشته و تلاش کنید با حضور در این بخش ها با فضاهای تجاری، مراجعه کنند گان و فروشندگان آشنا شده و در آنها نفوذ پیدا کنید.

این موارد نیاز اصلی دارندگان وب سایت های فروشگاهی یا افرادی که قصد راه اندازی چنین فعالیتی هستند، می باشد. اینکه فروشنده بداند یک خریدار دوست دارد چرا، کجا، کی و چگونه خرید کند، بسیار مهم بوده و مطمئنا اثرات بسیار زیادی در موفقیت یا عدم موفقیت یک فروشگاه اینترنتی داشته باشد. پس پیشنهاد می کنیم اگر شما هم از مخاطبین اصلی ما در این مقاله هستید، یک فرم طراحی کرده و برای هر محصول تمام پرسش هایی که مطرح کردیم را پر کنید و این فرم را برای هر محصول جدیدی که قصد فروش آن در وب سایت خود دارید نیز پر کنید.

منبع:http://www.ostovarit.com/single/article/874/خرید%۲۰اینترنتی:%۲۰چرا،%۲۰کجا،%۲۰کی%۲۰و%۲۰چگونه

در گوگل به صورت حرفه ای جستجو کنید

وقتی منبع عظیمی مثل گوگل در اختیار آدمیزاد باشد، ترجیح می دهد حتی برای پیدا کردن «آدرس زیره فروشی در خیابان سهروردی» هم به آن مراجعه کند. اگر بلد باشید خوب و حرفه ای جستجو کنید، همه چیز بدون تلاش خاصی زیر یوغ شماست!

۱- از سرویس های سریع و ساده استفاده کنید

می توانید بدون باز کردن یک سایت جانبی، خیلی از اطلاعات آب و هوا، فرموال های ریاضی و … را از گوگل بپرسید. مثلا برای پیدا کردن ساعت در کابل بزنید: time Kabul، پیش بینی آب و هوای کابل: weather Kabul، طلوع آفتاب در کابل: sunrise Kabul؛ یا برای به دست آوردن نتیجه یک محاسبه ریاضی، کافی است رابطه اش را در گوگل بنویسید و Enter را بزنید.

۲- کلماتی را که نمی خواهید، از جستجو حذف کنید

اگر دنبال موضوعی درباره وب دیزاین هستید، ولی نتیجه هایی را که در مورد تبلیغات است نمی خواهید، کافی است از کاراکتر خط تیره «-» استفاده کنید: web design – advertising.

۳- فقط محتویات یک سایت خاص را جستجو کنید

گاهی می خواهید در سایتی موضوعی را جستجو کنید تا سریع تر پیدایش کنید ولی آن سایت قابلیت جستجو ندارد یا طبق معمول اکثر سایت های ایرانی، قسمت جستجویش کار نمی کند. به راحتی می توانید تمام محتویات آن سایت را طبق این نمونه در گوگل جستجو کنید.

web design site yoursitedomain.com

۴- از کلمات مشابه و هم خانواده استفاده کنید

اگر از معنای دقیق کلمه ای خبر ندارید، می توانید از کلمات مشابه آن یا هم معنی هایش استفاده کنید تا جستجوی دقیق تری داشته باشید. برای این کار فقط در آخر سرچ، از علامت «~» بین کلمات مشابه یا هم معنی استفاده کنید:

web Design ~ web development

۵- فرمت فایل خود را مشخص کنید

اگر دنبال نتایجی هستید که به صورت PDF یا Word یا فرمتی خاص باشد، می توانید کلمه کلیدی، "Filetype"، و بعد فرمت مورئد نظر خود را جلوی موضوع بنویسید:

web design filetype.pdf

۶- از Range استفاده کنید

فرضا می خواهید مطلبی را بین سال های ۱۹۴۰ تا ۱۹۵۰ جستجو کنید. کافی است به این صورت سرچ کنید:

president 1940-1950

۷- واضح بنویسید

اگر می خواهید گوگل دقیقا عین عبارتی که در باکس جستجو نوشته اید را پیدا کند (برای مثال «طراحی وب سایت»)، آن را داخل علامت نقل قول قرار دهید: "web design".

