فیشینگ نوعی عمل مجرمانه است که در آن کلاهبردار (فیشر) سعی می‌کند با فریب دادن افراد، اطلاعات حساس آن‌ها مانند کلمات عبور، اطلاعات کارت بانکی یا چیزهایی شبیه به این را به دست آورد. به هر سایت و هر پیامی اعتماد نکنید، چون خطر فیشینگ یا همان سرقت اطلاعات شما را تهدید می‌کند. در این پست به زبان ساده فیشینگ، انواع آن و روش‌های جلوگیری از آن را توضیح می‌دهیم.

فیشینگ چیست؟

فیشینگ (Phishing) نوعی فعالیت کلاهبرداری است که در آن مجرمان سعی می‌کنند تا با فریب دادن افراد، اطلاعات حساس آن‌ها را به دست آورند. مهمترین اطلاعاتی که مجرمان برای دستیابی به آن‌ها فیشینگ انجام می‌دهند، کلمات عبور، اطلاعات کارت اعتباری، جزئیات حساب بانکی و ... هستند.

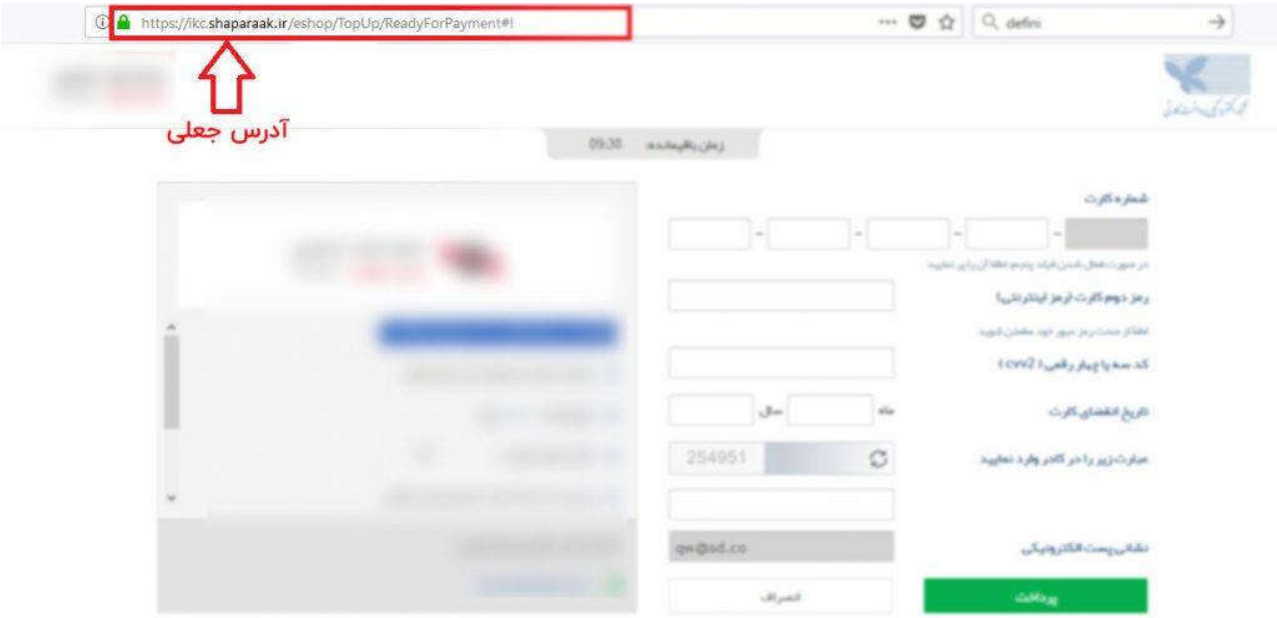
معمولا فیشینگ را از طریق جعل یک وب‌سایت (از نظر ظاهری و از نظر شباهت آدرس سایت)، ایمیل (ارسال ایمیل گول‌زننده) یا پیامک و تماس انجام می‌دهند.

