شیوع فیشینگ چالش نظام عدالت کیفری ایران

رشد و گسترش میزان بهره‌مندی از فضای مجازی و نقش اینترنت در تسهیل ارتباطات و ایجاد ساختارهای نوین اجتماعی انکارناپذیر است. افراد به طرق گوناگون، از جمله استفاده از لپ تاپ، گوشی‌های تلفن همراه، تبلت، ایکس باکس و غیره به اینترنت متصل می‌شوند. به عنوان مثال، طی چند سال اخیر استفاده از خدمات آنلاین، از سطح یک جستجوی ساده در گوگل، به جستجوی پیشرفته‌ی مکان‌ها، تقویم‌ها، نشانی‌ها، ویدیوها، سرگرمی‌ها، ایمیل‌های صوتی و تماس‌های تصویری رسیده است. بسیاری از افراد در سراسر جهان، جزئیات زندگی خود را بر روی شبکه‌های اجتماعی از جمله فیسبوک و توییتر قرار داده و با میل و اراده‌ی خویش روابط خود با دوستان، خانواده و همکاران خود را به نمایش عمومی می‌گذارند. میلیون‌ها برنامه‌ی اینترنتی جهت انجام کارهای مختلف از امور بانکی گرفته تا آرشیو کردن تصاویر، توسط کاربران دانلود می‌شود.

پایگاه اینترنتی «سازمان داده‌ها و آمار جهانی اینترنت» که مرکز آن در آمریکا می‌باشد، اخیراً لیستی از تعداد کاربران اینترنتی دنیا منتشر کرده است که ایرانیان در لیست فوق در رده سیزدهم تعداد کاربران جهان قرار دارند.

در آمار سازمان داده‌ها و آمار جهانی اینترنت ذکر شده است که ایران با داشتن ۳۳ میلیون و ۲۰۰ هزار کاربر که معادل ۴۳ درصد جمعیت ۷۷ میلیونی ایران است، مقام سیزدهم تعداد کاربران اینترنتی جهان را به خود اختصاص داده و جزو بیست کشوری می‌باشد که کاربران اینترنتی زیادی دارند.

امروزه اینترنت علاوه بر مزایای فراوانی که در جهت تسهیل بسیاری از امور کاربران به آنها ارائه می‌دهد، به بستری برای وقوع جرائم جدید و پیچیده مبدل گردیده است. جرائمی که تا پیش از ظهور فناوری‌های نوین در این حوزه هویت خارجی نداشتند اما امروزه به موضوعاتی جدی و قابل تأمل تبدیل گردیده اند که عدم توجه کافی به آنها می‌تواند موجب بروز مشکلات متعددی برای نظام‌های قضایی گردد.

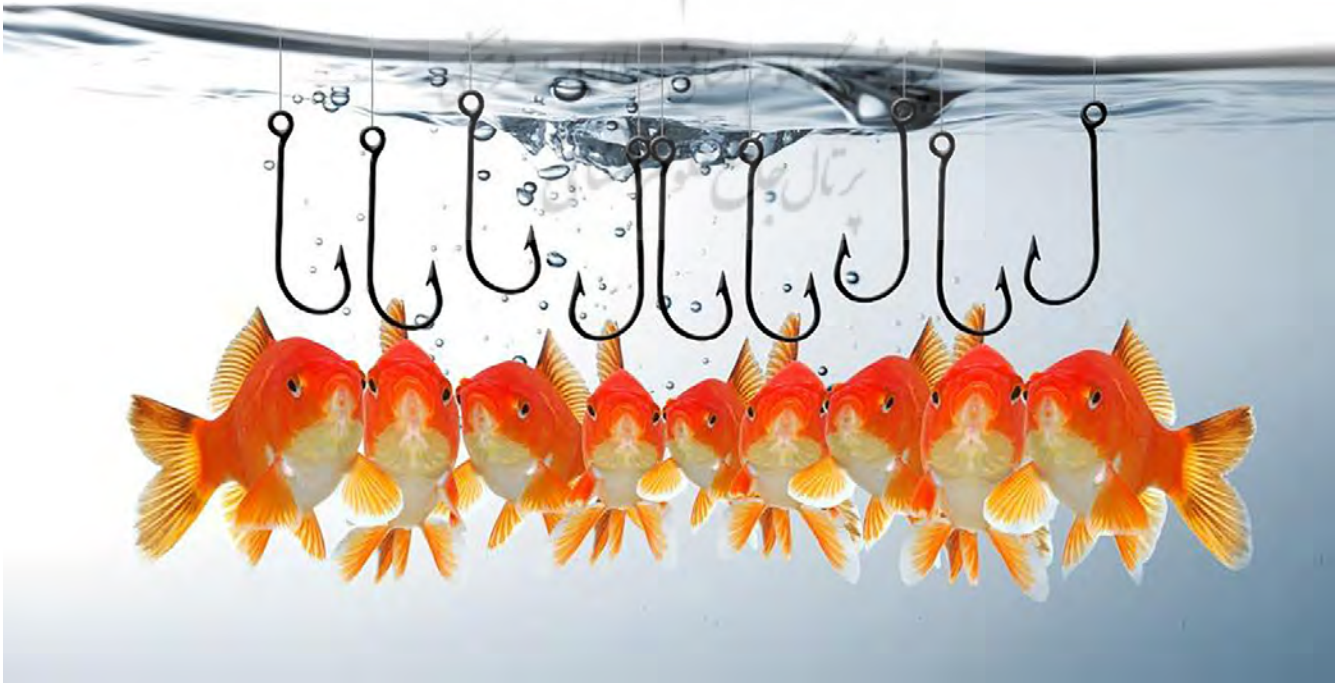
از آن جایی که جرائم حوزه‌ی سایبر در زمره‌ی موضوعات نسبتاً جدیدی قرار می‌گیرد که در سطح جهانی موجب بروز مشکلات و چالش‌های فراوانی برای نظام‌های قضایی گردیده است و با توجه به فراهم بودن امکان دسترسی به اینترنت به عنوان زمینه و بستر وقوع این نوع جرائم برای جامعه‌ی ایرانی و نیز مشاهده‌ی برخی از نشانه‌های وقوع آن در داخل کشور، اتخاذ تدابیر پیش دستانه در این باب و ارائه‌ی آموزش‌های لازم جهت پیشگیری از وقوع این قبیل جرائم امری ضروری به نظر می‌رسد.

