سومین همایش ملی مهندسی کامپیوتر، داده کاوی و داده های حجیم – ۹۸

حملات فیشینگ و چالش‌های آن در سرقت آنلاین اطلاعات

نسرین محمودی[۱]، دکتر فرساد زمانی بروجنی[۲*]

۱- دانشجوی کارشناسی ارشد،دانشگاه آزاد اصفهان (خوراسگان) ، ایران،
nasamahmoodi@gmail.com
۲- استادیار ، عضو هیئت علمی دانشگاه آزاد اصفهان(خوراسگان) ، ایران،
farsad.zamani@yahoo.com

چکیده

وب سایت‌های جعلی با جعل هویت وب‌سایت‌های قانونی اطلاعات کاربران در اینترنت را مورد سرقت قرار می‌دهند. حملات فیشینگ نوعی از حملات اینترنتی با رویکرد مهندسی اجتماعی است که هدف آن سرقت اطلاعات کاربران است و برای این منظور از وب‌سایت‌های جعلی استفاده می‌کنند. این نوع حملات دارای یک چرخه می‌باشند که در ابتدا یک سایت جعلی ایجاد می‌شود، سپس لینک‌های آن برای کاربران از طریق ایمیل ارسال می‌گردد و در ادامه کاربران با کلیک بر روی این لینک‌ها قربانی حملات فیشینگ می‌شوند زیرا آن‌ها با مشاهده‌ی شباهت وب‌سایت‌های جعلی با قانونی به آن‌ها اعتماد نموده و اطلاعات خود را در اختیار این وب‌سایت‌ها قرار می‌دهند. افزایش تعداد وب‌سایت‌های جعلی باعث شده است تا حملات فیشینگ در این چند سال اخیر رشد قابل توجهی داشته باشند و به علت سادگی مکانیزم حملات فیشینگ، این چالش امنیتی در بین چالش‌های امنیتی دیگر در فضای مجازی رشد زیادی را تجربه کرده است. در این مقاله تلاش شده است تا حملات فیشینگ و وب‌سایت‌های جعلی و مکانیزم آن‌ها برای کاربران تشریح و مرور شوند تا آن‌ها با مکانیزم وب‌سایت‌های جعلی برای سرقت اطلاعات آشنا شوند.

کلمات کلیدی

صفحات جعلی، وب‌سایت‌های فیشینگ، جعل هویت، سرقت اطلاعات، مهندسی اجتماعی

۱– مقدمه

امروزه سرویس‌های تحت وب خدمات بی‌نظیری به کاربران ارائه می‌نمایند که از جمله‌ی آن‌ها می‌توان خدمات بانکداری الکترونیک، خدمات مالی و فروش آنلاین را نام برد. امروزه وب‌سایت‌های زیادی در حوزه‌های مختلف به کاربران خدمات ارائه می‌دهند که از جمله‌ی آن‌ها می‌توان به وب‌سایت Amazon در حوزه‌ی فروش آنلاین و تجارت الکترونیک[۱] یا eBay در حوزه‌ی حراج آنلاین[۲] اشاره نمود[۱]. حجم تبادلات مالی در این حوزه‌ها قابل توجه است و از این جهت این نمونه وب‌سایت‌ها نقش مهمی در تبادل مالی و تجارت الکترونیک دارند. چالش‌های مختلفی تجارت الکترونیک و سرویس‌های تحت وب را تهدید می‌نماید که یکی از بارزترین آن‌ها وب‌سایت‌های جعلی[۳] است که هویت وب‌سایت‌های قانونی[۴] را جعل می‌نمایند. وب‌سایت‌های جعلی ظاهری شبیه وب‌سایت‌های قانونی دارند و در عملیات فیشینگ[۵] یا فارمینگ[۶] که جهت سرقت اطلاعات استفاده می‌شوند بکار گرفته می‌شوند[۲]. در این نوع از حملات تحت وب فیشر[۷] یا هکر[۸] کاربران را به سمت وب‌سایت‌های جعلی هدایت می‌نمایند و برای این منظور مجموعه‌ای از لینک‌های جعلی را برای آن‌ها ارسال نموده تا آن‌ها با کلیک بر روی این لینک‌ها به سمت وب‌سایت‌های جعلی هدایت شوند. در این موارد مشاهده می‌شود که هکر از روش‌های مبتنی بر بدافزار[۹] یا مهندسی اجتماعی[۱۰] برای فریب کاربران استفاده می‌نماید. حملات فیشینگ معمولاً توسط یک ایمیل و در قالب هرزنامه[۱۱] آغاز شده سپس هکر یک لینک جعلی[۱۲] را در ایمیل قرار داده و توسط تکنیک‌های مختلف مهندسی اجتماعی کاربران را ترغیب به کلیک نمودن بر روی لینک جعلی نموده تا کاربران با کلیک نمودن بر روی لینک مورد نظر به سمت وب‌سایت جعلی هدایت شوند. هکر برای فریب کاربران تغییراتی در لینک جعلی اعمال می‌نماید تا آن‌ها متوجه جعلی بودن لینک نشوند[۳].

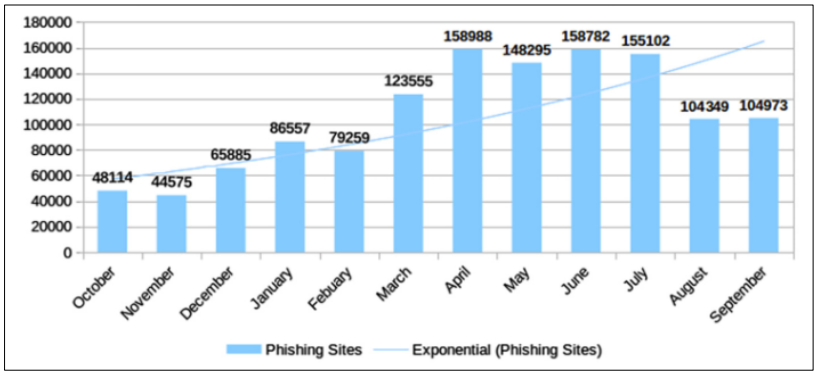
به عنوان نمونه هکر می‌تواند از آدرس آی‌پی[۱۳] به جای آدرس دامنه استفاده نماید یا کارکترهای کدگذاری[۱۴] شده را به جای کارکترهای عادی و مرسوم استفاده نماید و یا آدرس جعلی خود را در انتهای لینک قرار دهد. هکر علاوه بر جعل نمودن لینک ارسالی ظاهر سایت جعلی را بسیار شبیه سایت اصلی طراحی می‌نماید تا کاربران با ورود به سایت مورد نظر تفاوت را احساس نکنند و به راحتی به سایت مورد نظر اعتماد نمایند و اطلاعات با ارزش خود را در فیلدهای خاص وارد نمایند[۴].همچنین برای سرقت اطلاعات کاربران به طور معمول در صفحات جعلی امکاناتی نظیر ورود نام کاربری و کلمه عبور را قرار می‌دهند تا کاربران به اصطلاح بخواهند وارد سایت شوند و از امکانات و خدمات سایت استفاده نمایند غافل از اینکه ورود اطلاعات باعث می‌شود که یک نسخه از نام کاربری و کلمه عبور برای حمله‌کننده ارسال شود. هکرها با هوشمندی کامل سعی می‌کنند با ورود اطلاعات کاربر قربانی پیامی سیستمی مبتنی بر به روزرسانی سایت یا خطای دسترسی برای آن‌ها نمایش دهند تا آن‌ها به سایت مورد نظر شک نکنند و هکر فرصت مناسب برای ورود به حساب‌های کاربری آن‌ها را داشته باشد و بتواند اطلاعات مهم آن‌ها یا حساب‌های مالی را مورد سرقت قرار دهد. حملات سرقت آنلاین علی‌رغم استفاده از تکنیک‌های ساده دارای اثرگذاری بالایی می‌باشند به گونه‌ای زیان این حملات به بخش‌های مختلف اینترنت قابل توجه می‌باشد. تشخیص و شناسایی حملات فیشینگ باعث می‌شود که تجارت الکترونیک و فعالیت روزمره‌ی کاربران در فضای مجازی با امنیت بیشتری دنبال شود و از طرفی زیان این حملات نیز کاسته شود. در این مقاله مفاهیم مهم و پایه در مورد صفحات جعلی و روش‌های فیشینگ مورد بحث قرار گرفته می‌شود.

