

نوار ابزار ضد فیشینگ علم و صنعت

علیرضا صابری
دانشگاه علم و صنعت ایران
a_saberi@comp.iust.ac.ir

سید حسین سیادتی
دانشگاه علم و صنعت ایران
s_h_siadaty@comp.iust.ac.ir

محسن شریفی
دانشگاه علم و صنعت ایران
msharifi@iust.ac.ir

چکیده: فیشینگ یک حمله اینترنتی است که هم از بعد تعداد و هم از لحاظ نوع در حال افزایش است. در این مقاله ما طرحی برای یک نوار ابزار افزودنی به مرورگر اینترنتی مایکروسافت ارایه نموده‌ایم که کاربران را در زمان مواجهه با سایت های بدکار کمک می‌کند تا تشخیص دهند که با یک سایت درست یا فیشینگ مواجه می‌باشند. در صورتیکه نوار ابزار تشخیص دهد که کاربر با یک سایت فیشینگ مواجه می‌باشد، با ارایه چند لینک پیشنهادی به وی کمک می‌کند که مسیری به سایت درست مورد نظر خود بیابد. این نوار ابزار بر اساس یک الگوریتم ابداعی کار می‌کند که با دقت خوبی سایت‌های فیشینگ را تشخیص می‌دهد.

واژه‌های کلیدی: امنیت وب، فیشینگ، نوار ابزار ضد فیشینگ

۱- مقدمه

می‌باشد. صفحه فیشینگ از کاربر درخواست می‌کند تا اطلاعات شخصی‌اش مانند کلمه عبور مربوط به بانک یا اطلاعات کارت اعتباری‌اش را در صفحه وارد نماید و آن‌ها را ارسال نماید. تعداد حملات فیشینگ به سرعت افزایش یافته است. با توجه به گزارش های گروه ضد فیشینگ [1] APWG، تعداد سایت‌های فیشینگ یکتا ۳۷۴۴۴ سایت در اکتبر سال ۲۰۰۶ اعلام شده است درحالیکه تعداد سایت‌های فیشینگ یکتا در اکتبر ۲۰۰۵ به تعداد ۴۳۶۷ عدد گزارش شده بود. همچنین تعداد سایت‌های فیشینگ گزارش شده در اکتبر ۲۰۰۶ نسبت به یک ماه قبل آن ۵۲٪ رشد نشان داده است. علاوه بر این تعداد کمپانی‌هایی که تحت این حمله بوده‌اند ۱۷۶ کمپانی در اکتبر

حمله فیشینگ یک روش برای دزدی اطلاعات است که هدف آن اغفال کاربران به منظور دزدیدن اطلاعات خصوصی آن‌ها اعم از نام کاربری، کلمه عبور و اطلاعات مربوط به حساب‌های بانکی می‌باشد. سپس، اطلاعات ربوده شده مورد سوء استفاده مالی قرار می‌گیرد. یک حمله فیشینگ با یک نامه الکترونیکی شروع می‌شود. این نامه ادعا می‌کند که از یک کمپانی معتبر مانند eBay می‌باشد. محتویات نامه کاربر را ترغیب می‌کند تا بر روی لینکی که در نامه الکترونیکی وجود دارد کلیک نماید. لینک بدکار، کاربر را به یک صفحه غیر قانونی هدایت می‌کند که ظاهراً شبیه سایت یک کمپانی معتبر است. این صفحه، یک صفحه فیشینگ

۲۰۰۶ گزارش شده است درحالیکه تعداد این کمپانی ها در اکتبر ۲۰۰۵، ۹۶ مورد بوده است.

هر سایت فیشینگ هزاران یا صدها کاربر را فریب می دهد. تنها در سال ۲۰۰۳، حملات فیشینگ به صورت مستقیم موجب از دست رفتن ۱،۲ بیلیون دلار برای بانک های آمریکا و فراهم کنندگان کارت های اعتباری شده است [2]. حدود ۵٪ از بزرگسالان آمریکا که کاربران اینترنت هستند هر ساله بصورت موفقیت آمیز مورد هدف حملات فیشینگ قرار می گیرند [3].

