مهندسین مشاور سازه پردازی ایران (سهامی خاص)

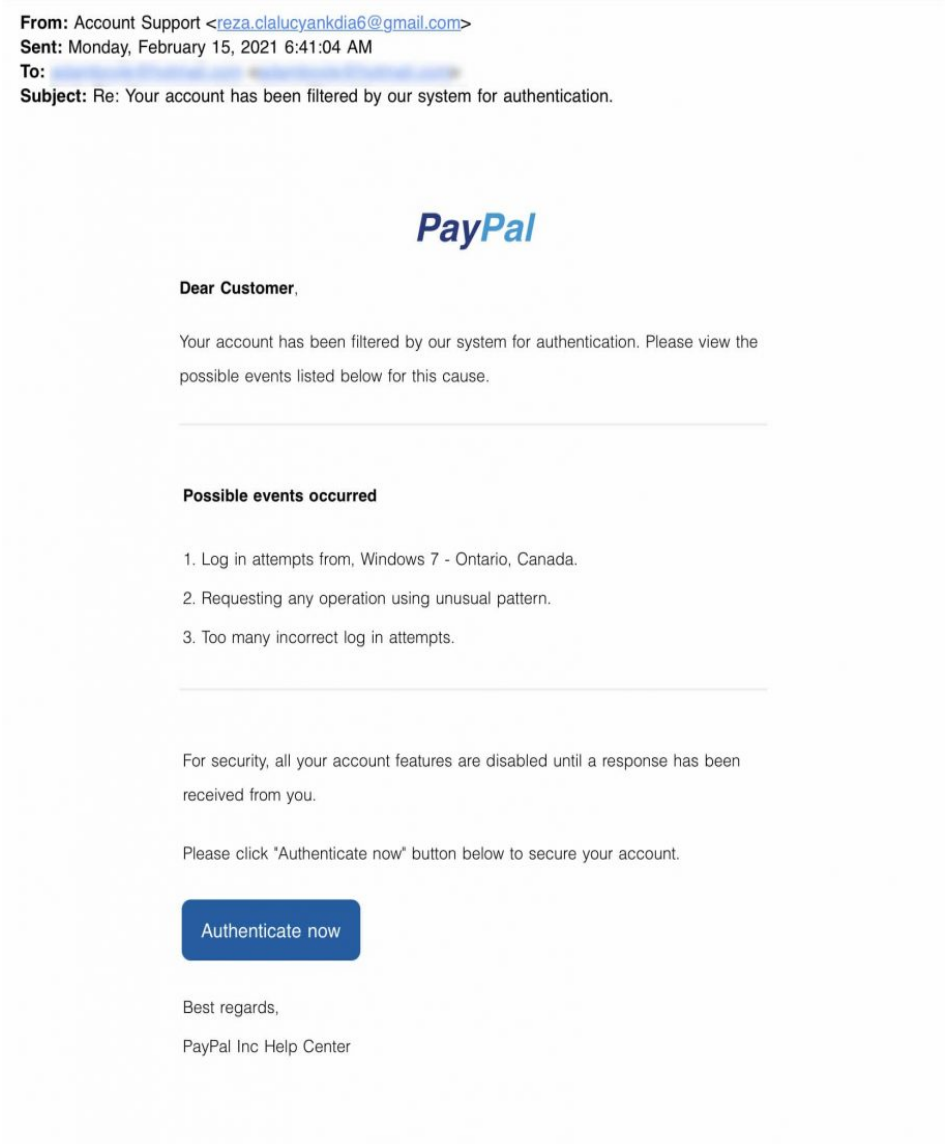
SAZEH PARDAZI IRAN
Consulting Eng. Co

فیشینگ ایمیل

فیشینگ یکی از انواع حملات روی بستر ایمیل است که کلاهبرداران سعی می‌کنند با جعل هویت خود؛ اعتماد قربانی را جلب کرده و او را وادار به اجرای دستورات خود کنند. این دستورات ممکن است هدایت قربانی به یک آدرس جعلی و دریافت اطلاعات مهمی مثل نام کاربری و گذرواژه یا اطلاعات حساب‌های مالی یا اعتباری باشد، یا درخواست پرداخت یک صورتحساب، یا دانلود یک فایل که حاوی بد افزار است. اما در اکثر ایمیل‌های فیشینگ، با کمی دقت به جزئیات ایمیل می‌توان نشانه‌هایی را پیدا کرد که حاکی از جعلی بودن پیام است.

