

# نت تاپ چیست؟



یک رایانه در ابعاد کوچک است حدود ~ 25(H)mm x 135(D) x W) (450g) که تمامی قابلیت‌های یک رایانه را در خود جای می‌دهد و به عنوان رقیب اصلی رایانه‌های رومیزی معمولی می‌باشد. علت نامگذاری این رایانه به این نام این است که NetTop از دو کلمه نت (Internet) و تاپ (Desktop) به معنای میزکار تشکیل شده است.

در مقایسه با رایانه‌های معمولی نت تاپ‌ها نه تنها کوچکتر ارزانتر و سبک‌ترند بلکه مصرف برق به مراتب کمتری هم دارند. یک نت تاپ در حدود ۲۳ وات برق مصرف می‌کند.

نت تاپ را می‌توان در پشت مانیتورها یا تان نصب کنید که به نسبت کیس‌های بزرگ امروزی فضای کمتری را اشغال می‌کند البته می‌توان آنها را با استفاده از پایه روی میز قرارداد.

NetTop ها از لحاظ سیستم خنک کننده به دو بخش عمده دسته بندی می شوند. دسته اول در قسمت تهویه خود دارای فن و دسته دوم که فاقد فن هستند از فناوری هوای خنک استفاده می کنند ، این قابلیت باعث شده که NetTop به عنوان یکی از کم صداترین تجهیزات فن آوری اطلاعات در منازل و دفاتر کار و شرکت ها مطرح شوند.



البته لازم به ذکر است که طراحی نت تاپ ها به گونه ای است که بیشتر بر روی دستیابی های مبتنی بر وب تمرکز دارند تا انجام فعالیت های محاسباتی پیشرفته، بنابراین معمولاً نسبت به کامپیوترهای شخصی همتای خود دارای قدرت پردازش و حافظه کمتری می باشند که این باعث اجرانشدن سریع و دقیق می شود.

همچنین با وجود اینکه کامپیوترهای امروزی کمتر بر روی رسانه های نوری مانند سی دی و دی وی دی جهت ذخیره سازی تمرکز دارند اما به طور کامل نمی توان آنها را نادیده گرفت و این در حالیست که بیشتر نت تاپ ها فاقد سی دی / دی وی دی رام می باشند.

### اجزا و ویژگی های یک نت تاپ:

- قابلیت نصب سیستم عامل های ویندوز و لینوکس را دارا می باشند.
- کارت شبکه مینیاتوری GB LAN و Wi-Fi IEEE 802.11b/g/n
- درگاه های USB 3.0 , HDMI
- کارت خوان داخلی SD/SDHC/MS/MS Pro/MMC
- درگاه های USB 2.0, DVI ، صدا و میکروفون
- استفاده از از هاردهای ۵۲۵ اینچی یا SSD و حافظه DDR3

Nettop ها را می توان بر اساس توان آنها در ادارات ، بانک ها ، مدارس ، شرکت های خصوصی ، کارخانجات و در خانه مورد استفاده قرار داد.

به منظور آشنایی بیشتر با مدل های ارائه شده نت تاپ ها در زیر چندین نمونه از آنها را معرفی خواهیم کرد.

**- نت تاپ سولمیت آمیس (Solmate AMIS Nettop)**

- \* پشتیبانی از DOS – XP – VISTA – SEVEN – LINUX
- \* پردازنده Intel Atom D525 1.8 Dual Core با تکنولوژی CUDA چهار هسته پردازشی
- \* گرافیک NVidia ION2 Geforce 9400 M 512 DDR3
- \* ۴/۲ گیگ رم DDR3 ، هارد ۳۲۰ گیگ پشتیبانی تا ۵۰۰ گیگ
- \* ۴ عدد پورت USB ، شبکه ۱ گیگ و شبکه وایرلس سری N ، خروجی گرافیک VGA و HDMI ، ورودی و خروجی صدا