۲- کارهای مرتبط

تاکنون تحقیقات بسیاری جهت ارائه راه حل هایی برای مقابله با حمله فیشینگ ارائه شده است. روش های ارائه شده تلاش می کنند تا حمله را در یک قسمت از مسیر متوقف نمایند. روش های سمت مشتری تلاش می کنند در هنگام مواجهه کاربر با یک سایت فیشینگ به کاربر هشدار دهند تا وی را از تعامل با سایت فیشینگ بازدارند. این روش ها را می توان در سه گروه مبتنی بر کاربر، مبتنی بر حافظه مرورگر و مبتنی بر لیست سیاه دسته بندی نمود.

۱-۲ روش های مبتنی بر کاربر

این نوع از روش ها با محاسبه و نشان دادن اطلاعاتی خاص از سایتی که کاربر با آن مواجه است تلاش می کنند تا در صورتیکه کاربر با یک سایت فیشینگ در تعامل است، بر اساس اطلاعات نمایش داده شده، از این امر اطلاع یافته و از ادامه کار با سایت مذکور منصرف شود. در این روش ها کاربر نقش اساسی در تصمیم گیری و شناخت سایتی که با آن روبرو می باشد ایفا می نماید و ابزارهای ارائه شده به کاربر تنها معرف هایی را ارائه می نمایند تا تصمیم گیری وی را آسان نمایند. در واقع این روش ها سعی می نمایند فاصله بسیار زیاد مابین کاربران و مفاهیم امنیت در سیستم های کامپیوتری را بوسیله ترجمه یا نمایش مفاهیم سیستم های کامپیوتری با نمادها و روش های قابل فهم برای کاربران عادی، کاهش دهند و تشخیص و تصمیم گیری کاربران را آسان نمایند.

ابزارها و تکنیک های که در این گروه قرار می گیرند، عبارتند از:

- [4] Spoof Stick
- [5] Trustbar
- [6] Passmark
- [7] DSS

۲-۲ روش های مبتنی بر حافظه مرورگر

این روش ها از تاریخچه سایت هایی که یک کاربر با آن ها در تعامل بوده است برای راهنمایی کاربر و هشدار به وی در مواجهه با سایت های فیشینگ استفاده می نمایند. مراجع [8, 9] از جمله نوار ابزارهایی می باشند که به این روش کار می کنند.

۲-۳ روش های مبتنی بر لیست سیاه

این روش ها از روش های شناسایی سایت های فیشینگ و یا استفاده از لیست های سیاه سایت های فیشینگ، جهت هشدار به کاربران در هنگام مواجهه با این نوع سایت ها استفاده می نمایند.

نوارابزارها می که از لیست سیاه برای تشخیص سایت فیشینگ استفاده می نمایند، شامل موارد زیر می باشند.

- [10] Sanitizing Proxy System
- [11] SpoofGurad
- [12] Cloudmark
- [13] Earthlink
- [14] eBay Toolbar
- [15] TrustWatch
- [16] Google Safe Browsing
- [17] SiteAdvisor
- [18] NetCraft
- [19] Netscape 8.1

۳- الگوریتم علم و صنعت برای تشخیص صفحات

فیشینگ

صفحات وب وابستگی خود به یک کمپانی را با بکار بردن آرم کمپانی نشان می دهند. صفحات فیشینگ نیز برای فریب کاربران با بکاربردن آرم کمپانی قربانی سعی به فریب کاربران دارند. بنابر این با استفاده از آدرس اینترنتی یک صفحه و نام کمپانی ظاهر شده در آرم صفحه وب و اجرای یک الگوریتم می توان صفحات فیشینگ را تشخیص داد. این الگوریتم به عنوان پارامتر

ورودی، یک آدرس اینترنتی و نام یک کمپانی را دریافت می‌نماید و هدف آن این است که بررسی نماید که آیا این آدرس اینترنتی مربوط به کمپانی مذکور است یا خیر.