فیشینگ نوعی حمله از طریق مهندسی اجتماعی است، زیرا در آن کاربر گول می‌خورد و خودش با دستان خودش اطلاعات را به مجرمان می‌دهد.

برای درک بهتر فیشینگ به این مثال توجه کنید:

فرض کنید که برای شما ایمیلی از طرف یک فروشگاه آنلاین کارت شارژ ارسال می‌شود که در آن نوشته شده است: «می‌توانید با کلیک بر روی لینک زیر کارت شارژ ۵۰۰۰ تومانی را با قیمت ۴۵۰۰ تومان خریداری کنید.»

شما با دیدن این تخفیف وسوسه شده، بر روی لینک خرید کلیک می‌کنید و به صفحه‌ای دقیقا مشابه با صفحه خرید اینترنتیِ بانک منتقل می‌شوید. اطلاعات کارت بانکی خود را برای خرید وارد می‌کنید. پس از مدت کوتاهی حساب بانکی شما خالی می‌شود، چون اطلاعات کارت بانکی خود را در یک صفحه تقلبی وارد کرده بودید که در نهایت به دست کلاهبرداران می‌رسد.



نمونه‌ای از فیشینگ درگاه بانکی

مثال فوق، فقط یک نمونه ممکن از فیشینگ بود. هزاران ترفند گوناگون می‌توانند برای انجام فیشینگ مورد استفاده قرار گیرند.

عاملان فیشینگ معمولا پیام‌های گول‌زننده را در قالب پیشنهادات وسوسه کننده (مثل همان مثال خرید ارزان کارت شارژ یا برنده شدن در قرعه‌کشی) یا در قالب اطلاعیه‌های هشدار (مثل تغییر سریع رمزعبور یا قطع حقوق و یارانه ماهانه) ارسال می‌کنند تا هر طور شده اطلاعات حساس کاربران را به چنگ آورند.

انواع Phishing

فیشینگ انواع مختلفی دارد و معمولا بر اساس هدف و نوع حمله طبقه‌بندی می‌شود. مشهورترین انواع فیشینگ عبارت‌اند از:

فیشینگ ایمیلی

این روش رایج‌ترین نوع فیشینگ است. کلاهبردار با ارسال یک ایمیل، خود را به جای فرد یا شرکت معتبر جا می‌زند و با تکنیک‌های گول‌زننده سعی می‌کند تا اطلاعات حساس را از قربانی بگیرد. این روش دو حالت دارد:

۱. قربانیان از فیشر (=کسی که قصد فیشینگ دارد) یک ایمیل دریافت می‌کنند که در آن فیشر خود را به عنوان یک فرد یا شرکت قابل اعتماد جا زده است و سعی می‌کند به صورت مستقیم اطلاعات مشخصی را از قربانیان بگیرد.
۲. قربانیان از فیشر یک ایمیل دریافت می‌کنند که در آن فیشر خود را به عنوان یک سایت قابل اعتماد جا زده و از قربانیان می‌خواهد که بر روی لینک موجود در ایمیل کلیک کرده و اطلاعات خود را وارد کنند.

حالت دوم بیشتر مورد استفاده قرار می‌گیرد.

فیشینگ هدف‌دار یا اسپیر فیشینگ(Spear Phishing)

این نوع فیشینگ، فرد یا افراد خاصی را مورد حمله قرار می‌دهد، به طوری که مهاجم ابتدا از قربانیان خود اطلاعاتی جمع‌آوری کرده و در پیام‌های خود از آن‌ها استفاده می‌کند تا فرد بیشتر اعتماد کند. مثلا در پیام خود از نام، نام خانوادگی، علایق، شماره تلفن و ... استفاده می‌کند تا قربانی به نامعتبر بودن ایمیل شک نکند.

مثلا این دو پیام را در نظر بگیرید:

۱. شما برنده قرعه‌کشی بانک **X** شده‌اید.
۲. جناب آقای محمد آذرنیوار، شما برنده قرعه‌کشی بانک **X** شده‌اید.

