حملات فیشینگ

!! نه اون ماهیگیری که شما انجام می دین

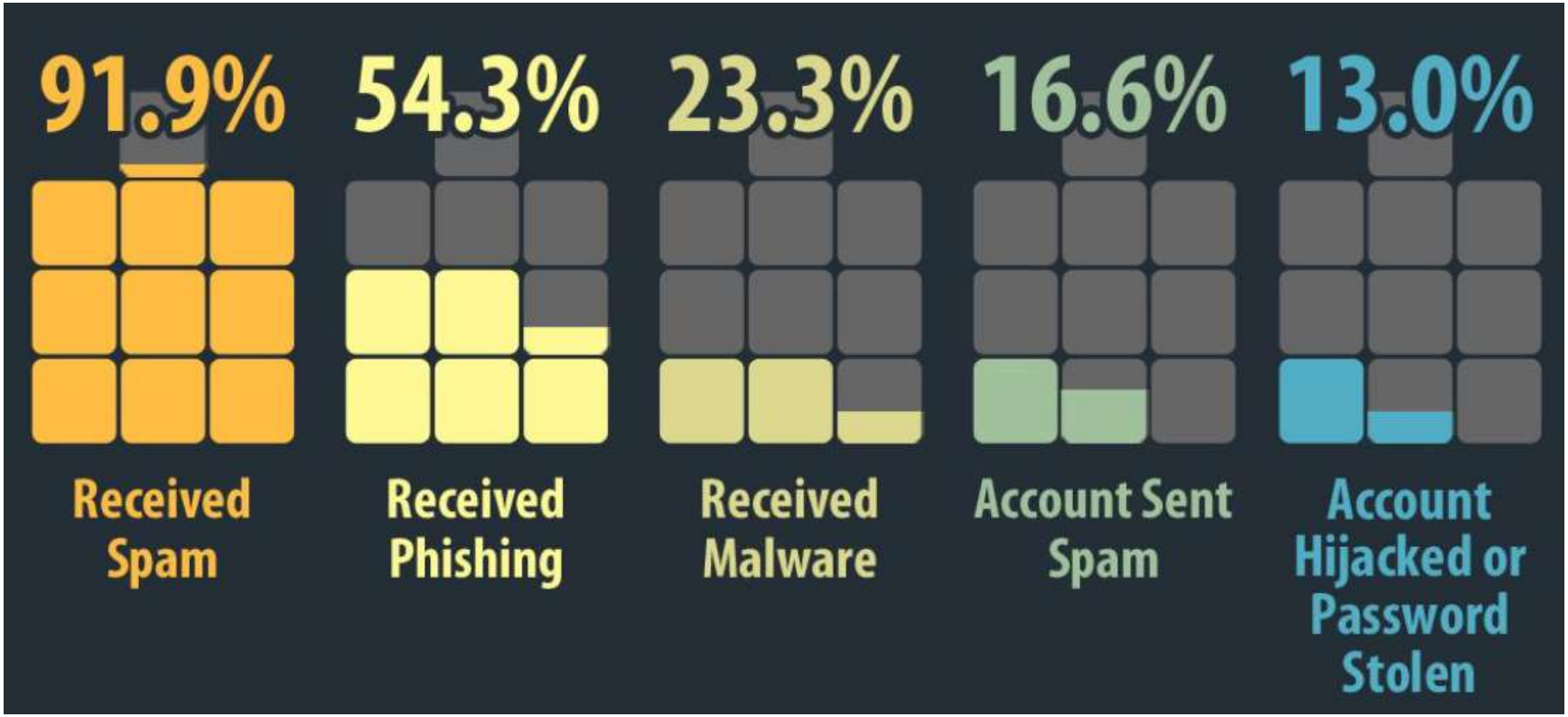
تهیه کننده: اقای بهنام

www.expertit.ir

فیشینگ چیست !؟

- فیشینگ یک تکنیک مهندسی اجتماعی است که به وسیله یک هکر یا حمله‌کننده برای دزدیدن اطلاعات حساس مانند نام کاربری، رمز عبور و رمز کارت‌های اعتباری استفاده می‌شود (در این حالت حمله‌کننده وانمود می‌کند یک شخص یا یک سازمان مورد اعتماد است).
- بالای 90 % از حملات فیشینگ از طریق ارسال ایمیل های اسپم صورت می گیرد
- گوگل می‌گوید بهترین حملات فیشینگ ۴۵ درصد موفق می‌شوند. و در بدترین حالت 3 % از حملات موفقیت آمیز بودند.
- هر چند فیشینگ یک بد افزار نیست ولی به این معنی هم نیست که خطر کمی دارد
- بهترین راه مقابله با فیشینگ، افزایش آگاهی خود از این نوع حملات است.

