فیشینگ چیست؟

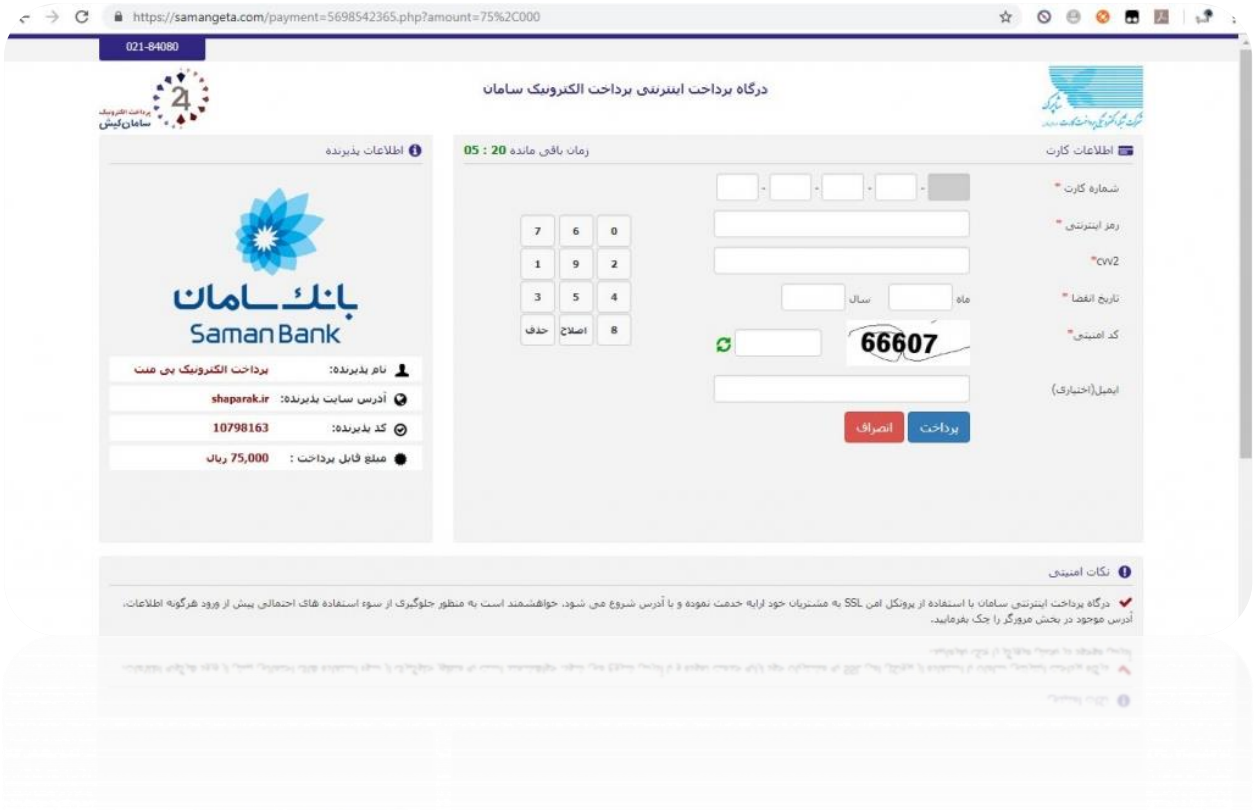
فیشینگ در زبان لاتین به معنای ماهی گیری می‌باشد و در اصطلاحات اینترنتی نوعی جرم محسوب می شود.فیشینگ روشی است که امروزه کلاهبرداران سایبری با استفاده از ابزارهای الکترونیکی ارتباطی و با فریب دادن و گمراه کردن کاربران، اطلاعات حساس و مهم کارت‌های بانکی، نام کاربری، رمز عبورو... را برای رسیدن به اهداف سودجویانه خود به سرقت می‌برند. در کلاهبرداری فیشینگ، قربانیان به‌صورت مستقیم اطلاعات حساس و محرمانه خود را در برنامه‌های کاربردی و وب‌سایت‌های جعلی که در ظاهر کاملاً شبیه به برنامه یا وب‌سایت اصلی و قانونی می‌باشد وارد می‌نمایند.یکی از شیوه‌های متداول و رایج در فیشینگ ارسال لینک‌ها و آدرس‌های جعلی و مخرب از طریق رایانامه می‌باشد .لینک‌هایی که ممکن است تنها تفاوت آن‌ها با آدرس اصلی یک یا دو حرف باشد، یا به روشی از آدرس‌های گمراه‌کننده برای فریب کاربران استفاده گردیده است.