قطعا پیام دوم بیشتر از پیام اول می‌تواند اعتماد قربانی را به خود جلب کند.

نرم افزارهای مخرب

در این روش، فیشرها سعی می‌کنند تا روی دستگاه قربانی، یک برنامه آلوده به بدافزار را اجرا کنند. پس از فعال شدن بدافزار، مجرمان می‌توانند با دسترسی به کامپیوتر یا موبایل قربانی، اطلاعات حساس او را به چنگ آورند. بدافزارها یکی از رایج‌ترین ابزارهای انجام فیشینگ هستند.

از نرم افزارهایی که حاوی لینک یک صفحه تقلبی هستند هم برای انجام فیشینگ استفاده می‌شود. نرم‌افزار و بازی‌های جنجالی و اغلب تحت عناوین مستهجن (مثل صیغه‌یاب، ماهواره جیبی و ...) از خطرناک‌ترین نرم افزارهای مورد استفاده برای فیشینگ هستند.

فیشینگ در تلگرام/ نرم‌افزارهایی که قربانی می‌گیرند.

قربانی پس از نصب نرم‌افزارهای جعلی، اقدام به پرداخت مبلغ خدمات در داخل نرم‌افزار می‌کند، غافل از اینکه اطلاعات کارت بانکی خود را در اختیار کلاهبرداران گذاشته است.

فیشینگ پیامکی

در این روش به جای ایمیل از پیامک استفاده می‌شود. مهاجم خود را به جای یک سازمان یا شرکت بزرگ جا می‌زند و برای هدف خود پیامک ارسال می‌کند. محتوای پیامک به‌گونه‌ای نوشته می‌شود که هدف را مجاب به ارسال مستقیم اطلاعات یا کلیک بر روی یک لینک کند.

به عنوان مثال پیامکی ارسال می‌شود که شما برنده یک جایزه بزرگ شده‌اید و باید برای دریافت آن روی یک لینک کلیک کنید.

گاهی اوقات هم این پیامک‌ها به صورت هشدارآمیز ارسال می‌شوند. مثلا همین چند وقت پیش پیامکی به افراد ایرانی ارسال می‌شد با این مضمون که یارانه نقدی کاربر قطع شده است و برای ثبت نام مجدد باید به

لینک داخل پیامک وارد شوند. پس از وارد شدن به صفحه، از کاربران درخواست وارد کردن اطلاعات کارت بانکیشان می‌شد.

فیشینگ پیامکی

فیشینگ تلفنی

در این روش، یک کلاهبردار با استفاده از تماس تلفنی، با تکنیک‌های مختلف فرد را فریب می‌دهد تا اطلاعات حساس خود را به او اعلام کند. در این روش معمولا اطلاعات کارت بانکی افراد هدف نهایی است.

به عنوان نمونه، چندی پیش در ایران، مجرمی از داخل زندان با افراد ناآگاه تماس می‌گرفت و با کشاندنشان به پای خودپرداز و فریب دادن آن‌ها، رمز دومشان را بدست می‌آورد و اقدام به خالی کردن حسابشان می‌کرد.