**- نت تاپ سولمیت جنریک (Solmate Generic Nettop)**

- \* پشتیبانی از DOS – XP – LINUX
- \* پردازنده Intel Atom D510 1.66 Doul Core
- \* گرافیک Intel GMA 3150 256
- \* ۲ گیگ رم DDR|| ، هارد ۲۵۰ گیگ پشتیبانی تا ۵۰۰ گیگ
- \* ۶ عدد پورت USB ، شبکه ۱ گیگ ، خروجی گرافیک VGA ، ورودی و خروجی صدا
- \* کاملاً بی صدا ، ۰.۵ لیتر حجم ، ۶۵۰ گرم وزن ، ۱۸ وات میانگین مصرف برق ، قابلیت اتصال پشت مانیتور

**- نت تاپ مکس دیتا**

- \* پشتیبانی از DOS – XP – VISTA – SEVEN – LINUX
- \* پردازنده Intel Atom 330 1.6 Dual Core با تکنولوژی CUDA چهار هسته پردازشی
- \* گرافیک NVidia ION Geforce 9400 M 512
- \* ۲ گیگ DDR|| ، هارد ۲۵۰ گیگ پشتیبانی تا ۵۰۰ گیگ
- \* ۴ عدد پورت USB ، شبکه ۱ گیگ ، خروجی همزمان گرافیک DVI و HDMI ، ورودی و خروجی صدا
- \* Card Reader ,Wlan 802 .11 b/g/n
- \* کاملاً بی صدا ، ۰.۵ لیتر حجم ، ۵۵۰ گرم وزن ، ۱۸ وات میانگین مصرف برق ، قابلیت اتصال پشت مانیتور

**- نت تاپ سولمیت مدیا (Solmate Media Nettop)**

- \* پشتیبانی از DOS – XP – VISTA – SEVEN – LINUX
- \* پردازنده Intel Atom 330 1.6 Dual Core با تکنولوژی CUDA چهار هسته پردازشی
- \* گرافیک NVidia ION Geforce 9400 M 512
- \* ۲ گیگ / ۴ گیگ رم DDR|| ، هارد ۲۵۰ گیگ پشتیبانی تا ۵۰۰ گیگ
- \* ۵ عدد پورت USB ، شبکه ۱ گیگ ، خروجی گرافیک DVI ، ورودی و

خروجی صدا

\* Card Reader , e-sata , Infra Red , WLAN 802 .11 b/g

\* کاملاً بی صدا ، ۰٫۷ لیتر حجم ، ۸۵۰ گرم وزن ، ۱۸ وات میانگین مصرف برق ، قابلیت اتصال پشت مانیتور

- نت تاپ سولمیت تاور

\* پشتیبانی از DOS - XP - VISTA - SEVEN - LINUX

\* پردازنده Intel Atom 330 1.6 Dual Core با تکنولوژی CUDA چهار هسته پردازشی

\* گرافیک NVidia ION Geforce 9400 M 512

۳ \* گیگ رم DDR || ، هارد ۲۵۰ گیگ پشتیبانی تا ۵۰۰ گیگ

\* ۶ عدد پورت USB ، شبکه ۱ گیگ ، خروجی گرافیک DVI ، ورودی و خروجی صدا

\* کاملاً بی صدا ، ۰٫۵ لیتر حجم ، ۶۵۰ گرم وزن ، ۱۸ وات میانگین مصرف برق ، قابلیت اتصال پشت مانیتور



---

تروجان چیست؟ و چگونه در مقابل  
آن ایمن شویم؟



در این مطلب قصد داریم راجع به شاخه ای از بدافزارها به نام «اسب تروجان» که به اختصار «تروجان» نامیده می شوند صحبت کنیم. تروجان ها برخلاف ویروس ها، کرم ها و ... توانایی تکثیر خود را ندارند. آنها بسیار شبیه نرم افزارهای مفید و کاربردی رفتار می کنند، اما در درون خود کدهای مخفی دارند که باعث دسترسی هکر سازنده تروجان به کامپیوتر هدف (کامپیوتر آلوده شده) و به دست گرفتن کنترل آن می شوند.



