KHAVARAN

دانشکده مهندسی کامپیوتر

فیشینگ چیست؟

محمد علی مجرب

استاد راهنما:

مهندس مهدیه پوستچی

تیرماه 88

بسم الله الرحمن الرحیم

تقدیم به آنها که گوهره ی وجودشان در گستره علم و دانش در حال رشد و تعالی است.

چکیده

هر روزه دزدان اینترنتی راه‌های جدیدی را برای بدست آوردن هویت شخصی افراد و دست یابی به اطلاعات شخصی آنها به کار می‌برند. یکی از روش‌هایی که اخیرا بسیار مورد توجه آنها قرار گرفته و البته کمی‌هم پیچیده می‌باشد، فیشینگ نام دارد. حملات موسوم به فیشینگ به آن دسته از حملات اینترنتی گفته می‌شود که معمولا طراحان آنها از ایمیلهای دارای آدرسهای فرستنده جعلی برای کشاندن کاربران به وب سایتهای مورد نظرشان استفاده می‌کنند.

در اینگونه حملات، معمولا ایمیل‌هایی برای کاربران ارسال می‌شود که دارای آدرس فرستنده مربوط به شرکتهای معروف و یا بانکهای معتبر هستند و درون آنها نیز لینکهایی قرار دارد که ظاهرا به همان مراکز تعلق دارند اما در حقیقت کاربر را به سوی سایتهای مورد نظر طراحان فیشینگ هدایت می‌کنند و اطلاعات حساس نظیر کلمات عبور و یا رمز کارتهای اعتباری کاربران را می‌ربایند. . این عمل مجرمانه جدید در شبکه اینترنت می‌رود که به یک پدیده و معضل گسترده تبدیل شود.

واژه‌های کلیدی :فیشینگ ، آنتی فیشینگ

فهرست مطالب

فصل 1: مقدمه **1**

1-1-مقدمه..... 2

فصل2:معنا و مفهوم فیشینگ 3

2-1- فیشینگ به چه معناست 4

2-2- فیشنگ چیست..... 4

فصل3: چگونگی انجام فیشینگ 6

3-1- نحوه کار فیشینگ..... 7

3-2- تکنیک های مورد استفاده در فیشینگ..... 7

3-2-1- دستکاری پیوند..... 7

3-2-2- گریز از فیلتر ها..... 7

3-2-3- جعل وب‌گاه..... 7

3-2-4- فیشینگ تلفنی.....8

3-2-5- تمرکز بر روی کاربر خاص 8

3-2-6- نرم افزارهای جاسوسی 8

فصل4: روشهای تشخیص فیشینگ و آنتی فیشینگ 10

4-1- روش‌های تشخیص فیشینگ 11

4-2- آنتی فیشینگ.....12

4 -3- نرم افزارهای آنتی فیشینگ.....14

4-3-1- IE & Windows Live Toolbar.....14

4-3-2-FireFox & Google Toolbar.....14

4-3-3-Toolbar Net Craft.....15

4-3-4- NC Toolbar.....15

4-3-5- GeoTrust Toolbar.....16

4-3-6- EarthLink Toolbar.....16

4-3-7- Trust Wach Toolbar.....16

4-3-8- Mcafee Site Advisor.....16

4-3-9- CoreStreet Spoot Stick.....17

4-3-10- Earthlink ScamBlocker.....17

4-3-11- webRoot Phish Net.....17

فصل 5:فیشرها و راه های حفاظت از هویت 19

5-1-فیشرها.....20

5-2- راه‌هایی برای حفاظت از هویت.....20

5-3- باز پس‌گیری هویت 22

مراجع 26

فصل 1:

مقدمه

1-1 - مقدمه

تا چند سال پیش کدهای مخرب برای انتشار سریع و در بسیاری از موارد آسیب رساندن به رایانه ها طراحی می شدند. اما امروزه تا حد زیادی اثری از این نوع کدهای مخرب وجود ندارد. اکنون نخستین هدف کدهای مخرب و طراحان آنها پول و مسائل مالی است. جالب این است که طراحی این نوع کدهای مخرب نیازی به دانش بسیار وسیع ندارد و هر فردی با دانش بسیار کم نیز می تواند این کار را انجام دهد. این کار بیشتر از دانش و آگاهی فنی به شیطنت و شخصیت نادرست نیاز دارد. این روش ها وابسته به هیچ کدام از انواع مختلف سیستم های عامل، مرورگرهای اینترنت و یا سیستم پستی نیستند. آنها فقط و فقط به کاربر وابسته هستند.

فصل 2:

معنا و مفهوم فیشینگ

2-1- فیشینگ به چه معناست

کلمه Phishing در زبان انگلیسی نیز یک واژه جدید است که برخی آن را مخفف عبارت Password Harvesting Fishing (شکار کردن رمزعبور کاربر از طریق یک طعمه) و برخی دیگر آن را استعاره‌ای از کلمه Fishing (ماهیگیری) تعبیر کرده‌اند. سازندگان این واژه کوشیده‌اند با جایگزین کردن Ph به جای F مفهوم فریفتن را به مخاطب القا کنند.