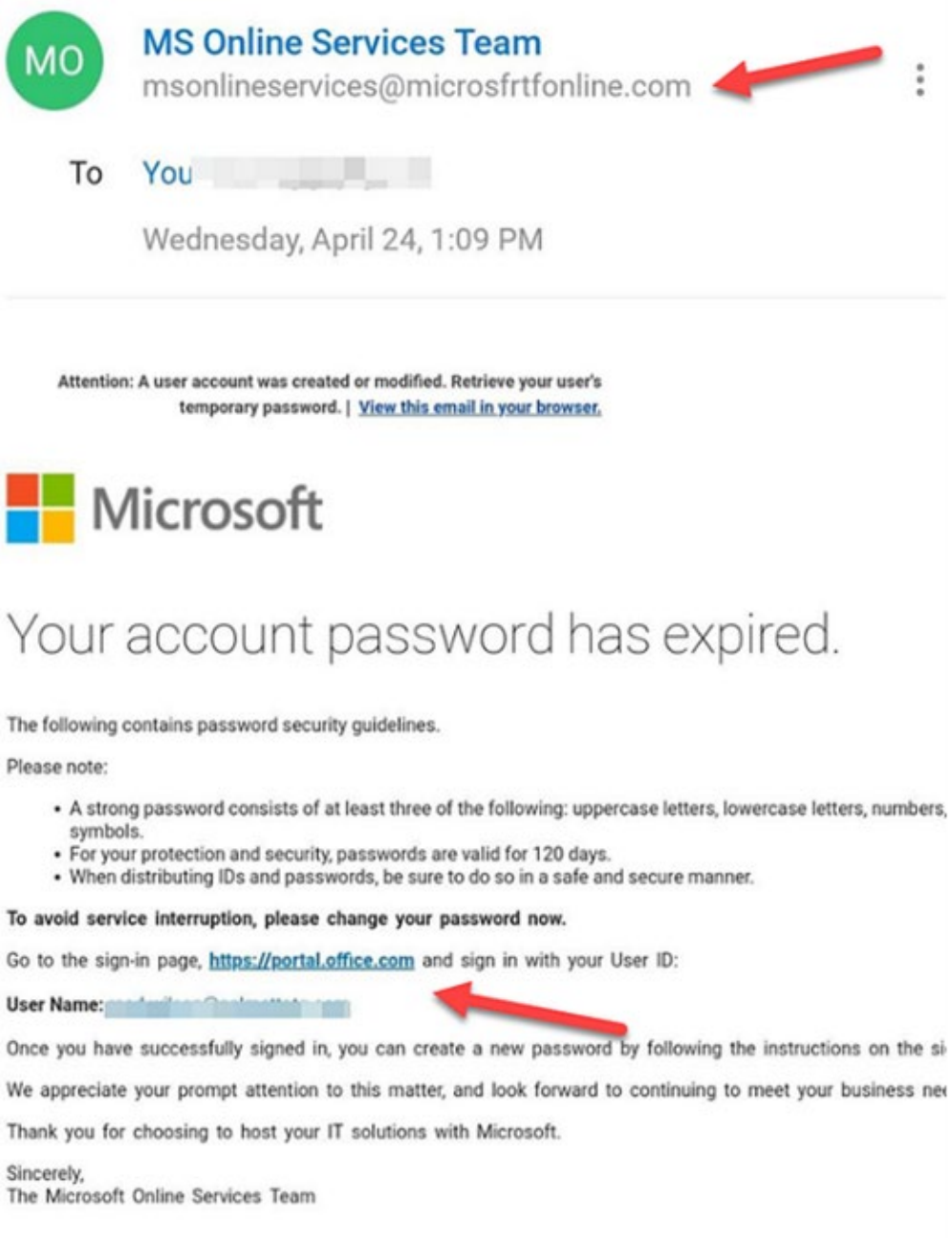
۱- پیام از یک دامنه ایمیل عمومی یا رایگان ارسال شده باشد

- یکی از اولین روش‌های تشخیص ایمیل فیشیگ، توجه به فرستنده پیام است. هیچ سازمان رسمی و معتبری از آدرسی با دامنه gmail.com یا yahoo.com (و به طور کلی از دامنه‌ای که سرویس ایمیل رایگان ارائه می‌دهد)، ایمیل رسمی ارسال نمی‌کند. اکثر سازمان‌ها، ایمیل سازمانی با دامنه اختصاصی یا شرکتی خود را برای تبادل پیام دارند. مثلا ایمیل‌های رسمی شرکت Google با دامنه «@google.com» ارسال می‌شوند. اگر نام دامنه فرستنده پیام (قسمتی که پس از @ در آدرس فرستنده وجود دارد، نام دامنه سرویس ایمیل است) مطابق با نام دامنه شرکتی باشد که نویسنده ایمیل ادعا می‌کند از طرف آن ایمیل زده است، می‌توان نتیجه گرفت که احتمالا پیام قانونی است. اما، اگر ایمیلی دریافت کردید که ظاهرا از طرف یک سازمان رسمی است؛ اما با آدرسی فرستاده شده باشد که هیچ ارتباطی با دامنه شرکت یا سازمان ادعا شده در ایمیل نداشته باشد، به طور قطع این ایمیل یک ایمیل کلاهبرداری است. واضح‌ترین راه برای شناسایی یک ایمیل جعلی این است که فرستنده از یک دامنه ایمیل عمومی مانند ‘@gmail.com’استفاده کند.