---

[1] E-commerce
[2] Online auction
[3] Fake websites
[4] Legal websites
[5] Phishing
[6] Pharming
[7] Phisher
[8] Hacker
[9] Malware
[10] Social engineering
[11] Spam
[12] Faked link
[13] IP Address
[14] Unicode

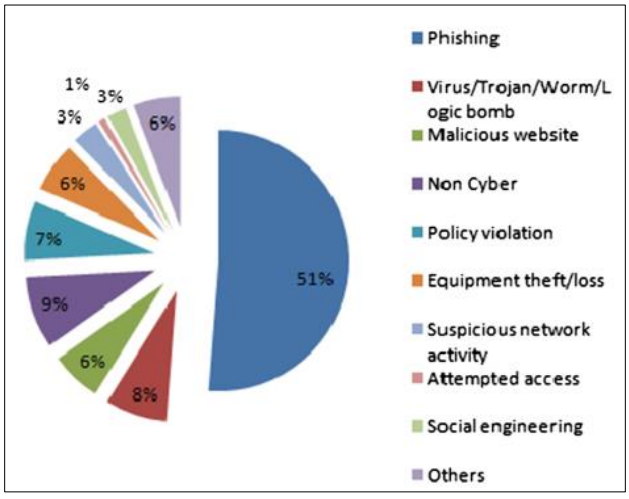
۲– اهمیت شناسایی صفحات جعلی

امروزه تعداد زیادی وب‌سایت در فضای مجازی به ارائه‌ی خدمات قانونی نظیر بانکداری الکترونیک، فروش آنلاین و حراج آنلاین می‌پردازند و بسیاری از کاربران از این وب‌سایت‌های قانونی جهت انجام فعالیت‌های روزمره خود استفاده می‌نمایند با این وجود تعدادی از وب‌سایت‌های قانونی توسط فیشرها مورد جعل قرار گرفته می‌شوند تا اطلاعات کاربران را به سرقت ببرند. پژوهش‌های امنیتی نشان می‌دهد تعداد وب‌سایت‌های فیشینگ یا جعلی به موازات وب‌سایت‌های قانونی مرتباً افزایش یافته و یک برآورد مطابق نمودار شکل(۱)، نشان می‌دهد می‌دهد که تعداد این وب‌سایت‌ها در سال‌های اخیر بخصوص در بازه زمانی ۲۰۱۵ تا ۲۰۱۶ رشد قابل توجهی را تجربه می‌نماید:



شکل ۱: تعداد وبسایت‌های جعلی در چند سال اخیر رشد قابل توجهی را داشته است[۵]

در نمودار شکل(۲)، میزان رشد چالش‌های مختلف امنیتی در چند سال اخیر نشان داده شده است و می‌توان به‌خوبی مشاهده نمود که سهم حملات فیشینگ در این میان حدود ۵۱٪ و بیشتر سایر چالش‌های امنیتی در فضای وب است:

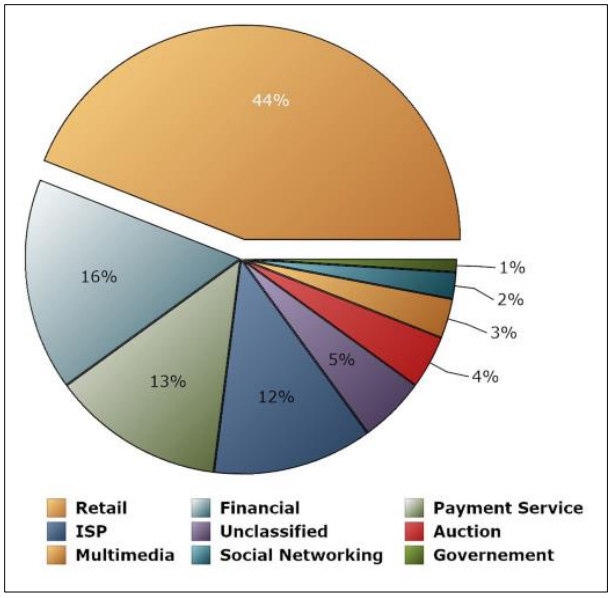


شکل ۲: حملات فیشینگ نسبت به سایر چالش‌های امنیتی در چند سال اخیر رشد بیشتری داشته است[٦]

علاوه بر رشد وب‌سایت‌های جعلی و تعداد حملات فیشینگ میزان سرقت اطلاعات و وب‌سایت‌های هدف در این حملات نیز از طرف هکر هوشمندانه انتخاب می‌شوند و او سعی می‌کند که وب‌سایت‌های مرتبط با پرداخت، مالی و صنعتی را بیشتر مورد جعل هویت قرار دهد. هکرها با جعل وب‌سایت‌های مالی سعی می‌نمایند مشتریان بانک را به سمت وب‌سایت‌های جعلی هدایت نمایند و حساب بانکی آن‌ها را مورد سرقت قرار دهند. در نمودار شکل(۳)، مشاهده می‌شود که بخش پرداخت، مالی و وب‌سایت‌های دولتی به ترتیب با سهم ۴۴٪، ۱۶٪ و ۱۳٪ بیشترین سهم در بین سایت‌های جعلی را دارند و این موضوع نشان می‌دهد که حملات فیشینگ تا چه اندازه می‌تواند ویرانگر باشد زیرا تجارت الکترونیک[۱] و خدمات دولتی در بستر وب را هدف قرار داده است. جعل وب‌سایت‌های مالی و مرتبط با تجارت الکترونیک نظیر