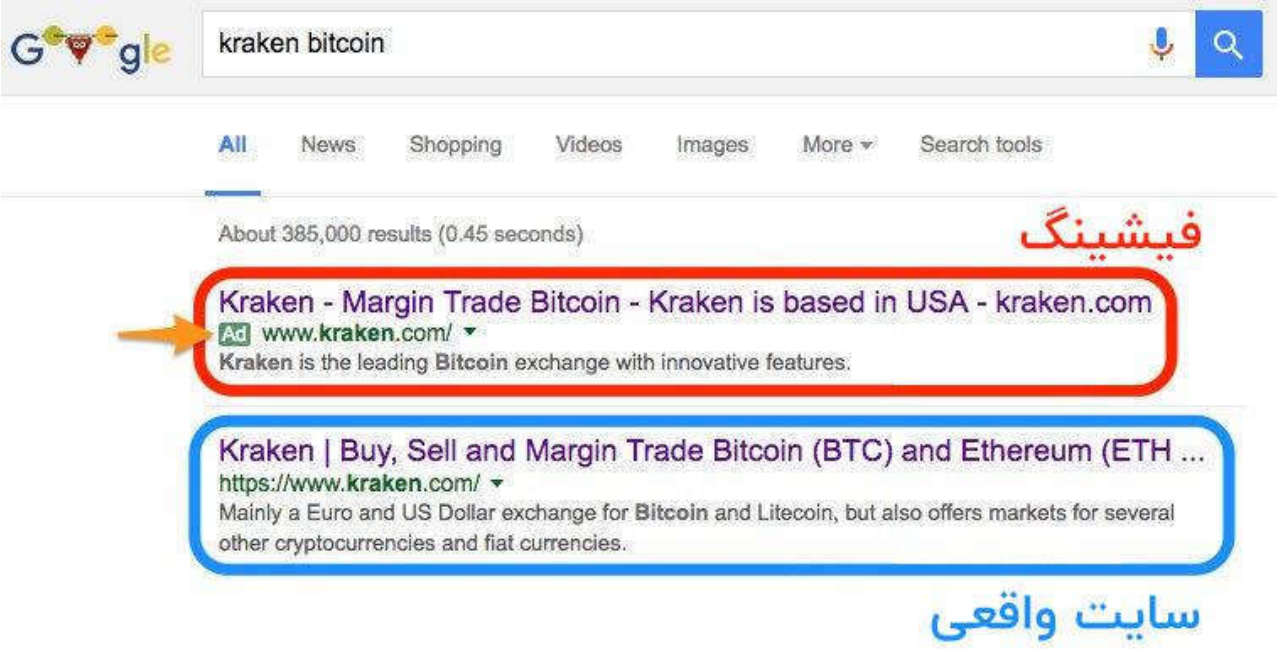
فارمینگ(Pharming)

در حمله فارمینگ، مجرمان سایبری فایل‌های هاست یک وب‌سایت یا سامانه نام دامنه (DNS) آن را دستکار می‌کنند. بنابراین وقتی کاربران برای ورود به سایت آدرس درست آن را وارد می‌کنند، بدون این‌که متوجه

شوند وارد یک صفحه تقلبی می‌شوند و در صورت وارد کردن اطلاعات، آن‌ها را تقدیم هکرها می‌کنند. این یکی از خطرناک‌ترین روش‌های فیشینگ است زیرا به دلیل صحیح بودن آدرس وب‌سایت، امکان تشخیص درست توسط کاربر وجود ندارد.

نتایج جستجو

در این حالت هکر با استفاده از روش‌های سئو یا تبلیغات در موتورهای جستجو، یک وب‌سایت جعلی را در نتایج بالا می‌آورد و کاربران بی خبر از همه جا، روی نتایج اولیه کلیک کرده و اطلاعات شخصی خود را در یک سایت مخرب وارد می‌کنند. البته این روزها موتورهای جستجوی بزرگ مثل گوگل با طرح‌های فیشینگ مبارزه می‌کنند اما گاهی اوقات این سایت‌ها هم در شناسایی این وب‌سایت‌های فیشینگ با مشکل مواجه می‌شوند.



نمونه واقعی. انجام فیشینگ با استفاده از تبلیغات گوگل با سوءاستفاده از صرافی کراکن/ خود صرافی کراکن در این خصوص یک اطلاعیه هشدار منتشر کرده است.

آدرس و صفحه مشابه تقلبی

در این روش، کلاهبردار از یک آدرس مشابه با سایت اصلی استفاده می‌کند تا کاربرانی را که سهوا آدرس سایت را اشتباه وارد می‌کنند به دام بیاندازد یا اینکه بتواند در ایمیل‌های تقلبی خود کاربران را دچار اشتباه کند.

به عنوان مثال آدرس سایت آمازون، Amazon.comاست. مجرم دامنه) Arnazon.com به حروف r و n دقت کنید که مشابه با m است (را خریداری کرده و سایتی با ظاهر سایت آمازون روی آن راه‌اندازی می‌کند. با این کار در صورتی که کاربران به اشتباه وارد سایت Arnazon.com شوند، با این خیال که در سایت اصلی آمازون هستند، اطلاعات کاربری خود را به کلاهبردار می‌دهند.