در فیشینگ یا سرقت آنلاین ابتدا از طریق ابزارهایی مانند ارسال رایانامه، آگهی‌های تبلیغاتی و سایت‌های دیگر، کاربر به بازکردن لینک جعلی ترغیب و به صفحه وب مخرب و غیرواقعی راهنمایی می‌شود. سپس از کاربر درخواست می‌شود تا به دلایل خاصی اطلاعاتی مانند اطلاعات کارت بانکی را در آنجا وارد نماید .در صورت گمراه شدن کاربر و وارد کردن اطلاعات خود، این اطلاعات در اختیار فرد غیرمجاز قرار گرفته و عملاً سرقت می‌شود. سرعت موفقیت حملات فیشینگ غیرقابل باور بوده و به‌طور میانگین تنها ۸۲ ثانیه از زمان آغاز یک حمله فیشینگ تا به دام افتادن یک قربانی طول می کشد.

انواع فیشینگ:

۱ - فیشینگ بانکی:

فیشینگ یک راه ساده کلاهبرداری هکرها یا دزدان اینترنتی برای به دست آوردن اطلاعات شماره ۱۶ رقمی کارت بانکی، رمز دوم، CVV2، تاریخ صدور کارت و سایر اطلاعات بانکی شما است. به عبارت ساده تر زمانی که کسی سعی در فریب شما برای به دست آوردن اطلاعات فوق می‌کند، یعنی شما در برابر حمله فیشینگ قرار گرفته‌اید.اگر بخواهیم به طور واضح‌تر و دقیق‌تر بگوییم، فیشینگ یعنی ساختن سایت‌ها و اپلیکیشن‌ها یا ارسال پیامک‌هایی مشابه واقعیت برای فریب و دسترسی به اطلاعات ورودی کاربران. فیشینگ انواع مختلفی دارد که در ادامه آنها را نام برده و راه‌های تشخیص و جلوگیری از آنها را به شما معرفی می‌کنیم.



توجه:

همانگونه که در تصویر بالا مشاهده میکنید این یک صفحه جعلی و البته فعال میباشد که در حال سرقت اطلاعات کاربران میباشد ! به آدرس بالای تصویر توجه کنید . برخی افراد تنها به https بودن لینک ها توجه میکنند و دیگر به ادامه آدرس توجه نمیکنند که این یک اشتباه بسیار بزرگ میباشد . امروزه استفاده کردن از https و ssl برای سایت بسیار راحت تر از گذشته است و در کنار توجه به این مورد باید به آدرس بعد از آن نیز توجه کرد . در ادامه آدرس های رسمی پرداخت های اینترنتی زیر نظر شاپرک را خدمت شما عرض میکنیم:

۲ - فیشینگ با ایمیل‌های فریبنده:

در این روش از حمله‌های فیشینگ، شخص کلاهبردار با ارسال ایمیل‌های فریبنده به قربانیانش می‌کوشد با بیان دلایل مجاب کننده مخاطبان را به وارد کردن اطلاعات بانکی خود وادار کند.ممکن است ایمیل به ظاهر از طرف بانک شما، یک شرکت معتبر و یا حتی بانک مرکزی ارسال شود و از شما درخواست کند ظرف زمان معینی اطلاعات بانکی خود را ارسال کنید. متاسفانه بارها افرادی فریب این حملات فیشینگ را خورده اند.

نکته: سیستم مالی و بانکی هیچگاه از طریق ایمیل از شما درخواست نمی‌کند اطلاعات بانکی تان را برای آن‌ها ارسال کنید، شما حتی مجاز به اعلام رمز بانکی خود به کارکنان بانک هم نیستید.

