؟ چیست فیشینگ Phishing

ادبیات اینترنت , سرقت هویت , حملات phishing , وب سایت مخرب , Phishing فیشینگ چیست ؟

اطلاعات افشای به کاربران نیرنگ با توام ترغیب به و مطرح اینترنت ادبیات عرصه در مهاجمان توسط که است هایی واژه جمله از Phishing حساس و شخصی آنان ، اشاره دارد . مهاجمان به منظور نیل به اهداف مخرب خود در اولین مرحله درخواست موجه خود را برای افراد بیشماری ارسال می نمایند و در انتظار پاسخ می مانند . آنان امیدوارند که حتی اگر بتوانند تعداد اندکی از افراد را ترغیب به افشای اطلاعات حساس و شخصی خود نمایند در رسالت خود موفق بوده اند . امیدواری آنان چندان هم بی دلیل نخواهد بود چراکه با توجه به گستردگی تعداد قربانیان اولیه احتمالی ، شانس موفیقت نهایی آنان از لحاظ آماری نیز افزایش می یابد .
مهاجمان به منظور افزایش ضریب موفقیت حملات سعی می نمایند خود را بگونه ای عرضه نمایند که مردم به آنان اعتماد نموده و آنان را به عنوان نمایندگان قانونی مراکز معتبری نظیر بانک ها قبول نمایند . ماهیت و یا بهتر بگوییم رمز موفقیت این نوع از حملات بر قدرت جلب اعتماد مردم استوار است و بدیهی است که مهاجمان از هر چیزی که بتواند آنان را موجه تر جلوه نماید ، استقبال خواهند کرد . مهاجمان پس از جلب رضایت و اعتماد کاربران از آنان درخواست اطلاعات حساس و مهمی نظیر شماره کارت اعتباری را می نمایند .
اکثر عملیات اشاره شده به صورت اتوماتیک انجام و با توجه به این که کاربران گسترده ای هدف اولیه قرار می گیرند و درصد بسیار زیادی از آنان دارای آگاهی لازم جهت تشخیص و مقابله با این نوع حملات نمی باشند ، شانس موفقیت مهاجمان به منظور سرقت هویت کاربران افزایش می یابد .
سرقت هویت چیست ؟
سرقت هویت ، استفاده از هویت شخص دیگر (اطلاعات حساس و یا شخصی) برای سوء استفاده مالی و یا سایر اهدف مخرب است . سوء استفاده یا کلاهبرداری با استفاده از کارت اعتباری دیگران ، یک نمونه از سرقت هویت است . در واقع Phishing ، روشی است که مهاجمان از آن به منظور سرقت هویت استفاده می نمایند .
آیا سرقت هویت صرفا گریبانگیر افرادی می گردد که اقدام به ارسال اطلاعات online می نمایند ؟ در صورتی که هرگز از کامپیوتر استفاده نکرده باشید ، ممکن است از جمله قربانیان سرقت هویت باشید . مهاجمان می توانند با بکارگیری روش های متعدد به اطلاعات شخصی شما نظیر شماره کارت اعتباری ، شماره تلفن ، آدرس و ... دستیابی پیدا نمایند . اکثر شرکت ها و موسسات ، اطلاعات مربوط به مشتریان خود را در بانک های اطلاعاتی ذخیره می نمایند و در صورت دستیابی سارقین به بانک های اطلاعاتی ، اطلاعات شخصی تعداد زیادی از افراد افشاء می گردد .اینترنت فضای لازم برای سارقین را فراهم نموده است تا بتوانند در زمانی مطلوب و در گستره ای وسیع تر به اطلاعات شخصی و مالی کاربران دستیابی نمایند . اینترنت ، همچنین امکانات مناسبی به منظور فروش و مبادلات تجاری اطلاعات سرقت شده را در اختیار مهاجمان قرار می دهد .
چرا می بایست از خود در مقابل حملات phishing حفاظت نمود؟
در یک سازمان ، افراد متفاوت اطلاعاتی را نزد خود نگهداری می نمایند که ممکن است حساس و یا برای سایر افراد و یا سازمان ها حایز اهمیت باشد . در حملات phishing ، مهاجمان عموما از روش های غیر فنی (نظیر مهندسی اجتماعی) برای دستیابی به اطلاعات حساس و مهم اشخاص و یا سازمان ها استفاده نموده و موارد زیر را هدف قرار می دهند :
اطلاعات بانکی نظیر کارت های اعتباری و یا حساب هایی نظیر paypal
اطلاعات مربوط به نام و رمز عبور
اطلاعات بیمه همگانی و ...
مهاجمان پس از دستیابی به اطلاعات فوق از آنان به منظور نیل به اهداف زیر استفاده می نمایند :
برداشت از حساب بانکی
سرویس های online متفاوتی نظیر eBay و یا Amazon
یک نمونه از حملات phishing
تعداد زیادی از حملات phishing از طریق email انجام می شود . مهاجمان email موجه خود را برای میلیون ها قربانی احتمالی ارسال می نمایند . این نوع نامه های الکترونیکی بسیار مشابه وب سایت شرکتی می باشند که email ادعا می نماید ، نامه از آنجا برای کاربران ارسال شده است .
مهاجمان به منظور فریب کاربران از روش های متعددی استفاده می نمایند :
استفاده از logo و سایر علایم تجاری شناخته شده و معتبر