نمونه‌ای از فیشینگ اکانت‌های آمازون

به عنوان یک نمونه دیگر می‌توان به دامنه jimail.com اشاره کرد که از نظر تلفظی شبیه به gmail.com است. این آدرس برای مدتی فیشینگ اکانت‌های گوگل را انجام می‌داد که سرانجام متوقف شد.

هک و نفوذ از طریق شبکه‌های ارتباطی

این نوع از فیشینگ نیازمند دانش فنی بالا در هک و نفوذ به شبکه‌های ارتباطی است که در آن یک هکر با دستکاری یک ارتباط سالم، در میان مبدا و مقصد داده‌ها قرار می‌گیرد و به داده‌های تبادلی دسترسی پیدا می‌کند.

نوع دیگر فیشینگ استفاده از اتصال‌های بی‌سیم (وایرلس) است که در آن هکر با ایجاد یک نقطه دسترسی (به عنوان مثال wifi تقلبی)، کاربران را به دام می‌اندازد و از آن‌ها می‌خواهد که مثلا برای استفاده از اینترنت رایگان، اطلاعات شخصی خود را وارد کنند.

فیشینگ در ارزهای دیجیتال چگونه است؟

فیشینگ در حوزه‌های مالی یا به عبارتی در فضاهایی که بحث پول و دارایی در میان است، بیشتر از همه‌ی حوزه‌های دیگر انجام می‌شود و حوزه ارزهای دیجیتال هم از این قاعده مستثنی نیست.

در بحث ارزهای دیجیتال، مجرمان سایبری برای اجرای فیشنیگ، معمولا از ایمیل، صفحات یا برنامه‌های جعلی استفاده می‌کنند و در تلاش هستند تا با هدایت کاربران به این صفحات، کلید خصوصی یا دارایی کاربران را به سرقت ببرد.

به جز ارسال ایمیل‌های گول‌زننده که یک موضوع متداول است، یک مجرم سایبری می‌تواند سایتی کاملا مشابه با آدرس یک سایت صرافی یا کیف پول معتبر بسازد و اطلاعات ورود کاربران هدایت شده به آن سایت را دریافت کند.

آدرس جعلی یا صفحه تقلبی صرافی/کیف پول

به عنوان نمونه، سایت بایننس به آدرس Binance.com یک صرافی معتبر است. چندی پیش هکری با ساخت دامنه bïnance.com مبالغ زیادی را از کاربران لاتین زبان که اشتباها آدرس را وارد کرده بودند، به سرقت برد.

همچنین سایت مای‌اترولت به آدرس Myetherwallet.com یکی از معتبرترین وب‌سایت‌ها برای ساخت و دسترسی به کیف پول‌های اتریوم است. مدتی پیش یک هکر با ثبت یک آدرس مشابه و جعل حرف «t» در پایان آدرس این وب‌سایت، مقدار زیادی اتریوم سرقت کرد.

فیشینگ سایت مای‌اتر ولت – به کارکتر حرف **t** دقت کنید

کیف پول و نرم افزارهای معاملاتی تقلبی

در چند مورد دیگر مشاهده شده است که برنامه‌های تقلبی کیف پول، چند صد هزار دلار ارز دیجیتال را به سرقت برده‌اند، به این صورت که کاربران کیف پولِ جعلی، دارایی‌های خود را به آدرس موجود در کیف پول ارسال می‌کنند، غافل از اینکه این آدرس متعلق به هکر است. ربات‌های معامله‌گر یا تریدینگ همچنین یکی از مواردی هستند که احتمال فیشینگ در آن‌ها بالاست. نحوه کار این ربات‌ها به این صورت است که کاربران می‌توانند اطلاعات عبور خود در صرافی را در این ربات‌ها وارد کنند تا این نرم‌افزارها کارهای معاملاتی برنامه‌ریزی شده مانند خرید و فروش ارزهای دیجیتال به صورت خودکار را انجام دهند. حال اگر در این نرم افزارها فیشینگ انجام شود، اطلاعات ورود مشتریان در اختیار سازندگان نرم افزار قرار خواهد گرفت.

