نکات استفاده از شبکه های Wi-Fi عمومی:

امروزه استفاده از Wi-Fi hotspotها در هتل‌ها، کتابخانه‌ها، فرودگاه‌ها، دانشگاه‌ها، و سایر مکان‌های عمومی رواج یافته است اما نکته حائز اهمیت ناامن بودن این hotspotها در اغلب موارد است. هنگام استفاده از hotspot به خاطر داشته باشید که اطلاعات خود را فقط برای سایت‌هایی که کاملاً رمزگذاری شده‌اند ارسال نمایید.

شما فقط زمانی می‌توانید از ایمن بودن hotspot مطمئن شوید که این hotspot زمان ورود به شبکه از شما درخواست یک کلمه عبور WPA نماید. اگر به hotspotای اطمینان ندارید، با آن شبکه مانند یک شبکه ناامن رفتار کنید.

موضوعاتی که در این مقاله به آنها خواهیم پرداخت عبارتند از:

- چگونگی عملکرد رمزگذاری
- مشخصات یک سایت رمز شده
- عدم ایمنی بیشتر hotspotها
- چگونگی محافظت از اطلاعات هنگام استفاده از شبکه Wi-Fi عمومی

چگونگی عملکرد رمزگذاری:

رمزگذاری، عامل حفظِ اطلاعات افراد به صورت ایمن است. رمزگذاری عاملی برای جلوگیری از دسترسی افراد ثالث به اطلاعات در هنگام ارسال آن در اینترنت است. برای ارسال اطلاعات شخصی هنگام استفاده از شبکه‌های بی‌سیم، باید مراقب بود. بهترین کار ارسال اطلاعات به صورت رمز شده است. اگر امکان این کار میسر نیست، اطلاعات

شخصی خود را زمانی ارسال کنید که از یک وب سایت رمزگذاری شده استفاده می‌کنید و یا در حال استفاده از یک شبکه Wi-Fi امن هستید. لازم به ذکر است که اگر وب سایت رمزگذاری شده باشد، فقط اطلاعاتی که به آن سایت ارسال می‌شود و یا از آن سایت دریافت می‌شود محافظت خواهد شد، اما یک شبکه بی‌سیم امن تمام اطلاعاتی را که شما از طریق آن شبکه ارسال می‌کنید رمز خواهد کرد.

مشخصات یک سایت رمز شده:

به خاطر داشته باشید که هنگام ارسال ایمیل، به اشتراک گذاری عکس و فیلم، استفاده از شبکه‌های اجتماعی یا خدمات بانکداری الکترونیک، شما در حال ارسال اطلاعات شخصی خود هستید. سایت‌هایی مانند سایت‌های خدمات بانکداری الکترونیک برای محافظت از اطلاعاتی که کاربر از کامپیوتر خود به سرور وب‌سایت آنها ارسال می‌کند از رمزگذاری استفاده می‌کنند.

مشخصه یک وب‌سایت رمز شده وجود https در اولِ آدرس آن سایت است (البته لازم به ذکر است که لزوماً وجود https کافی نبوده و باید مواظب حملات فیشینگ هم بود). برخی وب سایت‌ها فقط روی صفحات sign-in خود از رمزگذاری استفاده می‌کنند و ممکن است بخشی از نشست شما را رمزگذاری نکنند؛ این عدم رمزگذاری می‌تواند منجر به آسیب‌پذیر بودن کل حساب شما شود.

عدم ایمنی بیشتر hotspotها:

بیشتر hotspotها اطلاعاتی را که از طریق اینترنت ارسال می‌کنند رمز نمی‌کنند و بنابراین امن نیستند.

اگر از یک شبکه ناامن برای ورود به سایتی رمزگذاری نشده استفاده می‌کنید –یا از سایتی استفاده می‌کنید که از رمزگذاری فقط برای صفحه sign-in خود بهره می‌برد- دیگر کاربران شبکه می‌توانند آنچه شما می‌بینید و آنچه شما ارسال می‌کنید را ببینند. آنها می‌توانند نشست شما را ارتباط ربایی کنند و از طرف شما وارد سایت شوند. ابزارهای جدید ارتباط ربایی این کار را ساده‌تر کرده‌اند و متاسفانه کاربرانی با دانش فنی کم هم قادر به این کار خواهند بود. بنابراین مهاجم می‌تواند از حساب کاربری شما برای جعل هویت استفاده کند.

چگونگی محافظت از اطلاعات هنگام استفاده از شبکه Wi-Fi عمومی:

چه کارهایی می‌توان برای محافظت از اطلاعات خود انجام داد؟ در ادامه به برخی از این کارها اشاره می‌کنیم:

- هنگامی که از Wi-Fi hotspot استفاده می‌کنید فقط به وب‌سایت‌هایی وارد شوید و اطلاعات شخصی خود را فقط برای وب‌سایت‌هایی ارسال کنید که می‌دانید کاملاً رمزگذاری شده‌اند. برای حفظِ ایمنی، تمام بازدیدهایی که از هر سایتی دارید باید از زمان ورود به سایت تا زمان خروج از آن رمزگذاری شده باشد. اگر هنگام ورود به سایتی تصور کردید به سایتی رمزگذاری شده و امن وارد شده‌اید، اما بعد از مدتی خود را در صفحه‌ای که رمزگذاری نشده است یافتید، به سرعت از آن سایت خارج شوید.

- پس از ورود به حساب کاربری خود، برای مدتی طولانی در آن حساب نمانید. هر زمان که کارتان با حساب کاربری تمام شد از آن حساب خارج شوید.

- از یک کلمه عبور یکسان در چندین وب سایت استفاده نکنید. در غیراینصورت ممکن است با لو رفتن کلمه عبور، مهاجم امکان دسترسی به چند حساب کاربری شما را پیدا کند.

- بسیاری از مرورگرها، هنگام بازدید از وب سایت‌های کلاه‌برداری یا دانلود برنامه‌های مخرب به کاربران هشدار می‌دهند. به این هشدارها توجه کنید و مرورگر و نرم‌افزارهای امنیتی خود را به‌روز نگه دارید.

- اگر مرتب حساب‌های کاربری آنلاین خود را از طریق Wi-Fi hotspotها چک می‌کنید، از VPN قانونی استفاده کنید. VPNها ترافیک میان رایانه شما و اینترنت را حتی روی شبکه‌های ناامن رمز می‌کنند.

- برخی شبکه‌های Wi-Fi از رمزگذاری استفاده می‌کنند. WEP و WPA بیشترین پروتکل‌های رمزگذاری برای شبکه‌های Wi-Fi هستند. رمزگذاری WPA از اطلاعات شما در برابر برنامه‌های هکِ معمول محافظت می‌کند، اما WEP ممکن است این کار را انجام ندهد. همچنین WPA2 نسبت به WPA قوی‌تر است. اگر از شبکه Wi-Fi استفاده می‌کنید و مطمئن نیستید که این شبکه از WPA استفاده می‌کند، احتیاط کنید!

منبع: مرکز ماهر

لینک مطلب در وبلاگ صفر و یک امن: http://www.01amn.rozblog.com/post/80