ساختار و طراحی email تقلبی مشابه وب سایت واقعی است ، بگونه ای که در اولین مرحله تشخیص جعلی بودن آن برای بسیاری از کاربران غیرممکن است .
بخش from نامه الکترونکیی ارسالی ، مشابه ارسال یک email معتبر از شرکت مربوطه است .
در متن email ممکن است فرمی تعبیه شده باشد که از کاربران خواسته شود به دلایل خاصی (مثلا account شما در معرض تهدید است و ممکن است مورد سوء استفاده قرار گیرد و یا به دلیل بروز اشکالات فنی) ، مجددا اطلاعات خود را در فرم درج و آن را ارسال نمایند .
در برخی موارد ، مهاجمان به منظور افزایش اعتماد کاربران و معتبر نشان دادن email ارسالی از روش هایی فنی تری استفاده می نمایند .
مثلا ممکن است آنان از روشی موسوم به spoofing URL استفاده نمایند و با ایجاد یک لینک در متن email از کاربران بخواهند که جهت ادامه عملیات بر روی آن کلیک نمایند . با کلیک کاربران بر روی لینک فوق ، آنان در مقابل هدایت به یک سایت معتبر که انتظار آن را دارند به وب سایتی هدایت می گردند که مهاجمان آن را مدیریت می نمایند . شکل ظاهری وب سایت بگونه ای طراحی می گردد که کاربران نتوانند جعلی بودن آن را تشخیص دهند .
کلاهبرداران اینترنتی بی شک از بهترین استفاده کنندگان مهندسی اجتماعی به شمار می روند . آنها ابتکارات بسیاری در این خصوص از خود نشان داده اند .
به تازگی کلاهبردان اینترنتی سعی می کنند با بهره گیری از اوضاع نابسامان صنعت بانکداری ، با به کار بردن ترفندهایی ، کاربران را به لو دادن اطلاعات مالی خود وادارند .
به گزارش the register نسل جدید ایمیل های فیشینگ با تقلید کردن از اطلاعیه های رسمی مربوط به ادغام بانک ها ، می کوشد نظر کاربران را به خود جلب کند.
کمیسیون تجارت فدرال (FTC) روز پنجشنبه با صدور اطلاعیه ای، به مشتریان هشدار داد مراقب این نوع فریب کاری باشند . هشدار FTC که در سایت gov.ftc منتشر شده ، با عبارت « شکست های بانکی ؛ ادغام یا تصاحب مالکیتی » آغاز می گردد .
اگرچه ایمیل های جعلی قدمتی حداقل پنج ساله دارد (اگر نگوییم بیشتر !) اما باز هم به عنوان یک شیوه مفید و پربازده ، می تواند کاربران ساده لوح بسیاری را که نگران و پیگیر بحران اخیر بانکی در جهان هستند ، به دام اندازد.
گفتنی است در نیمه اول سال ۲۰۰۸ بیش از ۲۰ هزار وب سایت مخرب برپا شده که در قیاس با مدت زمان مشابه سال قبل ، با بیش از ۱۸۰ درصد رشد ، حدودا سه برابر شده است .
. است کرده بیان (APACS) انگلیس بانکداری انجمن از نقل به را مطلب این The register
آمار دیگری که در این زمینه ارائه شده نیز حیرت آور است : در شش ماه اول سال ۲۰۰۸ ، بانکداری آنلاین حدود ۴ ۲۱ میلیون پوند خسارت از ناحیه جرایم سایبری متحمل شده است که نسبت به ۵ ۷ میلیون پوند سال گذشته ، رشد سرسام آوری را نشان می دهد.
. است بوده ها خسارت این اکثر مسبب ، جاسوسی افزارهای نرم و فیشینگ است معتقد Apacs

---