فیشینگ در اصطلاح کامپیوتری به معنای شبیه سازی قسمتهایی از یک سایت اینترنتی (مثلا یک صفحه از سایت) آشنا و یا معروف است که به وسیله آن بتوان کاربر را گمراه کرده و اطلاعات شخصی وی را بدست آورد . این اطلاعات می تواند شامل نام کاربری و کلمه ی عبور فرد در آن سایت یا اطلاعاتی مربوط به شماره حساب بانکی فرد و خیلی موارد دیگر باشد .

2-2- فیشنگ چیست

فیشینگ یک نمونه از تکنیک مهندسی اجتماعی [1] به منظور گمراه کردن کاربران اینترنتی برای بدست آوردن اطلاعت محرمانه آنان است . در این تکنیک فیشرها ها (کسانی که عمل فیشینگ را انجام می دهند) با طراحی یک سایت که شبیه به سایت مورد نظر می باشد ، کار خود را آغاز می کنند. پس از انجام این مرحله آنها باید روشی را پیدا کنند که قربانیان خود را مجبور کنند تا در سایت آنها وارد شده و اطلاعات محرمانه خود را وارد کنند که به روش های مختلفی این کار عملی می شود .مثلا با ساخت یک خبر دروغین ، قربانیان را به سایت خود کشانده و... بقیه مراحل انجام می شود .شاید خود شما تا به حال به طور ناخواسته و بدون اینکه متوجه چیزی شوید ، یکی از قربانیان فیشینگ شده باشید (به اصطلاح در قلاب ماهیگیر افتاده باشید !)

1- در تکنیک مهندسی اجتماعی، یک مهاجم با برقراری ارتباط با کاربران و استفاده از مهارت های اجتماعی خاص (روابط عمومی مناسب ، ظاهری آراسته و ...) ، سعی می نماید به اطلاعات حساس یک سازمان و یا کامپیوتر شما دستیابی و یا به آنان آسیب رساند . یک مهاجم ممکن است خود را به عنوان فردی متواضع و قابل احترام نشان دهد . مثلا" وانمود نماید که یک کارمند جدید است ، یک تعمیر کار است و یا یک محقق و حتی اطلاعات حساس و شخصی خود را به منظور تائید هویت خود به شما ارائه نماید . یک مهاجم ، با طرح سوالات متعدد و برقراری یک ارتباط منطقی بین آنان،می تواند به بخش هائی از اطلاعات مورد نیاز خود به منظور نفوذ در شبکه سازمان شما دستیابی پیدا نماید در صورتی که یک مهاجم قادر به اخذ اطلاعات مورد نیاز خود از یک منبع نگردد ، وی ممکن است با شخص دیگری از همان سازمان ارتباط برقرار نموده تا با کسب اطلاعات تکمیلی و تلفیق آنان با اطلاعات اخذ شده از منبع اول ، توانمندی خود را افزایش دهد .

فیشینگ از جمله واژه هایی است که توسط مهاجمان در عرصه ادبیات اینترنت مطرح و به ترغیب توام با نیرنگ کاربران به افشای اطلاعات 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 کار 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 . 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.

فصل 3:

چگونگی انجام فیشینگ

3-1- نحوه کار فیشینگ

فیشینگ در عمل به صورت کپی دقیق رابط گرافیکی یک وب سایت معتبر مانند بانک های آنلاین انجام می شود. ابتدا کاربر از طریق ایمیل و یا آگهی های تبلیغاتی سایتهای دیگر، به این صفحه قلابی راهنمایی می شود. سپس از کاربر درخواست می شود تا اطلاعاتی را که می تواند مانند اطلاعات کارت اعتباری مهم و حساس باشد، انجا وارد کند. در صورت گمراه شدن کاربر و وارد کردن اطلاعت خود، فیشرها به اطلاعات شخص دسترسی می یابند. از جمله سایت های هدف این کار می توان سایت های eBay، PayPalو بانک های انلاین را نام برد.

3-2- تکنیک های مورد استفاده در فیشینگ

3-2-1- دستکاری پیوند

در این تکنیک برای گمراه کردن کاربر از اسامی معتبری در ادرس استفاده می شود مانند استفاده از زیر دامنه اشنای gmail در www.gmail.phisher.com ، که در واقع کاربر را به سایت phisher هدایت می کند و یا استفاده از حرف @، مثلاً درwww.google.com@members.tripod.com که در واقع کاربر را به سایت members.tripod.com هدایت می کند و نه گوگل.

3-2-2- گریز از فیلتر ها

فیشر ها برای جلوگیری از شناسایی متن های متداول فیشینگ در ایمیل توسط فیلترهای ضد-فیشینگ از عکس به جای نوشته استفاده می کنند.