در این مثال، می‌توانید ببینید که آدرس فرستنده با محتوای پیام، که به نظر می‌رسد از PayPal است، مطابقت ندارد. با این حال، محتوای پیام واقعی به نظر می‌رسد و مهاجم فیلد نام فرستنده را Account Support گذاشته است تا در صندوق ورودی گیرندگان به عنوان «پشتیبانی حساب» دیده شود.

البته ممکن است ایمیل‌های فیشینگ با درج نام سازمان در بخش نام کاربری ایمیل، برای شناسایی کمی پیچیده‌تر باشند. در این مثال، اگر ایمیل از آدرس "paypalsupport@gmail.com"ارسال شده باشد، در نگاه اول ممکن است با دیدن کلمه "PayPal" فرض کنید که آن ایمیل یک ایمیل رسمی و قانونی است. اما باید به خاطر داشته باشید که بخش مهم آدرس همان دامنه ایمیل است که بعد از علامت @ می‌آید. اگر ایمیل از «@gmail.com» یا دامنه عمومی دیگری است، مطمئن باشید که از یک حساب شخصی ارسال شده است.



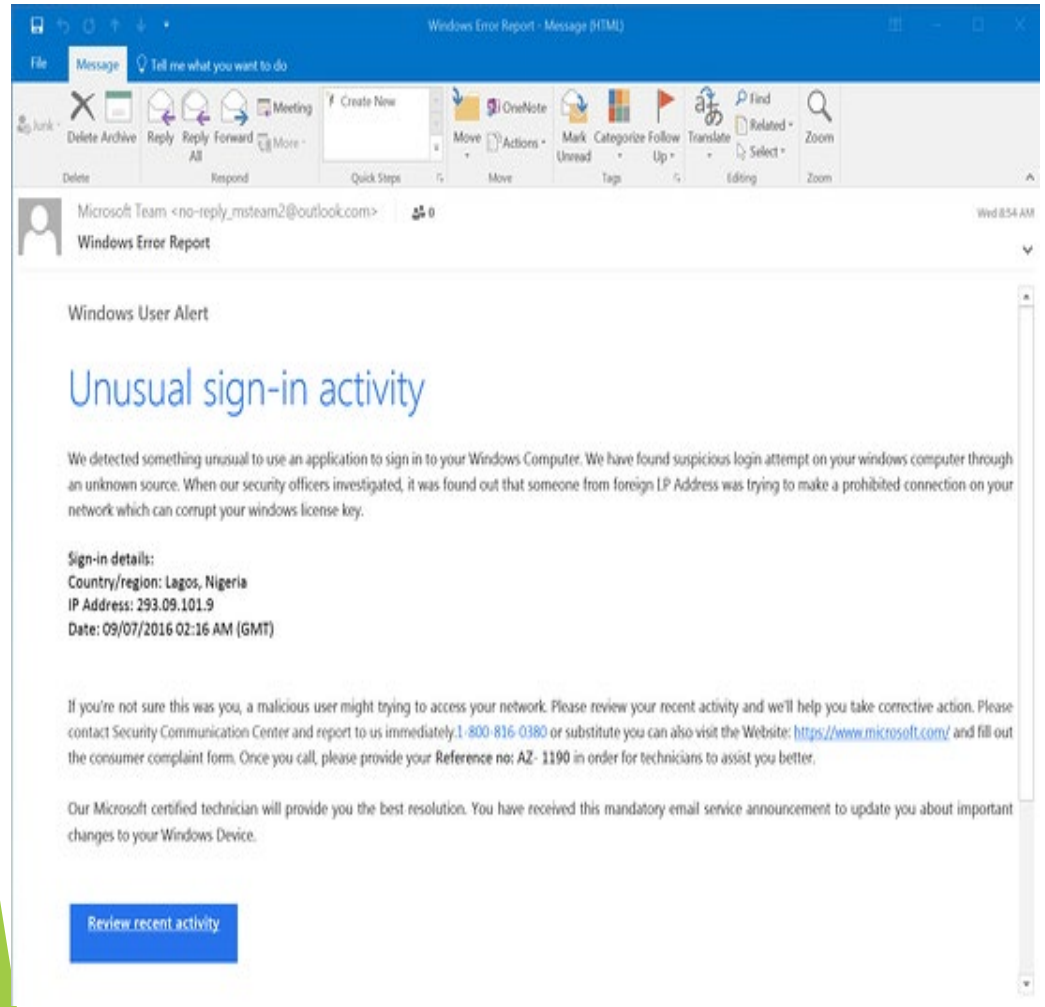
2 . نام دامنه اشتباه نوشته شده است

- سرنخ بعدی برای شناسایی ایمیل‌های فیشینگ، استفاده کلاهبرداران از دامنه‌های مشابه ولی جعلی است که متاسفانه تشخیص آنها کمی پیچیده‌تر از مثال اول است. همه می‌توانند یک نام دامنه را در شرکت‌های ارائه دهنده خدمات domain ثبت و خریداری کنند. اگرچه هر نام دامنه باید منحصربه‌فرد باشد، اما راه‌های زیادی برای ایجاد آدرس‌های جعلی وجود دارد که به راحتی قابل تشخیص نیستند.به این مثال توجه کنید :

- در این مثال، کلاهبرداران دامنه «microsfrtfonline.com» را ثبت کرده‌اند، که در نگاه اول ممکن است «Microsoft Online»خوانده شده و به عنوان آدرس معتبر قانونی شرکت مایکروسافت در نظر گرفته شود.
