توصیه های امنیتی

پیشرفت روز افزون فناوری اطلاعات طی چند سال اخیر زندگی بشر را به گونه ای تغییر داده است که بدون استفاده از تکنولوژی های جدید بسیاری از فعالیتهای اقتصادی ، سیاسی ، اجتماعی و... غیر ممکن یا فلج گردد.

جذابیت برخی از فعالیتها (مالی و اقتصادی) در حوزه فناوری اطلاعات موجب شده است که افرادی تحت عنوان هکرهای اینترنتی و الکترونیکی نسبت به هک نمودن مکاتبات و مناسبات مالی اقدام نمایند و از این طریق موفق به سوء استفاده و کلاه برداری های کلانی از تجار و فعالین اقتصادی شده اند.

در این راستا نظر به تجربه کارشناسان شرکت خدمات ارزی و صرافی دی در خصوص حفظ و صیانت از منافع مشتریان خود در حوزه حواله های ارزی و به منظور ایجاد امنیت لازم از سوی مشتریان در انجام معاملات ارزی ، این شرکت بر خود فرض می داند که تجارب و توصیه های امنیتی در خود را در اختیار مشتریان قرار دهد.

هکرها، عمدتا با چهار روش طعمه خود را شناسایی و مورد سوء استفاده قرار می دهند، که عبارتند از:

۱ استفاده از ابزارهای قدرتمند سخت افزاری و نرم افزاری جهت کشف کلمه کاربری و رمز عبور

بسیاری از ایمیل های موجود در سراسر دنیا و بررسی محتوی آنها برای انتخاب قربانیان و دستیابی به اهداف خود: دلیل این مدعا اخباری است که هر از چندگاه در رسانه ها و یا سایتهای خبری در این مخصوص اعلام می شود و در پی آن سایتهای ارائه دهنده خدمات ایمیل از کاربران خود می خواهند نسبت به تغییر رمز عبور و اطلاعات امنیتی ایمیل های خود اقدام نمایند.

راهکار امنیتی :

به کاربران سرویس های ایمیل پیشنهاد می گردد در فواصل زمانی کوتاه مدت نسبت به تغییر رمز عبور و اطلاعات امنیتی ایمیل خود اقدام نمایند.

۲ استفاده از روشی تحت عنوان phishingجهت به سرقت بردن کلمه کاربری و رمز عبور ایمیل کاربران:

در این روش هکر با ارسال یک ایمیل جعلی با موضوع مرتبط با فعالیت کاربر یا سازمان قربانی و مورد هدف ، موجب می شود کاربر ذیربط تشویق به باز نمودن ایمیل دریافتی گردد. در این ارتباط به محض باز نمودن ایمیل مذکور صفحه ابتدایی ورود کاربر به سرویس ایمیل به صورت جعلی مشاهده می گردد و کاربر ذیربط با تصور اینکه دسترسی به سرویس ایمیل خود را از دست داده

است ،نسبت به درج مجدد کلمه کاربری و رمز عبور خود در صفحه جعلی نمایش داده شده اقدام می نمایند که پس از آن کاربر مجدداً به سرویس ایمیل خود هدایت می شود . با انجام این عملیات جعلی اطلاعات مربوط به کلمه کاربری و رمز عبور ایمیل کاربر یا سازمان مذکور به سرقت رفته و در اختیار هکر قرار می گیرد.بدین ترتیب هکر میتواند از طریق ایمیل هک شده از تمامی فعالیت های کاربر یا سازمان مذکور مطلع گرددو به اهداف مورد نظر خود برسد.

راهکار امنیتی:

به کاربران سرویس های ایمیل پیشنهاد می گردد از باز نمودن ایمیل های ناشناس به شدت پرهیز نمایند و در صورت بروز چنین اتفاقی سریعاً نسبت به تغییر رمز عبور و اطلاعات امنیتی ایمیل مربوطه اقدام گردد.