3-2-3- جعل وب‌گاه

برخی از فیشرها از جاوااسکریپت برای تغییر ادرس در نوار ادرس مرورگر استفاده می کنند تا هیچ جای شکی برای قربانی نماند. یک مهاجم حتی می تواند از ایراد های موجود در اسکریپت های یک سایت معتبر نیز علیه خودش استفاده کند. به این نوع حمله cross-site scripting گفته می شود. در این مورد از کاربر خواسته می شود تا در بانک خودش_لاگین کند. ظاهراً همه چیز عادی است از ادرس وب‌گاه گرفته تا گواهینامه امنیتی (security certificates) . اما در واقعیت، پیوند به ان وب‌گاه

دستکاری می شود تا با استفاده از عیب های موجود در اسکریپت های ان وب‌گاه ، حمله انجام شود. با این حال این روش نیازمند دانش و اگاهی بالایی است. از این روش در سال 2006 برای حمله به وب‌گاه PayPal استفاده شد.

3-2-4- فیشینگ تلفنی

تمام حملات فیشینگ نیازمند وب‌گاه قلابی نیست. پیامهایی که ظاهراً از طرف بانک فرستاده شده و از کاربر می خواهد تا مثلاً به دلیل وجود ایراد در حسابشان، شماره خاصی را شماره گیری کنند، نیز می تواند حمله فیشینگ باشد. بعد از گرفتن شماره (که متعلق به فیشر است و با سرویس صدا از طریق آی پی محیا شده است) ، از کاربر خواسته می شود تا شماره حساب و پین (PIN) خود را وارد کند.

3-2-5- تمرکز بر روی کاربر خاص

یکی از این روشهای فیشینگ، متمرکز شدن بر یک کاربر خاص یا یک حوزه خاص در یک تشکیلات است. نامه جعلی ظاهرا بدون هیچ مورد غیر قانونی است واز او کمک میخواهد و خواسته است تا او رمز یا رمزهای عبور و یاID خود را ارسال کند و طوری نوشته شده است که گویاشخص فرستنده تنها به شخص گیرنده این درخواست را فرستاده است.

این روش با بهره بردن از ذکر نام یک شخص حقیقی به جای یک سیستم پشتیبانی، اعتماد بیشتری را جلب میکند و گاهی از کاربر میخواهد که بهدلیل خاصی اطلاعات خود را به روز درآورده یا صحت آنها را بررسی کند .به این ترتیب جاعلان و سوء استفاده گران وارد سیستم امن شبکه یک شرکت میشوند.

3-2-6- نرم افزارهای جاسوسی

یک روشی که آخرین بار برای کاربران وبسایت گوگل اتفاق افتاد این بود که به وسیله و ترفند مختلف مانند کلیک کردن بر روی یک لینک، نرم افزارهای جاسوسی spyware وارد سیستم میکند .این جاسوس افزار که در قالب یک کد مخرب است هیچ تخریب یا عمل دیگری انجام نمی دهد .اما هنگامی که کاربر آدرس یک وبسایت مانند گوگل http://www.google.com درج می کند ؛ این نرم افزار به کار افتاده و کاربر را به صورت خودکار به یک وبسایت جعلی که مانند گوگل هست هدایت می کند حال شما می خواهید پست الکترونیکی خود در جی میل چک کنید وارد باکس جی میل البته در وبسایت جعلی شده و با وارد کردن پسوردوشناسه کاربری ؛شما پسورد وشناسه کاربری اصلی گوگل

خود را از دست می دهید یا در مواردی گوگل جعلی از شما می خواهد کـه مشخصـات یـک فـرم را پـر کنید ، و اینگونه بدون هیچ مشکلی فیشینگ می شود

فصل 4:

روشهای تشخیص فیشینگ و آنتی فیشینگ

4-1- روش‌های تشخیص فیشینگ

برخلاف فایل‌های exe مملو از ویروس یا Spyware مخفی در مرورگر، که شناسایی آنها از طریق کاربر ممکن نمی‌باشد، در این مورد کاربر با داشتن آشنایی به کدهای منبع HTML و مطاله آنها و در نهایت با بکار بردن بعضی از آدرسهای IP موجود، می‌تواند یک سایت فیشینگ را از سایت واقعی تشخیص دهد.

بسیار راحت و آسان می‌توان فهمید که گرافیک سایت فیشینگ از سروری که ادعا دارد، آمده است یا نه اما از آنجا که در بیشتر مواقع ابزارهای موجود نمی‌توانند سایت‌های فیشینگ را درست تشخیص دهند و همچنین یک کاربر معمولی هم نمی‌تواند سایت فیشینگ را شناسایی کند، بعضی از شرکت‌هایی به کمک برخی از کاربران شروع به ساختن دیتابیس‌های بزرگی از سایت‌های فیشینگ شناخته شده کردندکه خیلی زود با استقبال سایر کاربران روبه رو شد.

با وجود کاربران یاری دهنده در سراسر دنیا برای ساخت دیتابیسی کامل، روند کار و پتانسیل رشد و تشخیص فیشرها، اکنون بسیار قابل توجه می‌باشد. اما زمان، در تشخیص سایت‌های فیشینگ از همه چیز مهمتر و اساسی‌تر به نظر می‌آید، پس به روز بودن اطلاعات دیتابیس به صورت مرتب باعث می‌شود نتیجه حاصل پر بازدهتر باشد، و دقیقا این همان دلیلی است که روشهای قدیمی‌در فیشینگ، دیگر به درد فیشر نمی‌خورد.