۸- معنای کلمات را بدانید

برای فهمیدم تعنا، ریشه و حتی تلفظ واژه ها می توانید به گوگل پناه ببرید. کافی است به این صورت تایپ کنید:

define.apple

۹- از ستاره استفاده کنید

فرض کنید ایده ای برای جستجو دارید اما دقیقا نمی دانید از چه کلیدواژه هایی باید استفاده کرد. برای این موارد می توانید از ستاره استفاده کنید. آن وقت جای ستاره، ترکیباتی از چند کلیدواژه اولیه ای که دارید قرارت می گیرد. برای مثال cartoon * tutorials در در گوگل سرچ کنید. نتایجی که به دست می آید، چیزهایی مثل Cartoon Character IllustrationTutorials یـــا Cartoon Coloring Tutorial خواهد بود یعنی به جای ستاره، از ترکیبا مناسبی برای بهتر شدن نتیجه استفاده می کند.

۱۰- از صفحه Advanced Search استفاده کنید

اگر می خواهید مطلع شوید مردم ملبورن بعد از گل خداداد عزیزی به مارک بوسنیچ در آن بازی طلایی، چند بار اسم او را سرچ کرده اند، برای این کار می توانید به Advanced Search گوگل بروید و با انتخاب تنظیماتی، به راحتی این اطلاعات را به دست بیاورید، بدون اینکه نیازی به دانستن ترفندهای جستجو داشته باشید. غول گوگل، مرکب فرمانبر شماست!

منبع:http://www.ostovarit.com/single/article/885/در%۲۰گوگل%۲۰به%۲۰صورت%۲۰حرفه%۲۰ای%۲۰جستجو%۲۰کنید

راه‌های تقویت قدرت آنتن در مودم‌های wifi

بسیاری از کاربران سرویس ADSL برای استفاده همزمان توسط گجت‌های دیگر،از مودم‌های وای فای استفاده می‌کنند. این مودم‌ها که بعضا قوی هم نیستند، ممکن است برخی اوقات کاربران را در آنتن‌دهی و سرعت کلافه کنند. برای تقویت آنتن‌دهی وای فای مودم، به‌طور مختصر در این مطلب پنج راهکار را به شما معرفی می‌کنیم.

۱ـ پیدا کردن بهترین مکان برای مودم:
اولین و مهم ترین مرحله، پیدا کردن بهترین جای ممکن برای مودمتان است. بهترین مکان برای قرار دادن روتر فضایی باز است که علاوه بر برخورداری از ارتفاع مناسب، قرار نگرفتن سر راه سیکنال های دیواری است. همچنین توجه داشته باشید اگر از تمام محیط خانه به اینترنت وصل می شوید، بهترین مکان برای مودم شما مرکز خانه است در غیر این صورت می توانید جای مناسب برای مودم را با آزمایش و

خطا پیدا کنید.

برای یافتن قدرت سیکنال در نقاط مختلف منزل، می توانید از نرم افزارهای قدرت یاب سیکنال مانند Inssider یا نرم افزارهای مشابه استفاده کنید. بهتراست نرم افزار را روی لپ تاپ خود نصب کنید، سپس در نقاط مختلف خانه از دسترسی و کیفیت سیکنال های شبکه با خبر شوید. با کنار هم گذاشتن اطلاعات به دست آمده می توانید بهترین مکان قرارگیری دستگاه روتر را تشخیص دهید. توجه داشته باشید بهتر است آنتن یا آنتن های مودمتان را به صورت عمودی تنظیم کنید.

۲- از شر سیکنال های مزاحم خلاص شوید:
روترهای دیگر فقط دستگاه هایی نیستند که روی سیکنال وای فای خانگی شما تاثیر می گذارند؛ وسایلی مانند تلفن های بی سیم، مایکرو ویوها و دیگر دستگاه های بی سیم یا موج دار تأثیرات منفی بر سرعت و کیفیت سیکنال دریافتی شما می گذارد. بنابر این بهتر است مودم خود را نزدیک این وسایل قرار ندهید. همچنین مطمئن شوید مودمتان نزدیک وسیله ای فلزی یا آینه بین مودم (روتر) و رایانه، لپ تاپ یا کنسول بازی نباشد. اجسام فلزی، آینه و هر وسیله الکترونیکی دیگر که در محدوده فرکانسی ۲٫۴ گیگاهرتز کار کند، باعث کاهش قدرت سیکنال و اختلال در ارتباط و کاهش کیفیت ارتباط می شود.

۳ـ تعویض آنتن:
معمولا دستگاه های روتر با یک آنتن از نوع omni-directional که کیفیت معمولی نیز دارد فروخته می شوند، بنابراین اگر می خواهید محدوده و جهات پخش شدن سیکنال های شبکه بی سیم خود را افزایش دهید، می توانید با خرید یک آنتن uni-directional قوی تر و نصب آن روی دستگاه روتر خود، این کار را انجام دهید. اگر آنتن بهتری را در بازار برای خرید پیدا نکردید، دست کم می توانید از آنتن های بهتر از مدل فعلی، آنتن روتر خود را که به فناوری omni-directional مجهز است، استفاده کنید.