- در یک بررسی که توسط یکی از تهیه کنندگان پادکست در Gimlet Media انجام شد، یک هکر استخدام شد تا کارمندان بخش‌های مختلف این شرکت را با حملات فیشینگ فریب دهد. هکر ابتدا دامنه «gimletrnedia.com»را خریداری کرد) به جای m-e-d-i-a r-n-e-d-i-a) و با این دامنه برای کارمندان مختلف این شرکت ایمیل‌های جعلی فرستاد. کلاهبرداری او به حدی موفقیت آمیز بود که مجریان برنامه، مدیر عامل Gimlet Mediaو رئیس آن را فریب داد. همین مسئله نشان می‌دهد که چطور عدم دقت به یک آدرس می‌تواند حتی قدیمی‌ترین کارمندها و کاربران یک سرویس ایمیل را هم به اشتباه بیاندازد.

3 . ایمیل حاوی اشتباهات املایی و نگارشی است

- اگر یک ایمیل ظاهرا رسمی حاوی اشتباهات املایی و دستور زبان ضعیف باشد، می‌توان گفت که احتمالا این ایمیل یک ایمیل کلاهبرداری است. بنابراین اگر به نحوه نگارش پیام توجه کنید، احتمال کمتری دارد که ایمیل‌های جعلی را تشخیص ندهید.کلاهبرداران معمولا هزاران پیام ساختگی و جعلی را برای افراد ناآگاه ارسال می‌کنند.
- اما چرا بسیاری از ایمیل های فیشینگ بد نوشته شده‌اند؟ واضح‌ترین پاسخ این است که کلاهبرداران معمولا از کشورهای مختلفی هستند که ممکن است به زبان کاربران دریافت کننده پیام تسلط زیادی نداشته باشند. با در نظر گرفتن این موضوع، تشخیص تفاوت بین اشتباه تایپی که توسط یک فرستنده واقعی ممکن است پیش بیاید با یک پیام جعلی که توسط کلاهبرداران نوشته شده است، بسیار ساده‌تر می‌شود. هنگام ایجاد پیام‌های فیشینگ، کلاهبرداران اغلب از یک مترجم آنلاین مانند گوگل ترنسلیت استفاده می‌کنند که احتمالا حاوی کلماتی درست ولی جملات بی معنی یا نامفهوم هستند.
- در این مثال یک کلاهبرداری با جعل پیام از طرف شرکت مایکروسافت را می‌بینید. این ایمیل فیشینگ ادعا می‌کند که در حساب کاربر "فعالیت غیرمعمول ورود به سیستم" رخ داده است.