سایت‌های Microsoft ، Google، Netcraft، Symantecو سایر سایتها معتبر دیگر محصولات و خدماتشان را با توجه به دیتابیس موجود ارائه می‌دهند تا بصورت هماهنگ این دیتابیس علیه فیشرها چک شود.

حملات فیشینگ معمولاً در قالب‌های زیر ظاهر می‌شوند:

- ایمیل از طرف فردی که ادعا می‌کند دوست یا همکار شما است.
- پیغام یا تبلیغ در شبکه‌های اجتماعی
- وب‌سایتی قلابی که که برای امور خیریه تقاضای کمک می‌کند.
- وب‌سایتی با نامی مشابه وب‌سایت‌هایی که شما متناوباً به آن‌ها سر می‌زنید.
- در برنامه‌های پیغام فوری مانند یاهو مسنجر یا ویندوز لایو مسنجر
- از طریق پیام‌های کوتاه تبلیغاتی بر روی تلفن همراه شما

چنین ای-میل هایی دارای مشخصات مشترکی هستند:

- این حملات شکل‌هایی نظیر درخواست اطلاعات از سوی بانکی قلابی، اعلام برنده‌شدن شما در قرعه‌کشی و یا پیغامی از طرف شبکه‌های اجتماعی به خود می‌گیرند.

- ایمیل‌های فیشینگ معمولاً دارای لوگوها و تیترهای رسمی از بانک‌ها یا موسسات مالی معتبر هستند و حاوی درخواست ارائه اطلاعات شخصی و حساس هستند.

- سازندگان این ایمیل‌ها معمولاً برای رسمی جلوه‌دادن بیشتر فعالیت‌های خود، لینکی از سایتی با ظاهری آراسته و رسمی به ایمیل‌های خود اضافه می‌کنند.

4-2- آنتی فیشینگ

اختلافات زیادی در زمینه بهترین راه محافظت کاربران از خطرات سایت‌های فیشینگ و نتیجه حاصل توسط آنها وجود دارد. تست نرم افزارهای آنتی فیشینگ بسیار مشکل به نظر می‌رسد، چرا که این نوع نرم افزارها کاملا نو و جدید بوده و دارای درصد ریسک بالایی می‌باشند. آخرین نسخه دو مرورگر بزرگ یعنی اینترنت اکسپلورر 7 و موزیلا فایر فاکس قابلیت آنتی فیشینگ را در خود به همراه آوردند که بسیار مورد توجه کاربران قرار گرفت. هنوز توافقی در مورد نرم افزارهای آنتی فیشینگ، برای رسیدن به یک استاندارد مشترک و توافقی

وجود ندارد. عمر بسیاری از سایت‌های فیشینگ به طور شگفت‌آوری کوتاه است. گاهی اوقات تنها تا چند ساعت بیشتر دوام ندارند.

همین طور یک نرم افزار آنتی فیشینگ تا زمانی موثر است که بصورت صحیح بتواند در کمتر از چند دقیقه سایت فیشینگ را تشخیص دهد و کاربر را آن آگاه سازد .عملا بعضی از ابزارهای آنتی فیشینگ کاملا بی‌استفاده هستند، زیرا در بسیاری از موارد به طور لحظه‌ای و برای زمانی کوتاه فیشینگ را از بین می‌برند و یا فیشینگ را در لحظه‌ای شناسایی می‌کنند که دیگر کار از کار گذشته است. سایتی به نام فیش تانک (http://www.phishtank.com) ادعا می‌کند که در تشخیص سایت‌های فیشینگ و راه‌های مقابله با آن کاربران را راهنمایی می‌کند. یکی از روش‌های لیست کردن سایت‌های فیشینگ در فیش تانک، خود کاربران می‌باشند با این توضیح که سایت‌های فیشینگ فعال یا غیر فعال که قبلا کاربر آنها را تجربه کرده‌اند را در نظر می‌گیرد و به دیتا بیس خود اضافه می‌کند. فیش تانک یک لیست کد باز است که می‌تواند منبع خوبی برای دسترسی بیشتر به سایت‌های مورد توجه فیشرها باشد و در نتیجه می‌تواند حتی هجوم فیشرها را به آن سایت‌ها افزایش دهد. تحقیقات نشان داده است که فیشینگ‌ها به طور مداوم در حال ایجاد شدن هستند، پس واضح است که ابزارهای آنتی فیشینگ باید به سمت اهدافی که دائما در حال تغییرهستند، سوق داده شوند، که این کار بسیار مشکل به نظر می‌رسد.

بعضی ابزارها یا برنامه‌ها هستند که به شما در تشخیص قلابی بودن سایت‌های اینترنتی کمک می‌کنند. البته بعضی سایت‌های خرید و فروش آن‌لاین مانند EBay دارای ابزاری به این منظور هستند. اما نرم‌افزارهای مستقل نیز به این منظور وجود دارند .

