امنیت در برابر باج افزارها

گاهی از طریق ایمیل‌های اسپم و .....کاربران برای کلیک کردن بر روی لینک‌های مخرب فریب داده می‌شوند، سپس باج افزار، سیستم‌های رایانه‌ای و دستگاه‌های یا فایل‌های آن‌ها را غیر قابل دسترس می‌سازد و در واقع آن‌هاراگروگان می‌گیرد تا قربانی باج مربوطه را پرداخت نماید.

قربانیان دو حق انتخاب خواهند داشت: پرداخت کردن مبلغ باج و یا از دست دادن تمام اطلاعات با ارزش خود برای همیشه. متأسفانه این روش برای مجرمان سایبری به خوبی کار می‌کند زیرا کاربران خانگی و کاربران شرکت‌های تجاری مختلف تدابیر لازم در رابطه با داده‌های خود را به کار نبسته‌اند و چاره‌ای جز پرداخت وجه مورد نظر ندارند و تقریباً ۵۰ درصد قربانیان به این کار دست می‌زنند.

برای اینکه باجی به هکرها ندهیم چه باید بکنیم؟

۱. تهیه فایل پشتیبان از اطلاعات خود: یک راه آسان و مقرون به صرفه برای حفاظت از اطلاعات شما استفاده از هارد دیسک‌های اکسترنال است که روز به روز از قیمت شان کاسته و بر ظرفیتشان افزوده می‌شود، تهیه نسخه پشتیبان بهترین تاکتیک عملی توسط شماست که می‌تواند برای محافظت شما در برابر باج افزاری به خوبی عمل کند.

۲. تنظیم یک برنامه برای بک‌آپ گیری: توصیه محققان به پشتیبان گیری از داده‌های خود حداقل هفته‌ای یک‌بار و به طور ایده‌آل، روزی یک‌بار است.

۳. نسبت به ایمیل‌های فیشینگ آگاهی داشته باشید: کارمندان باید نسبت به آخرین تاکتیک‌های مهندسی اجتماعی که برای فریب مردم به منظور کلیک بر روی لینک‌ها و پیوست‌های مخرب استفاده می‌شوند، هوشیاری کامل داشته باشند.
۴. به روز رسانی نرم افزارها: اگر شما برنامه‌های کاربردی خود را به روز نگه دارید، در معرض حملات احتمالی قرار گرفتن را به حداقل خواهید رساند.

۵. اطلاعات شخصی و اطلاعات کاری خود را از هم جدا سازید: در دنیای امروزی جدا کردن مرز کار از

زندگی شخصی سخت است اما جدا نگه داشتن این دو دنیا در محافظت از داده‌ها و به حداقل رساندن تأثیر یک حمله نقش بسزایی خواهد داشت.