این الگوریتم نام کمپانی را در یک موتور جستجوی قوی مانند گوگل جستجو می‌نماید و تعدادی از نتایج جستجو -مثلا ۱۰ تای اول- را بررسی می‌نماید. سپس الگوریتم، نام دامنه آدرس اینترنتی صفحه را با نام دامنه نتایج گوگل مقایسه می‌نماید. اگر یکی از عناصر نتیجه جستجو و آدرس اینترنتی صفحه در یک دامنه باشند، آدرس اینترنتی مربوط به یک صفحه درست می‌باشد در غیر این آدرس اینترنتی متعلق به یک صفحه فیشینگ می‌باشد.

روال شکل ۱ نحوه کار این الگوریتم را بصورت بهتری نشان می‌دهد. الگوریتم، یک آدرس اینترنتی و نام کمپانی را به عنوان ورودی می‌گیرد و در صورتی که صفحه فیشینگ باشد True و در غیر این صورت False بر می‌گرداند.

الگوریتم از تعدادی روال استفاده می‌نماید که آن‌ها را در اینجا بصورت دقیق‌تر بررسی می‌نماییم.

• GoogleSearch

این تابع کلمه کلیدی را در گوگل جستجو می‌نماید و ۱۰ آدرس اول را بر می‌گرداند. این تابع از رابط برنامه نویسی گوگل [20] برای جستجو در گوگل استفاده می‌نماید.

• AreInSameDomain

این تابع دو آدرس اینترنتی را به عنوان ورودی دریافت می‌نماید و بررسی می‌کند که آیا دو آدرس به یک سایت وب متعلق هستند یا خیر.

محاسبه اینکه چه صفحاتی به یک سایت وب متعلق می‌باشند یک مساله باز است با وجود این روشهای تخمینی برای این کار ارایه شده است. ما هر سایت را با صفحاتی که در یک دامین می‌باشند تخمین می‌زنیم.

یک آدرس اینترنتی مانند <http://iust.ac.ir> از چند قسمت تشکیل شده است که از راست به چپ نشان دهنده دامنه هابی است که یک سایت وب در آن سلسله مراتب قرار دارد. به دامنه iust.ac.ir، دامنه سطح اول، [ac](http://ac.iust.ac.ir) دامنه سطح دوم، [iust](http://iust.ac.ir) دامنه سطح سوم یا نام سایت می‌گویند. برای بررسی اینکه آیا دو صفحه متعلق به یک دامنه هستند یا نه از دامنه سطح اول شروع می‌نماییم. اگر دامنه های سطح اول دو آدرس اینترنتی متفاوت باشند آن‌ها به یک سایت وب متعلق نمی‌باشند. اگر آندو یکسان باشند به سراغ دامین سطح دوم می‌رویم. اگر آنها متفاوت باشند نتیجه می‌گیریم که دو آدرس اینترنتی متعلق به دو سایت وب مجزا هستند. در غیر این صورت دامنه سطح سوم را با هم مقایسه می‌نماییم. اگر قسمت سوم با هم برابر باشند دو صفحه در یک دامنه هستند و اگر نه دو صفحه متعلق به یک وب سایت نمی‌باشند.

برای مثال دو آدرس اینترنتی www.iust.ac.ir و www.iut.ac.ir را در نظر بگیرید. دامنه سطح اول و دوم برابر هستند بنابر این به سراغ [iut](http://iut.ac.ir) و [iust](http://iust.ac.ir) می‌رویم. به این دلیل که آنها یکسان نیستند این دو آدرس متعلق به یک سایت وب نیستند. البته این روش مقایسه یک روش مقایسه ساده است و در برخی حالات پیچیده مانند سایت های وبی که میزبان سایت های دیگر می‌باشند دچار اشتباه می‌شود. به عنوان مثال members.aol.com یک مجموعه از سایت های افراد و سازمان های کوچک می‌باشد و آدرس این وب سایت ها یک زیر دامنه از aol.com می‌باشد. در چنین موارد خاصی، روش ما در تشخیص اینکه هر یک از این زیر دامنه ها متعلق به سایت های مجزایی می‌باشند دچار اشتباه می‌شود.

```
1: Procedure Boolean ISPhishingPage( String varURL, String varCompanyName )
2: varGoogleResults = GoogleSearch( varCompanyName , 10 )
3: for i = 1 to 10
4: BEGIN
5:   varGResultURL = varGoogleResults[i].URL
6:   if( AreInSameDomain( varURL, varGResultURL ) )
7:     return False
8: END
9: return True
```

