

یکی از اقدامات کلاهبرداران این است که با راه اندازی سایت های جعلی که شبیه به سایت های اصلی است، به ربودن اطلاعات افراد، اغلب برای سوء استفاده های مالی اقدام می کنند؛ در این شیوه که اصطلاحاً به فیشینگ معروف است، از طریق اطلاعات وارد شده توسط کاربران در صفحات جعلی حساب های بانکی قربانیان خالی می شود

شگرد کلاهبرداران اینترنتی و نکته مهم امنیتی

گروه فناوری //

کلاهبرداران اینترنتی هم برای پیش بردن اعمال مجرمانه شان به سمت استفاده از HTTPS رفته اند. به همین دلیل پلیس فتا هشدار داد است که کاربران لازم است نسبت به سایت های فیشینگ که از HTTPS سوء استفاده می کنند، محتاط باشند.

با توجه به آگاهی کلاهبرداران نسبت به توجه کاربران به پروتکل های امن HTTPS، لازم است کاربران هنگام مراجعه به یک وبسایت، حتما به نشانه صحیح آدرس سایت نیز توجه کنند تا دچار حمله فیشینگ نشوند.

به گزارش اپتنا از ایسنا، یکی از اقدامات کلاهبرداران این است که با راه اندازی

سایت های جعلی که شبیه به سایت های اصلی است، به ربودن اطلاعات افراد، اغلب برای سوء استفاده های مالی اقدام می کنند؛ در این شیوه که اصطلاحاً به فیشینگ معروف است، از طریق اطلاعات وارد شده توسط کاربران در صفحات جعلی حساب های بانکی قربانیان خالی می شود.

از طرفی یکی از شگردهای کلاهبرداران سایبری برای در طعمه قرار دادن مردم این است که با سوء استفاده از احساسات شهروندان به ارسال لینک های حاوی بدافزار و سرقت اطلاعات شهروندان اقدام می کنند.

در این باره امیر صفری فروشانی -کارشناس نرم افزارهای امنیتی حوزه فناوری اطلاعات- با بیان این که فیشینگ یک تهدید سایبری

محسوب می شود، می گوید: اگر بخواهیم در برابر تهدیدات سایبری ایمن باشیم، باید موارد امنیتی را رعایت کنیم. یکی از موارد امنیتی این است که هوشیار باشیم، هر ایمیلی را باز نکرده و روی هر لینکی کلیک نکنیم، آدرس سایت ها را دقیق چک کنیم که همان آدرس مورد نظر باشد، زمانی که یک سایت ما را به مرحله پرداخت هدایت می کند، دقت کنیم که مثل همان نوشته شده باشد.

وی همچنین خاطرنشان می کند: بقیه موارد امنیتی هم این طور است که لازم است سیستم عامل و مرورگرمان را همیشه به روز کنیم، آنتی ویروس اصلی و معتبر داشته باشیم که ویژگی های امنیت اینترنتی داشته باشد، از جمله ویژگی حفاظت در برابر وبسایت ها

و لینک های آلوده، مرورگرها معمولاً از طرف آنتی ویروس افزوده می شود و آن ها بخش زیادی از فیشینگ را تشخیص می دهند. هم چنین اگر لینک پرداخت از طریق ایمیل ارسال شد، نباید از طریق آن به اینترنت بانک و ایمیل خود وارد شویم. کاربران باید توجه کنند که امنیت در فضای مجازی نسبی است. بنابراین عدم اعتماد و اطمینان به غریبه های آنلاین، عدم به اشتراک گذاری محتوای شخصی در شبکه های اجتماعی، دانلود نکردن فایل ها از سایت های نامعتبر و غیر مطمئن، به روزرسانی آنتی ویروس، دقت در وارد کردن نشانی درگاه های پرداخت الکترونیکی بانک ها و توجه به پروتکل امن HTTPS و عدم توجه به ایمیل



دانشجوی

شبکه های اجتماعی؛ بزرگ ترین خطر پیش روی بنگاه های تجاری

گروه فناوری //

تحقیقات جدید دریافته اند که بنگاه های تجاری با عدم پیگیری شمار رو به رشد نرم افزارهای شبکه هایشان خود را در معرض خطر بزرگی قرار می دهند.

تحقیقات جدید دریافته اند که بنگاه های تجاری با از عدم پیگیری شمار رو به رشد نرم افزارهای شبکه هایشان خود را در معرض خطر بزرگی قرار می دهند.