نمونه‌ای از حمله فیشینگ از طریق جی‌میل:

---------- Forwarded message ----------
From: **account iran** <kerioserver42@gmail.com>
Date: 2013/4/22
Subject: فرصت محدود برای استفاده از سرویس ویژه گوگل
To:

برای رهایی از فیلتر و چک کردن گروپ های خود در جیمیل کافی است از طریق سرور های جدید گوگل که ویژه کشور هایی مثل ایران که در تحریم است راه اندازی شده است به منظور ارایه سرویس و افزایش امار بازدید کنندگان.

تنها کافی است از طریق لینک زیر وارد جیمیل و گروپ های خود شوید.پس از ورود ظرف مدت 24ساعت کد فعال سازی توسط سرورهای گوگل برای شما ارسال میشود.و اکانت شما برای استفاده از این سرویس جیمیل اماده میشود.

*لطفا توجه فرمایید از public نمودن سرور ها ما به منظور ایجاد نشدن ترافیک سنگین خودداری نمایید.

در صورت بلوک گردیدن سرورها سریعا مسیر جدید برای شما ایمیل میشود.

برای ورود بر روی لینک زیر کلیک نمایید:

account.google.com

برای گروپ ها بر روی لینک زیر کلیک نمایید:

group.google.com

۳ – فیشینگ تلفنی:

هکرها در این روش از طریق تلفن با طعمه‌های خود ارتباط برقرار می‌کنند و ضمن اینکه خود را نماینده بانک، شرکت معتبر و یا سازمانی که شما می‌شناسید معرفی می‌کنند از شما می‌خواهند جهت دریافت جایزه خود اطلاعات بانکی خود را در اختیار ایشان قرار دهید.

نکته: برای واریز هر گونه وجه به حساب شما اعم از جایزه، پاداش و مزایا نیازی به اعلام رمز بانکی شما نخواهد بود. برای مقابله با هکرها و حملات فیشینگ این نکته را فراموش نکنید.

۴ – طراحی صفحه‌ای نظیر درگاه پرداخت بانک:

شخص هکر در این روش صفحه‌ای مشابه درگاه پرداخت آنلاین بانک‌ها طراحی می‌کند و با قرار دادن این صفحه جعلی در فروشگاه‌های صوری و با ارائه پیشنهادهای وسوسه کننده خرید سعی می‌کند شما را وادار کند وارد صفحه پرداخت جعلی که طراحی کرده بشوید و وجه انتقال دهید.به محض ورود به این صفحه جعلی و ارائه اطلاعات بانکی اطلاعات شما به صورت خودکار برای هکر ارسال می‌شود و او قادر خواهد بود حساب شما را خالی کند.

درگاه های پرداخت قانونی

امن ترین درگاه پرداخت، درگاه پرداخت بانک مرکزی به آدرس https://xxx.shaparak.ir است و در کنار آن حتما باید نام یکی ازpsp ها (شرکت‌های پرداخت الکترونیک) مطرح درج شده باشد.

شرکت‌های PSP مجاز کشور

در ادامه به شرکت های پی اس پی مجاز کشور که شهروندان لازم است برای هر گونه عملیات بانکی تنها از آنها استفاده کنند، اشاره می شود.

https://asan.shaparak.ir	**آسان پرداخت پرشین**
https://bpm.shaparak.ir	**به پرداخت ملت**
https://pec.shaparak.ir	**تجارت الکترونیک پارسیان**
https://sep.shaparak.ir	**پرداخت الکترونیک سامان**
https://pep.shaparak.ir	**پرداخت الکترونیک پاسارگاد**
https://pna.shaparak.ir	**پرداخت نوین آرین**
https://sadad.shaparak.ir	**پرداخت الکترونیک سداد**
https://ikc.shaparak.ir	**کارت اعتباری ایران کیش**
https://fanava.shaparak.ir	**فن آوا کارت**
https://mabna.shaparak.ir	**مبنا کارت آریا**
https://ecd.shaparak.ir	**الکترونیک کارت دماوند**
https://sayan.shaparak.ir	**سایان کارت**