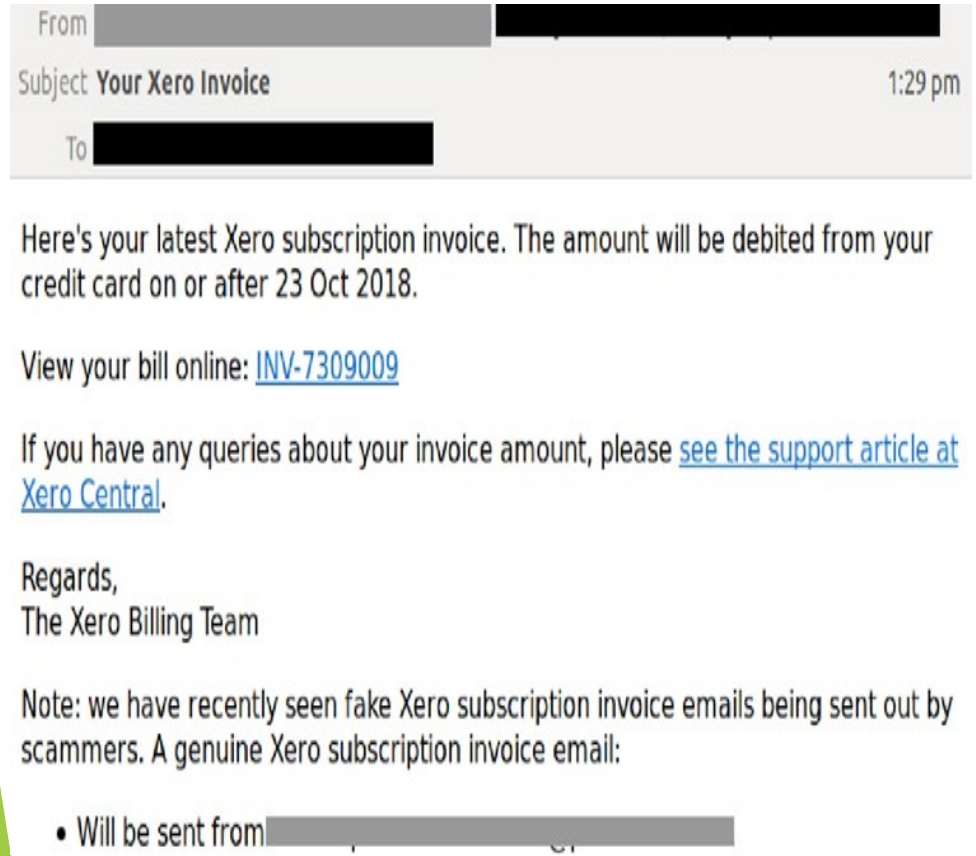
- در این ایمیل هیچ کلمه‌ای از نظر املایی نادرست نیست، اما پیام مملو از اشتباهات گرامری است که شخصی که مسئول این کار باشد مرتکب آن نمی‌شود. مثل جمله “We detected something unusual to use an applicationجمله درستی نیست .هر پیام ظاهرا رسمی که با این اشکالات نوشته شده باشد به احتمال بسیار بالا یک پیام جعلی و با هدف کلاهبرداری است. البته، این بدان معنا نیست که هر ایمیلی که اشتباهی در آن وجود داشته باشد، حتما جعلی است. همه گهگاهی اشتباه تایپی دارند، به خصوص زمانی که با عجله ایمیلی می‌زنند .شما می‌توانید تشخیص جعلی بودن ایمیل را با بررسی بیشتر ایمیل‌هایی که قبلا از فرستنده دریافت کرده‌اید انجام دهید. بهترین کار این است که با فرستنده از یک روش ارتباطی دیگر تماس بگیرید، خواه با مراجعه حضوری، تماس تلفنی، از طریق وب‌سایت یه با ارسال ایمیل به آدرس پشتیبانی، صحت ایمیل مشکوک را بررسی کنید.

4. ایمیل حاوی پیوست‌های آلوده یا پیوندهای مشکوک است

- ایمیل‌های فیشینگ اشکال مختلفی دارند. درست است که در این مقاله بر ایمیل‌های فیشینگ تمرکز کرده‌ایم، اما ممکن است پیام‌های جعلی و فیشینگ را از طریق تماس‌های تلفنی، پیام‌های واتساپ یا تلگرام یا پست‌هایی در شبکه‌های اجتماعی هم دریافت کنید. تمامی این حملات فیشینگ حاوی مسیری برای کلاهبرداری هستند.
- در برخی از این حملات، ممکن است شما ایمیلی با یک پیوست آلوده دریافت کنید که از شما درخواست شده است آنرا دانلود کنید. در برخی دیگر یک لینک (پیوند) به یک وب سایت جعلی برای شما ارسال شود تا وارد آن شده و دستورالعمل خواسته شده را انجام دهید. هدف از این فایل‌ها یا لینک‌ها به دست آوردن اطلاعات مهم شما مانند اطلاعات کاربری ورود به سیستم، جزئیات کارت اعتباری، شماره تلفن و شماره حساب یا در مرحله پیشرفته‌تر درخواست واریز وجه یا پرداخت یک صورت‌حساب باشد.

