ترفند ویندوز

شبکه بی‌سیم بدون روتر در ویندوز

وقتی لپ‌تاپ به دست، با یکی از دوستان لپ‌تاپ به دستتان ملاقات می‌کنید و قصد دارید چند فایل با هم رو بدل کنید، چه راه‌هایی در اختیار دارید؟

۱. استفاده از شبکه سیمی. البته معمولا کم‌تر کسی کابل شبکه با خود حمل می‌کند.

۲. استفاده از بلوتوث. بلوتوث کند است و برای جابه‌جا کردن فایل‌های حجیم نامناسب است.

۳. استفاده از فلش مموری. اگر فلش مموری در اختیار داشته باشید، باید زمان دوبار کپی شدن فایل‌ها را تحمل کنید.

۴. استفاده از شبکه بی‌سیم

شبکه‌های بی‌سیم کارایی‌زیادی دارند. بیشتر کاربران گمان می‌کنند که برای اتصال به شبکه، باید حتما یک روتر موجود باشد، در حالی که لزوما این طور نیست. دو رایانه یا تلفن همراه، بی‌آن‌که یک روتر در اختیار داشته باشند، می‌توانند با یکدیگر یک شبکه بی‌سیم تشکیل بدهند. این شبکه Wireless Ad Hoc Network نامیده می‌شود. شبکه Ad Hoc متشکل از حداقل دو یا چندین دستگاه مجهز به واسط ارتباط بی‌سیم یا Wi-Fi است. سرعت انتقال در این شبکه بسته به این موضوع که رایانه‌ها به کدام‌یک از نسل‌های B،G و یا N مجهز هستند، متفاوت است اما در هر صورت، حداقل سرعت این شبکه‌ها در نسل B ۱۱ مگابیت برثانیه است که به مراتب سریع‌تر از یک اتصال بلوتوث یا استفاده از فلش مموری عمل می‌کند. با وارد کردن عبارت Ad Hoc در منوی استارت در ویندوز ۷، می‌توانید یکی از این نوع شبکه‌ها ایجاد کنید. با استفاده از این شبکه‌ها به سادگی می‌توان بازی‌های گروهی را در یک شبکه محلی اجرا کرد. دقت داشته باشید که اتصال به این شبکه‌ها باعث قطع شدن از شبکه‌های بی‌سیم دیگر که در حیطه رایانه شما قرار دارد، خواهد شد. افزایش تعداد اعضای شبکه‌های Ad Hoc می‌تواند باعث گسترش رنج دسترسی دستگاه‌های بی‌سیم شود. به این معنا که دو دستگاه که لزوما نسبت به یکدیگر فاصله مناسبی ندارند و ارتباط معمول بی‌سیم در آن‌ها ممکن نیست، با واسطه قراردادن دستگاه دیگری که به دو دستگاه نزدیک است، می‌توانند با یکدیگر ارتباط برقرار کنند اما این کار باعث افت پهنای باند شبکه و افزایش تاخیر می‌شود.

