سازمان بورس و اوراق بهادار
Securities & Exchange Organization

بولتن آگاهی رسانی امنیت سایبری، شماره ۳

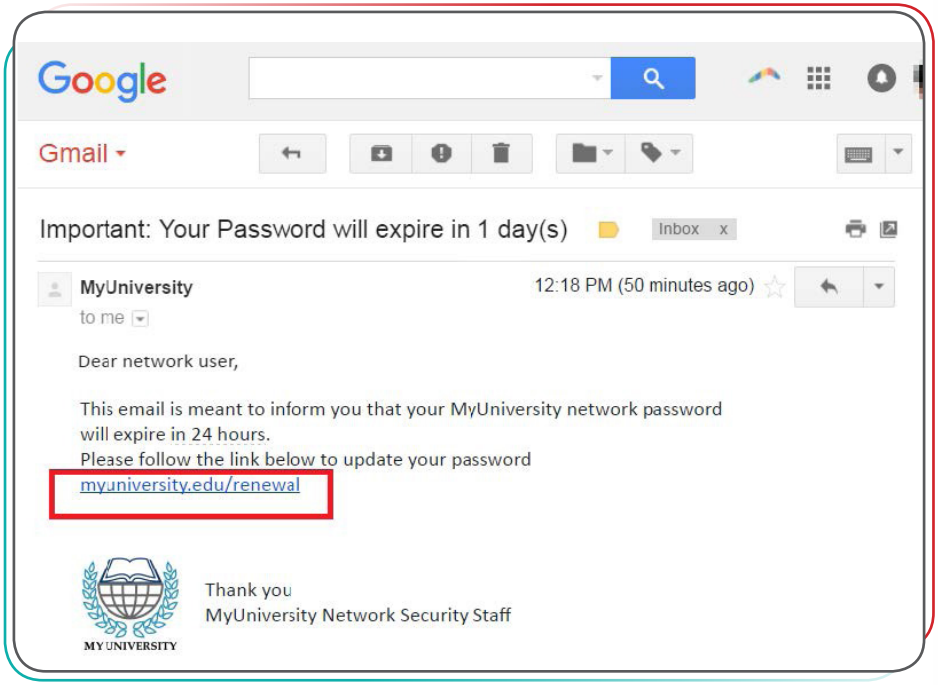
فیشینگ ایمیل

■ مرکز نظارت بر امنیت اطلاعات بازار سرمایه ■

فیشینگ ایمیل

به سناریوی زیر توجه نمایید:

۱. ایمیلی جعلی از دامین myuniversity.edu برای کلیه اعضاء هیئت علمی یک دانشگاه ارسال می‌شود.
۲. در این ایمیل ادعا می‌شود که رمز عبور کاربر در حال منقضی شدن است و توصیه می شود که برای تغییر پسورد خود ظرف ۲۴ ساعت آینده بر روی آدرس myuniversity.edu/renewal کلیک شود.



اتفاقات متعددی ممکن است پس از کلیک بر روی آدرس مذکور رخ دهد. به طور مثال:

کاربر به صفحه ای با آدرس myuniversity.edurenewal.com که مشابه آدرس اصلی است و محتوایی بسیار شبیه به آدرس اصلی دارد، منتقل شود و در آنجا رمز عبور فعلی و رمز عبور جدید از وی درخواست شود. به محض ورود رمزهای عبور، هکر با یافتن رمز عبور اصلی امکان دسترسی به اطلاعات حساب کاربری آن عضو هیئت علمی را خواهد داشت.

ممکـن اسـت کاربـر به صفحه اصلـی (غیر جعلی) تغییر پسـورد دانشـگاه هدایت شـود اما با اسـتفاده از ابزارهایی هکر امکان دسترسی به حسـاب کاربـری آن عضو هیئت علمی را خواهد داشـت.
همانطـور کـه مشـخص شـد، بـا یـک کلیـک سـاده بـر روی یک آدرس در یـک ایمیـل دریافتـی، امـکان هـک شـدن و لـو رفتـن اطلاعـات وجـود دارد. ایـن ایمیل ممکن اسـت در حوزه کاری شـما هـم بـا همیـن ترفند ارسـال شـود. بـه تکنیک‌هایـی مشـابه حمله فـوق، حملـه فیشـینگ گفته می‌شـود.