در همین راستا Yahoo و eBay در مبارزه با حملات فیشینگ در حال ارائه فناوری جدیدی هستند که ایمیل‌های جعلی را که به امضای eBay و PayPal برای کاربران ارسال می‌شود، مسدود می‌کند. eBayو PayPal بخشی از این شرکت برای پرداخت‌های روی وب، سامانه‌های انفورماتیکی خود را برای فعال کردن یک استاندارد فناوری جدید با عنوانDomainKeys (کلیدهای دامنه) که Yahoo مخترع آن است به روز کرده‌اند.

این فناوری به Yahoo این امکان را می‌دهد که مانع ورود ایمیل‌های ناخواسته (هرزنامه) مظنون به حملات فیشینگ یا حملات انفورماتیکی دیگر به صندوق پست الکترونیکی کاربران خود شود.

آیا کاربران استفاده کننده از آنتی فیشینگ باید همه سایت‌های فیشینگ را مسدود کنند یا اینکه باید صرفا به هشدار آنها دقت کنند؟ حتما در بسیار از موارد مشاهده کرده‌اید که در سایتی با پیغامی از قبیل"We are not sure about this site. Be carful" مواجه شده‌اید که معمولا به صورت pop-up می‌باشد.در بعضی موارد با بودن پیغامی از این قبیل، کاربر فقط می‌تواند زمینه سایت را ببیند و برای دیدن کل سایت حتما باید این دستور و یا اخطار توسط کاربر پذیرفته شود. در برخی اوقات هم وجود اخطار تاثیری در دیدن یا ندیدن کامل سایت ندارد و البته در بعضی موارد دیگر خود ابزار موجود در مرورگر به بهانه اینکه سایت مورد نظر آلوده است سایت را از دسترس کاربران خارج می‌کند که این کار هم به نوبه خود عجیب است.

4-3- نرم افزارهای آنتی فیشینگ

نرم افزارهای آنتی فیشینگ که سایت‌های فیشینگ را مسدود می‌کنند مزیت‌ها و معایب خاص خود را دارند. که در ادامه به توضیح هر چه بیشتر آنها می‌پردازم. [1]

IE & Windows Live Toolbar -1-3-4

مایکروسافت فناوری آنتی فیشنگ را در مرورگر IE7 ایجاد کرده و قابلیت نصب را برای IE6 با فناوری یکسان از طریق نوار ابزارWindows Live Toolbar فراهم آورده است. ظاهرا فیلتر IE7 و نوار ابزار مذکور در دیتابیسی واقع در سایت مایکروسافت در ارتباط هستند. مورد دیگری که در کار آنتی فیشینگ IE7 و نوار ابزار جدید وجود دارد این است که هیچ تغییری در سرعت لود صفحات در هنگام فعال بودن فیلتر مذکور دیده نمی‌شود که بسیار حائز اهمیت است. اما باید به این نکته توجه کنیم که طبق تحقیقات موجود، آنتی فیشینگ مایکروسافت در 51 درصد موارد درست عمل کرده که کمی‌عملکرد این فیلترها را زیر سئوال می‌برد.

FireFox & Google Toolbar-2-3-4

همان‌طور که می‌دانید گوگل و موزیلا رابطه خوبی با هم دارند. گوگل بی شک تجربه‌های زیادی در زمینه ساخت دیتابیس‌های گوناگون از وب سایت‌ها مختلف دارد.

پس تعجبی ندارد، اگر بگویم جمع آوری و تشکیل لیستی در زمینه سایت‌های فیشینگ هم برای این شرکت عظیم چندان مشکل نبوده و قرار دادن این لیست کامل در فایر فاکس هم کار مشکلی به نظر نمی‌آید. جالب است بدانید که فیلترهای آنتی فیشینگ موجود در فایر فاکس در هر ساعت دوبار به روز می‌شود که با توجه به سرعت ایجاد فیشرهای جدید این عمل در نوع خود بی نظیر است. سیستم گوگل ابزار (Google Toolbar) فایرفاکس بسیار کارآمد و مسدود کننده می‌باشد. که بر طبق آمار حدود 85 در صد از سایتهای فیشینگ را به خوبی تشخیص می‌دهد.

Toolbar Net Craft-3-3-4

این ابزار بصورت کارشناسانه‌ای ایجاد شده است که بسیار موثر است و جالب‌تر آنکه هم قابلیت نصب در اینترنت اکسپلورر و هم در دسترس فایر فاکس می‌باشد NetCraft .بر طبق آمار از 95 درصد فیشینگ‌ها بدون هیچ خطایی جلوگیری می‌کند.این ابزار حتی سایتهای فیشینگی که به اصطلاح ماسک زده اند وچهره خود را تغییر داده اند را شناسایی کرده و به کاربر گزارش می‌دهد.

