فیشینگ چیست؟

از ویکی‌پدیا، دانشنامهٔ آزاد

رمزگیری یا ماهیگیری یا تله‌گذاری یا فیشینگ Phishing به تلاش برای به دست آوردن اطلاعاتی مانند نام کاربری، گذرواژه، اطلاعات حساب بانکی و مانند آن‌ها از طریق جعل یک وبگاه، آدرس ایمیل و مانند آن‌ها گفته می‌شود.

به بیان ساده‌تر هنگامی که شخصی تلاش می‌کند دیگری را فریب دهد تا اطلاعات شخصی او را در اختیارش بگیرد، یک حمله فیشینگ رخ می‌دهد و یک بازار غیرقانونی چند هزار میلیاردی را تشکیل داده است.

شبکه‌های اجتماعی و وبگاه‌های پرداخت آنلاین از جمله اهداف حملات فیشینگ هستند. علاوه بر آن، ایمیل‌هایی که با این هدف ارسال می‌شوند و حاوی پیوندی به یک وبگاه هستند در اکثر موارد حاوی بدافزار هستند.

بر طبق گزارش سالانه شرکت پروف‌پوینت که ۳ اسفند ۱۴۰۰ منتشر شد بیش از ۸۰ درصد از سازمان‌ها، حداقل یک حمله موفق ماهیگیری را در سال ۲۰۲۱ تجربه کردند که در مقایسه با سال قبل از آن افزایشی حدود ۴۶ درصد را نشان می‌دهد.

تاریخچه

روش فیشینگ با جزئیات در سال ۱۹۸۷ (میلادی) توضیح داده شد. این واژه برای نخستین‌بار در سال ۱۹۹۵ (میلادی) مورد استفاده قرار گرفت. واژهٔ فیشینگ کوته‌نوشت گزاره Password Harvesting Fishing شکار گذرواژه کاربر از طریق یک طعمه است که در آن حرف Ph به جای F برای القای مفهوم فریفتن جایگزین شده‌است و از بنیان گذاران آن در ایران، می‌توان به فرشید امیر شقاقی و مانی رضوان اشاره کرد.

نحوه کار فیشینگ

فیشینگ یا سرقت آنلاین، در عمل به صورت کپی دقیق رابط گرافیکی یک وبگاه معتبر مانند بانک‌های آنلاین انجام می‌شود. ابتدا کاربر از طریق ایمیل یا آگهی‌های تبلیغاتی سایت‌های دیگر، به این صفحه قلابی راهنمایی می‌شود. سپس از کاربر درخواست می‌شود تا اطلاعاتی را که می‌تواند مانند اطلاعات کارت اعتباری مهم و حساس باشد آنجا وارد کند. در صورت گمراه شدن کاربر و وارد کردن اطلاعات خود، فیشرها به اطلاعات شخص دسترسی کاربر پیدا می‌کنند. از جمله سایت‌های هدف این کار می‌توان سایت‌های پی‌پال، ای‌بی و بانک‌های آنلاین را نام برد.

اطلاعاتی که سایت‌های فیشینگ ممکن است از کاربران بخواهند:

- نام کاربری و رمز عبور شما
- شماره تلفن های شما
- شماره های مربوط به حساب های بانکی
- کدهای خصوصی مربوط به هر شخص
- شماره های مربوط به کارت های اعتباری
- سال روز تولد شما
- اطلاعات مربوط به هویت شما
- پرسش سوال هایی مانند آنچه شما دوست دارید؟
- درخواست اطلاعات خانوادگی شما (نام پدر و مادر و...)

راه های پی بردن به صفحات فیشینگ

یکی از راه های اصلی پی بردن به جعلی بودن درگاه پرداخت این است که دامنه شاپرک فقط ir. است. بنابراین در صورتی که با دامنه های com. یا org. یا سایر دامنه ها مواجه شدید، قطعا درگاه پرداخت جعلی است.

بررسی اینکه آیا دامنه اصلی دقیقا برابر shaparak.ir است، جهت اطمینان حاصل کردن از اصلی بودن درگاه پرداخت کافی است.

ممکن است بخواهید جهت بررسی اصلی بودن درگاه پرداخت، در ابتدا رمز دوم خود را اشتباه وارد کنید و سپس در صورتی که پاسخ درگاه «رمز وارد شده صحیح نمیباشد » بود، از صحت درگاه پرداخت اطمینان حاصل کنید، اما این روش قابل اطمینان نمی‌باشد. زیرا که شخص هکر میتواند تمامی پاسخها را به «رمز وارد شده صحیح نمیباشد » تغییر دهد یا اینکه پاسخها را به صورت تصادفی به شما نشان دهد.

رمز دوم یکبار مصرف (رمز پویا) کارت بانکی خود را فعال کنید تا در صورتی که اطلاعات کارت بانکی شما به سرقت رفت، مهاجمان نتوانند مبلغ زیادی را از حساب شما برداشت کنند. سقف تراکنش غیرحضوری بدون رمز دوم پویا و با رمز دوم ایستا برای تمامی بانکها به مبلغ ۱۰۰ هزارتومان کاهش پیدا کرده است.