بدافزارهای فیشینگ در ارزهای دیجیتال

رایج‌ترین بدافزاری که برای سرقت ارزهای دیجیتال شما استفاده می‌شود، «تروجان» نام دارد. تروجان بعد از اجرا شدن در سیستم قربانی می‌تواند ورودی‌های کاربر به خصوص در کیبورد را برای هکر ارسال کند.

به عنوان مثال اگر در سیستم شما تروجان فعال باشد، بعد از تایپ کلمه عبور ورود به کیف پول، هکر هم از کلمه عبور شما اطلاع پیدا می‌کند و می‌تواند به سادگی دارایی‌های شما را به کیف پول خودش منتقل کند.

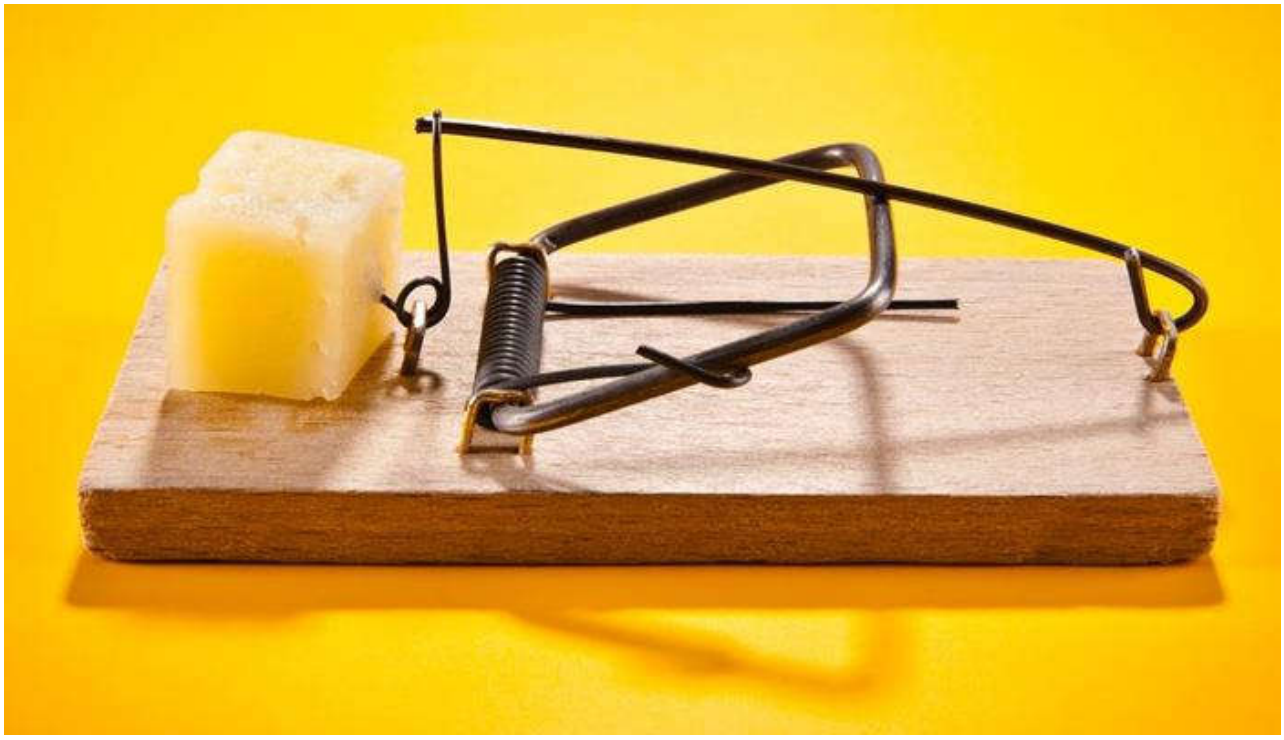
از دیگر بدافزارهای رایج در این زمینه «بدافزارهای کپی پیست» یا «کریپتو کلیپ‌برد هایجکر» (crypto clipboard hijacker) هستند. هنگامی که قربانی برای ارسال ارز دیجیتال آدرس یک کیف پول را کپی می‌کند، این بدافزار به طور خودکار آدرس کیف پول هکر را جایگزین آدرس کیف پول کپی شده می‌کند. به این ترتیب در صورت عدم توجه قربانی به آدرس گیرنده، ارزهای دیجیتال برای هکر ارسال می‌شوند.