نکته ای که باید اینجا به آن اشاره کرد آن است که بهترین روش مقابله با این نوع از حمله‌های فیشینگ دقت به URL درگاه پرداخت است. استفاده از سیستم‌های انتقال وجه معتبر مانند پی پینگ هم می‌تواند مفید باشد. هر کدام از سایت‌های بانک‌ها از آدرس مشخصی برای درگاه پرداخت خود استفاده می‌کنند هرآدرس دیگری می‌تواند نشانه یک حمله فیشینگ باشد.درگاه‌های پرداخت بانک‌ها از کدهای امنیتی باضریب اطمینان بالا استفاده می‌کنند و اغلب در آدرس سایت عبارت https:// قابل مشاهده خواهد بود.

۵ – فیشینگ با دستگاه‌های POS و ATM تقلبی:

برخی کلاهبرداران با استفاده از POS و ATM تقلبی کارت‌های بانکی طعمه‌های خود را کپی کرده و به بهانه فروش محصول و کالا رمز عبور آن‌ها را می‌پرسند و سپس به راحتی حساب بانکی افراد را خالی می‌کنند.بهتر است هیچ گاه رمز عبور خود را در اختیار فروشندگان قرار ندهید. با پیشرفت تکنولوژی شیوه‌های پرداخت متنوعی در اختیار شما قرار گرفته که با کمک آن می‌توانید استفاده از POS و ATM را به میزان قابل توجهی کاهش دهید .دریافت دستگاه‌های POS اختصاصی توسط شرکت‌ها و سازمان‌ها هم می‌تواند به جلب اعتماد بیشتر مشتریان کمک کند .

ربات تلگرام و فیشینگ

ربات‌های تلگرام این روزها به بسیاری از کارهای ما سرعت بخشیده اند، شرکت‌های معتبر فین‌تک هم در این خصوص خدمات خوبی را ارائه می‌دهند که گزارش گیری انتقال وجوه را ساده‌تر کرده است. اما به هر روی تلگرام بستر مناسبی برای انتقال وجه نیست و دیده شده به بهانه انتقال وجه اطلاعات بانکی افراد از این طریق سرقت شده است.از این رو لازم است تنها به شرکت‌های معتبر و فعال این عرصه اعتماد کنید و جهت انتقال وجه آنلاین روش‌های مناسب را انتخاب کنید.استفاده از خدمات بانکداری الکترونیک و شرکت‌های مجاز حوزه فین‌تک می‌تواند در وقت و پول شما صرفه جویی کرده و هزینه‌های شما را به میزان قابل توجهی کاهش دهد.فقط کافی است هنگام استفاده از این خدمات نکات امنیتی را رعایت کنید و همواره به سراغ مراکز معتبر و شناخته شده بروید تا عملیات انتقال وجه مطمئن و راحتی را تجربه کنید.

رئیس پلیس فتا متذکر شد: کاربران هرگونه موارد مشکوک در فضای مجازی را از طریق سایت پلیس فتا به آدرس www.cyberpolice.ir بخش مرکز فوریت‌های سایبری، لینک ثبت گزارش‌های مردمی به پلیس فتا اطلاع دهند.

شناسایی و راه‌های مقابله با حملات فیشینگ

نمونه‌ای از یک آدرس اینترنتی به همراه اجزای آن در ذیل نمایش داده‌شده است:

در نظر داشته باشید :

- زیردامنه‌های یک وب‌سایت همواره قبل از نام اصلی دامنه آورده می‌شوند. به‌عنوان مثال :

دامنه اصلی **e.karafarinbank.ir** :

دامنه جعلی **karafarinbank.e.ir** :

- نام دامنه وب‌سایت‌های جعلی با هدف فیشینگ عموماً مشابه نام دامنه اصلی وب‌سایت می‌باشد و تنها در یک یا دو حرف تفاوت دارند. به‌عنوان مثال:

دامنه اصلی **karafarinbank.ir** :

دامنه جعلی **karafariinbank.ir** :

هیچ‌گاه به عنوان و آدرس فرستنده رایانامه اعتماد نکنید و پیش از هر اقدامی ابتدا از صحت ارسال‌کننده رایانامه اطمینان حاصل نمایید.