شکل ۱: برنامه مربوط به الگوریتم شناسایی یک صفحه فیشینگ

۴- نوار ابزار ضدفیشینگ علم و صنعت

نوار ابزار ضدفیشینگ علم و صنعت بصورت یک ابزار افزودنی به مرورگر اینترنت اکسپلورر می‌باشد. شکل ۲ نشان دهنده رابط کاربر این نوار ابزار است.

هنگامی که کاربر با یک سایت مواجه می‌شود در صورتیکه بخواهد بررسی نماید که آیا با یک سایت درست یا فیشینگ مواجه است کافی است که نام کمپانی ای که صفحه ادعا می‌نماید که به آن متعلق است را در جعبه متن نوار ابزار وارد نماید و دکمه Go را فشار دهد. در این صورت نوار ابزار با اجرای الگوریتم مذکور تشخیص می‌دهد که آیا با یک سایت درست یا فیشینگ مواجه است.

در صورتیکه صفحه، سالم تشخیص داده شود پیغامی ظاهر می‌شود که وی را از این امر مطلع می‌نماید.

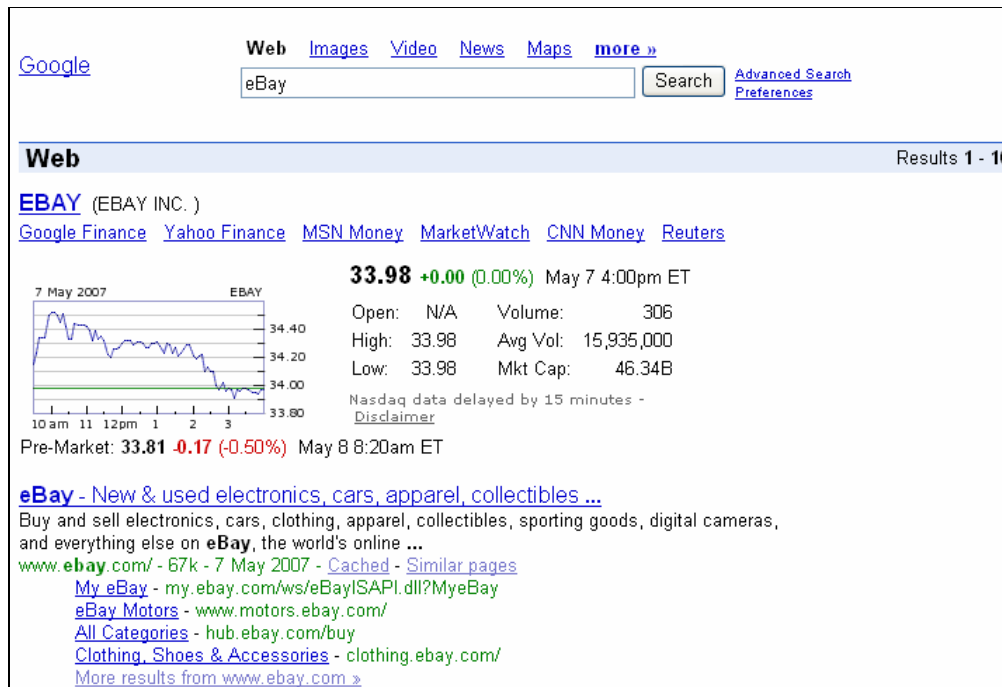
در صورتیکه صفحه، فیشینگ تشخیص داده شود یک پیغام برای کاربر نشان داده می‌شود و وی را از این امر مطلع می‌سازد. علاوه بر این نوار ابزار ما برای کاربر چند لینک پیشنهادی ارائه می‌دهد که سایت درست مورد نظر کاربر یکی از آنها می‌باشد. شکل ۳ نمای ظاهری نوار ابزار را در هنگام مواجهه کاربر با یک سایت فیشینگ نمایش می‌دهد. در صورتیکه کاربر گزینه "مشاهده پیشنهاد ما" را انتخاب نماید به یک صفحه از سایت گوگل ارجاع داده می‌شود که ۱۰ لینک را برای کاربر نمایش می‌دهد. یک صفحه پیشنهادی برای کاربری که با سایت فیشینگ مربوط به سایت eBay مواجه شده است در شکل ۴ نمایش داده شده است.



