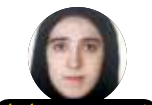
برخی هکرها می‌توانند سایتی را طراحی کنند که هیچ تفاوتی با ظاهر نسخه اصلی نداشته باشد اما سایت‌های معتبر یک نشان ای‌نماد یا دریافت کرده‌اند و در گوشه‌ای سایت خود نهاده‌اند

طبق تحقیقات انجام شده توسط ورایزن سایت‌های کلاهبردار توسط ۳۰ درصد افراد باز می‌شود و نیمی از این ۳۰ درصد در دام کلاهبرداران می‌افتند

چگونه حملات فیشینگ را شناسایی کنیم؟

فرار از دام جیب‌برهای مجازی



شیرین هنرمند اصل
روزنامه‌نگار

فیشینگ یکی از رایج‌ترین جرایم در فضای سایبری به شمار می‌رود و حمله فیشینگ به معنی فریب از طریق سایت‌ها و ایمیل‌های جعلی و سپس دزدیدن اطلاعات شخصی و محرمانه افراد مانند رمز عبور حساب‌های اینترنتی یا رمز کارت بانکی است. فیشینگ سهم بزرگی از انواع جرایم سایبری را در ایران در اختیار دارد و طرح رمز پویای کارت بانکی در همین راستا اجرا شده است. جالب است بدانید برخی افراد با وجود تأکیدات فراوان هنوز از رمز دوم ثابت برای مبالغ کمتر از ۱۰۰ هزار تومان استفاده می‌کنند و در خطر فیشینگ رمز کارت بانکی قرار دارند. فیشینگ درگاه پرداخت، فیشینگ پیامکی، فیشینگ تلفنی و فیشینگ حساب‌های اینترنتی مانند حساب جیمیل، اینستاگرام و سامانه دانشگاهی از انواع فیشینگ محسوب می‌شود.

برای درک بیشتر فیشینگ به یک مثال توجه کنید. مجرم یک لینک از طریق ایمیل یا پیامک‌هایی با موضوعاتی مانند دریافت جایزه یا پرداخت جریمه رانندگی به شخص هدف ارسال می‌کند. در حقیقت، مجرم با چنین موضوعاتی سعی دارد اعتماد فرد را به دست آورد تا او لینک پیامک یا ایمیل را باز کند. پس از بازشدن لینک توسط فرد ممکن است باج‌افزارهایی برای قفل‌کردن قسمتی از گوشی یا لپ‌تاپ و درخواست پول از قربانی و انواع بدافزارها بدون اطلاع او نصب شود.

همچنین ممکن است مجرم رمز بانکی یا رمز حساب کاربری دانشگاه یک فرد را از طریق سایتی جعلی که ظاهری کاملا شبیه درگاه بانک یا سایت دانشگاه دارد به دست آورد و از آن برای خالی‌کردن حساب بانکی یا فروش رمز برای کسب درآمد استفاده کند. در برخی مواقع، مجرم هیچ فردی را هدف قرار نداده و لینک مخرب را در شبکه‌های اجتماعی گذاشته است؛ بنابراین در شبکه‌های اجتماعی روی هر لینکی کلیک نکنید.

چگونه سایت‌های کلاهبردار را شناسایی کنیم؟

طبق تحقیقات انجام‌شده توسط ورایزن، سایت‌های کلاهبردار توسط ۳۰ درصد از افراد باز می‌شود و نیمی از این ۳۰ درصد در دام کلاهبرداران می‌افتند. در اولین مرحله برای شناسایی سایت‌های کلاهبردار، باید بدانیم سایت اصلی بانکی چه تفاوت‌هایی با سایت جعلی فیشینگ دارد. با ما همراه باشید تا با این تفاوت‌ها آشنا شوید.

به آدرس سایت دقت کنید

قبل از هر گونه خرید یا واردکردن هر گونه اطلاعات محرمانه، ابتدا به آدرس سایت دقت کنید. برای مثال، اگر شما به سوی سایتی شبیه شاپرک هدایت شده‌اید، آدرس آن سایت را با آدرس اصلی شاپرک مقایسه کنید. به احتمال زیاد اگر آدرس اصلی سایت را دقیق به خاطر نمی‌آورید، نام سایت را در گوگل یا سایر موتورهای جست‌وجو وارد می‌کنید تا آدرس دقیق سایت نمایش داده شود. بهتر است بدانید ممکن است آدرس سایت در اولین نتیجه جست‌وجو نباشد و هکرها سایت جعلی خود را در اولین نتیجه قرار داده باشند. همچنین ممکن است آن سایت آگهی گوگل باشد. به غلط املایی و حروف تکراری در آدرس و دامنه آنها دقت کنید. برای مثال، سایت‌های درگاه پرداخت باید به این شکل باشد: https://aaa.shaparak.ir.aaa. گاهی گوگل کروم با آیکونی قرمز نشان می‌دهد که سایت جعلی است یا ممکن است در صورت ورود با خطراتی مواجه شوید. روی نماد قفل در کنار لینک سایت در مرورگر کلیک کنید تا اطلاعاتی درباره امنیت سایت کسب کنید. علاوه بر گوگل کروم در مرورگرهای دیگر نیز نماد قفل وجود دارد.