افزونه‌های مرورگر هم می‌توانند در نقش بدافزار ظاهر شوند. تاکنون چندین مورد هک با افزونه‌های غیرمعتبر مرورگر گزارش شده است که توانسته بودند کلید خصوصی کاربران را به سرقت ببرند.

پروژه‌های ارز دیجیتال رایگان

طرح‌های کلاهبرداری که به کاربران وعده ارزهای دیجیتال رایگان را می‌دهند، یکی از ابزارهای خوب برای فیشینگ هستند. معمولا این طرح‌ها به کاربران وعده می‌دهند که در ازای کارهای ساده‌ای مثل عضویت در

سایت یا دعوت کردن افراد جدید، ارز دیجیتال رایگان پرداخت می‌کنند. این در حالی است که در نهایت هیچ ارز دیجیتالی پرداخت نمی‌کنند.



پنیر رایگان فقط در تله موش پیدا می‌شود!

ایمیل‌های جمع‌آوری شده از ثبت نام تعداد زیادی کاربر می‌تواند به کلاهبرداران در انجام فیشینگ کمک کند و جامعه هدف گسترده‌ای را در اختیارشان قرار دهد. همچنین در بعضی از این سایت‌ها، از کاربران خواسته می‌شود که با حساب‌های کاربری گوگل یا فیس‌بوک خود وارد شوند که خطر فیشینگ با صفحات تقلبی را به همراه دارد.

چگونه از فیشینگ جلوگیری کنیم؟

می‌توان بدون اغراق گفت که در نزدیک به ۹۹ درصد موارد، مقصر اصلی فیشینگ خودِ کاربر است، چون با کمی تفکر و توجه بیشتر می‌شود از آن جلوگیری کرد. همیشه پیام‌ها، تماس‌های دریافتی یا وب‌سایت‌هایی را که قصد وارد کردن اطلاعات حساس خود را دارید خوب و با دقت بررسی کنید. اجازه ندهید یک پیشنهاد وسوسه کننده یا احساس خطر، منطق را از شما بگیرد. همچنین:

لینک‌ها را بررسی کنید

در هر وب‌سایتی که نیاز به وارد کردن اطلاعات حساس بود، آدرس وب‌سایت را با دقت کامل بررسی کنید و به تمام کارکترهای آن دقت داشته باشید. به لینک‌هایی که با HTTP شروع می‌شوند وارد نشوید و حتما HTTPS بودن آن را بررسی کنید. البته به این نکته مهم توجه داشته باشید که HTTPS بودن تضمینی برای سالم بودن یک لینک نیست. همچنین مراقب لینک‌های کوتاه شده باشید زیرا ممکن است پشت آن یک لینک مخرب باشد.

به نتایج تبلیغاتی در موتورهای جستجو اعتماد نکنید

نتایجی که به صورت تبلیغات در موتورهای جستجو مثل گوگل به شما نمایش داده می‌شود، از دیگر نتایج قابل تشخیص است. نتایج تبلیغاتی که در کنار خود یک کلمه Ad (به معنای تبلیغات) دارند، یکی از روش‌های قدیمی برای انجام فیشینگ هستند. فیشر با پرداخت هزینه می‌تواند صفحه تقلبی خود را در موتورهای جستجو بالا بیاورند.

