۶ روش دزدیدن رمزعبور توسط هکرها

دی 19, 1395

آیا از امنیت رمزعبورهایمان مطمئن هستیم؟

هکرها می‌توانند دقیقه‌ها، ساعتها و حتی روزها وقت بگذارند تا رمزعبورها را بدزدند. این می‌تواند شغل آنها باشد، پس برایش وقت دارند. هکرها صدها روش برای بدست آوردن اطلاعاتی که لازم دارند را امتحان می‌کنند. آنها سخت‌کوش هستند.

دوباره فکر کنید! آیا رمزعبور های شما در امان هستند؟ عده‌ای فکر می‌کنند حتما باید یک هدف بزرگ و مهم برای **هکرها** باشند تا هک شوند. و یا عده‌ای نمی‌دانند که دزدیدن اطلاعات و رمزعبورها برای هکرها در برخی موارد چقدر می‌تواند ساده باشد. در ادامه مطلب به ۶ روشی که هکرها برای **دزدیدن رمزعبور** استفاده می‌کنند، اشاره می‌کنیم.

۱- مانیتور ترافیک شبکه Wi-Fi :

آیا در محیطهای عمومی مانند فرودگاه‌ها، کافی‌شاپ‌ها، سینماها و غیره به شبکه Wi-Fi باز وصل شده و وارد یکی از حساب‌های آنلایتان شده‌اید؟ اگر جواب شما بله است، احتمال دارد رمزعبور یا رمزعبورهای شما دزدیده شده باشد. یکی از ساده‌ترین راه‌های مانیتور ترافیک شبکه، استفاده از نرافزارهای مانیتورینگ شبکه Wi-Fi است که می‌توانید آنها را در اینترنت پیدا کرده و حتی رایگان دانلود کنید. هکرها از این ابزارها استفاده می‌کنند و با مانیتور شبکه می‌توانند ببینند شما از کدام سایت بازدید کرده‌اید، و نام کاربری و رمزعبورتان چه بوده است. در اینصورت باید امیدوار باشیم که این رمزعبور به سرقت رفته فقط برای یکی از حساب‌های آنلاین بوده است، در غیر اینصورت هکر به حساب‌های دیگر هم دسترسی پیدا می‌کند.

هرگز بدون وصل شدن به VPN مطمئن، به شبکه Wi-Fi اماکن عمومی وصل نشوید. فراموش نکنید کار با ابزارهای مانیتورینگ شبکه و سرقت بسته‌های شبکه کار سخت و پیچیده‌ای نیست. اگر مجبور به استفاده از شبکه Wi-Fi عمومی شدید، حتما از VPN استفاده کنید. با وصل شدن به VPN ، اطلاعات در یک تونل رمزگذاری شده به مقصد فرستاده و دریافت

می‌شود، و اگر هکری در حال ترافیک شبکه باشد، نمی‌تواند بسته‌های اطلاعاتی را بخواند .

۲– حمله فیشینگ :

حملات فیشینگ روز به روز متنوع‌تر و پیچیده‌تر میشوند. ایمیلی دریافت می‌کنید با این محتوا که برای تکمیل خریدتان روی این لینک کلیک کنید، سپس وارد سایتی می‌شوید که دقیقا مشابه سایت مورد انتظار شماست و اطلاعات ورود حساب یا اطلاعات بانکی خود را وارد می‌کنید. و تمام شد، هکرها اطلاعات شما را بدست آوردند.

حملات فیشینگ را شناسایی و با آنها مقابله کنید. هرگز روی لینک‌های ایمیل‌هایی که ادعا می‌کنند از طرف سرویس آنلاین، بانک، موسسه خیریه و … کلیک نکنید. مرورگر خود را باز کنید و مستقیم وارد وب‌سایت مد نظرتان شوید. حتی اگر لازم است با پشتیبانی بانک، موسسه، سازمان تماس بگیرید تا مطمئن شوید. قبل از کلیک، آدرس لینک‌های مقصد را به دقت چک کنید، حرف به حرف.

۳– استفاده از کی‌لاگر

هکرها می‌توانند بدون اطلاع شما روی دستگاهتان کی‌لاگر نصب کنند. برای مثال یک هکر می‌تواند با روش فیشینگ برای شما ایمیلی ارسال کند، به محض اینکه ضمیمه ایمیل را باز کنید و یا روی لینک آن ایمیل کلیک کنید، یک فایل جاوا اسکریپت روی مرورگر شما دانلود و نصب می‌شود. بدون اینکه متوجه شوید، هر چیزی که در مرورگر تایپ کنید از جمله آدرس وب‌سایت، نام کاربری، رمزعبور و غیره برای هکر فرستاده می‌شود.