به گزارش صبح ساحل و به نقل از اپتنا وبسایت خبری تحلیلی itproportal، گزارشی از Gigamon دریافت شده است که نرم افزار شبکه های اجتماعی، بالاترین حد نگرانی متخصصان امنیت است که این روزها با خطرات احتمالی شبکه احاطه شده اند.

در این میان نرم افزارهای استریم تلویزیون و خدمات پیام رسان و گیمینگ بزرگ ترین نگرانی احتمالی آنها را تشکیل می دهد.

شمار نگران کننده ای از کسب و کارها نیز اظهار کرده اند که در باره تعداد نرم افزارهای روی شبکه خود و سرویس های مورد نیاز برای مدیریت امنیتشان اطمینان ندارند.

به صورت کلی، ۲۶ درصد از سازمان ها اعلام کرده اند که در رابطه با چگونگی افزوده شدن هرروزه نرم افزارها به شبکه شان اطلاعی ندارند و این در حالی است که ۱۱ درصد از آنها نمی دانند که آیا ابزاری برای مدیریت امنیت آنها وجود دارد یا خیر. ۱۷ درصد از سازمان ها هرروز در حدود ده برنامه جدید را به شبکه های پروژه خود وارد می کنند که همین امر خطر آسیب پذیری ها و نقص های امنیتی را بالا می برد. علاوه بر این ۱۴ درصد از این سازمان ها اعلان کرده اند که برای مدیریت امنیت خود سیاست خاصی ندارند و همین امر منجر می شود که داده های سازمانی آنها در خطر قرار بگیرد.

اولی شریدان به عنوان مهندس امنیت Gigamon در این رابطه اظهار داشت که: «سازمان های امروزی به میزان زیادی در نرم افزارها متکی هستند و کارمندان اغلب از آنها برای انجام بخش های کلیدی شغلشان استفاده می کنند. با این حال، این امر همچنین به آن معنا است که این نرم افزارها می توانند به داده های حساس شرکت دسترسی داشته باشند و اگر در دست افراد غلط بیفتند سازمان را تهدید کنند.

بنابراین سازمان ها باید با نرم افزارها به عنوان بخشی از شبکه خود رفتار کنند و تادید کاملی از عملکردهای آنها داشته باشند. همواره هنگام استقرار برنامه های جدید، امنیت باید مهم باشد.»

آگهی افراز ۸۴۵ و ۸۴۶

آگهی افراز ۸۴۵ و ۸۴۶- اصلی قطعه یک بخش چهار

بدینوسیله به کلیه مالکین حقیقی و حقوقی پلاکهای ۸۴۵ و ۸۴۶- اصلی اعلام میگردد نظر به اینکه آقای رضا دوستی بموجب وکالتنامه رسمی شماره ۱۳۱۸۶ و ۱۹۴۹۶ و ۱۳۱۲۱ تنظیمی دفتر خانه اسناد رسمی شماره ۳۰۲ شیراز باوکالت از طرف جمعی ازمالکین پلاکهای فوق عبارتند از:

- ۱: آقای سعید سعادت مالک ۲ سهم مشاع از ۱۵ سهم مشاع از شش دانگ پلاک موصوف
 - ۲: محمد ابراهیم سعادت ۲ سهم مشاع از ۱۵ سهم از شش دانگ پلاک موصوف
 - ۳: حبیب اله سعادت ۲ سهم مشاع از ۱۵ سهم از شش دانگ پلاک موصوف
 - ۴: محمد حسین سعادت ۲ سهم مشاع از ۱۵ سهم از شش دانگ پلاک موصوف
 - ۵: وحیده سعادت ۱ سهم مشاع از ۱۵ سهم از شش دانگ پلاک موصوف
 - ۶: هادی نیک طبع از وارث شهین سعادت ۱ سهم مشاع از ۱۵ سهم از شش دانگ پلاک موصوف
 - ۷: خانم حشمت سعادت ۱ سهم مشاع از ۱۵ سهم از پلاک موصوف
 - ۸- وارث قانون حیات عرب زاده ۸/۱ سهم مشاع از شش دانگ پلاک موصوف
- تقاضای افراز سهمی مالکین یاد شده را نموده است و ازطرف افراد زیر مالک مشاع پلاک یادشده به شرح ذیل میباشد ۱- خانم ناهید سعادت فرزند میرزا خلیل الله به شماره شناسنامه ۲۷۷
- شماره ملی ۲۲۷۱۹۵۷۲۲۹۵ صادره از حوزه یک بندرعباس به نشانی شیراز فعلا مجهول المکان مالک یک سهم از ۱۵ مشاع از شش دانگ
- ۲- خانم ممتاز سعادت فرزند میرزا خلیل الله به شماره شناسنامه ۸۰۹ و شماره ملی ندارد محل صدور بندرعباس به نشانی شیراز فعلا مجهول المکان مالک یک سهم از ۱۵ مشاع از شش دانگ پلاک موصوف
- ۳- خیرالنسا سعادت فرزند میرزا خلیل الله به شماره شناسنامه ۳۵ و شماره ملی ۳۲۹۰۰۰۰۳۵۶ صادره از حوزه یک بندرعباس به نشانی شیراز فعلا مجهول المکان مالک یک سهم از ۱۵ مشاع از شش دانگ پلاک موصوف
- ۴- مرحمت سعادت فرزند میرزا خلیل الله به شماره شناسنامه ۳۴ و شماره ملی ۳۳۹۰۰۰۰۳۴۸ محل صدور بندرعباس به نشانی شیراز فعلا مجهول المکان مالک یک سهم از ۱۵ مشاع از شش دانگ پلاک موصوف
- ولذا بدینوسیله از کلیه مالکین فوق یا وارث قانونی آنها مراتب فراز به شرح ذیل به ایشان ابلاغ میگردد عملیات نقشه برداری در تاریخ ۱۳۹۸/۰۹/۱۶ راس ساعت ۸ صبح درمحل وقوع پلاک یادشده در شهر میناب بلوار آل محمد (ص) روبه رو کمیته امداد امام خمینی (ره) محله داوشتی برگزار می گردد عدم مراجعه مانع افراز نخواهد شد .