۴ـ استفاده از ورق های آلومینیومی
بیشتر روترها روی خود یک آنتن دارند که اطلاعات و سیکنال ها را به همه جهت ها ارسال می کنند، درست همانند یک لامپ معمولی که نور را پخش می کند. در صورتی که از دستگاه روتر خود در مرکز خانه خود استفاده می کنید، این ویژگی می تواند خیلی مفید باشد، اما اگر

روتر شما در گوشه ای از خانه قرار دارد، می توانید با استفاده از یک ورق آلومینیومی و حتی یک قوطی نوشابه باز شده به صورت ورقه بین دیوار و دستگاه روتر خود از هدر رفتن سیکنال ها جلوگیری کنید و آنها را دوباره به سمت محدوده کاری خود برگردانید. البته اگر می خواهید بهترین نتیجه را از این ترفند بگیرید، بهتر است کمی روی حالت ورق آلومینیومی در پشت روتر کار کنید و با انتخاب شکل های مختلف به بهترین حالت ممکن دست یابید.

۵ ـ استفاده از سخت افزارهای جانبی
افزایش محدوده قابل دسترسی بودن شبکه، یکی دیگر از مواردی است که کاربران شبکه های بی سیم خانگی به آن نیاز دارند. برای این کار بهترین روش ممکن استفاده از سخت افزارهای جانبی است که به چند مورد آن می پردازیم:

استفاده از دستگاه WiFi Repeater: این دستگاه همان طور که از اسم آن پیداست، قابلیت دارد که سیکنال های ارسالی دستگاه روتر بی سیم شما را دریافت کند. سپس آن را با کیفیت و قدرت اولیه در تمامی جهات پخش کند. بهترین حالت استفاده از این دستگاه در نقاطی است که مرز دریافت سیکنال های دستگاه روتر ماست. با این کار می توانیم محدوده شبکه خود را بدون نیاز به هیچ سیمی افزایش دهیم.

استفاده از یک روتر دیگر: یکی دیگر از روش هایی که برای افزایش محدوده های شبکه بی سیم به شما پیشنهاد می کنیم، خرید و استفاده از یک روتر دیگر در کنار روتر فعلی شماست. می توان روتر دوم را با یک کابل به شیوه LAN را به روتر اصلی وصل کرد.

استفاده از یک Access Point: با استفاده از یک دستگاه Access Point نیز می توانید به محدوده شبکه بی سیم خود وسعت بیشتری بدهید مانند استفاده از WiFi Repeater که در بالا با آن آشنا شدیم. از مزایای این روش می توان به قابلیت اتصال سیستم های بیشتر به شبکه و از معایب آن می توان به قیمت بالای این دستگاه نسبت به یک روتر اشاره کرد.همچنین دستگاه هایی برای افزایش کیفیت و برد سیکنال روتر شما به نام Range Extender در بازار موجود است که می توانید آن را در فواصل دور هم قرار دهید.

منبع:http://www.ostovarit.com/single/article/1677/راه‌های%۲۰تقویت%۲۰قدرت%۲۰آنتن%۲۰در%۲۰مودم‌های%۲۰wifi

نکاتی که در مورد اینستاگرام نمی دانید!

اینستاگرام اپلیکیشنی برای به اشتراک گذاشتن عکس و فیلم است که به کاربران اجازه آپلود تصاویر و اعمال فیلترهایی روی این تصاویر و به اشتراک گذاشتن آنها با فالوئرها را می دهد.

اینستاگرام اپلیکیشنی برای به اشتراک گذاشتن عکس و فیلم است که به کاربران اجازه آپلود تصاویر و اعمال فیلترهایی روی این تصاویر و به اشتراک گذاشتن آنها با فالوئرها را می دهد. اینستاگرام با "سلفی ها" معروف شد، زیرا کاربران در سفرها، رستوران ها و … عکس های سلفی خودشان را با اینستاگرام منتشر می کردند.

در عصر دیجیتال، رسانه های اجتماعی تبدیل به بخشی از زندگی مردم و حتی بهترین دوست آنها شده اند و اینستاگرام نیز پلتفرمی عالی برای این منظور است. با بیش از ۱۵۰ میلیون کاربرد و ۱۶ میلیارد تصویر به اشتراک گذاشته شده، شکی وجود ندارد که اینستاگرام بر دنیای شبکه های اجتماعی حکمرانی می کند.
البته این محبوبیت رو به رشد آماری هم دارد. ۱۵ نکته زیر جزو این

آمار هستند.