حمله فیشینگ

فیشـینگ یـک نـوع حمله مهندسـی اجتماعی اسـت که بـه منظور سـرقت اطلاعـات کاربران شـامل نـام کاربری، رمـز عبور، اطلاعات حسـاب کاربـری و ... انجام می‌شـود. نحـوه انجـام ایـن حملـه بدیـن صورت اسـت کـه هکر با تغییـر دادن هویـت خـود بـه یـک هویـت مـورد اعتمـاد، سـعی در جلب توجه شـخص مـورد حمله برای بـاز کردن یـک ایمیل دارد. شـخص مـورد حمله بـر روی یک لینک مخـرب کلیـک نمـوده و ممکن اسـت یک بـد افـزار و یا یـک باج‌افـزار بـر روی سیسـتم وی نصب شـود. در نتیجه این حمله، ممکن اسـت داده‌ها و فایل‌های سیسـتم قربانی تخریـب شـود و امکان دسـتیابی به محتـوای آن‌ها فراهم نخواهـد بود یا این که ممکن اسـت اطلاعات حسـاس آن سیسـتم برای هکر افشـا شـود. حملات فیشـینگ به چند روش قابـل انجـام هسـتند، در این مطلب آموزشـی تمرکز بـر فیشـینگ از طریق ایمیـل خواهد بود

اهداف حملات فیشینگ

- سرقت نام کاربری و رمز عبور حساب‌های کاربری
- سرقت شماره‌های حساب‌های بانکی
- سرقت اطلاعات بورسی (کد بورسی، تعداد سهام و ...)
- سرقت شماره کارت بانکی
- سرقت اطلاعات هویتی، شخصی و ...

تکنیک های حمله فیشینگ ایمیل

در این نوع حمله، هکر ممکن است با اهداف کلاهبرداری، هزاران ایمیل به گیرنده‌های مختلف ارسال کند حتی اگر تعداد کمی از گیرنده‌ها در تله وی گیر بفتند. همچنین آن‌ها برای بالا بردن میزان موفقیت خود، از تکنیک‌های متعددی استفاده می‌کنند.

استفاده از قالب‌های رایج

هکرها ایمیل‌های جعلی خود را با پیام‌هایی طولانی و ساختاری شبیه به ایمیل‌های یک سازمان (لوگو، فونت و امضاء و ...) طراحی می‌کنند تا ظاهری موجه به ایمیل خود داده باشند.

اضطراری جلوه دادن ایمیل

هکرها تلاش می‌کنند تا با فوریت بخشی به موضوع ایمیل، گیرنده‌های ایمیل را وادار به پاسخ‌دهی سریع کنند (همانند مثال انقضاء رمز عبور ایمیل اعضای هیئت علمی دانشگاه). ایجاد چنین شرایطی منجر به کاهش دقت و افزایش خطای کاربر خواهد شد.

استفاده از آدرس‌های جعلی مشابه با آدرس های اصلی

این تکنیک حمله به ٤ حالت کلی قابل دسته‌بندی است:

حالت اول) استفاده از نام و نام خانوادگی مشابه مخاطب مورد اعتماد شما

در این حالت، هکر سعی می کند ایمیل ارسالی خود را به گونه ای تنظیم کند که نام و نام خانوادگی مشابه با مخاطب مورد اعتمادتان برای ایمیل مشاهده شود. با مشاهده جزئیات آدرس ایمیل متوجه جعلی بودن فرستنده آن خواهید شد.

from:	**Morteza Hosseinabadi** <postmaster@hacker.com>
to:	my@gmail.com
date:	Sun, Jul 22, 2018 at 4:42 PM
subject:	Your Salary Details
mailed-by:	Bounce.hacker.com

در شکل فوق فرض بر این است که Morteza Hosseinabadi مخاطب مورد اعتماد شماست، اما توجه به آدرس ایمیل نشان می دهد که فرستنده اصلی شخص دیگری است.

حالت دوم) ارسال ایمیل از آدرسی مشابه با آدرس مخاطبان مورد اعتماد شما

مثال۱) آدرس ایمیل فرد مورد اعتماد شما:
hosseinabadi@gmail.com
آدرس جعلی مشابه با آدرس ایمیل فوق:
hoseinabadi@gmail.com

مثال ۲) آدرس ایمیل فرد مورد اعتماد شما:
hosseinabadi@seo.ir
آدرس جعلی مشابه با آدرس ایمیل اصلی:
hosseinabadi@seoir.ir

حالت سوم) آدرس دهی اشتباه در متن ایمیل (Hyperlink):

در این حالت در متن ایمیل از شما خواسته می شود بر روی یک لینک (آدرس) کلیک کنید، متن لینک ارسالی ممکن است آدرس درست و مورد اعتمادی باشد، اما زمانی که بر روی آن کلیک می کنید، به سایتی غیر از سایت اصلی هدایت می‌شوید. برای شناسایی آدرس نهائی قبل از کلیک بر روی لینک، کافی است چند ثانیه نشانه‌گر ماوس را بر روی آن لینک نگه دارید (مطابق شکل ذیل).