بنابراین، با توجه به نوظهور بودن موضوع جرائم سایبری در کشور ما و نیز ضرورت شناخت کافی نسبت به این نوع پدیده‌ها جهت مواجهه با آنها، در هر شماره از نشریه‌ی حاضر به یکی از پدیده‌های جدید در حوزه‌ی فناوری که ممکن است از مصادیق برخی جرائم نیز باشد، پرداخته می‌شود.

فیشینگ روشی است که در آن مجرمین در قالب یک وب سایت جعلی با ظاهری موجه و قانونی اقدام به کسب اطلاعات سودمند و معمولا مالی نظیر شماره و رمز کارت‌های اعتباری می‌نمایند.

فیشینگ

یکی از متداول ترین کلاهبرداری‌های اینترنتی تحت عنوان فیشینگ تعریف می‌شود. فیشینگ روشی است که در آن مجرمین در قالب یک وب سایت جعلی با ظاهری موجه و قانونی اقدام به کسب اطلاعاتی نظیر شماره و رمز کارت‌های



امروزه، گروه‌های سازمان یافته‌ی مجرمین که با استفاده از این روش کلاهبرداری می‌نمایند، تلاش می‌کنند تا کاربران را ترغیب به کلیک کردن بر روی لینکی کنند که آنها را به صفحه‌ی وب سایت جعلی که توسط کلاهبرداران کنترل می‌شود، وارد می‌کند. این صفحات تقلبی غالباً صفحه‌ی وب سایت بانک‌ها، شرکت‌های تلفن و ...

اعتباری می‌نمایند. اصطلاح فیشینگ از املای کلمه‌ی fishing به معنای ماهیگیری گرفته شده و شیوه‌ی انجام آن تلاش برای به دام انداختن یک ماهی بی‌گناه از طریق نوک زدن به طعمه که همان لینک مخرب است، می‌باشد. اصطلاح فیشینگ برای نخستین بار در سال ۱۹۹۶ و در مورد سرویس خبری وب سایت امریکا آنلاین مورد استفاده قرار گرفت و آنچه بعدها به یک موضوع مجرمانه‌ی مهم تبدیل شد، برای اولین بار در این وب سایت به وقوع پیوست. پیش از این‌ها، زمانی که امریکا آنلاین(AOL) بهترین ارائه دهنده‌ی خدمات اینترنتی محسوب می‌شد، میلیون‌ها نفر روزانه به طور آنلاین از سرویس‌های مختلف آن استفاده می‌کردند. طبیعتاً محبوبیت و درآمد فراوان این شرکت در آن زمان توجه مجرمین را به آن جلب می‌نمود. در ابتدا هکرها و کسانی که به کار تجارت نرم افزارهای غیرقانونی مشغول بودند، از خدمات اینترنتی این شرکت برای ارتباط با یکدیگر استفاده می‌کردند. کمی بعد، این گروه از مجرمین که به نام خانواده‌ی وارز شناخته می‌شدند، برای اولین بار حملات فیشینگ را طراحی و اجرا نمودند.