NC Toolbar -4-3-4

NCکه در واقع مخفف کلمه Norton Confidential می‌باشد، محصول شرکت Symantec است که ابزاری کارامد در زمینه آنتی فیشینگ به حساب می‌آید. در آزمایشی که برای این ابزار به عمل آمد 76 درصد سایت‌های فیشینگ را به صورت کامل بسته و 21 درصد را نیز با هشداری شدید نشان داد و تنها حدود4 ، 2در صد از سایت‌های فیشینگ را از دست داد که این رقم اصلا به حساب نمی‌آیدNC.فقط با IEکار می‌کند اما شرکت تولید کننده گفته است که در نظر دارد این محصول را برای سایر مرورگرهای وب ایجاد کند. در این ابزار همچنین یک فرم خودکار برای رهایی از دستKegloger ها هم تعبیه شده که نقطه قوتی برای این ابزار به حساب می‌آید.

eBay Toolbar -5-3-4

به نظر می‌رسد که بیشتر فیشرها تمایل دارند که به سایت‌های تجاری و بخصوص سایت ebay وارد شوند. به همین دلیل سایت ebay خود دست به کار شده و ابزاری ایجاد کرد که با آنها به مبارزه بپردازد. نوار سبز در ابزار مخصوص این شرکت نشان دهنده درست بودن سایت اصلی می‌باشد. اگر نوار مذکور مضر تشخیص داده شود این نوار قرمز خواهد شد و در صورتی که رنگ نوار به رنگ خاکستری تبدیل شود یعنی سایت برای ابزار تعرف نشده است و حالت خنثی دارد. ابزار ebay 90 درصد ازفیشینگ‌ها را مسدود می‌کند، پس اگر از ebayاستفاده می‌کنید شما توسط ابزارهای آن محافظت می‌شوید اما برای محافظت از حساب‌های دیگرتان مواظب حیله‌های فیشرها باشید .این ابزار بسیار کارآمد است اما همان‌طوری که گفتم مخصوص خود شرکت ebay است.

GeoTrust Toolbar -6-3-4

این ابزار هم که فعلا فقط برای IE موجود است دارای ظاهری مناسب بوده اما کارای آن کمی ضعیف می‌باشد. در آزمایش‌هایی که بر روی این ابزار انجام گرفته تنها در 32 درصد موارد خود را موفق نشان داده، اما این ابزار جای زیادی برای رشد دارد چون کاربران زیادی به طرف این ابزار تمایل دارند.

EarthLink Toolbar -7-3-4

این ابزار هم برای دو مرورگر یاد شد موجود است، اما با وجود جذابیت زیادی که دارد متاسفانه از قدرت مناسبی برای دفع فیشرها برخوردار نیست. و بیشتر حالت گرافیکی دارد تا کارایی.

Trust Wach Toolbar -8-3-4

نوار ابزار یاد شده دارای یک block بزرگ رنگی می‌باشد که به فیشینگ بودن سایت اشاره دارد. رنگ سبز در این ابزار به معنی آن است که سایت بررسی شده، رنگ زرد به معنی آن است که سایت بررسی

نشده و در نهایت رنگ قرمز نشان دهنده آن است که سایت فیشینگ است و شما را تهدید می‌کند. قدرت آنتی فیشینگ این ابزار چندان تعریفی ندارد اما این ابزار آدرسی دقیق از سایت جاری را به کاربر می‌دهد و قابلیت ورود آدرس امنیتی کاربر در این ابزار وجود دارد.

Mcafee Site Advisor -9-3-4

زمانی که از آنتی هکرهای تجاری صحبت می‌شود نام مکافی درخشش خاصی در بین سایر رقبا پیدا می‌کند، بویژه در زمینه آنتی ویروس، آنتی اسپم و.... اما باید اشاره کنم که این محصول مکافی، در زمینه آنتی فیشینگ کاربرد آنچنانی ندارد و حتی مسئولین خود شرکت به صراحت اشاره کرده‌اند که این محصول فعلا کارایی آنچنانی در زمینه فیشینگ ندارد.

CoreStreet Spoot Stick -10-3-4

برای هر دو مرورگر IE و Firefox موجود می‌باشد. قدرت این ابزار در حد مناسبی می‌باشد اما قدرت برسی صفحات pop-up را ندارد و با آنها دچار مشکل می‌باشد..

Earthlink ScamBlocker -11-3-4

نوار ابزار رایگان برای اغلب مرورگرها که فهرستی از معروف‌ترین سایت های کلاهبرداری را در اختیار دارد و به محض این‌که بخواهید به سراغ آن‌ها بروید، به شما هشدار می‌دهد. این ابزار هم فقط برای مقابله با سایت‌های تقلبی شناخته شده مناسب است .

webRoot Phish Net -12-3-4

برنامه‌ای رایگان که با اینترنت اکسپلورر نسخه 5 به بالا سازگار است. این برنامه داده‌های حساس شما از قبیل رمزهای عبور، اطلاعات بانکی، شماره تأمین اجتماعی و اسامی کاربری را از شما می‌گیرد و داخل

خود نگهداری می‌کند و هر زمان که برنامه‌ای بخواهد به آن‌ها دسترسی پیدا کند، به شما اطلاع می‌دهد.