شکل ۲: نوار ابزار ضدفیشینگ علم و صنعت



شکل ۳: نوار ابزار ضدفیشینگ علم و صنعت در مواجهه با سایت فیشینگ



شکل ۴: پیشنهاد نوار ابزار علم و صنعت به کاربر

۵- ارزیابی و مقایسه

ما الگوریتم خود را با دو مجموعه از صفحات وب آزموده ایم. تا میزان خطای مثبت و منفی این نوار ابزار را محاسبه نماییم. یک مجموعه شامل تعدادی سایت درست و قانونی می‌باشد و مجموعه دیگر شامل مجموعه ای از صفحات فیشینگ می‌باشد. از نمونه های سایت درست برای محاسبه میزان خطای مثبت و از نمونه های فیشینگ برای محاسبه میزان خطای منفی این روش استفاده می‌شود. نکته مهم این است که تعداد عناصری از گوگل که در الگوریتم پیاده سازی شده بررسی شده است ۲۰ عنصر می‌باشد.

برای اندازه گیری درست میزان خطای مثبت نوار ابزار، نمونه های مجموعه سایت های درست باید به یک روش نمونه گیری یکنواخت از وب انتخاب شود. ما این مجموعه را با استفاده از یک روش نزدیک به نمونه گیری یکنواخت ایجاد نموده ایم. برای انجام این کار از یک لغتنامه انگلیسی استفاده می‌شود و بصورت متوالی کلماتی را بصورت تصادفی از آن انتخاب می‌نمایند. هر یک از کلمات در گوگل جستجو می‌شود و چند پیوند از نتایج گوگل به عنوان آدرس های اینترنتی صفحات نمونه انتخاب می‌شوند.

ما برای ایجاد نمونه یکنواخت، از الگوریتم مذکور استفاده نموده ایم. لغتنامه مورد استفاده حاوی ۱۵۰۰۰۰ کلمه می‌باشد و با انتخاب هر کلمه تصادفی، ۵۰ پیوند اول مربوط به نتایج گوگل را به عنوان نمونه انتخاب نموده ایم و با این روش ۵۰۰ صفحه از صفحات وب را به عنوان نمونه انتخاب نموده‌ایم.

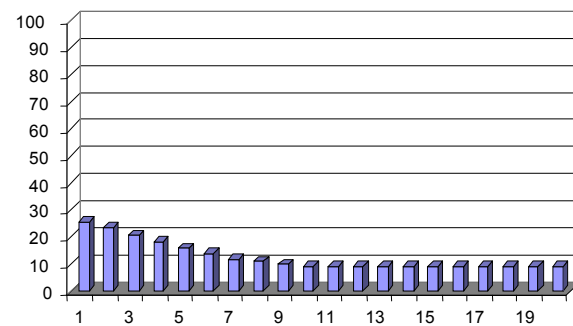
برای محاسبه میزان خطای منفی از ۳۰ نمونه از صفحات فیشینگ را به عنوان ورودی به الگوریتم خود دادیم. این نمونه ها بصورت تصادفی در سپتامبر ۲۰۰۶ از گزارش های فیشینگ گروه [21] PIRT انتخاب شده‌اند.