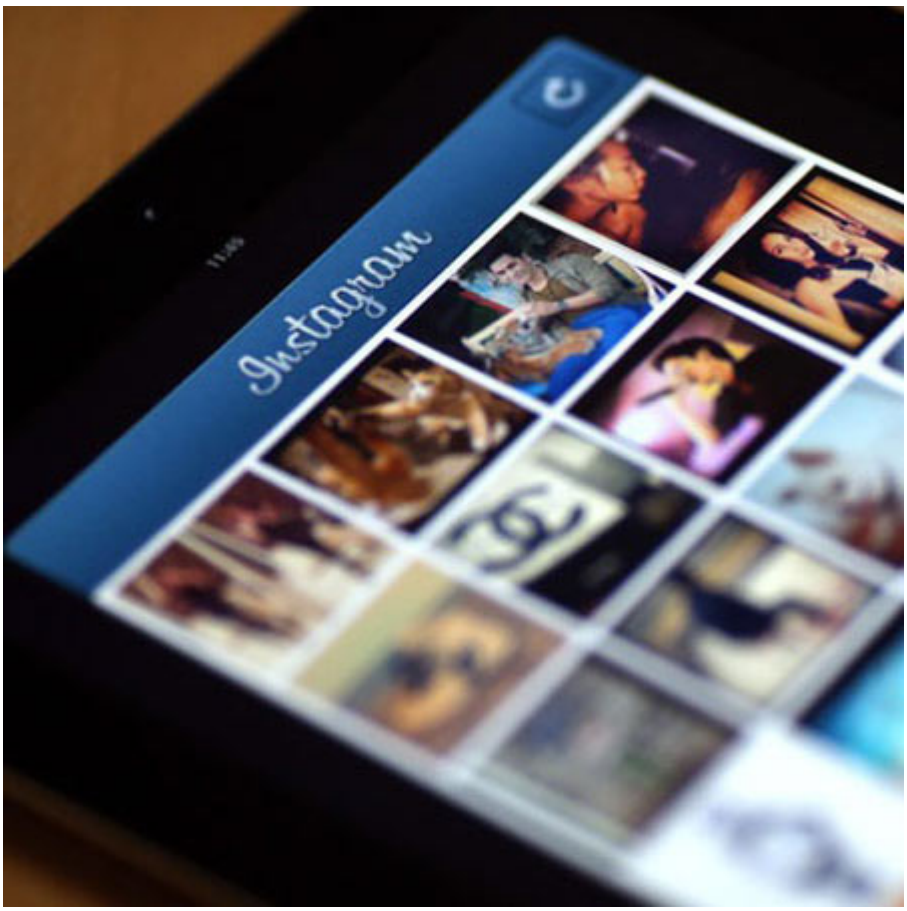
۱۵. خوشحال و ناراحت
بر اساس تصاویر به اشتراک گذاشته شده در اینستاگرام، بدعنق ترین قاره دنیا (بر اساس لبخندها) قاره آسیا است و شادترین شهر ایالات متحده، شهر سنت لوئی است.

۱۴. ژئوتگ
نیویورک سیتی در سال ۲۰۱۳ بیشترین برچسب جغرافیایی را خورده است و دیزنی لند از این لحاظ در رده دوم قرار دارد.

۱۳. هشتگ
۸۳ درصد از پست های اینستاگرام دارای هشتگ های (#) محبوب هستند. پرکاربردترین هشتگ سال ۲۰۱۳ هشتگ #love بوده است.

۱۲. لبخند بزنید!
تابحال ۲۰ میلیارد عکس در اینستاگرام آپلود شده است. این یعنی ۵۵ میلیون عکس در روز.

۱۱. کاربران
بیش از ۹۰ درصد کاربران اینستاگرام زیر ۳۵ سال هستند و ۶۸ درصد آنها خانم هستند.



۱۰. لایک!
در هر ثانیه نزدیک به ۸۵۰۰ بار لایک زده می شود.

۹. چیت چت
در هر ثانیه بیش از ۱۰۰۰ نظر ثبت می شود.

۸. بی فیلتر!
محبوب ترین فیلتر در میان کاربران “بی فیلتر” است و بیشترین لایک و نظر در میان عکس های فیلتر دار، فیلتر Mayfair است.