مواظب باشید صید نشوید

فیشرها همچنان قربانی می‌گیرند

حمله فیشری، از روش‌هایی است که طی ۳ سال گذشته عمومیت یافته است. به همین دلیل سازندگان مرورگرها محصولات رایانه‌ای خود را طوری ارتقا دادند که این حملات کمتر آسیب‌رسان باشد. به تازگی موج جدیدی از حملات فیشری آغاز شده است و البته انبوه کاربران اندروید و iOS نیز در بالا بردن سهم موفقیت حمله کنندگان، موثر بوده‌اند. یک فیشر، سایتی است که با ظاهری تقلبی، خود را چیزی به غیر از آنی که هست، معرفی کرده و کاربر را ترغیب به وارد کردن اطلاعات می‌کند. به عنوان مثال، فیشر می‌تواند شبیه به سایت بانک، Gmail و یا فیسبوک باشد و کاربر نیز به عادت همیشه، اطلاعات خود را در فیلدهای موجود وارد می‌کند. در روش‌های قدیمی فیشینگ، کاربر با کلیک کردن روی یک لینک خطرناک، به سایتی با ظاهر مشابه هدایت می‌شد، در حالی که لینکی که کاربر روی آن کلیک می‌کرد با مقصد هم‌خوانی نداشت. اکنون بیشتر مرورگرهای امروزی حتی نسخه‌های همراه و تبلتی در مقابل این نوع فیشرها مقاوم‌اند و اخطارهای مناسبی در این شرایط نمایش می‌دهند. همین موضوع باعث شده است که روش‌های جدیدی برای فیشینگ ایجاد شود که با روش‌های قبلی متفاوت است. جدیدترین این روش‌ها که تا به امروز قربانیان زیادی نیز داشته است، استفاده از ضمیمه کردن کدهای HTML درنامه‌های الکترونیکی است. یک ایمیل حاوی اطلاعات متنی و ضمایم است. در صورتی که اطلاعات متنی شامل کدهای HTML باشد، این کدها نمایش داده نمی‌شود، بلکه نتیجه اجرای آن‌ها نمایش داده می‌شود تا ایمیل‌ها بتوانند زیباتر باشند. کدهای HTML موجود در ایمیل نیز می‌توانند مانند HTML سایت‌ها، دکمه و لینک تولید کنند و نتیجه را به کاربر نشان دهد. این چنین اطلاعاتی خطرناک نیست، چون مرورگرها و نرم‌افزارهایی مانند Outlook برای مقابله با اعمال خطرناک کدهای HTML دوراندیشی‌های لازم را کرده‌اند. از همین رو سارقان اطلاعات به جای وارد کردن کدهای HTML در متن اصلی ایمیل، کدهای مخرب را ضمیمه می‌کنند. هیچ مرورگری به اجرا شدن کدهای HTML در فضای محلی مانند هارددیسک، ایرادی وارد نمی‌کند و هیچ خطایی نیز نمایش داده نمی‌شود. این کدهای ضمیمه بسیار بی‌خطر اجرا می‌شوند و حاوی هیچ اسکریپتی نیز نیستند. تنها ایراد این کدها این است که سایتی مشابه به سایتی مشهور ایجاد می‌کنند. در صورتی که کاربر اطلاعات کاربری سایت اصلی را در این صفحه فیشر وارد کند، کد PHP داخل یک سرور اجرا می‌شود و اطلاعات را سرقت می‌کند. سپس کاربر به سایت اصلی هدایت می‌شود و اطلاعات کاربری او به سایت اصلی ارسال می‌شود و از منظر یک کاربر معمولی، هیچ اتفاق عجیبی رخ نمی‌دهد و در این شرایط حتی کاربر متوجه سرقت شدن اطلاعات شخصی خود نمی‌شود. بدیهی است که سارق در هر لحظه به اطلاعات سرقت شده سر نمی‌زند و از همین رو کاربر نباید به سرقت شدن اطلاعات خود پی‌برد تا سارق زمان کافی را برای سرقت منابع مالی و یا اطلاعات ارزشمند، به دست آورد.

یکی از روش‌های تازه مرسوم شده در گوشی‌های هوشمند تلفن همراه، استفاده از پیامک‌های فیشر است. این پیامک‌ها حاوی یک لینک اینترنتی است و کلیک روی آن‌ها، مستقیم می‌تواند کاربر را به سایتی شبیه به یکی از سایت‌های مشهور ببرد و اطلاعات کاربر را سرقت کند، در حالی که گوشی‌های هوشمند هیچ ابزاری برای شناسایی لینک‌های فیشری در متن یک پیامک ندارند.

در صورتی که فرستنده یک ایمیل یا پیامک را نمی‌شناسید و یا دلیل ارسال یک فایل HTML را به عنوان یک ضمیمه نمی‌دانید، از مراجعه به لینک و یا باز کردن ضمیمه خودداری کنید. به طور کلی سایت‌های رسمی مانند بانک‌ها و یا سرویس‌دهندگان پست الکترونیک و یا شبکه‌های اجتماعی، هیچ‌گاه هیچ فایلی ضمیمه ایمیل‌های ارسالی خود نمی‌کنند، پس اگر ایمیلی به همراه یک ضمیمه دریافت کردید که به ظاهر از طرف این گونه سایت‌ها ارسال شده بود، در جعلی بودن ایمیل شک نکنید. این نوع ایمیل‌ها مانند اسپم‌ها ارسال می‌شوند و هر کسی می‌تواند یکی از گیرندگان آن‌ها باشد، پس خود را از این گونه خطرات در امان ندانید و همیشه نکات امنیتی را رعایت کنید.

برای مقابله با این نوع سرقت‌ها، قبل از وارد کردن اطلاعات شخصی خود، ابتدا از صحیح بودن حرف به حرف آدرس سایت اطمینان حاصل کنید و سپس اطلاعات شخصی خود را وارد کنید.