## علت نام گذاری

نام این بدافزارها به ماجرای تسخیر تروا توسط یونان برمی گردد، که با ساختن یک اسب چوبی و مخفی شدن درون شکم آن به شهر تروا نفوذ کرده و آن را به تصرف خود درآوردند. در این داستان اسب تروا نقش یک بدافزار را دارد و شهر تروا مانند کامپیوتر کاربری است که توسط اسب تروا آلوده می شود. به همین دلیل بعضی بکار بردن کلمه «تروجان» برای بدافزار را اشتباه و کلمه «اسب تروجان» را صحیح می دانند.

## مقدمه

تروجان ها برخلاف ویروس ها، کرم ها و ... توانایی تکثیر خود را ندارند. آنها بسیار شبیه نرم افزارهای مفید و کاربردی رفتار می کنند، اما در درون خود کدهای مخفی دارند که باعث دسترسی هکر سازنده تروجان به کامپیوتر هدف (کامپیوتر آلوده شده) و به دست گرفتن کنترل آن می شوند. البته در مواردی که چند کاربر از یک

کامپیوتر استفاده می کنند سطح دسترسی هکر بسته به سطح دسترسی کاربر آلوده و نوع تروجان تفاوت می کند.

## اهداف و عملکرد

زمانی که هکر به کامپیوتر هدف نفوذ می کند، احتمالاً قصد انجام این اعمال را در کامپیوتر هدف داشته باشد: استفاده از کامپیوتر به عنوان یک ابزار برای نفوذ به دیگر سیستمها و شبکه ها

دزدیدن اطلاعات (مثل رمزهای عبور)

نصب نرم افزارها (مثلاً یک بدافزار)

دانلود و آپلود فایلها و استفاده از پهنای باند

تغییر یا حذف فایلها

Key Logging (ثبت فعالیت هایی که کاربر انجام می دهد. برای مثال یک Key Logger می تواند تمام دکمه های صفحه کلید را که فشار می دهید به ترتیب ثبت کند و آنها را به هکر سازنده اش ارسال کند.)

دیدن صفحه نمایش کامپیوتر هدف

پر کردن فضای خالی کامپیوتر هدف

تروجان برای انجام اهداف خود نیاز به ارتباط با هکر سازنده اش دارد. البته این گونه نیست که هکر برای هر کدام از تروجان های خود دستور خاصی بدهد، بلکه می تواند در اینترنت جستجو کرده و کامپیوترهای آلوده را پیدا کند. سپس کنترل هر کدام را که بخواهد به دست می گیرد.

## انتقال و نصب

تروجان به روشهای زیر کامپیوتر را آلوده می کند:

۱-دانلود نرم افزارها (تروجان قسمتی از نرم افزاری است که کاربر آن را از اینترنت دانلود و نصب می کند.)

۲-سایت های دارای کدهای مخرب (مثلاً زمانی که وارد یک سایت می شوید، سایت یک برنامه روی کامپیوتر اجرا می کند و تروجان را روی کامپیوتر کپی می کند.)

۳-فایل های ضمیمه ایمیل (Email attachments) ممکن است همراه یک ایمیل فایلی باشد که اگر آن را باز کنید، تروجان منتقل شود.)

۴-استفاده از نقص های نرم افزارها (تروجان از طریق ایرادهایی که در نرم افزارهایی مثل مرورگرهای اینترنتی، مدیا پلیرها و مسنجرها وجود دارد، به کامپیوتر کاربر نفوذ می کند.)