[۱] E-commerce

سایت‌های فروش آنلاین باعث می‌شود که سرمایه و حساب مالی افراد مورد سرقت قرار گرفته و اعتماد آن‌ها به زیرساخت‌های وب و تجارت الکترونیک کاهش یابد:



شکل ۳: حملات فیشینگ بیشتر حوزه‌های مالی، پرداخت و سامانه‌های دولتی را جعل می نمایند[۷]

تشخیص وب‌سایت‌های فیشینگ باعث می‌شود زیان ناشی از آن‌ها که میلیاردها دلار در سال بالغ می‌شود تا حد زیادی تعدیل شود و به بانک‌ها، موسسات مالی و به طور کلی تجارت الکترونیک آسیب‌کمتری وارد شود. برای درک بهتر زیان وب‌سایت‌های جعلی و حملات متناظر به آن می‌توان به نمودار شکل(۴)، توجه نمود که همانگونه مشاهده می‌شود این زیان قابل توجه است و از این جهت شناسایی وب‌سایت‌های جعلی از اهمیت بالایی برخوردار است:

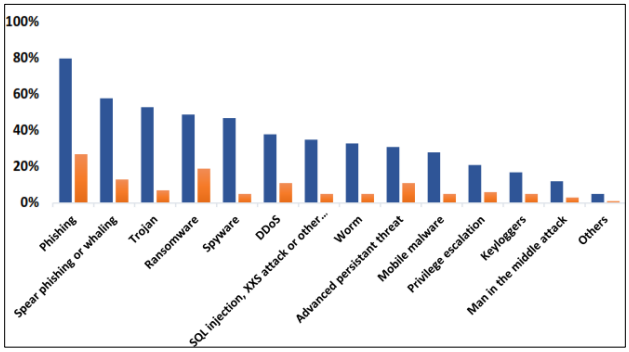
شکل ٤: زیان ناشی از حملات فیشینگ و سرقت‌های آنلاین [٦]

در واقع می‌توان گفت که حملات فیشینگ بیشتر بخش مالی و فعالیت‌های مرتبط با آن را هدف قرار داده است تا از این طریق هکر منابع مالی لازم را از کاربران سرقت نماید از طرفی حملات فیشینگ علاوه بر موسسات مالی و کاربران اینترنت می‌تواند به شرکتهای بیمه نیز آسیب وارد نماید و تجارت الکترونیک نظیر فروش آنلاین و حراج آنلاین را دچار اختلال نماید. حمات فیشینگ به صورت غیر مستقیم باعث ارسال هرزنامه و ایمیل نیز در شبکه می‌شوند و این پدیده باعث می‌شود که حجم زیادی از پهنای باند اینترنت صرف ارسال این پیام‌های مخرب شوند. وب‌سایت‌های فیشینگ می‌توانند تعداد مشتریان وب‌سایت‌های نظیر ای بی[1] و آمازون[2] را با ایجاد بی‌اعتمادی کاهش دهند از این جهت تشخیص حملات فیشینگ از اهمیت بالایی برخوردار است[۷].

[1] ebay
[2] Amazon

۳– حملات فیشینگ

حملات فیشینگ یا سرقت آنلاین اطلاعات به کمک لینک‌های جعلی یک فرآیند چالش‌برانگیز برای سرقت اطلاعات کاربران به کمک وب سایت‌های جعلی است. افزایش تعداد کاربران اینترنت آسیب‌پذیری افراد آنلاین را در مواجه با این تهدید امنیتی افزایش داده است. امروزه بسیاری از کاربران اینترنتی برای دسترسی به اینترنت از تلفن‌های همراه و هوشمند خود استفاده می‌نمایند که با سهولت کامل می‌تواند به انواع خدمات وب دسترسی داشته باشند با این وجود به علت آنکه در تلفن‌های همراه تسلط کاربران بر لینک‌ها و آدرس‌ها کاهش می‌یابد لذا امکان فریب آن‌ها نیز افزایش می‌یابد. طبق برآورد فوق می‌توان دریافت که در سال ۲۰۱۴ حدود ۱,۵۷ میلیارد نفر از طریق تلفن هوشمند به اینترنت وصل شده‌اند و این مقدار در سال ۲۰۲۰ به حدود ۲,۸۷ میلیارد عدد می‌رسد که رقم قابل توجهی است. افزایش این تعداد کاربر در اینترنت آن‌ها را مستعد چالش‌های امنیتی مختلفی نظیر سرقت قرار می‌دهد و یکی از این چالش‌های مهم فیشینگ یا وب‌سایت‌های جعلی می‌باشد. مطالعات مختلف نشان می‌دهد بیشتر لینک‌های جعلی در اینترنت در صفحاتی قرار داده می‌شود که کاربران بیشتر در آن صفحات حضور دارند و نمونه این صفحات می‌توان به وب‌سایت‌های بازی، صفحات ایمیل، ورزشی و اخبار اشاره نمود[۹]. مطالعات نشان می‌دهد که وب‌سایت‌های جعلی و حملات فیشینگ در سال‌های اخیر نسبت به سایر چالش‌های امنیتی نسبت قابل توجهی داشته‌اند و مطابق نمودار شکل(۵)، می‌توان دید که حملات فیشینگ ۸۰٪ در سال‌های اخیر رشد داشته است و میزان تأثیرگذاری و موفقیت حملات نیز بیش از ۲۰٪ بوده است و این موضوع نشان می‌دهد این چالش در صدر چالش‌های امنیتی وب‌گردی کاربران است:



شکل ۵: سهم حملات فیشینگ نسبت به سایر حملات[۹]

۳–۱– تاریخچه‌ی حملات فیشینگ

از آغاز سرقت به کمک لینک جعلی در سال ۱۹۹۷ که بر روی یک سایت فروش آنلاین انجام شد تا هم اکنون سرقت‌های آنلاین و حملات فیشینگ توانسته‌اند به رویکرد خود ادامه دهند و این موضوع نشان می‌دهد این حملات کارایی خود را حفظ کرده و حتی به نوعی تکامل رسیده‌اند. در جدول(۱)، یک سیر تاریخی از جملات فیشینگ و لینک‌های جعلی را می‌توان مشاهده نمود به گونه‌ای که در هر سال نوع خاصی از این چالش اینترنتی و امنیتی بروز نموده است. مطابق این رویکرد می‌تواند دید در سال‌های اخیر نوع خاصی از حملات فیشینگ ارائه شده است که از جمله‌ی آن‌ها حملات فیشینگ تلفنی، حملات فیشینگ پیامکی، حملات فیشینگ مهندسی اجتماعی و غیره است به نحوی که پیشرفته‌تر از سابق می‌باشند. با توجه به جدول ذیل می‌توان دریافت که حملات فیشینگ روز به روز در حال پیشرفت بوده و بر تنوع تکنیک‌های آن افزوده می‌شود و این چالش ابعاد تازه‌ای به خود می‌گیرد. امروزه پیشرفت حملات فیشینگ و سرقت اطلاعات مرتباً در حال تکامل بوده و شیوه‌های مؤثرتری برای این حملات ابداع می‌شود. به عنوان مثال نوع خاصی از حملات فیشینگ به کمک تماس تلفنی به نام حملات Vishing در حال رایج شدن است که هکر به کمک ابزار ارتباطی تلفن قصد دارد اطلاعات کاربران نظیر شماره کارت‌های اعتباری و کلمه‌ی عبور آن‌ها را مورد سرقت قرار دهد[۱۰]:

جدول ۱: تاریخچه‌ی حملات فیشینگ و سرقت اطلاعات[۱۰]

سال	رویداد مبتنی بر جعل هویت و سرقت
۱۹۹۶	شروع اولین سرقت اینترنتی به کمک وب‌سایت‌های جعلی
۱۹۹۷	ورود مفاهیم حمله فیشینگ به ادبیات امنیت شبکه
۱۹۹۸	بکارگیری پیام‌رسان‌ها و ابزار ایمیل برای فریب کاربران اینترنتی
۱۹۹۹	تکنیک ارسال انبوه ایمیل جهت فریب کاربران با تعبیه نمودن لینک‌های جعلی درون آن‌ها
۲۰۰۰	ورود ابزار جاسوسی نظیر keylogger ها برای ثبت کلمات عبور کاربران
۲۰۰۱	بکارگیری آدرس‌های جعلی جهت انجام حملات فیشینگ
۲۰۰۲	بکارگیری ابزارهای Screen loggers جهت مشاهده اطلاعات کاربران به صورت مخفیانه
۲۰۰۳	بگارگیری گپ‌های زنده و چت در مهندسی اجتماعی برای سرقت اطلاعات کاربران
۲۰۰۴	وقوع نوع خاصی از حملات فیشینگ به نام pharming که آدرس سایت‌های قانونی را در سرویس‌دهنده دامنه جعل می‌نماید.
۲۰۰۵	وقوع حملاتی از نوع spear phishing که در آن اطلاعات کاربران جهت سرقت اطلاعات آن‌ها جمع‌آوری می-شود.
۲۰۰۶	سرقت اطلاعات به کمک تکنیک VoIP
۲۰۰۷	زیان حملات فیشینگ در این سال به چند میلیارد دلار برآورد شده است.
۲۰۰۹	شناسایی و فیلترنیک ۱۰۷۹ سایت جعل هویت و فیشینگ
۲۰۱۰	ایجاد صفحات جعلی متعدد مطابق سایت قانونی facebook
۲۰۱۲	تعداد زیادی بدافزار که نقش هدایت کاربران به سایت‌های فیشینگ را داشتند در این سال شناسایی شدند.
۲۰۱۳	۶۹ کشور دنیا دستخوش وقوع حملات فیشینگ در این سال شدند.
۲۰۱۴	۷۵۰۰۰۰ ایمیل جعلی جهت انجام حملات فیشینگ کشف و شناسایی شد.
۲۰۱۵	تمرکز حملات فیشینگ به بخش‌های مالی و صنعتی در وب

۳-۲- صفحات جعلی

صفحات قانونی[1] در اینترنت به صفحات وبی گفته می‌شوند که خدمات قانونی به کاربران ارائه می‌دهند و این وب‌سایت‌ها مورد اعتماد و توجه کاربران مختلف می‌باشند و طیف مختلفی از مشتریان به این وب‌سایت‌ها مراجعه می‌نمایند. سایت‌های جعلی در برخی موارد شباهت فوق‌العاده‌ای با سایت‌های اصلی دارند و این شباهت باعث می‌شود کاربران نتوانند به درستی جعلی بودن یک وب‌سایت را تشخیص دهند. میزان شباهت بین دو سایت می‌تواند شامل صفحه‌بندی، تصاویر، نوشته‌ها و فیلدهای ورودی وب‌سایت باشد که در مورد فوق مشاهده می‌شود این موارد تا حد زیادی به هم شباهت دارند. شباهت زیاد بین وب‌سایت‌های جعلی به وب‌سایت‌های قانونی باعث می‌شود کاربران به آن‌ها اعتماد نمایند و به خیال آنکه در وب سایت مورد نظر و قانونی قرار دارند اطلاعات حساس خود مانند نام کاربری و کلمه عبور خود را افشاء می‌نمایند. از جمله وب‌سایت‌های قانونی می‌توان به وب‌سایت Paypal اشاره نمود که در فعالیت‌های انتقال پول بین کاربران عمل می‌نمایند و هر کاربر می‌تواند یک حساب کاربری در این وب‌سایت داشته باشد و به ازای خدمات ارائه شده توسط شخص هزینه‌ی خدمات به حساب کاربری مورد نظر واریز می‌شود. در شکل(۶)، دو نمونه از ایمیل‌های جعلی و واقعی که به ترتیب توسط هکر و سایت Paypal برای مشتریان ارسال می‌شوند نمایش داده شده است و مطالعه‌ی آن‌ها به‌خوبی نشان می‌دهد که ساختار این ایمیل‌ها شبیه هم بوده با این تفاوت که در ایمیل جعلی لینک‌های جعلی و مشابه لینک‌های قانونی قرار داده می‌شود. مطابق شکل فوق می‌توان دریافت که ساختار ایمیل‌های جعلی و قانونی تا حد زیادی مشابه است اما لینک‌های بکار رفته در آن تفاوت خاص خود را دارد و هکر با دستکاری نوشته

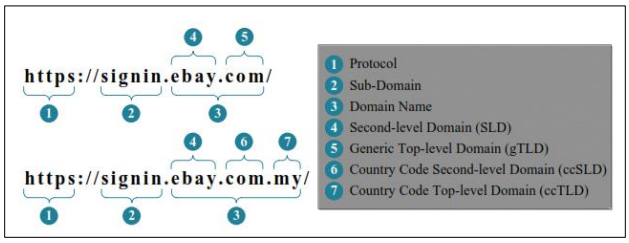
[1] Legal pages

لینک‌ها و جعل نمودن آن‌ها سعی می‌نمایند آن‌ها را شبیه لینک قانونی نماید اما در محتوای آن‌ها و آدرس واقعی آدرس جعلی تعبیه می‌شود. در ایمیل‌های جعلی مشابه ایمیل‌های رسمی هکر سعی می‌نماید با درخواست‌های رسمی اما غیرقانونی کاربران را ترغیب به لو دادن اطلاعات نماید تا هکر بتواند در فرصت مناسب اعمال مجرمانه خود را انجام دهد[۱۱]:

شکل ٦: نمونه ایمیل‌های جعلی و قانونی[۱۱]

۳-۳- جعل لینک

برای جعل هویت وب‌سایت‌ها و ساخت آدرس‌های جعلی که کاربران به آن‌ها شک نکنند روش‌های متنوعی ایجاد شده است که هر کدام از آن‌ها سعی می‌نمایند تا اعتماد کاربران را به خود جلب نمایند. برای شناخت تکنیک‌های جعلی نیازاست که چارچوب یک آدرس اینترنتی به خوبی درک شود از این جهت بخش‌های آدرس مطابق شکل(۷)، نمایش داده شده است:



شکل ۷: ساختار و بخش‌های یک لینک آدرس [۱۲]

مطابق شکل فوق، یک آدرس اینترنتی شامل بخش‌های مانند پروتکل، زیردامنه، دامنه، بخش اول، دوم، سوم و غیره است. مشاهده می‌شود در تکنیک‌های جعل لینک‌های اینترنتی آدرس دامنه یک سایت قانونی به عنوان یک زیر دامنه‌ی آدرس جعلی در نظر گرفته می‌شود که نمونه آن در شکل(۸)، نشان داده شده است:

شکل ۸: استفاده از آدرس قانونی به عنوان زیر دامنه [۱۳]

مطابق شکل فوق، آدرس جعلی دارای دامنه pay-me است و هکر برای فریب کاربران آدرس قانونی سایت paypal.com را به عنوان زیر دامنه‌ی این سایت معرفی نموده است تا کاربران به خیال اینکه وب‌سایت متعلق به سایت معروف paypal.com می‌باشند به آن اعتماد نمایند. در برخی موارد هکر آدرس جعلی سایت را در کنار یک دامنه‌ی قانونی قرار می‌دهد تا اعتبار وب‌سایت خود را بالا نشان دهد. در نمونه‌ای دیگر مشاهده می‌شود که هکر آدرس Microsoft را جعل نموده و با جابجایی دو حرف سعی نموده تا کاربران را فریب دهد

و آدرس جعلی Mircosoft.de را ایجاد نماید و یا نمونه anrazon را به صورت arnazon جعل نموده است. در برخی از موارد هکر برای فریب کاربران وب‌سایت‌های مطرح نظیر facebook را جعل نموده و یک دامنه و آدرس جعلی به آن‌ها انتساب می‌دهد. در برخی موارد هکر آدرس قانونی را در بخش اول آدرس قرار داده و آدرس جعلی را در بخش دوم و بعد از کارکتر @ قرار می‌دهد زیرا بیشتر مرورگرها آدرس قبل از این کارکتر را نادیده گرفته و آدرس بعدی آن را استفاده می‌نمایند. در برخی از موارد هکر برای گمراهی کاربران نیز از آدرس‌های آی‌پی، عددی در مبنای هگز و دسیمال یا حتی ترکیبی استفاده می‌نماید[۱۴]. هکر می‌تواند آدرس‌های جعلی را درون یک ایمیل قرار داده و آن‌ها را برای کاربران ارسال نماید و سپس کاربران با کلیک برروی این لینک‌ها موارد سایت فیشینگ شده و اطلاعات آن‌ها مورد سرقت قرار گرفته می‌شود. در موارد دیگر کاربر وارد یک سایت فیشینگ شده و توسط کدهای جاوا اسکریپت و بدون کلیک بر روی یک لینک جعلی وارد سایت جعلی می‌شود. در شکل(۹)، یک نمونه از هدایت کاربران به سایت‌های فیشینگ به کمک تکنیک جاوا اسکریپت و پنجره لغزان[1] نمایش داده شده است. در تکنیک مورد نظر کاربر بدون آنکه بر روی لینک جعلی کلیک نماید به طور اتوماتیک و توسط کدهای جاوا اسکریپت وارد سایت جعلی در پنجره لغزان می‌شود. در واقع وجود بخش‌های مرتبط با ورود اطلاعات در صفحات لغزان یا PopUp یک نشانه محتمل از حملات فیشینگ است.

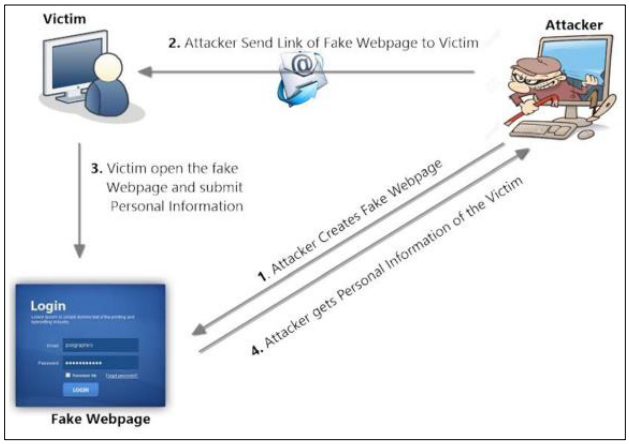
شکل ۹: استفاده‌ی تکنیک جاوا اسکریپت برای هدایت به سایت‌های فیشینگ [۱٤]

ویژگی حملات فیشینگ به موارد ذکر شده محدود نمی‌شود بلکه ویژگی‌های مختلفی وجود دارد که می‌توان توسط آن وقوع حملات فیشینگ را تعیین نمود. به عنوان مثال عمر دامنه، اطلاعات مرتبط با موتورهای جستجوگر، ویژگی کد صفحات و غیره در تعیین فیشینگ بودن آن‌ها موثر است.

۳-۴- چرخه‌ی حملات فیشینگ

حملات فیشینگ از یک فرآیند مشخص و سیتماتیک برای فریب کاربران استفاده می‌نمایند که به آن سیکل حملات فیشینگ گفته می‌شود. یک نمونه از سیکل حملات فیشینگ که برای این حملات چهار مرحله مختلف را در نظر می‌گیرد در شکل(۱۰)، نمایش داده شده است. در این سیکل حملات چهار مرحله‌ی مختلف نظیر ایجاد صفحات تقلبی توسط فیشر، ارسال ایمیل‌های جعلی به کاربران با تعبیه لینک‌های جعلی درون آن‌ها، کلیک نمودن بر روی لینک‌های جعلی و ورود کاربران به سایت‌های جعلی و در نهایت ارسال اطلاعات کاربران به هکر وجود دارد. مطابق چرخه‌ی ذیل می‌توان دریافت که هکر و مهاجم آدرس‌های جعلی را درون ایمیل تعبیه نموده و آن‌ها را از طریق سرویس دهنده‌ی ایمیل به کاربران ارسال می‌نمایند و در این مرحله سرویس‌دهنده‌ی ایمیل چک می‌کند آیا آدرس‌های فعلی جزء لیست سیاه می‌باشد و اگر پاسخ مثبت باشد اخطار لازم به کاربران صادر می‌شود. در چرخه‌ی حیات فوق مشاهده می‌شود حملات فیشینگ یک مکانیزم چند مرحله‌ای است که سرویس‌های وب و پست الکترونیک را شامل می‌شود. در این چرخه هکر وب‌سایت‌های جعلی را بر روی یک وب‌سرویس قرار داده و لینک این وب‌سایت‌های جعلی برای کاربران ارسال می‌شود.