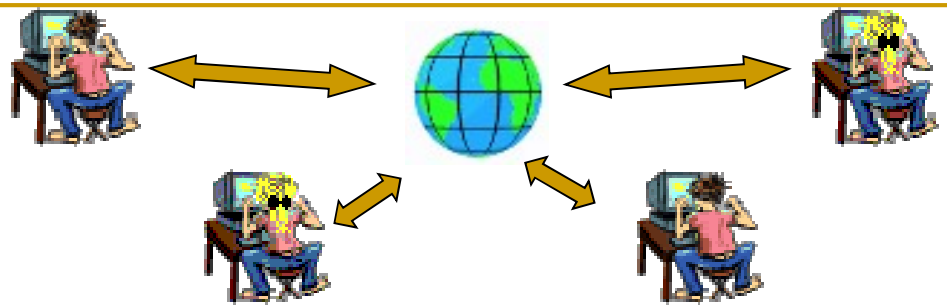
آماری از حملات فیشینگ!



چگونگی انجام فیشینگ

- ایمیل های فیشینگ اکثرا با ایمیل هایی که از سمت منابع مطمن مثل بانک ها ، شرکت های معتبر و غیره ارسال می شوند سروکار دارند.
- ابتدا کاربر از طریق ایمیل و آگاهی های تبلیغاتی سایت های دیگر، به صفحه یا فرم یا فایل مورد نظر هکر راهنمایی می شود. سپس از کاربر درخواست میشود تا اطلاعاتی مانند اطلاعات کارت اعتباری و رمز اکانت های خود را وارد کند
- اکثر ایمیل فیشینگ ها شامل کرم ها و ویروس ها و تروجان هایی هستند که در پیوست ایمیل ظاهر می شوند و زمینه را برای سناریوهای بعدی هکر اماده می کنند.
- سایت های ebay و paypalبیشترین درصد این حملات را شامل میشوند.

چگونگی انجام فیشینگ



- از جمله سناریوهای رایج در ایمیل فیشینگ می توان به پیوست کرم های اینترنتی اشاره کرد.
- کرم های اینترنتی قابلیت تبدیل شدن به جاسوس بر روی سیستم ها را دارا هستند و اکثر اوقات آنتی ویروس ها آن ها را تشخیص نمی دهند.
- از جمله قابلیت های کرم ها ، ارسال لیست مخاطبین کاربر به هکر می باشد
- همچنین هکر می تواند حملات مردی در میان را با حملات فیشینگ حاوی پیوست های مخرب به صورت ترکیبی انجام دهد و طرفین یک معامله را مورد حملات فیشنگ قرار دهد (سناریوی پیاده شده در شرکت رجال)
- کارکنان شرکت ها باید توجه داشته باشند که شبکه های اجتماعی از جمله مراکز حملات فیشینگ هستند که امکان دارد شامل فایل های مخرب باشد و سیستم های شرکت را آلوده به این نوع کرم ها بکند.

تکنیک های مورد استفاده در فیشینگ

- دستکاری پیوند ها:

در این تکنیک برای گمراه کردن کاربر از اسامی معتبری در آدرس استفاده می شود.
مانند استفاده از زیر دامنه ی آشنای gmail در لینک زیر:

- http://www.gmail.goolgee.com

که در واقع کاربر را به سمت سایت فیشر هدایت می کند.

یا مثلا www.google.com@members.tripod.com که در واقع کاربر را به ایمیل سایت tripod.com هدایت می کند نه به سایت گوگل!

غالبا این تکنیک از حملات فیشینگ از طریق ایمیل های اسپمی که حاوی لینک هایی دستکاری شده هستند صورت می گیرد و با ترفندهای مهندسی اجتماعی
ازجمله برنده شدن در قرعه کشی ، از کار افتادن حساب و ایمیل در صورت توجه نداشتن به این پیام وغیره سعی در به دام انداختن کاربران دارند.