اگر سایت جعلی باشد افزونه Shaparak Verifier یک پیام هشدار می‌فرستد و سپس شما را به یک صفحه اینترنتی سوق می‌دهد تا اطلاعات بیشتری کسب کنید

به نشان ای‌نماد سایت دقت کنید

ظاهر زیبا و آراسته سایت‌ها نمی‌تواند اعتبار آنها را نشان دهد. برخی هکرها می‌توانند سایتی را طراحی کنند که هیچ تفاوتی با ظاهر نسخه اصلی نداشته باشند. سایت‌های معتبر یک نشان ای‌نماد یا نماد اعتماد الکترونیکی از مرکز توسعه تجارت الکترونیکی دریافت کرده‌اند و در گوشه‌ای سایت خود نهاده‌اند. البته توجه کنید هر نشانی اصلی نیست. برخی سایت‌ها نشان ای‌نماد را جعل کرده و اقدام به کلاهبرداری می‌کنند. روی نشان ای‌نماد کلیک کنید و به تفاوت‌های نشانی باز شده با نشانی enamad.ir توجه کنید. آدرس سایت مشکوک باید به‌صورت دقیق و بدون هیچ‌گونه غلط املایی در مشخصات این صفحه معرفی شده باشد. توجه کنید این صفحه نباید یک عکس باشد.

به کد امنیتی سایت و کیبورد سایت مشکوک توجه کنید

یکی دیگر از راه‌های شناسایی سایت‌های کلاهبردار این است که صفحه را رفرش یا دوباره باز کنید. اگر کد امنیتی و جای اعداد صفحه کیبورد امن سایت تغییر نکند، سایت جعلی است. البته این راه نمی‌تواند برای همه سایت‌های جعلی کاربردی باشد؛ زیرا برخی هکرهای باتجربه می‌توانند سایتی را طراحی کنند که با هر بار رفرش، کد امنیتی و اعداد صفحه کیبورد امن تغییر کند.

افزونه ضدفیشینگ نصب کنید

اگر سایت جعلی باشد، این افزونه یک پیام هشدار خواهد فرستاد و سپس فرد را به یک صفحه اینترنتی سوق می‌دهد تا اطلاعات بیشتری کسب کند. جالب است بدانید افزونه ضدفیشینگ درگاه بانکی نیز در ایران طراحی شده و با نصب این افزونه از نشانی cert.semnan.ac.ir یا افزونه دیگری به نام Shaparak Verifier می‌توانید سایت‌های کلاهبردار را در مرورگر فایرفاکس و کروم شناسایی کنید.

به مطالب سایت مشکوک دقت کنید

یکی دیگر از راه‌های شناسایی سایت‌های کلاهبردار این است که نحوه نوشتار آنها را بررسی کنید. اگر مطالب آنها شامل غلط‌های املایی و نگارشی بسیاری است ممکن است سایت جعلی باشند. سایت‌های معتبر و قانونی در نگارش مطالب خود دقت می‌کنند و آنها را بدون هیچ‌گونه غلط املایی و علائم عجیب و غریب منتشر می‌کنند.

از سایت‌های بررسی لینک‌های مشکوک بپرسید

از این روش می‌توانید قبل از ورود به سایت مشکوک استفاده کنید. تنها کافی است آدرس سایت را در پیامک و ایمیل مشکوک کپی کنید و در سایت‌هایی مانند AVG Theatlabs، Kaspersky، PhishTank، ScanURL، VirusDesk و Google Transparency Report وارد کنید تا لینک شما را بررسی کنند و گزارشی درباره آن به شما تحویل دهند. تمرکز PhishTank روی بررسی لینک‌های فیشینگ است و بقیه سایت‌های معرفی‌شده می‌توانند امنیت سایت را نیز بررسی کنند. اگر سایت مشکوک موردنظر شما در PhishTank نباشد، یک کد پیگیری دریافت خواهید کرد. به خاطر داشته باشید هیچ کدام از روش‌های معرفی‌شده این گزارش نمی‌توانند به میزان صددرصد از حملات فیشینگ جلوگیری کنند. پس فقط به یک روش اکتفا نکنید. با افزایش دانش خود درباره انواع روش‌های فیشینگ می‌توانید به‌راحتی از بسیاری از حملات کلاهبرداران جلوگیری کنید.