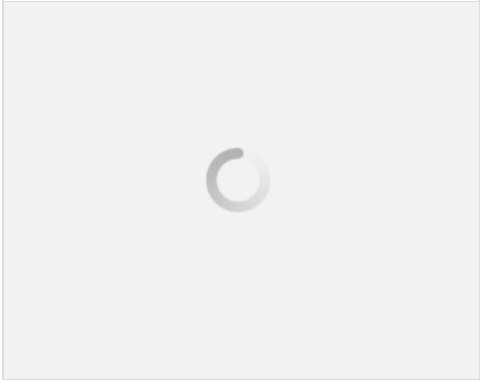
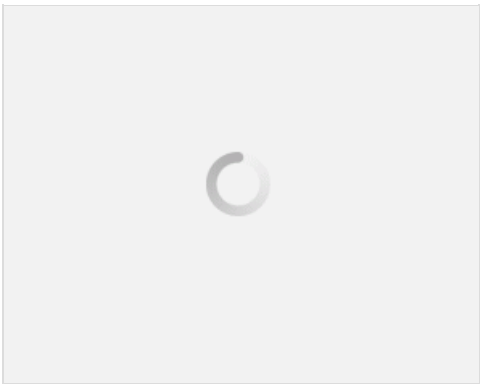
معرفی خطرات امنیتی وایرلس و ۳ راهکار مقابله با خطرات WiFi عمومی (نسخه PDF)

معرفی خطرات امنیتی وایرلس و ۳ راهکار مقابله با خطرات WiFi عمومی (نسخه چاپی)

وقتی به یک شـبکه عمومی WiFi متصـل می شویم ، چگونه از خطرات امنیتی دوری کنیم؟ بسـیاری از مردم مهمترین فعالیت های روزمره خود را در اینترنت دارنـد که بسـیار هم مفیـد است.در برخی موارد برای رفتن به اینترنت نیـاز به دسترسـی های مربوطه دارنـد تا بتوانند فعالیت خود را اسـتمرار بخشند. وقتی درباره ارتباطات و دسترسی های اینترنت صحبت می کنیم تکنولوژی WiFi به طور حتم یک برکت یا نعمت است. همین نعمت یک اتصال WiFi در خانه خودمان است.



زمانی که بخواهیم یک چیز متفاوت و کامل بگوییم،وقتی می شود که شـما به یک شبکه WiFi در حیطه یک گروه کاری یا مکانهای عمومی دیگر متصل شوید.وقتی شما به یک شبکه WiFi عمومی یا ناامن متصل می شوید،به سرویس ها و تهدیدات جدی امنیتی آسیب پذیر شده اید. به سـبب این امر دزدان اینترنتی به اطلاعات شخصـی و پسوردهای امنیتی شـما دسترسی کامل خواهند داشت که باعث رنجش شما خواهد شد.بسیاری ضروریست که شما قبل از اتصال به شبکه WiFi عمومی از خطرات آن مطلع شوید.در اینجا راه حل هایی برای مقابله با این خطرات به شما ارائه خواهد شد.



چرا این اتفاق می افتد؟

دلیل آن پیچیده است.یکی از دلایل آن ناشـی از امواج رادیو و تلویزیون است.وقتی شـما به یک شبکه WiFi متصل می شوید، سیگنالها به همراه امواج رادیو و تلویزون در جهات مختلف انتقال پیدا می کنند. هر دسـتگاه رادیویی می تواند این سـیگنال ها را در یافت کند.تفاوت بین یک شـبکه خانگی دارای امنیت و یک شـبکه ناامن عمومی در رمزگذاری آن است.شبکه خانگی امن اطلاعات خود را بصورت رمزنگاری شده ارسال و دریافت می کند. از همین رو نمی توان اطلاعات خواندنی آنرا شـنود کرد ولی در شـبکه های عمومی ناامن و آسـیب پذیر به راحتی می توان اطلاعات را مشاهده کرد چون هیچ کدام از این اطلاعات رمز نگاری نشده اند.

استفاده از فرآیند Tunneling

اولین متـد در این بحث فرآینـد تونل کردن است. این مکانیزم براساس یک پروتکل پوسـته یا حفره امن عمل می کند که در این خصوص بهتر است درباره پروتکل SSH بیشتر بـدانیم.اطلاعات برای بسـته ها در محیط شـبکه ارسال می شوند.تونل کردن زمانی اجرا می شود که داده ها و اطلاعات ارسالی شـما از یک شـبکه بخصوص و ویژه به یک شبکه متفاوت از یک پروتکل متفاوت ارسال و دریافت می شوند. در این مکانیزم بسته ها در قالب سیستم رمز نگاری SSH آماده ارسال شده و به سرورهای SSH ارسال می شوند.

VPN : Virtual Private Network

یک راه دیگر برای امن کردن یک شبکه WiFi عمومی استفاده از یک شبکه خصوصی مجازی یا به اصطلاح VPN است. ساختار VPN از یک ارتباط امن بین دو سـرور تشکیل شده است.اگر ارتباط شما عمومی است اصلا مهم نیست.این ارتباط از یک مکانیزم و تکنولوژی رمز نگاری شـده ساخته شـده. این در حالی است که تمامی داده ها یا اطلاعاتی را که ارسال می کنیـد بصورت رمز نگاری در می آینـد و امن خواهند ماند.شـما می توانید از یک سرویس رایگان VPN به سادگی و بصورت آنلاین اسـتفاده کنیـد.بیشتر نقاط معتبر دنیا از سـرویس های امن VPN استفاده می کنند.حداقل اینکه پاکستان هم از این سیستم استفاده می کند!

HTTPS : Hypertext Transfer Protocol Secure

روش دیگری برای امن کردن همه اطلاعـات حساس در یک شـبکه WiFi عمومی آنلاین، اسـتفاده از پروتکل HTTPS است. این سیستم از ارسال رمز های شـما بصورت ساده اجتناب می کند مگر اینکه بوسـیله HTTPS رمز نگاری شده باشد .این سیسـتم فقط برای رمز های شما نیست بلکه کلیه اطلاعات حساس شـما را نیز در بر میگیرد.شـما در عنوان سایت های مشهور می توانید ببینید، تمامی آنها بصورت امن از گذرگاه HTTPS عبور می کنند.می تواند در قسمت URL مرورگر، قبل از نام سایت واژه HTTPS را مشاهده کنید. مسلما این روش خطرات موجود را کاهش می دهد.البته این را مد نظر قرار دهید که شـما با سیستم HTTPS هم نمیتوانید امنیت کامل را برقرار سازید.بنابراین راه های زیادی در امن کردن تبادل اطلاعات در یک محیط شبکه WiFi عمومی وجود دارد.انتظار می رود برای حفظ اطلاعات شخصی و امنیت

تمامی فایل های خود از مکانیزم های ارائه شده استفاده نمائید.

نویسنده : علی گلستانی فر

منبع : انجمن تخصصی فناوری اطلاعات ایران

مطلب اصلی