پیوست‌های آلوده ایمیل فیشینگ

در این نوع ایمیل فیشینگ، در پیوست ایمیل یک یا چند فایل به ظاهر ساده قرار دارد که در پس آن یک بدافزار نهفته است. در ایمیل زیر نمونه‌ای از این نوع ایمیل فیشینگ را می‌بینید:


From [redacted]

Subject **Your Xero Invoice** 1:29 pm

To [redacted]

Here's your latest Xero subscription invoice. The amount will be debited from your credit card on or after 23 Oct 2018.

View your bill online: INV-7309009

If you have any queries about your invoice amount, please see the support article at Xero Central.

Regards,
The Xero Billing Team

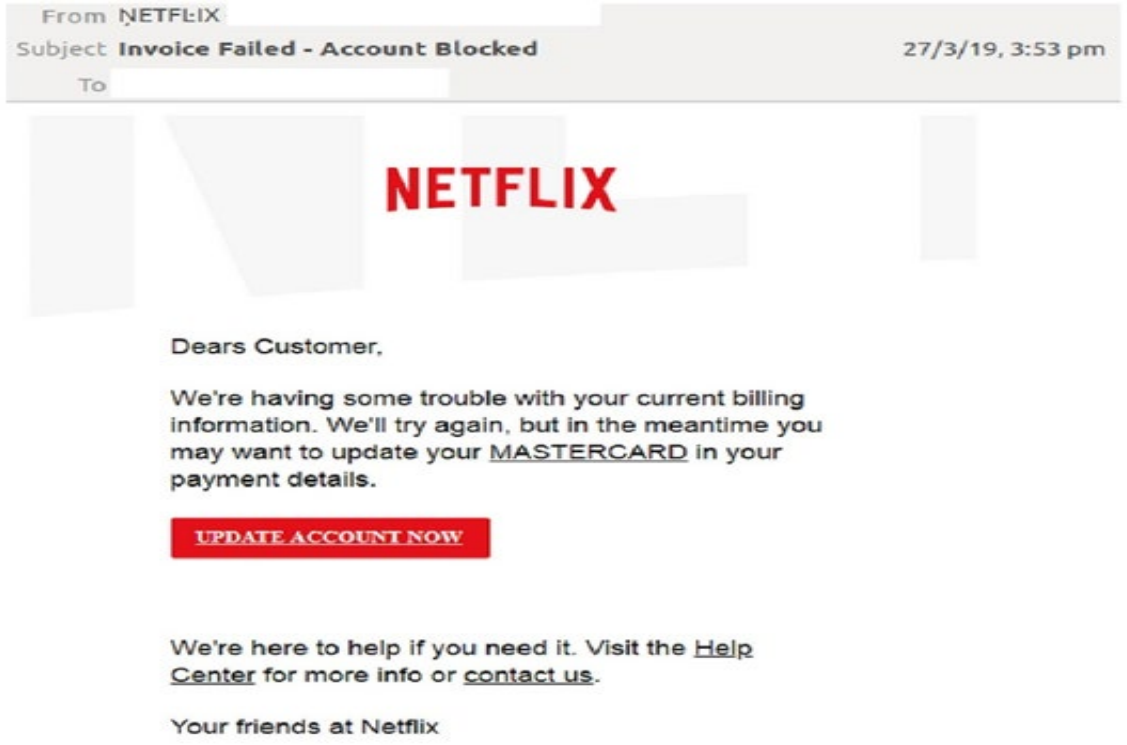
Note: we have recently seen fake Xero subscription invoice emails being sent out by scammers. A genuine Xero subscription invoice email:

- Will be sent from [redacted]

- در مثال فوق ظاهرا یک فاکتور در پیوست برای مخاطب ارسال شده است. در مواردی مانند این مثال، با وجود این که گیرنده انتظار دریافت فاکتور از فرستنده را ندارد، پیوست ایمیل را باز می‌کند تا آنرا بررسی کند. وقتی پیوست را باز می‌کند، مطمئن می‌شود که فاکتور برای او ارسال نشده است، اما دیگر خیلی دیر شده است. این پیوست به محض دانلود شدن، بدافزاری را روی سیستم قربانی منتشر می‌کند که می‌تواند کلاهبرداران را به اهداف خود برساند.
- بهترین روش پیش‌گیری از این نوع فیشینگ‌ها این است که هرگز پیوستی را باز نکنید مگر اینکه کاملا مطمئن شوید پیام از طرف یک فرد واقعی ارسال شده باشد. حتی در این صورت هم باز باید مراقب فایل‌های پیوست باشید و اگر برنامه آنتی ویروس به شما هشدار داد، آنرا جدی بگیرید. چون ممکن است ایمیل همکار یا دوست شما هک شده باشد.