تکنیک های مورد استفاده در فیشینگ

- دستکاری پیوند ها:

از جمله روش های استفاده شده در این تکنیک کم و زیاد کردن کاراکترهای سایت ها و ایمیل ها و شماره های تماس می باشد.

- Fake : Real :

Tel : +49 5307 9285 140 Tel : +49 5207 9285 140
Fax : +49 5307 9285 141 Fax : +49 5207 9285 141
Mail: r.brok@miter-mmb.de r.brok@mitter-mmb.de

- از جمله روش های دیگر این تکنیک استفاده از متنی معتبر که البته در پشت آن آدرس سایت فیشر قرار دارد است . قبل از کلیک کردن بر روی این هایپر لینک ها حتما موس را بر روی آن نگه دارید تا از سایت پشت آن مطلع شوید

تکنیک های مورد استفاده در فیشینگ

- گریز از فیلترها:

سیستم های آنتی فیشینگ زیادی وجود دارند که بر اساس متن های متداول فیشینگ عملیات شناسایی و جلوگیری را انجام می دهند.

فیشر ها برای دور زدن این سیستم ها با قرار دادن لوگو و نشان شرکت های معتبرو بانک ها به جای لینک سایت خود استفاده می کنند که با کلیک کردن بر روی این تصاویرکاربران به سایت های فیشرها هدایت می شوند.

- به هیچ وجه بر روی این تصاویر کلیک نکنید مگر آنکه منتظر دریافت تصویری از کسی هستید!

تکنیک های مورد استفاده در فیشینگ

- جعل وب گاه ها:

در این تکنیک وب سایت هایی با ظاهر کاملا شبیه به وب سایت های اصلی ساخته می شوند ، این صفحات جعلی که به شکل حقیقی ظاهر می شوند ، تنها ظاهر وبسایت مقصد را حفظ می کنند ؛ اما در عمل تمامی اطلاعات که کاربر در هنگام پر کردن فرم در فیلدهای مورد نظر وارد می کند را در اختیار فیشر ها قرار می دهد.

- در سایت هایی که اطلاعات مهم خود اعم از اطلاعات بانکی و شخصی را وارد می کنید حتما URL آن سایت را با دقت نگاه کنید و از سایت مطمن شوید.
- سایت های بزرگ اکثرا برروی پروتکل https فعال هستند که در موقع باز کردن این سایت ها فولدر زردرنگی در صفحه ظاهر می شود

تکنیک های مورد استفاده در فیشینگ


- فیشینگ تلفنی:

تمامی حملات فیشینگ نیاز به وبگاه جعلی نیاز ندارند ! پیام هایی که از طرف یک بانک زده می شود و با ادبیات بانکی مثلا از کاربر می خواهد تا مثلا به دلیل وجود ایراد در حسابشان شماره خاصی را شماره گیری بکنند. (بعد از گرفتن شماره که متعلق به فیشر است و با سرویس تلفن اینترنتی است) از کاربر خواسته شده تا شماره حساب و پین خود را وارد کند.

- هیچ سازمان معتبری از شما نمی خواهد از طریق تلفن و ایمیل اطلاعات بانکیتان را تصحیح کنید!

تکنیک های مورد استفاده در فیشینگ

- تمرکز بر روی کاربر خاص:

یکی از روش های فیشینگ متمرکز شدن بر روی یک کاربر خاص یا یک حوزه خاص در تشکیلات است. نامه جعلی ظاهرا بدون هیچ مورد قانونی است و از او کمک می خواهد . در این روش با بهره بردن از ذکر نام یک شخص حقیقی به جای یک سیستم پشتیبانی، اعتماد بیشتری جلب می کند و گاهی از کاربر می خواهد که به دلایل خاصی اطلاعات خود را بروز کرده یا صحت آن ها را بررسی کند.

- در نامه های دریافتی حتما سعی شود منبع آن نامه به دقت بررسی شود در صورت نیاز تلفن چک و فکس چک انجام شود.