درباره انتخاب آنتی فیشر باید بگویم که این انتخاب می‌تواند تحت تاثیر نوع مرورگر شما باشد اما اگر مرورگر در انتخاب شما تاثیر ندارد به شما ابزار Toolbar Net Craftرا پیشنهاد می‌کنیم که هم برای دو مرورگر IE و Firefox موجود است و هم دارای قابلیت مناسبی می‌باشد و در عین حال رایگان می‌باشد . NCهم بسیار کاربردی است اما دقت کنید که فعلا فقط برای مرورگر IE وجود دارد و در ضمن رایگان هم نمی‌باشد.

نصب ابزارهای آنتی فیشینگ در کامپیوترهای معمولی باعث کاهش سرعت می‌شوند و این روند تقریبا در همه آنها یکسان و طبیعی می‌باشد.اما این کاهش در کامپیوترهای پرسرعت به چشم نمی‌خورد. اما با توجه به ارزشی که این نوع ابزارها دارند ارزش نصب آنها بسیار بیشتر از هر چیز دیگر می‌باشند.

فصل 5:

فیشرها و راه های حفاظت از هویت

5-1-فیشرها

چه کسی در پشت فیشینگ است و چرا افرادی که در پس پرده فیشینگ هستند متخصصین جعل اینترنتی هستند .آنها به معنای واقعی کلمه میلیونها ای - میل جعلی را پست می کنند به امید اینکه در نهایت تعداد اندکی به آنها پاسخ داده و اطلاعات خود را در اختیارشان قرار دهند.

یکی از شیوه‌هایی که فیشرها ها به کار می‌برند و از شیوه‌های دیگرشان پیچیده‌تر استو نیاز به روش‌های مشخص و شناسایی هوشمندانه‌تری دارد استفاده از نرم‌افزارهایی است که آدرس‌های وب‌های قلابی و جعلی را درون سایت‌های معتبر به‌گونه‌ای پنهان می‌کنند که کاربر متوجه آنها نمی‌شود. بدین‌ترتیب که این دزدان لوگوها و تصاویری را از سایت‌های معتبر، درون سایت قلابی خود کپی می‌کنند و بعد هم کدهای مخرب خود را درون این سایت‌ها می‌گنجانند، به‌گونه‌ای که شما به نشانی درستی می‌روید اما در حقیقت اطلاعات خود را درون یک پنجره که توسط هکرها در این سایت تعبیه شده وارد می‌کنید.

درحقیقت درون یک سایت معتبر و قانونی یک فعالیت غیرقانونی شکل گرفته است که شما هم قربانی همین فعالیت شده‌اید.

5-2- راه‌هایی برای حفاظت از هویت

- در طی سال، دوبار گزارش مالی حساب‌تان را دریافت کنید تا همه چیز تحت کنترل باشد.

- روی لینک‌ها یا تصاویر ایمیل‌هایی که از واقعی بودن آن‌ها اطمینان ندارید، کلیک نکنید. اگر از شرکتی که با آن کار می‌کنید، نامه‌ای دریافت کردید، مستقیماً به سایت آن شرکت بروید و به حسابتان داخل شوید. در غیراین‌صورت بهتر است با آن‌ها تماس تلفنی بگیرید.

- از برنامه‌های ضد اسپم مناسب استفاده کنید. به این طریق بسیاری از ایمیل‌های فریبکارانه هرگز به صندوق‌پستی شما وارد نخواهند شد.

● نرم‌افزارهای جاسوس‌یاب روی کامپیوترتان نصب کنید. استفاده از برنامه‌هایی مانند spybot search Destroy و Lavasoft Ad-Aware دو نمونه خوب از چنین برنامه‌هایی هستند.

● از یکی از شرکت‌های بزرگ، سرویس زیر نظر داشتن اعتبار (Credit Monitoring) را خریداری کنید. این سرویس‌ها با چیزی حدود پنجاه دلار در سال قابل تهیه هستند و با ارسال ایمیل، تغییرات انجام شده در حساب شما را اطلاع می‌دهند.

● برداشت‌های کارت اعتباری‌تان را کنترل کنید. بسیاری از کلاهبرداران، در طی مدت زمان طولانی، اقدام به برداشت مبالغ اندکی می‌کنند تا توجه دارنده کارت به تغییرات حساب جلب نشود.

● اطلاعات کارت اعتباری را روی هارددیسک نگهداری نکنید و در صورت لزوم آن‌ها را روی CD ذخیره نمایید. آن CD هم نباید در درایو کامپیوتر باشد. در واقع اگر شما از اطلاعات استفاده نکنید، هکرها هم به آن‌ها دسترسی نخواهند داشت. اگر هم ناچار به نگهداری آن‌ها روی هارددیسک کامپیوتر هستید، از رمز عبور برای حفاظت از آن‌ها بهره بگیرید.

● حتی‌الامکان شماره تأمین‌اجتماعی خود را مخفی نگه دارید. اگر شرکت‌های اعتباری از آن شماره به عنوان بخشی از شماره حساب شما استفاده می‌کنند، درخواست کنید که آن را تغییر دهند.