لینک‌های جعلی

معمولا در این نوع ایمیل‌های فیشینگ، لینک‌هایی داخل ایمیل وجود دارند که با آدرس واقعی سایتی که ایمیل از طرف آن ارسال شده است، مطابقت ندارد. به عنوان مثال، در ایمیل زیر پیامی از نتفلیکس دریافت شده است و انتظار می‌رود لینک موجود در ایمیل شما را به آدرسی هدایت کند که با «netflix.com» شروع می‌شود. البته متاسفانه، در بسیاری از ایمیل‌ها، چه ایمیل واقعی باشند و چه ایمیل جعلی، لینک‌ها را برای زیباتر شدت ایمیل در یک دکمه پنهان می‌کنند، به همین دلیل از روی ظاهر دکمه مشخص نیست که لینک مورد نظر به کجا می رود.



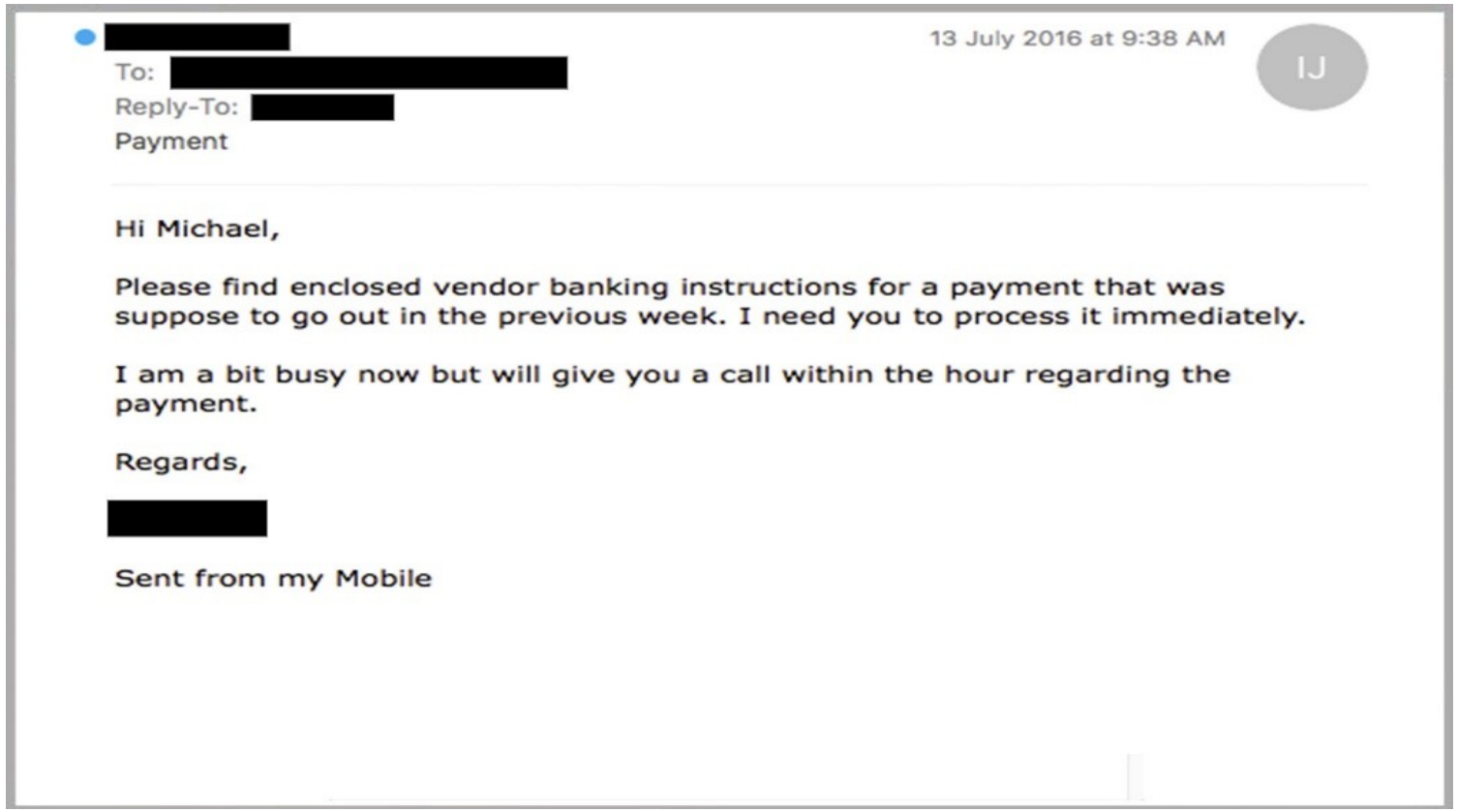
- در مثال فوق، ایمیل به گونه‌ای طراحی شده است که دریافت کننده را به یک نسخه جعلی از وب سایت نتفلیکس هدایت کند، جایی که از وی خواسته می‌شود جزئیات مربوط به پرداخت خود را وارد کند.
- کلاهبرداران با قرار دادن پیوند درون دکمه‌ای که می‌گوید «اکنون حساب را به‌روزرسانی کنید» به دو هدف دست می‌یابند. اول اینکه پیام را واقعی جلوه می‌دهند و سپس آدرس مقصد را به وسیله دکمه پنهان می‌کند تا دریافت کننده پیام با زدن آن به لینک مورد نظرشان هدایت شوند.