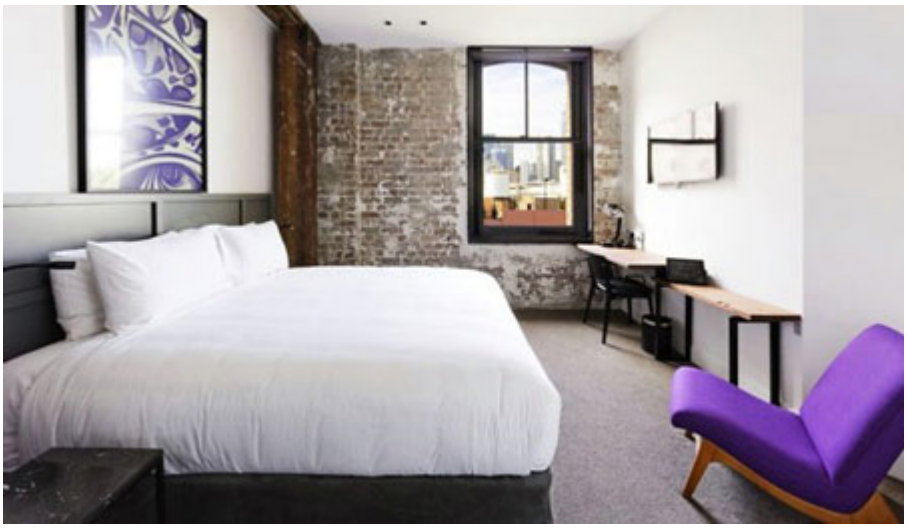
۷. Checking In
۷۰ درصد از کاربران اینستاگرام حداقل یک بار در روز check in می کنند. ولی نکته عجیب اینجاست که ۳۶ درصد از کاربران هرگز تصویری آپلود نکرده اند.

۶. سرآغاز

اینستاگرام در سال ۲۰۱۰ توسط کوین سیستروم و مایک کرایگر، فارالتحصیلان دانشگاه استنفورد، تأسیس شد و در ابتدا برای خدمات check in در یک مکان ساخته شده بود.

۵. هتل اینستاگرام

هتل ۱۸۸۸ سیدنی اولین هتل اینستاگرام دنیا است. در این هتل مکانی مخصوص عکس سلفی وجود دارد و اگر بیش از ۱۰۰۰۰ فالوئر در اینستاگرام داشته باشید می توانید یک شب رایگان در این هتل بمانید.



۴. آبی شوید.

تصاویری که رنگ غالب آنها آبی است، ۲۴ درصد بهتر از عکس هایی که تراکم رنگی قرمز و نارنجی دارند عمل می کنند. همچنین عکس های روشن بهتر از عکس های تاریک هستند.

۳. روز بوقلمون

محبوب ترین روز برای پست گذاشتن در اینستاگرام، به خصوص برای کسب و کار ها، روز پنج شنبه است. در روز شکرگزاری نیز ترافیک این اپلیکیشن زیاد می شود.

۲. فروخته شد!

در سال ۲۰۱۲ فیسبوک اینستاگرام را به قیمت ۱ میلیارد دلار خرید. مارک زاکربرگ مؤسس فیسبوک اعلام کرد که علیرغم آنکه اینستاگرام را خریده، ولی این اپلیکیشن همچنان مستقل از فیسبوک هدایت خواهد شد.

۱. پول پول پول!

وقتی فیسبوک اینستاگرام را خرید، اینستاگرام فقط ۱۳ کارمند داشت. هر کدام از این کارمندان بعد از فروش اینستاگرام، مولتی میلیونر شدند.

منبع:http://www.ostovarit.com/single/article/1898/نکا تی%۲۰که%۲۰در%۲۰مورد%۲۰اینستاگرام%۲۰نمی%۲۰دانید

---

۷ نکته درباره اینترنت که احتمالا نمی‌دانید!

امروزه عادت بر این است که معمولا کاربران دیگر پرسش‌های خود را از کسی نمی‌پرسند، بلکه مستقیم به سراغ گوگل و Bing رفته و از اینترنت پاسخ خود را می‌خواهند؛ اما اگر از ما بپرسند اطلاعات ما از اینترنت چیست، چه باید بگوییم و از اینترنت چقدر می‌دانیم؟

امروزه عادت بر این است که معمولا کاربران دیگر پرسش‌های خود را از کسی نمی‌پرسند، بلکه مستقیم به سراغ گوگل و Bing رفته و از اینترنت پاسخ خود را می‌خواهند؛ اما اگر از ما بپرسند اطلاعات ما از اینترنت چیست، چه باید بگوییم و از اینترنت چقدر می‌دانیم؟ ما در اینجا شما را با هفت نکته جالب درباره اینترنت آشنا می‌سازیم که احتمالا از آنها بی‌خبرید!