در زیر راه های مقابله با موارد بالا را به ترتیب می آوریم:

۱- دانلود نرم افزارها نرم افزارهای اینترنتی به دو گروه کلی تقسیم می شوند: رایگان و پولی. زمانی که می خواهید از یک نرم افزار رایگان استفاده کنید، حتما آن را از سایت اصلی اش دانلود کنید. اگر آدرس سایت اصلی را نمی دانید، نام نرم افزار را در گوگل - یا هر موتور جستجوی دیگر - جستجو کنید و سایتی که در بالای نتایج می آید را برای دانلود برگزینید. البته معمولا آدرس آن سایت شباهت زیادی به نام نرم افزار دارد. مثلا برای دانلود آنتی ویروس «اوست» به سایت «[avast.com](http://avast.com)» مراجعه کنید. ماجرای دربارۀ نرم افزارهای پولی پیچیده تر است.

برای خرید اینترنتی این نرم افزارها به کارت اعتباری و یک حساب بانکی بین المللی نیاز است که در دسترس همگان نیست. خب برای رفع این مشکل باید نسخه کرک شده (قفل شکسته) نرم افزار را پیدا کنیم و یا به جای نرم افزار پولی از یک نرم افزار مشابه و رایگان استفاده کنیم. ما توصیه می کنیم حتی الامکان از نرم افزار جایگزین و رایگان استفاده کنید، اما برای بعضی نرم افزارها - مثل Photoshop - جایگزین مناسبی وجود ندارد و کاربران مجبور به استفاده از نسخه های کرک شده هستند.

همان طور که می دانید این کار خلاف قانون کپی رایت بوده و دقیقا از همین جا است که خطرات آغاز می شود. بسیاری از نرم افزارهای کرک شده حاوی انواع بدافزارها خصوصا تروجان هستند. این امر کاملا طبیعی است. شما خودتان را جای یک هکر بگذارید. آیا حاضرید برای رضای خدا مدت ها وقت و انرژی خود را بگذارید تا بتوانید یک نرم

افزار را کرک کنید و آن را به رایگان در اختیار دیگران قرار دهید؟ مسلماً نه.

بسیار از کاربران می‌خواهند که بتوانند نرم‌افزارهای دیگر را به رایگان در اختیار بگیرند. اما این کار با رعایت حقوق مالکانه سازگار نیست. اگر شما نرم‌افزاری را کرک کنید و به دیگران بدهید، در واقع به آنها اجازه می‌دهید که بدون پرداخت هزینه، از کار شما استفاده کنند. این کار می‌تواند به ضرر شما باشد، زیرا شما نمی‌توانید از فروش نرم‌افزار خود درآمد داشته باشید. همچنین، اگر نرم‌افزار شما حاوی کدهای مخرب یا بدافزار باشد، می‌تواند به کاربران آسیب برساند. بنابراین، توصیه می‌شود که نرم‌افزارهای خود را به صورت قانونی و با رعایت حقوق مالکانه توزیع کنید.

خب پس تکلیف چیست؟ توصیه ما این است که حتی الامکان از نرم افزارهای کرک شده استفاده نکنید و اگر مجبور بودید، قبل از اینکه نرم افزار را نصب کنید، پوشه حاوی نرم افزار را با آنتی ویروس و دیگر نرم افزارهای امنیتی خود کنترل (scan) کنید. سپس نرم افزار را نصب کرده و این بار کل کامپیوتر خود را اسکن کنید. اگر در اسکن چیزی پیدا نشد که خوش به حال تان و می توانید دفعات بعد هم از همین نسخه کرک شده استفاده کنید. ولی اگر در اسکن بدافزاری پیدا شد، ضمن آنکه به آنتی ویروس می گوئید که آن بدافزار را پاک کند، توصیه می شود دفعات بعد از نسخه دیگری استفاده کنید. البته اگر نرم افزارهای امنیتی شما قوی و آپدیت (به روز) باشند احتمالاً خطر زیادی شما را تهدید نمی کند. یادآوری: یکی از معمول ترین فایل های آلوده به بدافزارها کی جن (Keygen) ها هستند. کی جن ها همان نرم افزارهایی هستند که برایتان رمزعبور تولید (Generate) می کنند.