روش انجام آزمون به این صورت بوده است که ما هر یک از آدرس های اینترنتی از هر مجموعه را در میله آدرس مرورگر وارد نمودیم تا صفحه مربوط به آن در مرورگر نشان داده شود. سپس، از ظاهر صفحه و با استفاده از آرم صفحه نام کمپانی ای که صفحه ادعا می‌کند که به آن متعلق است را در جعبه متن نوار ابزار علم و صنعت وارد نموده ایم. نوار ابزار با توجه به الگوریتم پیاده سازی شده نتیجه را باز می‌گرداند.

حاصل انجام آزمون بر روی نمونه های مذکور نشان می‌دهد که میزان خطای منفی روش ما صفر درصد می‌باشد و این بدان

معنی است که روش ما قادر است تمام صفحات فیشینگ را تشخیص دهد. دلیل این امر این است که با وجود اینکه سایت های فیشینگ از نام کمپانی مورد حمله در محتویات خود استفاده می نمایند اما با توجه به الگوریتم **Pagerank** مربوط به گوگل نمی توانند رتبه بالایی را نسبت به صفحات سایت اصلی و سایت های مرتبط با کمپانی اصلی بدست آورند. الگوریتم **Pagerank** گوگل علاوه بر شاخص گذاری صفحات بر اساس کلماتی که بکار می برند از نحوه ارجاع صفحات وب به یکدیگر برای بررسی میزان معتبر بودن یک صفحه و رتبه بندی صفحات استفاده می نماید. با توجه به اینکه صفحات فیشینگ توسط صفحات معتبری در وب ارجاع داده نشده اند بنابر این در جستجوی گوگل رتبه بالایی ندارند و در نتیجه هنگامی که الگوریتم ما نتایج بالای گوگل را بررسی می نماید پیوند مربوط به سایت فیشینگ در بین این نتایج ظاهر نمی شود. میزان خطای مثبت الگوریتم ما ۹٪ می باشد و این بدین معنی است که در ۹٪ از موارد، الگوریتم ما به اشتباه یک سایت درست را فیشینگ تشخیص می دهد. البته این میزان خطا با کاهش تعداد عناصری از گوگل که الگوریتم مورد بررسی قرار می دهد افزایش خواهد یافت. نمودار شکل ۵ میزان خطای مثبت نوار ابزار را بر اساس تعداد عناصر مورد بررسی از نتایج گوگل نشان می دهد.

درصد خطای مثبت



تعداد عناصر مورد بررسی از نتایج گوگل

شکل ۵: میزان خطای مثبت نوار ابزار علم و صنعت - براساس تعداد عناصر مقایسه شده از گوگل

معنی است که هنگامی که ما الگوریتم تخمینی خود را روی یک سایت فیشینگ اعمال می نمایم، اولین عنصر در نتایج گوگل که به کاربر جهت پیشنهاد نشان می دهیم با احتمال ۷۴/۴٪ آدرس اینترنتی سایتی است که مورد نظر کاربر بوده است. علاوه بر آزمون فوق، ما ۴ نوار ابزار اسپوف گارد، نت کرافت، ارتلینک و مرور امن گوگل را نیز با استفاده از سه مجموعه از سایت های درست و سایت های فیشینگ برای محاسبه میزان خطای مثبت و منفی، آزموده ایم. مجموعه سایت های درست شامل ۸۰ آدرس اینترنتی از سایت های قانونی است. این مجموعه به روش نمونه گیری یکنواخت که قبلاً توصیف شد انتخاب شده است. مجموعه دوم شامل ۴۵ سایت فیشینگ زنده است که از گزارش های گروه **PhishTank** انتخاب شده اند و مجموعه سوم شامل ۹ سایت فیشینگ می باشد که ما آن ها را ساخته ایم. همچنین این نمونه ها را بصورت مجدد روی نوار ابزار ضد فیشینگ علم و صنعت آزموده ایم. جدول ۱ میزان خطای مثبت و منفی هر نوار ابزار را براساس نتایج بدست آمده نشان می دهد. با توجه به نتایج بدست آمده، نوار ابزار ضد فیشینگ علم و صنعت با خطای منفی صفر درصد در شناسایی سایت های فیشینگ بسیار موفق تر از روش های دیگر عمل می نماید. حداقل تفاوت میزان میزان خطای منفی روش های دیگر ۲۵٪ می باشد بنابر این روش ما در شناسایی سایت های فیشینگ پیشرفت مشهودی ارایه نموده است. میزان خطای مثبت روش ما از اسپوفگارد کمتر است اما از نت کرافت، ارتلینک، مرور امن گوگل بیشتر می باشد. اما با توجه به اینکه هدف روش های تشخیص سایت های فیشینگ، شناسایی سایت های فیشینگ می باشد، شناسایی سایت های فیشینگ و میزان خطای منفی کمتر در اولویت می باشد. در ضمن تفاوت میزان خطای مثبت روش ما با بهترین آنها تنها ۹٪ می باشد که به نسبت بهبودی که در تشخیص سایت های فیشینگ ارایه نموده ایم قابل توجیه است.

