ماهنامه ای برای آگاهی کاربران رایانه از امنیت اطلاعات

OUCH!

دراین شماره..

فیشینگ

مقدمه

ایمیل یکی از راههای اصلی ارتباطی است. ما نه تنها هر روز از آن برای اهداف کاری استفاده می کنیم بلکه با آن با خانواده و دوستان هم در تماسیم. بعلاوه، امروزه ایمیل راهی است که بیشتر شرکت ها خدمات آنلاینشان مثل تایید خرید اینترنتی یا وجود صورتحساب بانکی را ارائه می دهند. چون بسیاری در سراسر دنیا به ایمیل وابسته هستند، مجرمان سایبری از ایمیل بعنوان یکی از روشهای اصلی حمله استفاده می کنند. در این خبرنامه ما فیشینگ، روش معمول حمله به ایمیل، و گامهایی که می توانید جهت استفاده امن از ایمیلتان بردارید را توضیح خواهیم داد.

سردبیر مهمان

دکتر Lance Hayden مدیر عامل گروه تحقیقات برکلی, متخصص تاثیر فرهنگ و رفتار در امنیت و نویسنده کتاب امنیت مردم-محور: فرهنگ امنیت شرکت خود را تغییر دهید چاپ شرکت مك گرا هیل است. او را در آدرس www.linkedin.com/in/drhayden بیابید.

فیشینگ

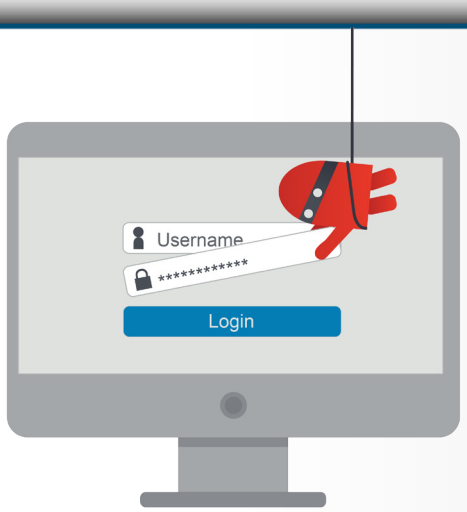
فیشینگ به حمله ای گفته میشود که از ایمیل یا سرویس پیام رسانی مثل سایت های شبکه های اجتماعی استفاده می کند تا شما را بفریبانند تا عملی انجام دهید مثلا روی لینکی کلیك کنید یا فایل ضمیمه ای را باز کنید. اگر قربانی اینگونه حمله شوید به احتمال زیاد ممکن است اطلاعات حساستان دزدیده شود و/یا کامپیوترتان آلوده شود. حمله کنندگان تلاش می کنند که ایمیل های فیشینگ متقاعد کننده ای بسازند. برای مثال آنها ایمیلی می سازند که ظاهرا از طرف کسی یا جایی که می شناسید آمده است، مثلا دوست یا شرکتی مورد اعتماد که مرتبا استفاده می کنید. آنها حتی لوگوی بانکتان یا حتی آدرس ایمیل جعل می کنند تا پیام بیشتر طبیعی به نظر برسد. سپس حمله کنندگان این ایمیل را به میلیونها نفر می فرستند. آنها نمی دانند چه کسی قربانی خواهد شد. آنها فقط می دانند هر چه بیشتر ایمیل بفرستند شانس موفقیتشان بیشتر خواهد شد. فیشینگ شبیه استفاده از تور ماهیگیری است، نمی دانید چه چیزی خواهید گرفت اما می دانید هر چه تور بزرگتری داشته باشید ماهی بیشتری خواهید یافت. حمله کنندگان از چندین راه برای فیشینگ استفاده می کنند تا چیزی که می خواهند بدست آورند.