برخی از کاربران گمان می‌کنند با استفاده از Private Browsing امنیت حریم خصوصی خود را حفظ می‌کنند. واقعیت این است، در حالی که وب‌گردی در حالت Private در مرورگر هرچند به افزایش ضریب امنیت تا حدی کمک می‌کند، به هیچ وجه شما را نامرئی نمی‌کند! در این حال هنوز شما قابل رصد و هک شدن هستید و هکرها هنوز هم می‌توانند به سادگی اطلاعات شما را بدزدند.

در حالی که هر روزه از اینترنت به عنوان یکی از ابزارهای اصلی برای ارتباطات و حتی و کسب و کار خود بهره می‌بریم، باید یک بار از خود بپرسیم چقدر از اینترنت می‌دانیم. اینکه اینترنت بواقع چیست و چگونه می‌توان از آن بهره برد؟!

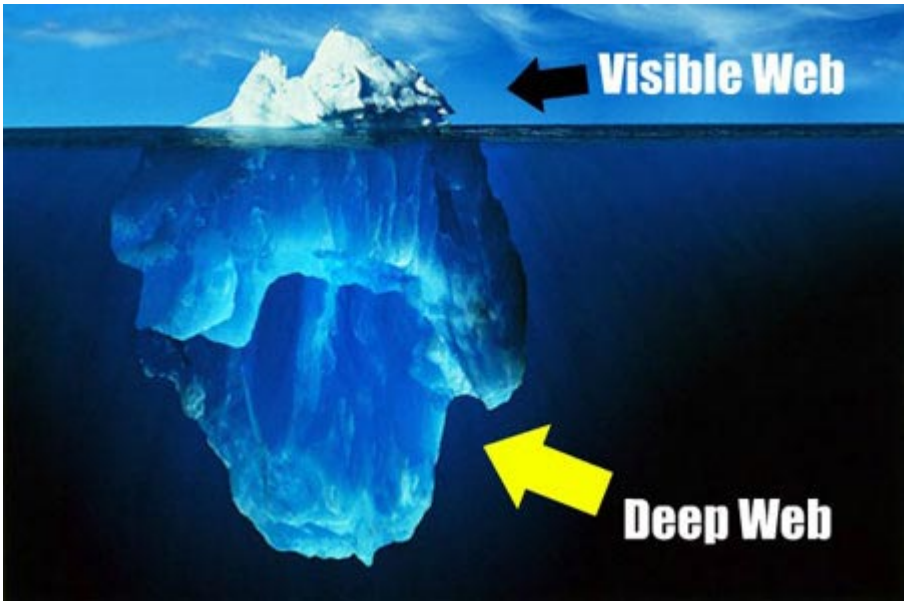
شاید به اندازه‌ای در فضای وب و سایبری مشغول و غرق شده‌ایم که اساسا فراموش کرده‌ایم در چنین فضایی هستیم؛ اما لازم است گاهی سری بالا کنیم و از ماهیت آنچه در آنیم و تاریخچه آن بیشتر آگاهی به دست آوریم.

البته در اینجا ما نمی‌خواهیم وارد مبحث ماهیت اینترنت و وب و یا

تاریخچه آن شویم، چرا که این موضوع مباحث مفصل و چالشی در بر دارد و قطعا تعریف ماهیت اینترنت چیزی نیست که در یک گزارش کوتاه بتوان جامع به آن پرداخت، بلکه هدف ما در اینجا این است که شما را با هفت نکته جالب در خصوص اینترنت و وب آشنا سازیم که در آن ضمن تمرکز بر جنبه سرگرم‌کننده، کمی چاشنی اطلاعات عمومی در خصوص اینترنت نیز مخلوط است.

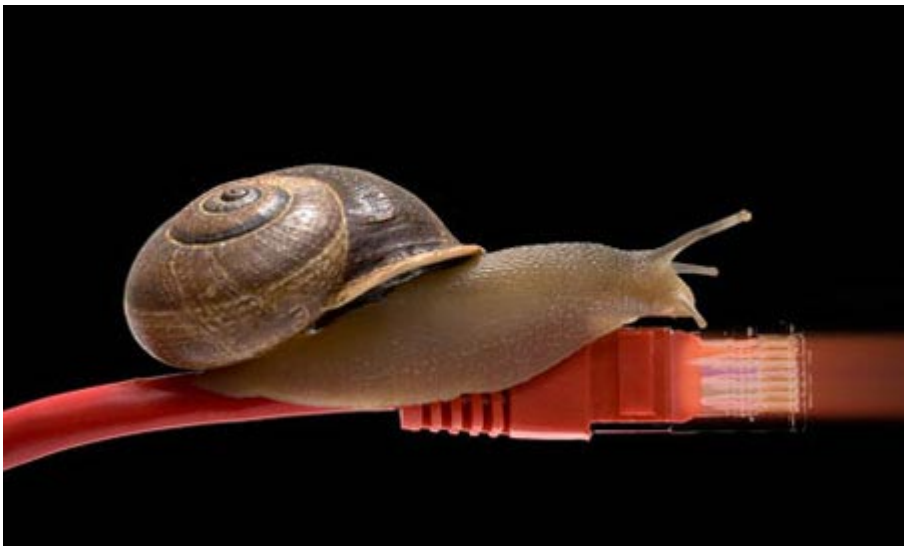
۱ ـ انسان ها تنها ۴۹ درصد از کل ترافیک اینترنت را شکل داده‌اند. الباقی ۵۱ درصد ترافیک اینترنت توسط Bot ها (ربات‌های رایانه‌ای که در واقع برنامه‌هایی برای انجام امور تعریف شده به شکل خودکار هستند) شکل داده شده است.