با توجه به نمودار فوق در ۷۴/۴٪ موارد، رتبه سایتی که به دنبال آن هستیم در نتایج جستجوی گوگل یک می باشد. این بدان

جدول ۱: میزان خطای مثبت و منفی روش های تشخیص سایت های فیشینگ

مقدار - درصد نوار ابزار	درصد خطای مثبت	درصد خطای منفی نمونه فیشینگ از PhishTank	درصد خطای منفی نمونه فیشینگ ساخته شده
SpoofGurad	۱۴/۹۴	۵۲/۳۸	۱۰۰
NetCraft	۰	۰	۱۰۰
Earthlink	۰	۶۸/۷۵	۰
مرور امن گوگل	۰	۲۵	۱۰۰
علم و صنعت	۹	۰	۰

۶- چالش های تکنیک ارایه شده

میزان خطای مثبت روش ما ۹٪ می باشد. این میزان خطا به دلایل مختلفی بروز می نماید که این دلایل شکست را در این قسمت مورد بررسی قرار داده ایم.

• یک صفحه قانونی با آرم کمپانی دیگر

برخی از صفحات قانونی آرم کمپانی های دیگر را به عنوان آرم خود بکار می برند. این صفحات یکی از منابع تولید اشتباه درست می باشد. در حالتی که یک صفحه قانونی لوگوی یک کمپانی دیگر را بکار می برد، از ظاهر صفحه چنین استنتاج می شود که صفحه ادعا می کند که متعلق به کمپانی است که آرم آن در صفحه این کمپانی ظاهر شده است. با وارد نمودن نام کمپانی در جعبه متن نوار ابزار، نوار ابزار علم و صنعت چنین صفحه ای را به عنوان یک سایت فیشینگ تشخیص می دهد.

• کمپانی های چند دامنه ای

وب سایتهای یک کمپانی ممکن است در بین دامین های مختلف گسترده شده باشند. مشتری های فعال در کشورهای مختلف و سرویس های متعددی که یک کمپانی فراهم می نماید انگیزه هایی هستند که برخی کمپانی ها از چند نام دامنه برای سایت خود استفاده می نمایند. دامین اصلی کمپانی دارای رتبه بالایی در نتایج گوگل است اما دامنه های دیگر دارای رتبه های پایین تر یا بسیار پایین هستند. تفاوت بین رتبه ها یک امر منطقی است زیرا الگوریتم Page Rank گوگل نتایج جستجوها گوگل را بر اساس مشهوریت صفحات مرتب می نماید. با توجه به

این حقیقت که صفحه اصلی یک سایت مشهورتر از بقیه است و بوسیله صفحات بسیاری ارجاع داده شده است، این صفحه رتبه بالاتری نسبت به صفحات دیگر بدست می آورد. صفحات دامین های دیگر کمپانی ممکن است حتی در ۱۰ تای اول نتایج ظاهر نشود.

• دامنه های با رتبه بسیار پایین

برخی از سایت ها هنگامی که نام آنها در گوگل جستجو می شود رتبه پایینی بدست می آورند و حتی در ۱۰ نتیجه اول ظاهر نمی شوند. یک دلیل احتمالی این امر این است که این صفحات به گونه درستی ساخته نشده اند که اطلاعات درستی برای موتور جستجو فراهم نمی نمایند تا آنها را بدرستی نمایه گذاری نماید. این مشکل همچنین می تواند موجب اشتباه مثبت در الگوریتم ما شود.