۳ جعل ایمیل طرف معامله (ذینفع) و مکاتبه با متقاضی از طریق ایمیل های جعلی:

در این روش هکر به طور نسبی اطلاعات قابل ملاحظه ای از طرف معامله(ذینفع) و متقاضی (نظیر نوع فعالیت ، روابط تجاری ، آدرس ایمیل و سایت و....) را در دست دارد، همچنین از نیاز متقاضی نیز مطلع می باشد. برای این منظور هکر می تواند با هک کردن ایمیل و سایت طرف معامله (ذینفع) و متقاضی و یا همدستی با عناصر نفوذی در هر دو طرف معامله (به عنوان مثال همدستی با یکی از پرسنل طرفین معامله و یا افرادمطلع.....) به اطلاعات اشاره شده دستیابی داشته باشد. در این شیوه هکر با ایجاد یک ایمیل جعلی که با تغییر و یا جابجایی یک حرف از ایمیل اصلی طرف معامله (ذینفع) امکان پذیر می باشد ، با متقاضی وارد مکاتبه شده و پیش فاکتورهای جعلی و اسناد لازم جهت واریز وجه را در اختیار متقاضی قرار می دهد و با این ترتیب متقاضی با اعتماد به اسناد دریافتی نسبت به انتقال وجه به حساب مورد نظر هکر اقدام می نماید.

راهکار امنیتی:

به طرفهای تجاری پیشنهاد می گردد به منظور اطمینان از صحت و اصالت ایمیل دریافتی از طرف معامله خود (ذینفع) مراتب را با تماس تلفنی و نمابر کنترل نماید.همچنین می تواند با ایجاد یک پوشه در سرویس ایمیل خود به نام طرف معامله (ذینفع) و با استفاده از ابزارفیلترینگ (که در تمام سرویس دهنده ایمیل وجود می باشد) ، ایمیلهای دریافتی از طرف معامله (ذینفغ) را فیلتر نموده و بدین ترتیب ایمیل اصل را ازایمیلهای جعلی و مشابه تشخیص داده و شناسایی نماید.

۴ وارد معامله شدن با متقاضی:

محدودیتهای ایجاد شده در تجارت بین الملل موجب شده است که تهیه و خریداری برخی از کالاها وخدمات در سطح دنیا برای تجار و فعالین اقتصادی بسیار دشوار گردد به نحوی که خریداری و یا تهیه برخی ازآنها تنها از طریق چندین عرضه کننده یا دلال و واسطه بین المللی امکان پذیرگردد. در این بین بسیاری از هکرهای از این بازار آشفته سوء استفاده کرده و خود را به عنوان فروشنده یا واسطه به متقاضیان معرفی می کنند و با ارسال مستندات جعلی و اعلام قیمتهای فریبنده اعتماد متقاضی را جلب

نموده و با آنها وارده معامله می گردند و اسناد مربوط به واریز را از طریق ایمیل در اختیار متقاضی قرار می دهند.

راهکار امنیتی:

عدم اعتماد به عرضه کنندگان، واسطه ها و دلال های ناشناس بین المللی و مشکوک شدن به قیمتهای غیر واقعی آنها از مهمترین راهکارهای امنیتی می باشد. در هر حال، در صورت ضرورت معامله با عرضه کنندگان و واسطه های ناشناس کالا و خدمات و به منظور ایجاد امنیت معاملات و در امان ماندن از هکرهایی که خود را به عنوان عرضه کننده یا دلال معرفی می کنند بایستی متقاضی از طرق مختلف نظیر برقراری تماس تلفنی و ارسال نمابر و دریافت پاسخ از طریق همان تلفن یا نمابرو همچنین جستجو و انجام تحقیقات کامل و ....در خصوص اصالت آنها اقدام نماید. همچنین ضروریست متقاضی در ابتدای امر با انجام معاملات بسیار خرد و سبک عملکرد و ایفای تعهدات اینگونه عرضه کنندگان و واسطه ها را بیازمایند.

نکته بسیار مهم

همانطورکه از محتوای مطالب فوق ملاحظه می شود مهمترین ابزار جلوگیری از هک شدن معاملات، استفاده از تلفن و نمابر در کنار ایمیل های مبادله شده می باشد؛ زیرا می توان طی تماس مستقیم با طرف معامله از اصالت ایمیل دریافتی و محتوای آنها اطمینان حاصل نمود.