- در حملات فیشینگ، از طریق رایانامه، پیامک یا پیام‌های دریافتی از مرورگر و دیگر رسانه‌های ارتباطی، حاوی درخواست-های نامتعارف و جعلی مانند مراجعه به یک لینک و تصدیق هویت یا تغییر کلمه عبور حساب کاربری می‌باشند. هیچ‌گاه این‌گونه درخواست‌ها را قبل از اطمینان صحت پیام، رایانامه‌های ارسالی و فرستنده آن‌ها، پاسخ ندهید.
- پیام‌ها و رایانامه‌های حملات فیشینگ معمولاً دارای پرسش‌هایی مرتبط با اطلاعات حریم خصوصی و محرمانه کاربران می‌باشند، لذا پیش از ارسال پاسخ از صحت پیام و پست الکترونیک ارسالی، اطمینان حاصل نمایید.
- پیام‌ها یا رایانامه‌های حملات فیشینگ ممکن است کاربر را از طریق پیشنهادهای گمراه‌کننده مانند شرکت در قرعه‌کشی یا حضور در یک برنامه تفریحی خاص به اهداف خود وادار نمایند. لذا در صورت مشاهده این‌گونه موارد، در صورت عدم اطمینان از هویت ارسال‌کننده، آن‌ها را حذف نمایید.
- هیچ‌گاه پیوست رایانامه‌های غیرعادی و ناشناس را بارگیری و اجرا نکنید. ممکن است پیوست، آلوده به بدافزار بوده و موجب اختلال یا سرقت اطلاعات شما گردد.
- توصیه می‌گردد حتی‌الامکان برای مراجعه و استفاده از وب‌سایت‌هایی که نیاز به احراز هویت و ورود اطلاعات حساب کاربری مانند کلمه عبور دارند، از بازنمودن لینک‌های درج‌شده در رایانامه‌ها و پیام‌های ارسالی استفاده نکنید و شخصاً آدرس وب‌سایت موردنظر را در مرورگر تایپ نمایید.

- در پیام‌های حملات فیشینگ عموماً مخاطب پیام به‌صورت مشخص ذکر نمی‌شود. ممکن است به‌جای نام دقیق شخص، آدرس رایانامه یا نام کاربری فرد ذکر گردد. البته گاهی با عناوین کلی مانند کاربر گرامی، آقای/خانم و ...شروع می‌گردند.

- در رایانامه‌های فیشینگ، معمولاً لینک‌هایی وجود دارد که دامنه و URL آن با دامنه وب‌سایت اصلی مغایرت دارد. در مواردی نیز این مغایرت در ظاهر قابل مشاهده نیست. (آدرس لینک جعلی با آدرس وب‌سایت اصلی در ظاهر یکسان است(.
- گواهینامه دیجیتال به‌منظور احراز هویت سرور وب‌سایت موردنظر در پروتکل HTTPS توسط کاربر، مورد استفاده قرار می‌گیرد که در صورت نامعتبر بودن این گواهینامه، پیام‌های خطای امنیتی مشاهده می‌شود. ضروری است که در این موارد صفحات وب را باز ننمایید.
- در زمان مراجعه به آدرس‌ها و لینک‌های درج شده در پیام‌های ارسالی در صورت استفاده از پروتکل(HTTPS (SSL/TLS، توصیه می‌گردد. حداقل برای وب‌سایت‌های مهم، از صحت گواهینامه دیجیتال مطابق تصویر ذیل، اطمینان حاصل نمایند. بررسی شود:

۱) نام دامنه و آدرس وب‌سایتی که در گواهینامه ثبت‌شده با آدرس وب‌سایتی که در مرورگر واردشده است، یکسان باشد.
۲) تاریخ اعتبار گواهینامه دیجیتال، منقضی نشده باشد.

۳) مرکز صدور گواهینامه دیجیتال، جز مراکز معتبر باشد .