## ۲- سایت های حاوی کدهای مخرب

خطر آلودگی از این طریق بستگی مستقیمی به عادات وبگردی تان دارد. اگر شما همیشه به یکسری سایت های شناخته شده و معتبر سر بزنید، خطر زیادی تهدیدتان نمی کند. مشکل زمانی پیش می آید که به دنبال چیزی در موتورهای جستجو می گردید. در این موارد موتور جستجو سایت هایی پیشنهاد می دهد که هیچ شناختی از آنها ندارید و ممکن است حاوی کدهای مخرب باشند.

توصیه هایی برای وبگردی امن تر:  
از مرورگر فایرفاکس استفاده کنید.

اگر سرعت اینترنت خوبی دارید از حالت «گشت و گذار محرمانه» استفاده کنید. برای فعال کردن این حالت در فایرفاکس در منوی Tools روی گزینه Private Browsing Windows کلیک کنید. در پنجره

بعد روی دکمه Start Private Browsing کلیک کنید. با این کار تمام Tab های فعلی فایرفاکس تان بسته می شوند و پنجره Private Browsing باز می شود. پس از گشت و گذار در اینترنت زمانی که پنجره را می بندید، تمام تاریخچه، کوکی ها و هر فایل دیگری که در زمان وبگردی محرمانه ذخیره شده است، پاک می شوند و در آخر Tab های فایرفاکس عادی تان باز می گردند.

استفاده از افزونه Noscript در فایرفاکس.

۳- ضمیمه هایی که به ایمیل ها الصاق می شوند

هیچ گاه ایمیلی که فرستنده آن را نمی شناسید باز نکنید. بلکه با خیال راحت آن را حذف کنید. اگر از جیمیل استفاده می کنید آن ایمیل را تیک زده و روی دکمه Report Spam کلیک کنید، تا دیگر ایمیلی از این شخص برای تان نیاید.

نکته: نام فرستنده این ایمیل ها معمولا نام یک بانک معتبر است و در Subject ایمیل نوشته که شما پول فراوانی برنده شده اید و یا از یک نام زیبای زنانه استفاده شده.

۴- استفاده از نقص های نرم افزاری

برای حل این مشکل سعی کنید همیشه نرم افزارهایتان را به روز نگه دارید. خصوصا به روز رسانی های امنیتی (Security Updates) را حتما نصب کنید.

### **اگر به تروجان آلوده شدید**

نرم افزارهای آنتی ویروس توانایی پاک کردن تروجان ها را دارند. آنها حتی می توانند قبل از نفوذ تروجان به سیستم جلوی آن را بگیرند. البته اگر از عملکرد یک تروجان آگاهی کافی داشته باشید، حتی خودتان می توانید آن را پیدا کرده و پاک کنید. البته در مورد تروجان هایی که دسترسی هکر را به سیستم فراهم می آورند، ماجرا کمی پیچیده تر است. در این موارد اگر امنیت کامپیوتر اهمیت زیادی دارد، توصیه می شود کل هارد کامپیوتر را فرمت (پاک) کنید و از ابتدا روی آن سیستم عامل و نرم افزارهای مورد نیاز را نصب کنید.

### **و در آخر شیوع تروجان ها**

با توجه به علاقه روز افزون هکرها به مبحث کنترل کامپیوتر از راه دور، شیوع تروجان در میان بدافزارها در حال افزایش است. طبق آمار مختلف در سه ماهه آخر سال ۲۰۰۹ بین ۷۰ تا ۸۰ درصد از بدافزارهای

کشف شده در سراسر دنیا تروجان بودند و این میزان در حال افزایش است. پس بهتر است آنها را جدی بگیرید.

---

# 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!



Google Chrome  
نیازان چارم

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

البته اکثر ایمیل‌های خطرناک و ویروسی غیر منتظره هستند و معمولاً 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 به IP معروف 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 های IP با یک نام مشخص می شود که با وارد کردن آن در مرورگر می توان به سایت مورد نظر دسترسی پیدا کرد. مسلماً بدون این IP کامپیوتر 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 شماره IP آنها 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 ایمیل هایی با نام مقامات سیاسی و عنوان «احضاریه پلیس» و نامه ای 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.