همانطور که در شکل مشخص شده است، ظاهر لینک به گونه ای است که با کلیک بر روی آن به سایت www.seo.ir منتقل می شوید، اما در عمل به سایت مدنظر هکر seo-ir.hack.com هدایت خواهید شد.

حالت چهارم) استفاده از ابزارهای هک برای ارسال ایمیل دقیقا مطابق با آدرس ایمیل مخاطبان مورد اعتماد شما (پیچیده ترین حالت)

ایمیل اصلی: hosseinabadi@seo.ir

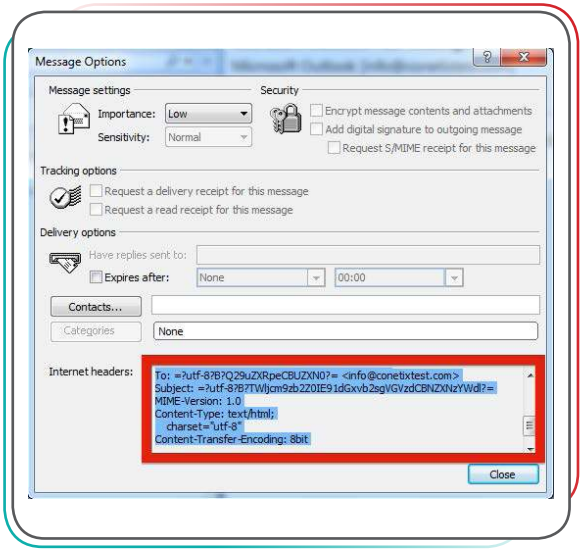
ایمیل جعلی: hosseinabadi@seo.ir

ایمیل جعلی دقیقا همانند ایمیل اصلی است. راهکارهایی برای مقابله با این حالت نیز وجود دارد که تا حدی تخصصی است و در ادامه به آن‌ها اشاره خواهد شد.