[1] Pop up



شکل ۱۰: سیکل چهار مرحله‌ای از حملات فیشینگ [۱۵]

کاربر می‌تواند با مکانیزم‌های اکتشافی، شباهت بصری و لیست سیاهی که در اختیار دارد این حملات را تشخیص دهد و در صورتی که نتواند این حملات را شناسایی نماید اطلاعات شخصی خود را به هکر لو می‌دهد و مهاجم می‌تواند اطلاعات مهم کاربران را مورد سرقت قرار دهد.

۳-۵- ویژگی مهم صفحات جعلی

به طور کلی در ارتباط با وب‌سایت‌های فیشینگ و جعلی مجموعه ویژگی‌های مرتبط با آدرس سایت، ویژگی‌های مرتبط با حالت غیرعادی در صفحات وب، ویژگی‌هایی که در ارتباط با کدهای منبع و در ارتباط با دامنه‌ی وب‌سایت می‌باشند نقش مهمی در شناسایی آن‌ها ایفا می‌نماید. در جدول(۲)، لیست تعدادی از ویژگی‌های مهم و مرتبط با صفحات جعلی که در شناسایی آن‌ها نقش دارد نمایش داده شده است. ویژگی‌های ارائه شده در این جدول فقط بخشی از ویژگی مرتبط با حملات فیشینگ است و ویژگی حملات فیشینگ می‌تواند شامل بخش‌های مختلفی از ویژگی‌های بدنه، ویژگی‌های آدرس، ویژگی موضوعی، ویژگی مرتبط با کد و ویژگی مرتبط با ارسال‌کننده ایمیل باشد که در فصل چهارم مورد بحث و بررسی قرار گرفته می‌شود. به عنوان نمونه یکی از ویژگی‌هایی که مرتبط با کد منبع است و در تشخیص وب‌سایت‌های جعلی کمک می‌نماید، تعداد لینک‌های خالی در صفحات است. به عبارت بهتر مشاهده می‌شود که در صفحات جعلی تعداد زیادی لینک وجود دارد که مقداردهی و آدرس‌دهی نشده است زیرا هدف هکر بیشتر دکمه‌ی ورود اطلاعات است و لینک‌های کار گذاشته شده در صفحه فقط برای ایجاد شباهت بصری ایجاد شده است:

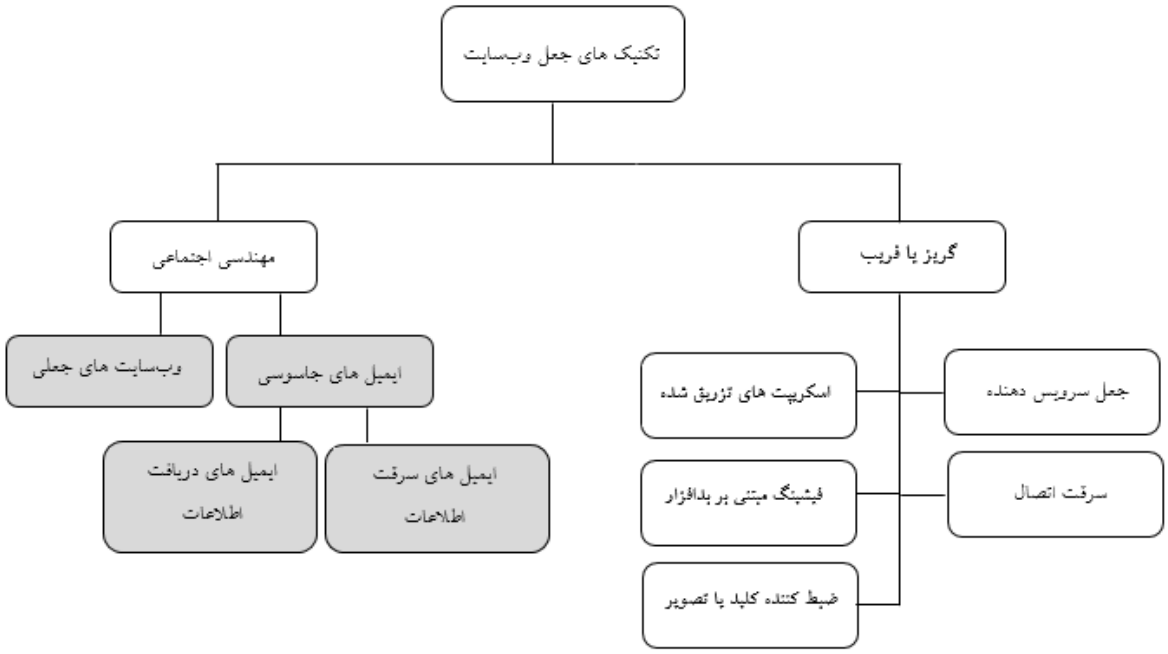
جدول ۲: ویژگی مهم صفحات جعلی و حملات فیشینگ[۱۶]

ویژگی	مشخصه ویژگی
طول آدرس	در سایت‌های فیشینگ این مقدار از حد نرمال بزرگتر است.
بکارگیری کارکتر @ در آدرس	در برخی آدرس‌های جعلی این کارکتر قرار داده می‌شود تا آدرس جعلی بعد ازاین کارکتر مد نظر قرار گرفته شود
تعداد نقاط	در سایت‌های جعلی تعداد نقاط به طور میانگین بیشتر از سایت‌های قانونی ظاهر می‌شود.
وجود آدرس IP	در سایت‌های قانونی کمتر از آدرس IP استفاده می‌شود و استفاده ازاین ویژگی در وب-سایت‌های جعلی رایج‌تر است.
رتبه‌ی سایت	سایت‌های قانونی رتبه بالاتری در سایت‌های نظیر آلکسا دارند اما سایت‌های جعلی در این سایت‌ها شاخص‌بندی نمی‌شوند.

جستجو در گوگل	سایت‌های فیشینگ در سایتی نظیر گوگل رتبه‌بندی نمی‌شوند و این نشان‌دهنده‌ی آن است که عمر و اهمیت آن‌ها و تعداد مراجعه کننده‌ی به این وب‌سایت‌ها مانند سایت قانونی نمی‌باشد.
شاخص بندی در موتورهای جستجوگر	سایت‌های فیشینگ در موتورهای جستجوگر شاخص‌بندی نمی‌شوند.
تعداد کلمات در صفحات	تعداد کلمات در یک وب‌سایت یا یک دامنه می‌باشد.
وجود آدرس کوتاه	آدرس‌های کوتاه شده می‌توانند نشانه وب‌سایت‌های فیشینگ و مخرب باشند.
قرار دادن آدرس Https در زیر دامنه	قرار دادن آدرس Https در زیر دامنه‌ی یک سایت غالباً برای جلب اعتماد کاربران به این پروتکل رمزنگاری است و از ویژگی‌های صفحات جعلی است.
وجود دابل اسلش در آدرس	وجود دابل اسلش در آدرس نشانه انتقال خودکار یک آدرس به یک آدرس دیگر و غالباً فیشینگ است.