۲ ـ مجموع وب‌سایت‌های نامرئی و ثبت نشده که در موتورهای جستجو یافته نمی‌شوند (Deep Web) پانصد برابر بزرگتر و بیشتر از وب‌سایت‌های مرئی و قابل جستجو و بازدید (Surface Web) است.



۳ ـ سرعت اینترنت در پایگاه بین‌المللی فضایی بیشتر از متوسط سرعت اینترنت در استرالیاست و متوسط سرعت اینترنت در استرالیا، بیش از سه و نیم برابر متوسط سرعت اینترنت در ایران است.

۴ ـ هنگ کنگ با متوسط سرعت اینترنت ۸۲.۶ Mbps سریع‌ترین اینترنت دنیا و نیجر با ۰.۶ Mbps تنبل‌ترین اینترنت دنیا را دارند. ایران با متوسط سرعت ۴.۰۲ Mbps در رتبه ۱۵۴ در بین ۱۹۲ کشور قرار گرفته است.



۵- چهار تا پنج سال طول کشید تا رقم کاربران اینترنت به پنجاه میلیون رسید. در حالی که برای رسیدن تلویزیون به همین میزان کاربر، سیزده سال و برای رادیو، هجده سال زمان صرف شد.

۶ – نخستین وبسایت دنیا در سال ۱۹۹۱ ساخته شد. شما می‌توانید این وبسایت را در (www.info.cern.ch) ببینید.

۷ – نخستین وبکم در دانشگاه کمبریج و در سال ۱۹۹۳ برای رصد و دیدن یک قهوه جوش مورد استفاده قرار گرفت.

منبع:http://www.ostovarit.com/single/article/2384/7%20نکته%۲۰د رباره%۲۰اینترنت%۲۰که%۲۰احتمالا%۲۰نمی‌دانید!

فضای ابری چه کاربردی دارد؟

به گزارش ایتنا از مرکز ماهر، داریوش زندی اظهار کرد: تعداد کثیری از شرکت‌های مختلف به این فضای ابری علاقه نشان داده‌اند و مقدار محدودی از این فضا را در اختیار کاربران به صورت رایگان قرار می‌دهند.

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 توسعه‌یافته 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[1] 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 دارپ 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%۲۰ابری%۲۰چه%۲۰کاربردی%۲۰دارد؟

روش های برقراری امنیت رمز عبور

۸نکته مهم برای امنیت بیشتر رمز عبور

معمولا اکثر کسانی که از کامپیوتر استفاده می کنند، رمز عبورهای خیلی ساده را انتخاب می کنند. به نظر من این یک نوع سهل انگاری است. چون رمز عبورهای خیلی ساده و خیلی معمولی در مدت زمان چند ثانیه هک می شوند. اطلاعات شخصیتان مثل شماره حساب بانکی و یا شماره کارت اعتباریتان در اختیار هکرها قرار می گیرد و به راحتی می توانند با کارت اعتباریتان خرید کنند و یا از حسابتان پول برداشت کنند.