- **بدست آوردن اطلاعات**: هدف حمله کننده دستیابی به اطلاعات شخصی شما مانند رمز عبور، شماره کارت اعتباری، یا اطلاعات بانکی شماست. برای این منظور آنها لینکی را به شما ایمیل می کنند که شما را به وب سایتی می برد که در ظاهر واقعی می رسد. سپس این وب سایت از شما می خواهد که اطلاعات حسابتان یا داده های شخصی تان را وارد کنید. در حالیکه این سایتی ساختگی و جعلی می باشد، و هر اطلاعاتی که وارد کنید مستقیما بدست حمله کننده می رسد.
- **لینك های مخرب**: هدف حمله کننده کنترل دستگاه شماست. برای این منظور آنها ایمیلی با یك لینك به شما می فرستند. اگر روی

فیشـینگ

لینـك كلیـك كنیـد، شـما را بـه وبسـایتی مـی بـرد كـه شروع بـه حملـه بـه دستگاهتان مـی كنـد، كـه اگـر موفـق بـه ایـن كار شـود، سیستم شما را آلـوده مـی كنـد.

- **ضمیمـه مخرب:** هـدف حملـه كننـده مشـابه قبـل اسـت، آلـوده كـردن و بدسـت گـیری كنـترل دسـتگاه شـما. امـا بجـای ایمیـل كـردن لینـك بـه شـما، فایـل آلـوده بـه شـما ایمیـل مـی كنـد، مثلا یـك فایـل ساخته شـده بـا نـرم افـزار Word بـا بـاز كـردن ایـن ضمیمـه حملـه راه انـدازی مـی شـود، بطـور بالقـوه كنـترل سیسـتم شـما بـه حملـه كننـده مـی دهـد.
- **كلاهـبرداری:** بعـضی ایمیـل هـای فیشـینگ چـیزی بیـش از حقـه بـاز هـای دیجیتـال نیسـتند. آنهـا بـا گفـتن اینكـه شـما بلیـت بخـت آزمـایی بـرده ایـد، یـا وانمـود كننـد كـه سـازمان خیریـه هسـتند و بـه كمـك انساندوسـتانه احتیـاج دارنـد و یـا بـه كمـك شـما بـرای انتقـال میلیونهـا دلار پـول احتیـاج دارنـد تـلاش در فریـب دادن شـما دارنـد. اگـر بـه هـر كـدام از اینهـا جـواب دهیـد، آنهـا خواهنـد گفـت كـه بایـد پـولی بپردازیـد و یـا بایـد بـه حسـاب بانـكی شـما دسـترسی پیـدا كننـد تـا بتواننـد بـه شـما خدمـات ارائـه دهنـد و بـه ایـن ترتیـب از شـما كلاهـبرداری مـالی مـی كننـد.



بهترین مدافع شـما عقلانیت اسـت. اگر ایمیل یا پیامی عجیب، مشـكوك، یا بیش از انتظار خوب اسـت، ممكن اسـت حمله فیشینگ باشد.

از خودتان محافظت كنید

تقریبـا در همـه مـوارد، بـاز كـردن و خوانـدن ایمیـل مشـكلی نـدارد. بـرای اینكـه حملـه فیشـینگ عملـی شـود تبهـكاران احتیـاج دارنـد كـه شـما را بـه انجـام كاری بفریبنـد. خوشـبختانه سرنـخ هـایی هسـت كـه مشـخص مـی كنـد كـه كـدام پیـام یـك حملـه اسـت. اینهـا رایـج تریـن مـوارد هسـتند:

- اینگونـه ایمیـل هـا حـس فوریـت بـه شـما مـی دهنـد، خواسـتار «اقدامـی فـوری» سـت قبـل از اینكـه اتفـاق بـدی مثـل بسـته شـدن حسـابتان بیفتـد كاری بكنیـد، حملـه كننـده مـی خواهـد كاری را سریـع و بـدون فكـر انجـام دهیـد.
- ایمیـلی كـه منتظـرش نبودیـد و شـامل یـك ضمیمـه اسـت دریافـت مـی كنیـد. اینگونـه ایمیـل هـا شـما را بـه بـاز كـردن ضمیمـه تحریـك مـی كننـد. مثـلا ایمیـلی كـه مـی گویـد ضمیمـه شـامل جزئیـات اسـامی از كار بركنـار شـدگان اعـلام نشـده اسـت، اطلاعـات دریافـتی كاركنـان یـا نامـه ای از طـرف (اداره مالیـات) IRS كـه مـی گویـد شـما تحـت پیگـرد قانـونی هسـتید.
- بجـای اسـتفاده از نامتـان، ایمیـل از تعارفـات عمومـی و كلـی اسـتفاده مـی كنـد مثـل «مشـتری عزیـز». بیشـتر شـركت هـا و دوسـتان كـه بـه شـما ایمیـل مـی زننـد نـام شـما را مـی داننـد.
- ایمیل اطلاعات خیلی حساس شما را می پرسد، مثل شماره كارت اعتباری یا رمز عبور.
- ایمیـل مـی گویـد كـه از طـرف موسسـه رسـمی اسـت، امـا اشـتباه گرامـری و املایی دارد، یـا از ایمیـل شـخصی ماننـد @yahoo.com, @gmail.com, @hotmail.com اسـتفاده مـی كنـد.

فیشـینگ

- لینـك عجیـب و غـیر رسـمی بـه نظـر مـی رسـد. یـك روش اینسـت کـه نشـانگر مـوس را روی لینـك بگیریـد تـا پنجـره بـاز شـده نشـان دهـد کـه ایـن لینـك واقعـا شـما را بـه کجـا مـی بـرد. اگـر لینـك در ایمیـل بـا لینـك مقصـد کـه پنجـره نشـان مـی دهـد یکسـان نیسـت ، روی آن لینـك کلیـك نکنیـد. در موبایـل هـا نگهداشـتن دسـت روی لینـك همـان پنجـره مـورد نظـر را بـاز مـی کنـد. یـك راه حـتی مطمـئن تـر کـپی و پیسـت کـردن URL از ایمیـل و پیسـت کردنـش در مرورگـر یـا تایـپ لینـك صحیـح اسـت.
- پیامـی از کسـانی کـه مـی شناسـید دریافـت مـی کنیـد، امـا لحـن ایمیـل بـا لحـن آن شـخص متفـاوت اسـت. اگـر مشـکوك هسـتید بـا فرسـتنده از طریـق دیگـری (مثـلا تلفـن) تمـاس بگیریـد تـا صحـت آن را بـررسی کنیـد. بـرای یـك حملـه کننـده سـایبری تهیـه ایمیـلی کـه بـه ظاهـر از طـرف دوسـت یـا همـکار اسـت بسـیار آسـان اسـت.

اگر فکر می کنید ایمیل یا پیامی حمله فیشینگ است، به سادگی آنرا پاك کنید. در نهایت، عقلانیت بهترین حامی شماست.

بیشتر بدانید

بـا مراجعـه بـه آدرس زیـر، مشـترک ماهنامـه OUCH! شـوید و بـه آرشـیو خبرنامـه آگاهـی از امنیـت OUCH! دسـترسی داشـته باشـید، و در مـورد راه حل‌هـای افزایـش آگاهی‌هـای امنیـتی موسسـهSANS بیشـتر بدانیـد.

آدرس: http://www.securingthehuman.org

یادداشت مترجم

سایت www.sycurity.com مرجع امنیت اطلاعات برای کاربران فارسی زبان در سراسر دنیا.

منابع

مهندسی اجتماعی:	https://www.securingthehuman.org/ouch/2014#november2014
پنج راه برای امن ماندن:	https://www.securingthehuman.org/ouch/2014#october2014
من هك شده ام، حالا چکار کنم؟:	https://www.securingthehuman.org/ouch/2014#may2014
دفاع آنلاین:	https://www.onguardonline.gov/phishing
نکات امنیتی روز SANS:	https://www.sans.org/tip_of_the_day.php

هیأت تحریریه : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
ترجمه شده توسط : سعید میرجلیلی