۳-۶- تکنیک‌های حملات فیشینگ

گوپتا و همکاران در سال ۲۰۱۸ [۷]، برای انجام حملات فیشینگ مطابق شکل(۱۱)، یک دسته‌بندی مبانی بر روش‌های مهندسی اجتماعی[1] و گریز یا فریب[2] ارایه دادند:



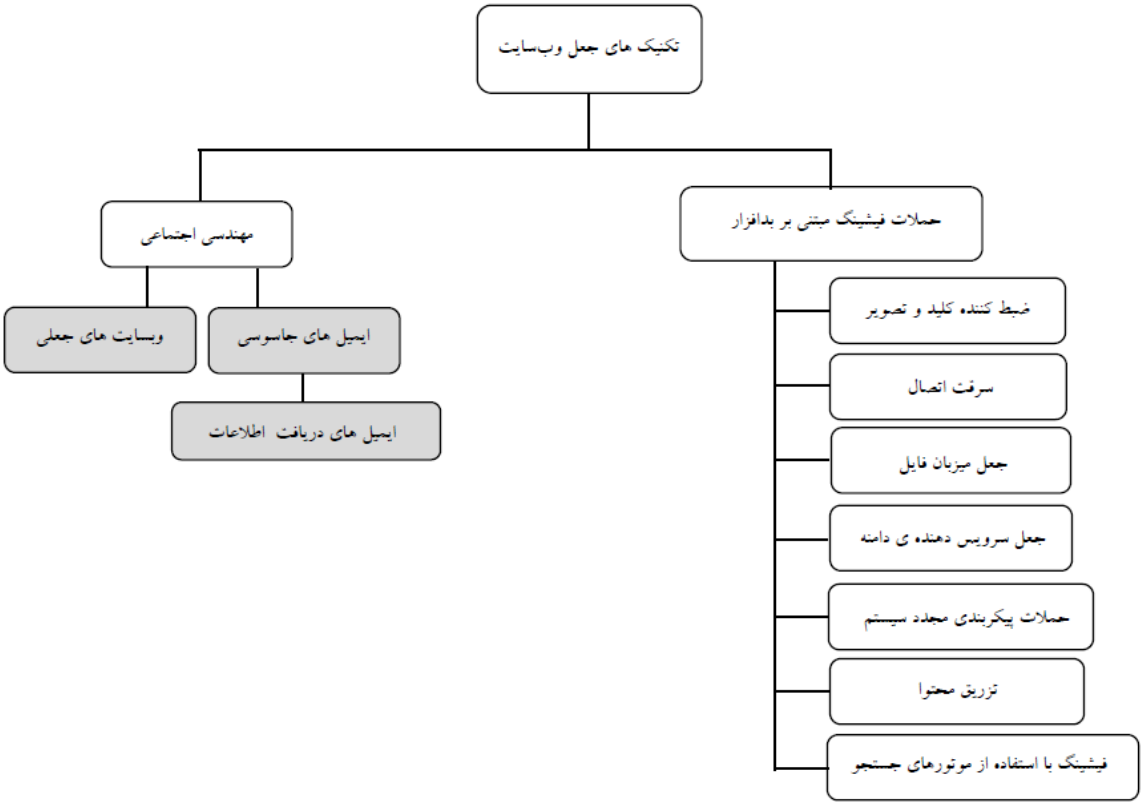
شکل ۱۰: روش‌های انجام حملات فیشینگ در مطالعه گوپتا و همکاران [۷]

روش‌های مبتنی بر مهندسی اجتماعی به روش‌های گفته می‌شود که هکر یا فیشر با روابط اجتماعی بالا و با استفاده از ابزارهای ارتباطی نظیر ایمیل سعی می‌کنند کاربران را از طریق ایمیل‌های جعلی یا وب‌سایت‌های جعلی مورد فریب قرار داده و اطلاعات با ارزش آن‌ها را سرقت نمایند. در تکنیک‌های مبتنی بر گریز یا فریب فرد مهاجم با فرد قربانی ارتباط برقرار نمی‌نماید بلکه بیشتر از طریق انواع بدافزار سعی می‌نماید که قربانی را به سمت وب‌سایت‌های جعلی هدایت نماید که از این دسته می‌توان به موارد ذیل اشاره نمود:

[1] Social engineering
[2] Technical Subterfuge

- اسکریپت‌های تزریق شده[1]: در این شیوه‌ی سرقت آنلاین هکر مجموعه‌ای از کدهای مخرب را به عنوان ورودی وب‌سایت‌ها در فیلدهای ثبت‌نامی وارد نموده و آن‌ها را در سمت سرویس‌دهنده یا سرویس‌گیرنده اجرا نموده تا از این طریق اطلاعات با ارزش مانند کوکی‌ها را سرقت نماید.
- سرقت اتصال[2]: در این حالت اتصال بین کاربر و وب‌سرویس توسط فیشر مورد سرقت قرار گرفته می‌شود و جهت اتصال در راستای وب‌سایت مخرب قرار داده می‌شود.
- فیشینگ مبتنی بر بدافزار[3]: در این شیوه‌ی مجموعه‌ای از نرم‌افزارهای مخرب توسط فیشر به کاربران وب ارسال می‌شود و آن‌ها را ناخواسته به سایت‌های فیشینگ هدایت می‌نماید.
- جعل سرویس‌دهنده دامنه[4]: این تکنیک فیشینگ اطلاعات سرویس دهنده‌ی دامنه را در شبکه جعل نموده و کاربران را به جای دامنه اصلی به دامنه جعلی هدایت می‌نماید.
- ضبط کننده کلید و تصویر[5]: در این تکنیک مجموعه بدافزارهای جاسوسی کلیدهای فشرده شده توسط کاربر و تصویر صفحه مانیتور کاربر را برای فیشر ارسال می‌نماید.