تاریخ انتشار آگهی ۱۳۹۸/۰۷/۰۱

رئیس ثبت اسناد و املاک شهرستان میناب عقیل قاسمی
۱۸۹۱۶۶ الف/م/۱۷۸۴

اخطاریه

قابل توجه اعضای محترم شرکت تعاونی مسکن مهر محله چهارراه فلسطین شیلات : دومین اخطاریه جهت تعیین تکلیف وضعیت عضویت و پرداختی اعضای اعلامی

بدینوسیله اعلام می گردد آقایان داود زمانی فرزند محمدعلی به شماره ملی ۶۴۴۹۲۳۱۹۸۱ ، فریدون غلامی فرزند محمد به شماره ملی ۲۵۹۳۶۶۷۴۱۹ ، مرتضی حیدری فرزند حسین به شماره ملی ۲۵۱۰۵۵۹۲۵۷، محمد ترین فرزند عبدالله به شماره ملی ۳۳۹۱۹۲۴۴۱۱، مهدی حسین زاده فرزند حبیب الله به شماره ملی ۳۳۹۱۶۴۹۳۷۲، محمد زرین کفش فرزند یوسف به شماره ملی ۵۴۴۹۹۵۳۰۶۴، امید محمودی تختی فرزند حسن به شماره ملی ۳۳۹۰۵۴۳۰۶۶، علی بهرامی سعادت آبادی فرزند بختیار به شماره ملی ۳۴۷۹۷۹۵۸۹۷، ابراهیم عمرانی هنگامی فرزند اسحق به شماره ملی ۳۳۹۰۱۸۴۸۰۵، اسماعیل قاسمی فرزند ابراهیم به شماره ملی ۳۳۹۱۷۵۳۱۱۰، حبیب درگیری فرزند بهزاد به شماره ملی ۳۳۹۱۵۷۶۳۶۲۴، محمد صفرپور فرزند علی به شماره ملی ۳۳۹۰۱۹۸۵۹۱، علی اکبر شجاعی تیاب فرزند حسن به شماره ملی ۳۴۲۱۸۰۳۱۰۲، ماجد دوست وطن فرزند حمید به شماره ملی ۱۸۹۹۵۰۸۶۰۰ می بایست حداکثر ظرف مدت ۱۵ روز از تاریخ انتشار این آگهی جهت تعیین تکلیف وضعیت عضویت و تکمیل سهم آورده خود به دفتر شرکت تعاونی مسکن مهر محله چهارراه فلسطین تا شیلات به آدرس : بندرعباس -بلوار سیدجمال الدین اسدآبادی -چهارراه فاطمیه- جنب مسجد فاطمیه- ساختمان پزشکان فاطمیه طبقه ۶ واحد ۲۴ مراجعه نمایند در غیر اینصورت شرکت تعاونی فوق الذکر طبق اساسنامه و ماده ۱۳ بخش تعاون اقدام می نماید .

◀ هیات مدیره شرکت تعاونی چهارراه فلسطین تا شیلات

آگهی شرکت های

تعاونی سراسر هرمزگان

در صبح ساحل

تلفن پذیرش: ۰۵-۳۲۲۲۴۱۴۶۲