نرم‌افزارهای غیرمعتبر را نصب نکنید

نرم‌افزارهای مورد نیاز خود را فقط از منابع رسمی و معتبر دریافت کرده و از نصب نرم‌افزارهای مشکوک از منابع غیررسمی مانند شبکه‌های اجتماعی (مثل کانال‌ها و گروه‌های تلگرام) جدا خودداری کنید.

آپدیت مرورگرها و نصب آنتی ویروس‌ها را جدی بگیرید

به‌روزرسانی مرورگرهای وب و نصب آنتی ویروس‌ها تا حد زیادی در مقابله با فیشینگ به شما کمک می‌کند. مرورگرهای معروف وب مثل کروم، فایرفاکس و اپرا در نسخه‌های جدید خود به صورت مداوم الگوریتم‌های مبارزه با فیشینگ خود را تقویت می‌کنند. آنتی ویروس‌ها هم به شدت در مبارزه با بدافزارهای فیشینگ کاربردی هستند.


روشهای تشخیص کلاه‌برداری فیشینگ
چهار نکته مهم برای هر موقعیتی
ArzDigital
۱
شبکه‌های اجتماعی
به پیشنهادات رایگان اعتماد نکنید.
در شبکه‌های اجتماعی چنین چیزهایی رایگان توزیع نمی‌شوند.
مراقب نرم افزارهای استخراج آسان باشید.
آنها اغلب دارای بداقزار هستند. استخراج ارزهای دیجیتال نیازمند تخصص است و باید قبل از اقدام تحقیق کنید.
رمز و کلیدهای خصوصی خود را به هیچکس ندهید.
دادن کلید خصوصی به یک فرد مساوی است با دادن دارایی‌های موجود در آن کیف پول
۲
تبلیغات
هیچ‌وقت روی نتایج تبلیغاتی کلیک نکنید.
(به‌ویژه تبلیغات گوگل)
تعداد لینک‌های فیشینگ در تبلیغات گوگل به شدت بالاست.
آدرس سایت ورودی را حداقل دو بار بررسی کنید.
حتی اگر یک حرف از آدرس، متفاوت با آدرس سایت مورد نظر باشد، در سایت دیگری هستید.
سایت‌هایی که مرتبا بازدید می‌کنید را بوک‌مارک کنید.
یک راه آسان برای جلوگیری از هدایت به سایت های فیشینگ، این است که سایت‌هایی که مرتبا بازدید می‌کنید را بوک‌مارک یا ذخیره کنید.
۳
چت‌روم و موبایل
مراقب لینک‌های کوتاه شده باشید.
لینک‌های کوتاه شده آدرس مقصدی که شما به آن هدایت خواهید شد را مخفی میکنند.
تحت تاثیر ترس از دست دادن و عدم اطمینان قرار نگیرید.
کلاه‌برداران دوست دارند از ترس و عدم اطمینان به نفع خود استفاده کنند. همیشه منبع اطلاعات به دست رسیده را بررسی کنید.
برندگان واقعی گروه‌های پامپ و دامپ را بشناسید.
(شما هیچ‌وقت برنده نیستید)
مطمئن باشید همیشه گروه‌های سازمانی برنده هستند.
۴
فیشینگ ایمیل
همیشه فرستنده ایمیل را بررسی کنید.
فیشرهای ایمیل علاقه دارند که ایمیل‌های مخرب را از آدرسی بسیار شبیه به آدرس ایمیل‌های کسب وکار اصلی ارسال کنند.
از منابع نامعلوم هیچ فایلی دانلود نکنید.
(پی‌دی‌اف و عکس‌ها و غیره)
بله، حتی فایلهای پی دی اف و تصاویر ساده هم می‌توانند به نرم‌افزارهای مخرب پیوست شوند.
روی لینک‌های نامعلوم کلیک نکنید.
بهترین راه برای جلوگیری از هدایت به سایت‌های فیشینگ این است که همیشه آدرس خود را تایپ کنید یا از سرویس بوک‌مارک استفاده کنید.
ArzDigital
تهیه شده توسط ارز دیجیتال