بالابردن امنیت آنلاین کارت های بانکی در هنگام خرید اینترنتی

امروزه فاصله بین دنیای مجازی و واقعی هر روز درحال کم شدن است، بسیاری از اموری که در دنیای واقعی درحال انجام شدن است در دنیای مجازی یک معادل پیدا کرده است. یکی از این امور که در دنیای حقیقی انجام می شود تبادلات مالی بین انسانها است که در طول روز انجام می شود و در این چند سال اخیر جای زیادی را در دنیای مجازی باز کرده است.

در این میان روشهای زیادی برای خرید از اینترنت وجود دارد یکی از این روش ها خرید از طریق کارت های عابربانک است. خرید از طریق عابربانک مزایای زیادی دارد ولی در کنار این مزایا خطراتی را نیز برای کاربرانی که آگاهی کافی از موارد امنیتی در رابطه با این موضوع ندارند ایجاد می کند.یکی از خطرات جدی در خرید و فروش آنلاین، لو رفتن شماره کارت های اعتباری و رمز عبور آنها است که سالانه میلیونها دلار خسارت به بانکها و دارندگان کارت ها وارد می آورد.

تشخیص سایت های جعلی

یکی از روش های متداول سرقت اطلاعات تقلید از وب‌سایت‌های معتبر و فریب خریداران است. درحقیقت کلاهبرداران اینترنتی اطلاعات حساب کاربران را از طریق ایجاد وب‌سایت‌هایی به ظاهر حرفه‌ای که از شرکت های قانونی تقلید کرده‌اند، به سرقت می برند. واضح است که هوشیاری کاربران می تواند از بروز این مشکل جلوگیری کند.
خریداران باید از طریق تایپ آدرس وب سایتی که می خواهند از آن خرید کنند به سایت وارد شوند و از وارد کردن اطلاعات کارت اعتباری خود در صفحاتی که از طریق لینک های مشکوک به آنها وارد شده اند، خودداری کنند.

قابلیت اعتماد طرفین

در معاملات آنلاین، فروشندگان باید به مشتریان خود انتخاب‌های مطمئن و راحتی را برای نحوه پرداخت ارایه دهند، به طوری که بهترین نتیجه را برای مشتری و واحد تجاری در بر داشته باشد. از جمله روشهای متداول پرداخت می توان به پرداخت وجه به صورت آنلاین اشاره کرد.
یکی دیگر از مواردی که منجر به سرقت اطلاعات کارت های اعتباری می شود، مربوط به عدم رعایت نکات ایمنی توسط فروشندگان است.
زمانی که تراکنش معامله به صورت باز و بدون امنیت و رمزگذاری مناسب به اینترنت ارسال می شود، هکر ها می توانند با استراق سمع این تراکنش به اطلاعات حساسی همچون شماره کارت های اعتباری و رمز عبور آنها دسترسی پیدا کنند.
به همین دلیل فروشندگان در دنیای مجازی باید اصول امنیتی را کاملاً رعایت کنند که یکی از آنها رمزنگاری اطلاعات حساس مشتریان است.
رمزنگاری (Encryption) فرآیند تبدیل اطلاعات برای تغییر شکل آن به صورت غیر قابل فهم برای همه بجز برای گیرنده اطلاعات می باشد که زمینه سلامت و پوشش مورد نیاز تجارت الکترونیک را برای اطلاعات رد و بدل شده فراهم می آورد.

استفاده ازچندین کارت بانکی

اگر شما از چندین کارت بانکی استفاده می کنید هیچوقت تمامی کارت های اعتباری خود را به یک رمز خاص تخصیص ندهید می توانید برای هر کارت یک رمزجداگانه استفاده کنید. اگر قادر به خاطرسپردن اطلاعات هر یک از کارت ها نیستید اطلاعات آنها را در یک فایل متنی قراردهید اما توجه کنید که اطلاعات را بصورتی که فقط خود از آن مطلع هستید ذخیره کنید .مثلا رمزهای عبور را بصورت مورب یا عمودی تایپ کنید. اگراطلاعات کارت بانکی خود را در گوشی هوشمند خود ثبت می کنید توجه کنید که فایل متنی خود از امنیت بالایی برخودار باشد می توانید از نرم افزارهای رمزگذاری بر روی فایل متنی استفاده کنید.

فقط در سایت های امن اطلاعات کارت اعتباری خود را وارد کنید.

در آدرس بار مرورگر زمانی که می خواهید اطلاعات بانکی کارت خود از جمله رمز عبور را وارد کنید توجه کنید که از ویژگی HTTPS استفاده گردد . این گواهی امنیت دیجیتال برای ردوبدل کردن اطلاعات بین بانکی است.پس توجه داشته باشید که حرف S در انتهای HTTP وجود داشته باشد.

تنظیمات مرورگر خود را بررسی کنید

در مرورگر نیز توجه داشته باشید که تنظیمات ذخیره فرم های ثبت نامی و ذخیره سازی نام و کارت اعتباری شما انجام نگیرد زیرا با استفاده از کوکی های مرورگر نیز میتوان به اطلاعات کارت بانکی دست یافت.

هنگامی که مرورگر درخواست ذخیره رمزعبور می کند آن را بصورت منفی پاسخ دهید. بخصوص اگر در اماکن عمومی مانند کافی نت ها در حال خرید اینترنتی هستید.

سایت های منقضی شده

یکی دیگر از خطراتی که خریداران اینترنتی را تهدید می کند، خرید از فروشگاه هایی است که عملاً مدتهاست غیرفعال شده اند ولی وب سایت آنها همچنان در فضای اینترنت موجود است و یا خرید کالاهایی است که متفاوت از کالای ادعا شده در فروشگاه های آنلاین هستند. در این مورد هم عامل تأثیرگذار در کاهش خطر، هوشیاری خریداران است.

منبع :

http://www.worldit.ir/