۷- جمع بندی و نتیجه گیری

در حال حاضر روش های بسیاری برای محافظت از کاربران در مقابله با حمله فیشینگ ارایه شده است. دسته بزرگی از این ابزارها از روش های تشخیص صفحات فیشینگ و لیست های سیاه استفاده می نمایند. روش ما بدلیل استفاده از خصوصیات پایدار صفحات فیشینگ برای تشخیص آن ها توانسته است روشی کارآمدتری را برای تشخیص سایت های فیشینگ ارایه نماید و با توجه به کاهش فوق العاده ۲۵ درصدی میزان خطای منفی در تشخیص سایتهای فیشینگ توسط روش ابداعی ارایه شده، نوار ابزار ارایه شده برای استفاده جهت محافظت از کاربران در مقابل حمله فیشینگ مناسب می باشد.

[21] PIRT, Accessed December 14, 2006,
<http://wiki.castlecops.com/PIRT>

٨-مراجع

- [1] Anti-phishing working group, "Phishing Activity Trends Report Combined Report for September and October 2006", 2006.
- [2] T. McCall, R. Moss, "Gartner survey shows frequent data security lapses and increased cyber attacks damage consumer trust in online commerce", *Gartner*, 2005.
- [3] A. Litan, Phishing attack victims likely targets for identity theft, FT-22-8873, *Gartner Research* (2004)
- [4] Spoofstick, Accessed December 14, 2006,
<http://www.spoofstick.com/>
- [5] TrustBar, Accessed December 14, 2006,
<http://www.cs.biu.ac.il/~herzbea/TrustBar/>
- [6] Passmark, Accessed December 14, 2006,
www.passmarksecurity.com
- [7] R. Dhamija, J.D. Tygar, "The battle against phishing: dynamic security skins", *Usable Privacy and Security (SOUPS) 2005*, Pittsburgh, PA, USA, July 2005.
- [8] E. Kirda, C. Kruegel, "Protecting users against phishing attacks with antiphish", *Computer Software and Applications Conference*, 2005
- [9] M. Wu, R.C. Miller, G. Little, "Web wallet: preventing phishing attacks by revealing user intentions", *Second symposium on Usable privacy and security*, Pittsburgh, Pennsylvania, USA, 2006.
- [10] D. Miyamoto, H. Hazeyama, Y. Kadobayashi, "SPS: a simple filtering algorithm to thwart phishing attacks", *Asian Internet Engineering Conference*, Thailand, 2005
- [11] N. Chou, R. Ledesma, Y. Teraguchi, C. Mitchell, "Client-side defense against web-based identity theft", *Proceedings of the Network and Distributed System Security Symposium*, 2004
- [12] Cloudmark, Accessed December 14, 2006,
<http://www.cloudmark.com/serviceproviders/authority/phishing>
- [13] EarthLink, Inc. EarthLink Toolbar, Accessed December 14, 2006,
<http://www.earthlink.net/software/free/toolbar/>
- [14] Ebay, Account Guard, Accessed December 14, 2005
http://pages.ebay.com/toolbar/accountguard_1.html
- [15] TrustWatch, Accessed December 14, 2006,
<http://toolbar.trustwatch.com/tour/v3ie/toolbar-v3ie-tour-overview.html>
- [16] Google Inc., Google Safe Browsing, Accessed December 14, 2006.
<http://www.google.com/tools/firefox/safebrowsing/>
- [17] McAfee SiteAdvisor, Accessed December 14, 2006,
http://www.mcafee.com/us/about/press/corporate/2007/20070123_201010_r.html
- [18] Netcraft, Netcraft Browser, Accessed December 14 2006, <http://www.netcraft.com/>
- [19] Netscape, Netscape browser, Accessed December 14, 2006, <http://browser.netscape.com/ns8/>
- [20] Google API, Accessed December 14, 2006,
<http://code.google.com/apis/soapsearch/>