هرگز ضمیمه ایمیلی که از فرستنده آن اطمینان کامل ندارید را باز نکنید و روی لینک‌های ایمیلها کلیک نکنید. اضافه میکنیم که برای اینکه هکر روی دستگاه کی‌لاگر نصب کند، حتما برای شما ایمیل نمی‌فرستد. یک هکر می‌تواند وب‌سایتی را آلوده کند. به این معنی که هر کاربری از این وب‌سایت بازدید کرد روی دستگاهش کی‌لاگر دانلود شود. به همین دلیل است که ما همیشه توصیه می‌کنیم هر وب‌سایتی را بازدید نکنید، هر نرم‌افزاری را دانلود ونصب نکنید و جاوا اسکریپت مرورگر خود را غیرفعال کنید.

۴– حمله بروت فورس Brut Force –

رمزعبور 123456 رایج‌ترین رمزعبور روی این کره خاکی است. و متاسفانه بیشتر رمزعبورها ساده و قابل حدس هستند که با چند بار سعی کردن، می‌توان آنها را بدست آورد. هکرها از ابزارهایی برای بروت فورس کردن استفاده می‌کنند، که در عرض چند ثانیه، چندین هزار رمزعبور تست می‌شود تا بالاخره رمزعبور اصلی پیدا شود. این ابزارها را می‌توان رایگان از اینترنت نیز دانلود کرد. هر چقدر رمز عبور ساده و کوتاه باشد، این ابزارها آن را سریعتر پیدا می‌کنند.

رمزعبورهای طولانی، پیچیده، قدرتمند و منحصر بفرد بسازید. هرگز این رمزعبورها را روی یک فایل در کامپیوترتان ذخیره نکنید. برای اینکه به یاد سپاری آنها ساده باشد از نرم‌افزارهای مدیریت رمز عبور Last Pass و KeePass استفاده کنید.

۵- از طریق مشاهده

مشاهده کردن و زیر نظر گرفتن محیط و اطرافیان یکی دیگر از روش‌های هکرها برای بدست آوردن اطلاعات است. هکر می‌توانند به آرامی و زیرکی لپ‌تاپ یا موبایل شما را زیر نظر داشته باشند و اگر شما در این حین، وارد یکی از حساب‌های کاربری آنلاینتان شوید، آنها نام کاربری و رمزعبورتان را می‌بینند. عده‌ای عادت دارند رمزعبور سیستم یا ایمیل خود را روی کاغذی نوشته و روی میزکارشان بچسبانند، و هکرها فقط با نگاه کردن به میز کار یا میز شخصی بقیه، می‌توانند اطلاعات زیادی بدست آورند.

هنگام وارد شدن به حساب‌های کاربری و وارد کردن رمزعبور، دقت کنید که کسی شما را زیر نظر نداشته باشد. هرگز اطلاعات مهم و حساستان را جلوی دید یا روی میز کار قرار ندهید.

۶- مهندسی اجتماعی

یکی از راحتترین راه‌ها برای بدست آوردن اطلاعات از جمله رمزعبور، مهندسی اجتماعی است. این روش بر اساس جلب اعتماد قربانی است. و متاسفانه منابع انسانی آسیب‌پذیرترین جز یک سیستم هستند. مهندسین اجتماعی با جلب اعتماد قربانی، رمزعبور را از خود فرد می‌گیرند. شاید مسخره به نظر برسد اما اتفاق می‌افتد.

اعتماد از جهاتی مانند امنیت است. امنیت هرگز ۱۰۰ درصد نیست، به همین ترتیب اعتماد کردن هم ۱۰۰ درصد نباید باشد. اگر شخصی از ما اطلاعات خواست، باید از خودمان بپرسیم چرا باید این اطلاعات را به

این فرد بدهم؟ آیا او را کامل می‌شناسم؟ آیا او را از نزدیک دیده‌ام؟ آیا همه چیز عادی به نظر می‌رسد؟

با یک ابزار مدیریت رمزعبور، هوشیار بودن نسبت به اتفاق‌های پیرامون، به روز کردن مرورگر و سایر نرم‌افزارها، استفاده از VPN مطمئن، ترک عادت کلیک کردن روی هر لینک و باز کردن هر ضمیمه و دانلود هر نرم‌افزاری میتوان تا حدی مطمئن شد که امنیت رمزعبورهایمان را حفظ کرده‌ایم.