ایمیل فیشینگ

دانشگاه فردوسی مشهد

مرکز فناوری اطلاعات و ارتباطات دانشگاه

تابستان 1398

ایمیل فیشینگ[1] چیست؟

یکی از قدیمی‌ترین و پرسودترین ابزاری که توسط هکرها استفاده می‌شود فیشینگ است؛ روشی که شما را فریب می‌دهد تا اطلاعات حساس و شخصی خود مانند اطلاعات کارت‌های اعتباری، رمزهای عبور، تاریخ تولد و هرگونه اطلاعاتی که هویت شما را در بردارند را فاش کنید.

ایمیل فیشینگ یکی از راه های متداول نفوذ توسط هکرها یا سایر خلاف کاران اینترنتی است .با گذر زمان تکنیک های ایمیل فیشینگ و به طور کلی هک از طریق فیشینگ تغییر یافته است اما همچنان اساس کار استفاده از نا آگاهی کاربران در شبکه اینترنت است.

در عملیات های فیشینگ اتفاقی که رخ می دهد این است که کاربر فکر می کند که یک ایمیل عادی دریافت کرده یا وارد یک صفحه عادی شده است. تقریبا هم همه چیز مشابه ایمیل یا صفحات عادی است. کاربران به این علت که به جزئیات دقت نمی کنند در دام هکرها خواهند افتاد و اطلاعات مهم نظیر نام کاربری و رمز عبور یا اطلاعات بانکی خود را در صفحه ایی که در واقع به عنوان یک دام توسط هکرها ساخته شده وارد می کند. در نتیجه مورد دستبرد یا کلاه برداری قرار می گیرند.

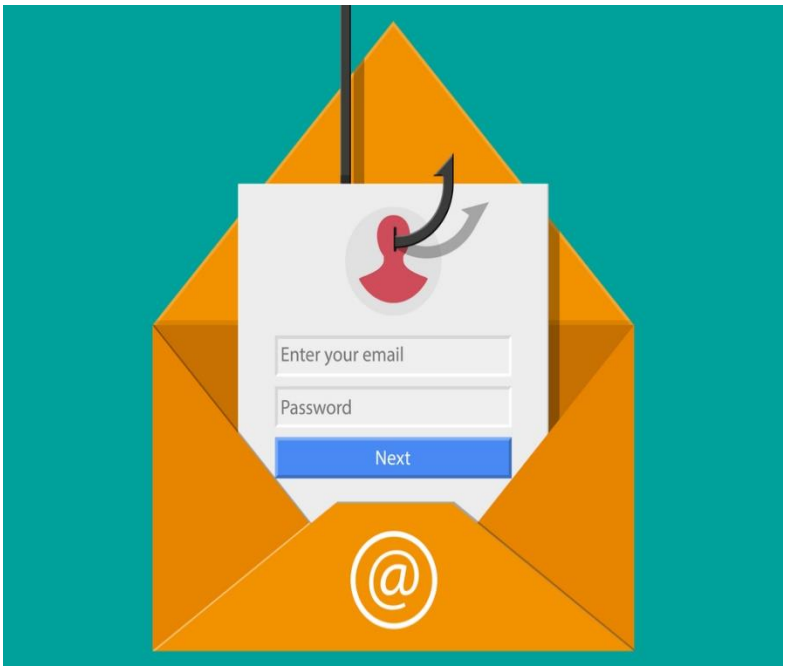
ایمیل فیشینگ از اواسط دهه 90 میلادی توسط مجرمین اینترنتی ایجاد شد. در این روش هکر ها یا کلاه برداران سعی می کنند با فرستادن ایمیل های تقلبی مشابه ایمیل یک شرکت معروف و با محتوا و موضوع اغواءکننده مانند برنده شدن در قرعه کشی، کاربران را به دام بیاندازند. سپس از آن ها می خواهند تا وارد یک لینک نا امن شوند یا یک بد افزار را دانلود کنند. با این که سالها است که از این روش استفاده می شود اما همچنان طبق اخرین آمار ها 48 درصد اینگونه ایمیل ها توسط کاربران باز می شود. همین موضوع سبب شده که کلاه برداران همچنان از این روش برای کار خود استفاده کنند.