بهترین راه برای این که در دام این دست ایمیل‌های فیشینگ نیافتید، این است که عادت کنید پیش از کلیک روی هر دکمه‌ای، آدرس آنرا بررسی کنید. این کار بسیار ساده است. اگر با کامپیوتر ایمیل را دریافت کرده باشید موس را بدون این که کلیک کنید، روی دکمه حرکت دهید تا آدرس مقصد در نوار کوچکی در پایین مرورگر ظاهر شود. اگر با موبایل ایمیل را باز کرده باشید هم کافی است دکمه را نگه دارید تا یک پنجره کوچک اطلاع رسانی یا پاپ آپ حاوی پیوند ظاهر شود.

۵ . پیام حاوی درخواستی ضروری با فوریت بالا است

- معمولا اگر زمان کافی برای بررسی پیام داشته باشید، احتمال این که در دام کلاهبرداران بیافتید کمتر است. این مسئله‌ای است که کلاهبرداران هم به خوبی می‌دانند. در نتیجه معمولا لحن ایمیل‌های فیشینگ بگونه‌ای است که از شما می‌خواهد به سرعت و در اولین زمان ممکن درخواست را پاسخ دهید وگرنه خیلی دیر خواهد شد .مجرمان به خوبی می‌دانند که اگر رئیس شما یک ایمیل حاوی درخواست حیاتی و فوری را ارسال کند، احتمالا همه چیز را کنار می‌گذارید، به‌خصوص زمانی که ظاهرا بسیاری از همکاران دیگر منتظر اقدام فوری شما در خصوص ایمیل هستند. به مثال زیر توجه کنید:
- این نوع پیام‌های فیشینگ از بقیه خطرناک‌تر هستند. در ایمیل بالا از ظاهرا یکی از مدیران از کارمند خود خواسته است به سرعت پرداختی را انجام دهد و به دلیل این که در حال حاضر بسیار مشغول است، پس از پرداخت در مورد آن تماس خواهد گرفت .همه چیز به نظر درست است و به نظر می‌رسد کارمندی که ایمیل را دریافت کرده به سرعت باید کار پرداخت را انجام دهد.

- این دست پیام‌ها با فیشینگ‌های انبوه متفاوت هستند. زیرا نیاز به شناخت قربانی و اطلاعاتی برگرفته از مهندسی اجتماعی دارند تا بتوانند به درستی لحن رئیس در نوشتن پیام را تقلید کرده و کارمند را وادار به پرداخت صورت حساب کنند.


[redacted]
13 July 2016 at 9:38 AM
IJ
To: [redacted]
Reply-To: [redacted]
Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

نتیجه‌گیری

- همانطور که گفته شد، همچنان ایمیل‌های فیشینگ قربانی می‌گیرند و خبر خوب این است که با شناخت نشانه‌های آن می‌توان بسیاری از آنها را تشخیص داد و اقدامات پیشگیرانه را برای مسدود کردن فرستنده و جلوگیری از فریب دیگر همکاران فراهم کرد. در این مقاله سعی کردیم راه‌هایی برای تشخیص ایمیل فیشینگ و روش‌های جلوگیری از آن را بر اساس مثال‌های واقعی بررسی کنیم. بدون تردید، یکی از روش‌های موثری که می‌تواند از ما و سازمان ما در مقابل کلاهبرداری‌های فیشینگ محافظت کند، آگاه سازی در مورد این حملات و کمک به تشخیص آنها است.