جعل و دستکاری پیوندها و آدرس‌ها

این روش یکی از شیوه‌های متداول فیشینگ است. در این روش، پیوندها و آدرس‌های سازمان‌ها و شرکت‌های غیرواقعی و جعلی از طریق ایمیل ارسال می‌شوند. این آدرس‌ها با آدرس‌های اصلی تنها در یک یا دو حرف تفاوت دارند.

گریز از فیلترها

فیشرها برای جلوگیری از شناسایی متن‌های متداول فیشینگ در ایمیل‌ها توسط فیلترهای ضد فیشینگ از نگاره به جای نوشته استفاده می‌کنند.

جعل وبگاه

برخی از فیشرها از جاوااِسکریپت برای تغییر آدرس در نوار آدرس مرورگر استفاده می‌کنند تا هیچ جای شکی برای قربانی نماند. یک مهاجم حتی می‌تواند به کمک تزریق اسکریپت از طریق وبگاه از ایرادهای موجود در اسکریپت‌های یک سایت معتبر علیه خودش استفاده کند. در این نوع فیشینگ، از کاربر خواسته می‌شود تا در بانک خودش لاگین کند. ظاهراً همه چیز عادی است. از آدرس وبگاه گرفته تا گواهینامه امنیتی Security Certificates اما در واقعیت، پیوند به آن وبگاه دستکاری می‌شود تا با استفاده از عیب‌های موجود در اسکریپت‌های آن وبگاه، حمله انجام شود. با این حال این روش نیازمند دانش و آگاهی بالایی است. از این روش در سال ۲۰۰۶ برای حمله به وبگاه پی‌پل استفاده شد.

فیشینگ هم‌نگاره

ماهیگیری هم‌نگاره Homograph Phishing تکنیکی است که در آن از نویسه های مشابه با نویسه های یک سایت واقعی به‌منظور جعل نشانی سایت و در نتیجه قابل باور ساختن آن از دید کاربر استفاده می‌شود.

فیشینگ تلفنی

همه حملات فیشینگ نیازمند وبگاه قلابی نیستند. پیام‌هایی که ظاهراً از طرف بانک فرستاده شده و از کاربر می‌خواهد تا مثلاً به دلیل وجود ایراد در حسابشان، شماره خاصی را شماره‌گیری کنند نیز می‌تواند حمله فیشینگ باشد. پیش از گرفتن شماره (که متعلق به فیشر است و با سرویس صدا روی پروتکل اینترنت فراهم شده‌است)، از کاربر خواسته می‌شود تا شماره حساب و پین PIN خود را وارد کند.

فیشینگ نیزه‌ای

فیشینگ نیزه‌ای Spear Phishing تلاش‌های فیشینگ برای افراد یا شرکت‌های خاص، «فیشینگ نیزه‌ای» یا «هدفمند» نامیده می‌شود. برخلاف فیشینگ فله‌ای، مهاجمان فیشینگ نیزه‌ای، بیشتر برای افزایش احتمال موفقیت از هدف خود، اطلاعات شخصی، گردآوری کرده و از آن استفاده می‌کنند.

گروه خرس فانتزی روسیه از روش فیشینگ نیزه‌ای برای هدف گرفتن ایمیل‌های ستاد انتخاباتی هیلاری کلینتون در هنگام انتخابات ریاست‌جمهوری ایالات متحده آمریکا (۲۰۱۶) استفاده کردند. آن‌ها به بیش از ۱۸۰۰ حساب کاربری گوگل حمله کردند و دامنه accounts-google.com را برای تهدید کاربران هدف، به کار گرفتند.

روش‌های مقابله

استفاده از نرم‌افزارهای ضد هک و فیشینگ مانند کومودو اینترنت سکیوریتی که با دیوار آتش قدرتمند خود مانع هک شدن می‌شود. برای جلوگیری از افزایش آمار فیشینگ و سرقت اطلاعات باید آگاهی کاربران را افزایش داد. نباید به ایمیل‌هایی که از شما در آن‌ها خواسته شده تا فرمی را پر کنید اطمینان کرد. نباید اطلاعات حساب کاربری خود را در اختیار سایت‌ها قرار داد. کاربران برای پرداخت آنلاین باید از درگاه‌های مخصوص بانک‌ها استفاده کنند. تلاش کنید به ایمیل‌های داخل اسپم در حساب کاربری‌تان بی‌اعتنا باشید و آن‌ها را پاک کنید.

توجه به پیوندها

یکی از ساده‌ترین روش‌های مقابله با فیشینگ، دقت به آدرس وبگاه یا ایمیل دریافت شده‌است. برای نمونه در زمان ورود به حساب‌های حساس مانند ایمیل یا بانک، پیش از وارد کردن نام کاربری و گذرواژه، دقت به آدرس وبگاه حیاتی است.