# از ترفند عجیب ویندوز ۱۰ جا نمائید + آموزش



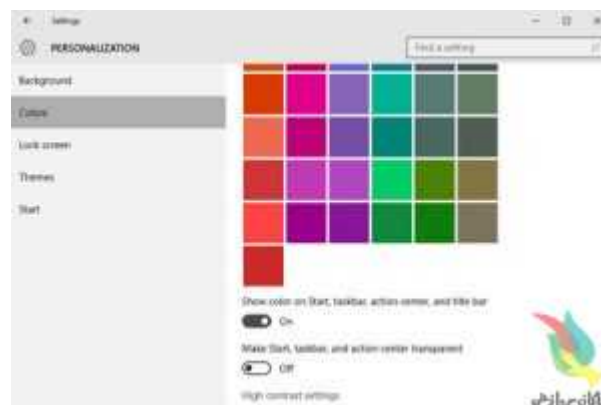
یکی از قابلیت‌های ویندوز ۱۰ امکان تغییر رنگ محیط ویندوز به رنگ‌های دلخواه کاربر است، اما اگر دوست داشته باشید رنگ Start Menu بدون توجه به رنگ بخش‌های دیگر همواره تیره باشد، می‌توانید با راه‌حلی که برای شما داریم این کار را انجام دهید.



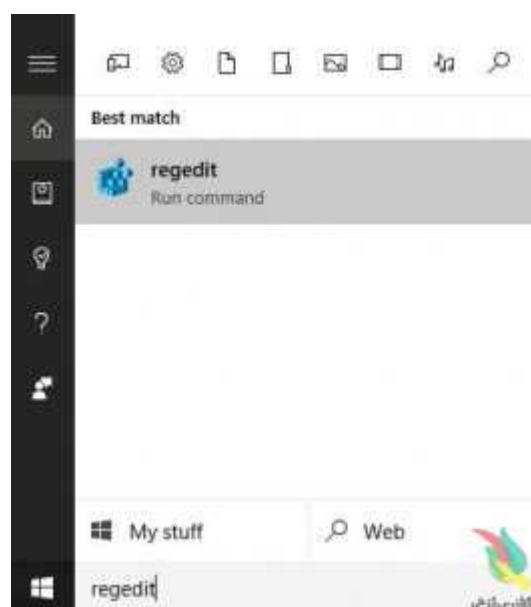
مایکروسافت نام تم‌های رنگی ویندوز را Accent گذاشته است تا رنگ قسمت‌های مختلف به انتخاب کاربر تغییر کند، اما اگر نخواهید این رنگ‌ها را در نوار وظیفه و استارت منو ببینید چه راهی وجود دارد؟ متأسفانه در این صورت نمی‌توانید از هیچ رنگی استفاده کنید، اما نگران نباشید زیرا با کمی دستکاری در رجیستری ویندوز ۱۰ می‌توانید از تم رنگی به همراه استارت منو تیره بهره ببرید.

برای بهره بردن از چنین روشی، مراحل زیر را به ترتیب انجام دهید:  
۱. بخش Settings را باز کنید و سپس وارد قسمت Personalization شوید. در پایین‌ترین قسمت از تب Colors، گزینه «Automatically pick an accent color from my background» را در حالت Off قرار

دهید .



۲. با تایپ «regedit» در نوار جستجو/کورتانا ، رجیستری ویندوز را اجرا کنید.



۳. پس از باز شدن رجیستری به مسیر

```
HKEY_CURRENT_USER>SOFTWARE>Microsoft>Windows>  
CurrentVersion>Explorer>Accent
```

بروید .