پس برای امنیت بیشتر رمز عبور ، مقاله زیر را به دقت مطالعه نمائید :

۱- اصلا برای پسورد از اسم استفاده نکنید، چه اسمتان چه فامیلیتان یا اسم مورد علاقه و یا هر اسم خاص دیگری. چون هکرها از برنامه های فرهنگ لغات خاصی استفاده می کنند که می توانند در عرض چند ثانیه پسوردتان را هک کند.
۲- برای پسوردتان، از ترکیبی از حروف بزرگ و کوچک و یا اعداد و یا علامت های خاصی استفاده کنید. البته از علامت های خاص به تنهایی استفاده نکنید. مثلا علامت خاص همراه با عدد و یا همراه با حروف را انتخاب کنید. بیشتر کاربران از علامت ! به همراه اسمشان استفاده می کنند که به راحتی قابل هک است.
۳- برای پسورد، حروف و اعدادی را که کنار هم قرار دارند انتخاب نکنید. مثلا پسوردهایی مثل "ghjkl" و یا "zxcvb" و یا اعداد

“۱۲۳۴۵۶۷” به راحتی قابل دسترس برای هکرها هستند.
۴- برای پسوردتان، حداقل از ۸ کاراکتر استفاده کنید.
برای پسوردهایی که از ۴ کاراکتر تشکیل شده اند، حدود ۴۵۰۰۰ حالت وجود دارد، ولی برای پسوردهایی که از ۸ کاراکتر و علامت های خاص تشکیل شده اند، در حدود یک میلیارد حالت وجود دارد.

۵- پسوردتان را همواره تغییر دهید.
اگر زمان استفاده از پسوردتان طولانی شود احتمال هک شدن پسوردتان بیشتر است. بهتر است که هر ۳ ماه یک بار پسوردتان را تغییر دهید.
۶- پسوردتان را به هیچ کس ندهید.
اگر کسی از شما به هر طریقی پسوردتان را خواست، به او ندهید! هکرها معمولا خودشان را به عنوان یکی از کارکنان شرکت های بزرگ، یا سرویس کار کامپیوتر معرفی می کنند و یا توسط تلفن و یا ایمیل، پسوردتان را برای حل کردن مشکلتان از شما می خواهند. ولی این نکته را فراموش نکنید که هیچ شرکت معتبری از شما پسورد نمی خواهد.
۷- تا حدی که امکان دارد پسوردتان را در جایی ننویسید.
اگر روی یک کاغذ آن را بنویسید و آن را در جای امنی مثل کیفتان قرار دهید، باز هم امکان هک شدنش وجود دارد. یا کاغذ را روی مانیتور یا هر جای دیگری نچسبانید و یا زیر کیبورد یا پد ماوس و یا هر جای دیگری که در معرض دید باشد نگذارید.
۸- پسوردتان را در کامپیوتر ذخیره نکنید.
کامپیوتر می تواند پسوردتان را ذخیره کند تا شما مجبور نباشید هر دفعه که می خواهید وارد شوید پسوردتان را بزنید. به این ترتیب اگر که مرتبا می خواهید وارد شوید احتیاج ندارید که پسورد را هر بار وارد کنید، این باعث می شود که خیلی زود پسورد را فراموش کنید. این نکته را یادتان باشد که اگر بخواهید پسورد را عوض کنید، باید حتما پسورد قبلی یادتان باشد.

۷ تکنیک ایجاد رمز عبور حرفه ای با امنیت بالا

۱- برای ایجاد کردن پسورد، از حروف بزرگ و کوچک به صورت یک در میان یا دو در میان استفاده کنید. مثل: InTeRnEt و یا INteRNet
۲- یک جمله را در ذهن خود در نظر بگیرید. حر.ف اول کلمات این جمله را برای پسوردتان انتخاب کنید. مثلا: " Man Har Ruz Be Site Amoozesh Computer Sar Mizanam" حالا پسورد من : ""MHRBSACSM
۳- اسم خودتان یا یک لغت را در نظر بگیرید، حالا حروف سمت راست یا چپ آن را که روی کیبورد است برای پسوردتان انتخاب کنید. مثلا: COMPUTER پسورد من است و حروف سمت راست آن : pdysfroy
۴- عدد یا تاریخی برای خودتان انتخاب کنید و سپس بر طبق آن دکمه ی Shift را نگهدارید و تایپ کنید. مثلا: ۱۳۶۸و۲۵و۶۹ که می شود: !#^*<@%>^)
۵- در پسوردتان از علامت های خاص استفاده کنید. مثال: C/om\@p{u$t%er*&
۶- لغات یک جمله را به اختصار بنویسید. این اختصارات مربوط به خودتان است و قاعده و قانون خاصی ندارد. جمله: "I have a best site for my lessons" پسورد: ""ihvbstsfrmls
۷- لغت یا ترکیبی از لغات و اعداد را برای خود انتخاب کنید. بعد آن را به هم بریزید مثلا حرف اول را به جای حرف آخر قرار دهید و یا جای اعداد را با حروف را با هم عوض کنید. مثال: com319put410er36 پسورد:ut36ter410comp319

منبع:http://www.amoozesh-computer.ir/security/password-scurity