در شکل(۱۱)، یک طبقه‌بندی دیگر در مورد حملات فیشینگ به دو دسته اصلی مبتنی بر مهندسی اجتماعی و بدافزار در نظر گرفته می‌شود. مشاهده می‌شود در عمل این دسته‌بندی با رویکرد شکل(۱۰)، تفاوت فاحشی ندارد و تفاوت آن‌ها در این است که در این دسته‌بندی حملات مبتنی بر موتورهای جستجوگر نیز معرفی شده است:



شکل ۱۱: دسته‌بندی حملات فیشینگ به دو رویکرد مبتنی بر مهندسی اجتماعی و بدافزار[٦]

[1] Cross Site Scripting
[2] Session Hijacking
[3] Malware Phishing
[4] DNS Poisoning
[5] Key/Screen Logger

۴- نتیجه‌گیری

امنیت فضای اینترنت به عنوان یکی از چالش‌های مهم در حوزه‌ی امنیت فضای مجازی شناخته می‌شود. امروزه چالش‌های امنیتی مختلفی نظیر ویروس[۱]، کرم[۲]، تروجان[۳] و بدافزارها[۴] امنیت اینترنت را به چالش می‌کشانند و باعث می‌شوند که گسترش فضای مجازی[۵] و تجارت الکترونیک با مشکلات مختلفی مواجه شوند. از جمله چالش‌های امروزی در اینترنت می‌توان به انواع حملات مختلف به زیرساخت‌های اینترنت نظیر حملات سایبری[۶] و سرقت اطلاعات یا حملات فیشینگ[۷] اشاره نمود. حملات فیشینگ از جمله حملات مخرب است که کاربران آنلاین و اطلاعات شخصی آن‌ها را هدف قرار می‌دهد. حملات فیشینگ نوعی از حملات مهندسی اجتماعی[۸] محسوب می‌شود که در آن حمله‌کننده[۹] یا هکر[۱۰] سعی می‌کند اعتماد کاربران را جلب نموده و آن‌ها را به سمت صفحات وب جعلی[۱۱] که ظاهر بسیار شبیهی به صفحات قانونی و اصلی[۱۲] دارند، هدایت نمایند سپس در فرصت مناسب اطلاعات مهم آن‌ها نظیر نام کاربری و کلمه عبور آن‌ها را سرقت نموده و از این اطلاعات با ارزش جهت سرقت اطلاعات آن‌ها نظیر حساب‌های مالی استفاده نمایند. سایت‌های جعلی به صورت برق‌آسا در اینترنت ایجاد می‌شوند و به سرعت عملیاتی می‌شوند و حجم انبوهی از ایمیل‌های جعلی نیز در زمان اندک برای کاربران ارسال می‌شوند تا آن‌ها را فریب داده و به وب‌سایت‌های جعلی هدایت نمایند. یکی از دلایل اینکه سایت‌های جعلی عمر اندکی دارند می‌تواند دلایلی مانند بلوکه شدن دامنه‌ی آن‌ها و پنهان نمودن ماهیت سرقت باشد و با انجام چندین سرقت سایت جدیدی ایجاد می‌شود. حملات فیشینگ نوعی از حملات فریب و مبتنی بر مهندسی اجتماعی است که هدف آن‌ها سرقت اطلاعات کاربران اینترنتی است و در این نوع حملات یک وب‌سایت جعلی به جای وب‌سایت اصلی خود را معرفی نمود و اطلاعات کاربران را مورد سرقت قرار می‌دهد. سرقت اطلاعات کاربران توسط وب‌سایت‌های جعلی در حملات فیشینگ زیان قابل توجهی به کاربران وارد می‌نماید و از این جهت تلاش زیادی می‌شود تا این حملات شناسایی شوند و برای شناسایی آن‌ها می‌تواند ویژگی حملات را به کمک روش‌های کشف دانش مورد یادگیری قرار داد تا یک مدل جهت تشخیص وب‌سایت‌های جعلی از وب‌سایت‌های قانونی ایجاد شود. در این مقاله‌ی مروری بر صفحات جعلی و حملات فیشینگ مرتبط با آن‌ها کار شد تا کاربران بتوانند این صفحات جعلی را شناسایی و کمتر در تله‌ی آن‌ها گرفتار شوند. در پژوهش آتی تلاش می‌شود با استفاده از روش‌های یادگیری ماشین صفحات جعلی در اینترنت تشخیص داده شود.

منابع

[1]. Jain, A. K., & Gupta, B. B. (2018). PHISH-SAFE: URL Features-Based Phishing Detection System Using Machine Learning. In *Cyber Security: Proceedings of CSI 2015* (pp. 467-474). Springer Singapore.

[2]. Pande, D. N., & Voditel, P. S. (2017, March). Spear phishing: Diagnosing attack paradigm. In *Wireless Communications, Signal Processing and Networking (WiSPNET), 2017 International Conference on* (pp. 2720-2724). IEEE.

[1] Virus
[2] Worm
[3] Trojans
[4] Malware
[5] Cyberspace
[6] Cyber attacks
[7] Phishing
[8] Social engineering
[9] Phisher
[10] Hacker
[11] Fake web pages
[12] Legitimate web pages

[3]. Choudhary, N., & Jain, A. K. (2017, March). Comparative analysis of mobile phishing detection and prevention approaches. In *International Conference on Information and Communication Technology for Intelligent Systems* (pp. 349-356). Springer, Cham.

[4].Nakamura, Y., Kanazawa, S., Inamura, H., & Takahashi, O. (2018, February). Classification of unknown Web sites based on yearly changes of distribution information of malicious IP addresses. In *New Technologies, Mobility and Security (NTMS), 2018 9th IFIP International Conference on* (pp. 1-4). IEEE.

[5].Sonowal, G., & Kuppusamy, K. S. (2017). PhiDMA–A phishing detection model with multi-filter approach. *Journal of King Saud University-Computer and Information Sciences*.

[6].Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629-3654.

[7].Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247-267.

[8]. Oest, A., Safei, Y., Doupé, A., Ahn, G. J., Wardman, B., & Warner, G. (2018, May). Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis. In *APWG Symposium on Electronic Crime Research (eCrime), 2018* (pp. 1-12). IEEE.

[9]. Goel, D., & Jain, A. K. (2017). Mobile phishing attacks and defence mechanisms: state of art and open research challenges. *Computers & Security*.

[10]. Airehrour, D., Vasudevan Nair, N., & Madanian, S. (2018). Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. *Information*, *9*(5), 110.

[11]. Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review*, *17*, 1-24.

[12]. Tan, C. L., Chiew, K. L., & Wong, K. (2016). PhishWHO: Phishing webpage detection via identity keywords extraction and target domain name finder. *Decision Support Systems*, *88*, 18-27.

[13]. Volkamer, M., Renaud, K., Reinheimer, B., & Kunz, A. (2017). User experiences of TORPEDO: tooltip-powered phishing email detection. *Computers & Security*, *71*, 100-113.

[14]. Iuga, C., Nurse, J. R., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, *6*(1), 8.

[15]. Jain, A. K., & Gupta, B. B. (2016). A novel approach to protect against phishing attacks at client side using auto-updated white-list. *EURASIP Journal on Information Security*, *2016*(1), 9.

[16]. Babagoli, M., Aghababa, M. P., & Solouk, V. (2018). Heuristic nonlinear regression strategy for detecting phishing websites. *Soft Computing*, 1-13.