●اگر نسبت به پیغامی شک دارید آنرا تائید نکنید و از پیوندهای های ارسالی آن استفاده نکنید. در عوض به شرکت تلفن زده و یا مستقیما به سایت آنها بروید.

●از پر کردن فرمهایی که توسط نامه برای شما رسیده و اطلاعات اعتباری و شخصی شما را می خواهند اجتناب کنید و برای اطمینان از واقعی بودن سایت، آدرس داده شده بصورت پیوند را جداگانه و در یک مرورگر با پیشوند "http//:" یا "https//:" امتحان کنید.

●بطور دوره ای و مرتب به حساب خود سر بزنید، یعنی آنرا برای مدت طولانی بدون کنترل رها نکنید.

●مرتبا بانک، اعتبار و بدهی خود را کنترل کرده تا از عملیات انجام شده و صحت و سقم آن اطلاع حاصل نمایید. اگر مورد مشکوکی مشاهده شد فورا موضوع را به بانک و سایر موسسات اعتباری که عضو آنها هستید اطلاع دهید.

●اطمینان حاصل کنید که مرورگر شما به روز بوده و تمام برنامه های اصلاحی (Patch) آن نصب شده اند. کاربرانی که از مرورگر مایکروسافت استفاده می کنند باید هرچند وقت یکبار (زود به زود) به سایت مایکروسافت مراجعه کرده و برنامه های اصلاحی های مرتبط با Phishing را برداشته و روی سیستم شان نصب نمایند.

●همیشه نامه های مربوط به حملات Phishing و کلاهبرداری را به گروههای زیر ارسال نمایید :

reportphishing@antiphishing.com

spam@uca.gov

5-3- باز پس‌گیری هویت

برای قربانیان دزدی هویت، تشخیص سریع مشکل بسیار مهم است. طبق گزارش FTC، زمانی که قربانیان متوجه سوءاستفاده‌هایی از اطلاعات شخصی خود در طول یک ماه شدند، حدود 90 درصدشان قادرند که از ایجاد حساب‌های اعتباری جدید با استفاده از نامشان که توسط دزدان صورت می‌گیرد جلوگیری کنند و از زیان‌های جدید پیشگیری کنند. اما اگر زمان تشخیص از یک ماه به 6 ماه برسد، یعنی قربانی طی 6 ماه متوجه سوءاستفاده از حساب اعتباری خود نشود، در طول این مدت حدود 45درصد مجرمان با استفاده از نام قربانی حساب‌های اعتباری جدید می‌گشایند. شاید اولین مانع بر سر راه تشخیص و دستگیری دزدان متقاعد کردن شرکت‌های کارت‌های اعتباری، آژانس‌های تهیه گزارش از حساب‌های اعتباری و بعضی اوقات افراد متخصصی هستند که شما باید برایشان توضیح دهید که چه کسی هستید و چه اتفاقی برایتان افتاده است. فرآیند تشخیص و دستگیری با تهیه یک گزارش پلیسی از حوزه‌ای که جرم در آن اتفاق افتاده شروع می‌شود. اصولاً

متقاعد کردن پلیس برای این‌که شما یک قربانی هستید یا یک گناهکار، کار ساده‌ای است. البته FTC گزارش داده است که قربانیان با مقاومتِ پلیسِ محلی، برای تهیه گزارش مواجه می‌شوند. 28درصد افراد هم از عملکرد پلیس بسیار ناراضی هستند. گرفتن گزارش بسیار واجب و ضروری است حتی اگر لازم باشد شما به ادارات مختلف پلیس محلی یا پلیس کشوری و یا حتی مأمورین ایالاتی مراجعه کنید. تا اگر پلیس دزدان را دستگیران نمود، شما با استفاده از همان گزارش، مؤسسات مالی را قانع به پاکسازی سابقه حساب اعتباری خود کنید. همچنین شما باید با سرعت درخواست fraud alert (هشدار کلاهبرداری) که برای قربانیان مجانی است، بکنید. با یک alert fraud، شرکت‌هایی که اعتباری با نام شما ایجاد کرده‌اند باید قبل از افتتاح اعتبار با شما تماس بگیرند و شما اعتبار آن حساب را تأیید یا رد کنید. سپس شما باید یک سری نامه و گزارش تهیه شده توسط پلیس را برای مأموران مربوطه می‌فرستید.

این نامه‌ها را می‌توانید از سایت‌های www.consumer.gov/idtheft یا www.identitytheft.org تهیه نمایید.

قربانیانی که همه فعالیت‌های بالا را انجام بدهند می‌توانند امیدوار باشند که قبل از یک‌ماه حساب اعتباری خود را پاکسازی نمایند و به زندگی عادی خود بازگردند. اما از این به بعد باید بیشتر مواظب باشند و جهان اطراف خود را محتاطانه‌تر بنگرند. [2]

مراجع

مراجع

[1] سید فیروز ایازی ، "نرم افزارهای آنتی فیشینگ" ، رایانه خبر، شماره32، 1386

http://www.ictna.ir/[2]