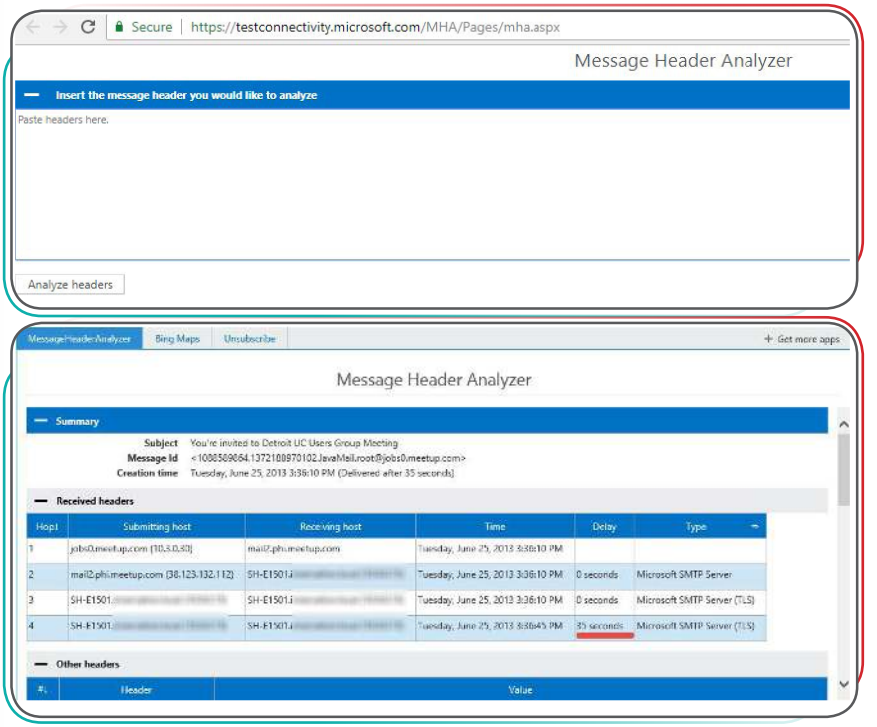
راهکارهای تشخیص حملات فیشینگ ایمیل

- به ایمیل‌هایی که اطلاعات شخصی شما را درخواست می‌کنند، پاسخ ندهید.
- در هر ایمیل دریافتی، به دقت نام شخص ارسال کننده، آدرس ایمیل شامل هر دو بخش قبل و بعد از @ را از لحاظ نگارشی بررسی کنید تا با ایمیل اصلی مخاطب مدنظر شما یکسان باشد. (تشخیص حملات حالت اول و دوم)
- بر روی لینک‌هایی که از طریق ایمیل برای شما ارسال می‌گردد، کلیک نکنید. در صورت ضرورت و اطمینان از فرستنده ایمیل، برای کلیک بر روی لینک، ابتدا اشاره‌گر ماوس را بدون کلیک بر روی لینک مربوطه قرار داده و آدرسی را که در کنار آن ظاهر می شود، به دقت بررسی کنید. از صحت آدرس مطمئن شوید. (تشخیص حمله حالت سوم)

- فریب تبلیغات و مطالب ارسالی از طریق ایمیل را نخورید.
- ایمیل‌های مشکوک و غیر مرتبط را Spam کنید و از باز کردن ایمیل‌های Spam خودداری نمائید.
- در مواجهه با هر ایمیل دریافتی، رویکرد خود را مبتنی بر عدم اعتماد قرار دهید.
- در صورتی که ایمیلی با نام و نام خانوادگی و آدرس ایمیل دقیقا مطابق با آدرس مخاطب مورد اعتماد خود دریافت نمودید (حالت چهارم)، برای تشخیص مشکوک بودن ایمیل دریافتی، ضرورت دارد جزئیات فنی آن ایمیل دریافت و تحلیل شود. روش مشاهده جزئیات فنی ایمیل دریافتی (Email Header) در نرم افزارهای مختلف ایمیلی متفاوت است. در این مطلب، نحوه مشاهده جزئیات فنی ایمیل دریافتی در دو نرم افزار outlook و exchange توضیح داده می‌شود. در نرم افزار outlook می‌بایست بر روی ایمیل دریافتی دو بار کلیک کنید و سپس از منوی File گزینه Properties را انتخاب نمائید. در صفحه جدید، محتویات قسمت Internet headers را انتخاب و کپی نمائید.



بـرای دریافـت جزئیـات فنـی خـود در نـرم افـزار تحـت وب Exchange، می‌توانیـد پس از انتخـاب ایمیل، با اسـتفاده از گزینـه More actions و انتخـاب view message details، جزئیـات فنـی ایمیـل خـود را مشـاهده و کپـی کنید.
پـس از کپی جزئیات فنی ایمیل خود، بـه وب‌سـایت https://testconnectivity.microsoft.com/MHA/Pages/mha.aspx مراجعـه نمـوده و محتـوای کپی شـده را در محل مشـخص شـده paste نمائید. بـر روی دکمـه Analyze headers کلیک نمائید تا جزئیـات ایمیـل دریافتـی را بـه طـور کامل به شـما نمایش دهد. با بررسـی گزینه های نمایش داده شـده مـی توانید موارد مشـکوک ایمیل دریافتی را بیابید.



با توجه به پیچیدگی‌های تشخیص حملات فیشینگ ایمیل، راهکاری ساده برای ایمیل‌های مهم کاری پیشنهاد می شود: چنانچـه ایمیـل مهمـی از همکار خـود دریافـت نمودید و قصد اقـدام کاری مهم متناسـب بـا اطلاعات دریافتـی از آن ایمیـل داشـته باشـید، و یا این که اطلاعات مهمی از شـما مطالبه نموده باشـد، قبـل از هرگونه اقـدام، از راه های دیگر ارتباطـی، اصالـت ایمیـل را از همـکار خود جویا شـوید. در این مطلب آموزشـی برخـی از راهکارهای تشـخیص ایمیل فیشـینگ مطرح شـده اسـت و راهکارهای بیشـتری در این خصوص وجـود دارد.

توصیه های امنیتی ما را جدی بگیرید!
مرکز نظارت بر امنیت اطلاعات بازار سرمایه

مرکز نظارت بر امنیت اطلاعات بازار سرمایه

تهران، میدان ونک، ابتدای ملاصدرا، شماره ۱۳، سازمان بورس و اوراق بهادار
صندوق پستی: ۶۳۶۶-۱۹۹۳۵
مرکز ارتباط بورس: ۶۳۷۵-۰۲۱ تلفن: ۵-۸۸۶۷۹۶۴۰-۰۲۱

www.seo.ir