# 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 یست 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 تویتر 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

---

## آموزش غیر فعال کردن جلوه های تصویری در ویندوز ۱۰ (برای

# افزایش سرعت ویندوز)



ویندوز ۱۰ دارای جلوه های انیمیشنی است تا محیط کاربری زیباتری را برای کاربران ایجاد کند. اما این جلوه های گرافیکی و انیمیشنی ها ممکن است باعث ناراحتی بعضی کاربران حرفه ای شود که نیاز به سرعت عملکرد بالا در ویندوز دارند. چون این جلوه های تصویری بخشی از منابع سیستم را اشغال کرده و سرعت سیستم را کاهش میدهند.

در ادامه مطلب روش غیر فعال کردن جلوه های تصویری ویندوز ۱۰ را آموزش خواهیم داد.



ابتدا Settings ویندوز ۱۰ را از طریق منوی استارت باز کنید.

سپس قسمت Ease of Access را انتخاب کنید.

از بخش Other Options اهرم گزینه Play animations in Windows را به سمت چپ هدایت کنید تا وضعیت آن Off شود.

اکنون حالت انیمیشن برای کل ویندوز غیرفعال شده و تمامی پنجره ها و صفحه استارت به صورت ساده و بدون انیمیشن باز خواهد شد.

# معرفی پردازنده نسل هفتم اینتل K 7700



مشخصات پردازنده جدید اینتل از نسل هفتم خانواده Core با معماری ریز پردازنده Kaby Lake منتشر شد. پردازنده چهار هسته ای Intel Core i7-7700 که مشخصات آن در بنچمارک SiSoft SANDRA منتشر شده، به هشت رشته مجازی مجهز است و در مجموعه پردازنده های سوکت LGA1151 اینتل دسته بندی می شود. پس از فروکش کردن تب و تاب پردازنده های Skylake و مادربرد های مجهز به چیپ ست سری ۱۰۰ اینتل، اکنون زمان معرفی پردازنده جدید فرا رسیده تا کاربرانی که در سال ۲۰۱۶ قصد خریداری یک کامپیوتر شخصی قدرتمند را دارند، از پردازنده جدید اینتل استفاده کنند.



پردازنده چهار هسته ای Core i7-7700 با فرکانس پایه ۳.۶ گیگاهرتز فعالیت می کند که با استفاده از فناوری Turbo Boost به ۴.۲ گیگاهرتز افزایش خواهد یافت. در مقایسه با فرکانس پایه و توربو بوست در پردازنده Core i7-6700، افزایش ۲۰۰ مگاهرتز در هر دو

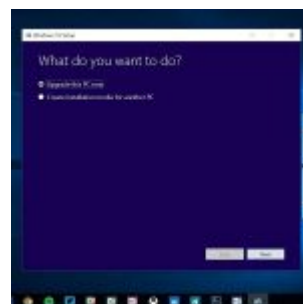
بخش مشاهده می شود. هشت مگابایت حافظه نهان سطح سوم (L3 Cache) و ۲۵۶ کیلوبایت حافظه نهان سطح دوم به ازای هر هسته (L2 Cache Per Core) برای افزایش قدرت پردازشی در نظر گرفته شده است.



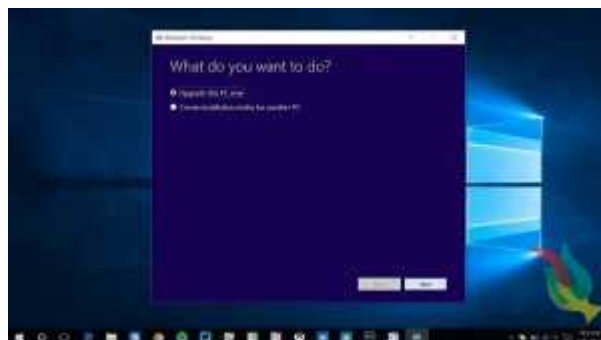
فناوری ساخت در معماری ریز پردازنده Kaby Lake از نوع ۱۴ نانومتری است و در مقایسه با پردازنده های Skylake، تلاش بیشتری برای بهینه سازی توان مصرفی صورت گرفته است. پردازنده Core i7-7700 با مادربرد های مجهز به چیپ ست سری ۱۰۰ اینتل که هم اکنون در بازار موجود هستند، سازگاری کامل دارد و مادربرد های مجهز به چیپ ست سری ۲۰۰ اینتل که در آینده نزدیک معرفی می شوند، سازگاری کامل با پردازنده Core i7-7700 را دارند.