سایر تکنیک های مورد استفاده در فیشینگ

- نوع دیگری از حملات که موفقیت آن ثابت شده است ارجاع دادن قربانی به وب سایت اصلی بانک است. سپس یک پنجره پاپ آپ در بالای صفحه سایت به نمایش در می آید و به شکلی که به نظر برسد این صفحه و این سایت متعلق به بانک است، اطلاعات حساس قربانی را درخواست می کنند.
- یکی از جدیدترین روش های فیشینگ قاپیدن تب است. این برنامه از صفحاتی که کاربر باز کرده استفاده می کند و به طور آهسته کاربر را به سایت ساختگی ارجاع میدهد.
- دوقلوهای شر روشی است که شناسایی و کشف آن کار بسیار سختی است. یک فیشر یک شبکه بی سیم (وایرلس) ساختگی ایجاد می کند. این شبکه همانند شبکه های معتبر عمومی و قانونی می تواند در مکان هایی مانند فرودگاه ها، هتل ها و کافی شاپ ها وجود داشته باشد.

نرم افزارهای جاسوسی

- یک روشی که برای کاربران شرکت گوگل افتاد این بود که یک نرم افزار جاسوسی با ترفندهای خاص مانند بر روی من کلیک کن و غیره بر روی سیستم قربانی وارد میشد و هیچ تاثیر منفی بر روی سیستم نمی گذاشت فقط وقتی یک کاربر می خواست به سایت گوگل مراجعه کند ، او را به یک سایت جعلی که کاملا شبیه گوگل بود هدایت می کرد و مثلا وقتی شما بخواهید جمیل خود را چک کنید اطلاعات خود را در این سایت جعلی وارد می کنید و اطلاعات شما برای فیشرها ارسال می شده است!
- شدیدا توصیه می شود بر روی لینک های تبلیغاتی و غیره که نمی شناسید آن ها را کلیک نکنید . چون اکثرا حاوی حملات فیشینگ و بدافزارها هستند.

روش های تشخیص فیشینگ

- حملات فیشینگ معمولا در قالب های زیر ظاهر می شوند.
  - ایمیل از طرف فردی که ادعا می کند دوست یا همکار شماست.
  - پیغام یا تبلیغ از طرف شبکه های اجتماعی
  - وب سایت قلابی که برای امور خیریه تقاضای کمک می کند.
  - وب سایت با نامی مشابه وبسایت هایی که شما متناوبا به آن ها سر می زنید.
  - در برنامه های پیغام فوری مانند یاهر مسنجر و ویندوز لایو مسنجر
  - از طریق پیام های کوتاه تبلیغاتی بر روی تلفن همراه شما
  - درخواست تصحیح و تایید اطلاعات از سمت بانک قلابی
  - برنده شدن شما در قرعه کشی

حفاظت در برابر فیشینگ

- برای شناسایی یک ایمیل مطمئن تنها به موضوع و آدرس ایمیل ارسالی اکتفا نکنید، چرا که کلاهبردار می تواند با تکنیک‌های موجود آدرس ایمیل شرکت اصلی را به جای ایمیل ارسالی خود قرار دهد .
- حتی امکان ایمیل ها را reply نکنید و به آدرس ایمیل را دستی تایپ کنید در صورت reply دادن مطمن شوید که ایمیل را به چه کسی reply می دهید (کاراکترهای ایمیل را به دقت بررسی کنید.)
- ایمیل ارسالی ممکن است با آرم، لوگو و شکل قالب ایمیل‌های ارسالی شرکت اصلی فرستاده شود، بنابراین به شکل ظاهری و عکس های موجود در آن بسنده نکنید.
- فراموش نکنید که بهترین راه برای دستیابی به صفحات وب، تایپ کردن آدرس به طور مستقیم در Browserاست.

حفاظت در برابر فیشینگ

- پاسخ ندادن به ایمیل های ساختگی و مشکوک درخواست کننده ی اطلاعات شخصی ، بویژه رمز کاربری ایمیل
- پیوست های ناخواسته را باز نکنید
- فایل های مشکوک را اسکن کنید
- تغییر دادن رمز کاربری به صورت هفتگی و انتخاب رمز پیچیده
- آدرس ایمیل خود را بدون دلیل در اختیار دیگران قرار ندهید و آدرس ایمیلتان را در هر سایتی ثبت ننمائید.
- ایمیل شرکت و مخصوصا ایمیل های مربوط به امور بازرگانی جدا از سایر ایمیل های کم ارزش و شخصی باشد
- هرگز ایمیلتان را آنگونه که هست نمایش ندهید

تهیه کننده: اقای بهنام

www.expertit.ir