نخستین روشی که از طریق آن مجرمین اقدام به حملات فیشینگ کردند استفاده از الگوریتم هایی جهت ایجاد شماره‌های تصادفی کارت‌های اعتباری بود. از این شماره‌های تصادفی برای باز کردن حساب‌های AOL استفاده می‌شد. در همان سال، شرکت به منظور جلوگیری از چنین سوء استفاده هایی از حساب‌های کارت‌های اعتباری کاربران، اقدام به ایجاد تمهیدات امنیتی پیشرفته تر در سیستم‌های خود کرد.

با جلوگیری از سوء استفاده از شماره‌های تصادفی کارت‌های اعتباری، مجرمین اقدام به طراحی تکنیک‌های دیگری نمودند که بعدها به یک روش متداول جهت کلاهبرداری تبدیل گردید. آنها از طریق سیستم پیام رسان و ایمیل شرکت AOL، و با معرفی خود به عنوان کارمندان این شرکت اقدام به ارسال پیام به کاربران نمودند. در این پیام‌ها از کاربران خواسته می‌شد که اطلاعات حساب خود را به روز رسانی نمایند و یا اطلاعات مربوط به پرداخت صورتحساب خود را تأیید نمایند. در اکثر موارد کاربران به دام مجرمین می‌افتادند؛ چرا که این روش کاملاً جدید بوده و تا آن زمان از چنین ترفندی برای کلاهبرداری استفاده نشده بود. به دنبال وقوع این نوع خاص از سوء استفاده‌ی اینترنتی، شرکت AOL مجبور شد تا به کاربران سیستم پیام رسان و ایمیل خود هشدار بدهد که از ارائه‌ی اطلاعات مهم و حساس خود از این دو طریق اجتناب نمایند.

امروزه، گروه‌های سازمان یافته‌ی مجرمین که با استفاده از این روش کلاهبرداری می‌نمایند، تلاش می‌کنند تا کاربران را ترغیب به کلیک کردن بر روی لینکی کنند که آنها را به صفحه‌ی وب سایت جعلی که توسط کلاهبرداران کنترل می‌شود، وارد می‌کند. این صفحات تقلبی غالباً صفحه‌ی وب سایت بانک‌ها، شرکت‌های تلفن، سامانه‌های مربوط به امور بازنشستگان و اپراتورهای تلفن همراه سراسر جهان بوده و بیشترین قربانیان آن، شهروندان ایالات متحده‌ی امریکا، انگلستان و آلمان می‌باشد. تمامی حملات سایبری مبتنی بر روش فیشینگ به یک کاربر نامطمئن وابسته است که بر روی لینک یا پیوست یک ایمیل کلیک نموده و از این طریق یا به یک صفحه‌ی وب سایت جعلی وارد می‌شود و یا یک بدافزار را روی سیستم کاربری خود نصب می‌کند.

به عنوان مثال، شخص کاربری که دارای حساب در بانک ملی ایران است، ایمیلی با آدرس security@bmi.ir دریافت می‌کند که در آن به وی اعلام می‌شود که لازم است پروفایل خود را به روزرسانی کند و یا اینکه حساب بانکی او به علت مشاهده‌ی فعالیت‌های مشکوک مسدود شده است. در این حالت و از آنجایی که محتویات ایمیل مهم به نظر می‌رسد، کاربر ترغیب می‌گردد که آن را باز کند. با وارد شدن به صفحه، از شما خواسته می‌شود که برای ورود به سامانه ابتدا نام کاربری و رمز عبور و یا سایر اطلاعات شخصی خود را وارد نمایید و پس از آن است که مجرمین کار خود را آغاز می‌نمایند. این اولین مرحله‌ی کار مجرمین است که از طریق آن به داده‌های مورد نظر خود دست پیدا می‌کنند و در مرحله‌ی بعدی اقدام مجرمانه‌ی خود مانند سرقت هویت، کلاهبرداری مالی، کلاهبرداری مالیاتی و کلاهبرداری بیمه‌ای را علیه شما به انجام می‌رسانند.

منابع:

1. Goodman, M. (2015). Future Crimes: everything is connected, everyone is vulnerable and what we can do about it. New York: Doubleday.

2. سرویس اقتصادی (2016). کاربران اینترنت در ایران 187 برابر شد. Retrieved 2017, from TasnimNews: www.tasnimnews.com

3. Main. (2014). Retrieved 2017, from Webopedia: http://www.webopedia.com/TERM/P/phishing.html

4. History of Phishing. (n.d.). Retrieved 2017, from Phishing: http://phishing.org/history-of-phishing.html