منبع: رایان صبا

## مایکروسافت نصب ویندوز ۱۰ و حذف نرم افزارهای پیش فرض را آسان می کند



مایکروسافت در حال تست یک ابزار تازه برای نصب آسان تر ویندوز ۱۰ روی رایانه های رومیزی است. در شرایطی که نسخه جدید ویندوز امکان "reset" یک رایانه و بازگرداندن آن به تنظیمات اولیه را در اختیار کاربران قرار می دهد، ابزار جدید می تواند تمام نرم افزارهای اضافه ای که تولیدکننده کامپیوتر روی آن نصب کرده را حذف و یک نسخه تمیز از ویندوز ۱۰ را دوباره نصب نماید.



بیشترین کاربرد ابزار جدید برای رایانه های تازه خریداری شده است که شما می توانید با استفاده از آن از دست تمام نرم افزارهای پیش فرض کارخانه ای خلاص شوید.

این ابزار فعلاً تنها در اختیار کاربران عضو ویندوز اینسایدر قرار دارد، اما گمان می رود که فاصله زیادی تا عرضه عمومی آن نداشته باشیم. به طور قطع کاربران بسیاری از این امکان جدید استقبال می کنند، به خصوص که فاصله چندانی با عرضه آپدیت بزرگ سالیانه ویندوز ۱۰ در تابستان نداریم.

علاوه بر ابزار مذکور، مایکروسافت در حال ایجاد تغییراتی در ویندوز ۱۰ موبایل است؛ قابلیت Kids Corner به دلیل عدم استقبال کاربران حذف خواهد شد، اما در عوض ویژگی Apps Corner حفظ می گردد تا کاربران همچنان بتوانند پروفایل های محدود شده ای را برای دسترسی از پیش تعیین شده به برخی نرم افزارها ایجاد نمایند. لازم است اضافه نماییم که این شخصی سازی شامل «صفحه استارت» نیز خواهد شد.

منبع: رایان صبا

# 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 WPA، WEP 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 مستقیماً به منزل یا محل کار شما راهنمایی خواهد شد؛ در حالی که روح شما از اتفاقاتی که افتاده بی اطلاع است. فرضاً که تصمیم بگیرید روی شبکه رمز هم بگذارید؛ اما واقعاً 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 تقریباً 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 می‌توان WPA-PSK نامید که توسط آن می‌توان 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 الگوریتم های 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 تقریباً بدون نقطه ضعف بزرگ بوده و عمده نگرانی های پیرامون آن به امنیت بخش های تجاری مربوط می شود. متأسفانه بزرگ ترین نگرانی های 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 حفره های امنیتی در آن احساس می شود.

## کدام را انتخاب کنیم؟

حالا که با اسامی مختلف این روش های 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 روش های رمزگذاری را بر حسب میزان نفوذناپذیری آنها به این صورت در نظر گرفت: قوی ترین و امن ترین حالت در شبکه های 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 روش ها باید یک نکته را در نظر داشت و آن، پشتیبانی تجهیزات شبکه شما از روش های مختلف رمزگذاری است. برای مثال اگر از یک مودم قدیمی استفاده می کنید ممکن است شرایط به کار گرفتن روش های 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 مودم ها استفاده می کنید حتماً به روزرسانی های امنیتی آن را در وب سایت تولید کننده دنبال کنید و همچنین پیش از خرید یک مودم جدید مطمئن شوید دستگاهی که انتخاب می کنید قابلیت به کار گیری روش های رمزگذاری جدید را دارد.

منبع: سخت افزار مگ