[1] Phishing

راهکارهای پیشنهادی تشخیص ایمیل فیشینگ

- نشانگر موس را بر روی لینک، دکمه یا فرم ارسال داخل ایمیل نگه دارید (به هیچ عنوان روی آن کلیک نکنید) تا بتوانید مقصد نهایی لینک را مشاهده کنید، حتی در ایمیلهایی که از منابع آشنا ارسال می‌شوند.

- معمولا کلاه برداران در فیشنگ شما را متقاعد می‌کنند که روی لینک های ارسالی در ایمیل کلیک کنید. سپس در صفحه جدید که ممکن است مشابه صفحه بانک یا سازمان شما باشد از شما درخواست می‌شود رمز عبور و نام کاربری خود را وارد کنید. به این ترتیب می توانند به حساب کاربری شما دسترسی داشته باشند یا اطلاعات حساب و کارت بانکی شما را به دست آورند.

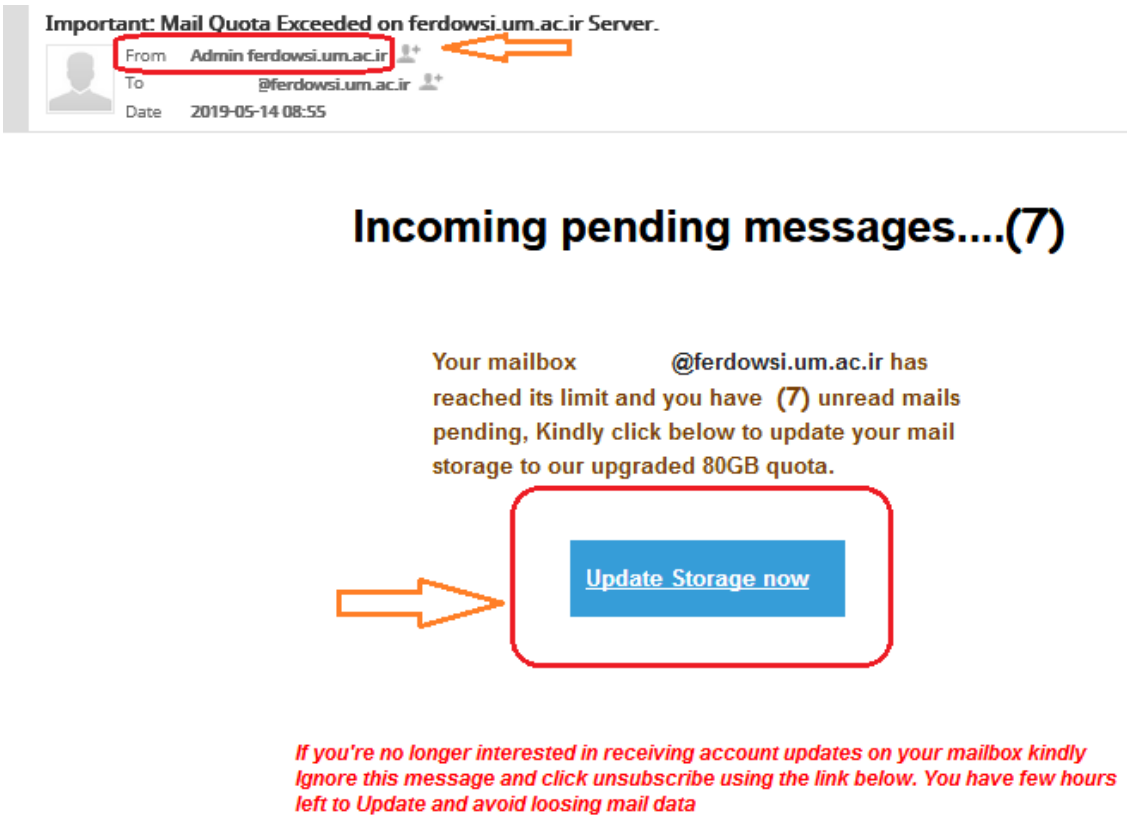


- هیچگاه اطلاعات شخصی و حساس خود نظیر نام کاربری، پسورد، اطلاعات کارت اعتباری را در یک درخواست پاسخ ندهید.
- به لینک ها و فایل های پیوست شده در ایمیل های مشکوک، اعتماد نکنید.

نمونه‌ای از ایمیلهای فیشینگ

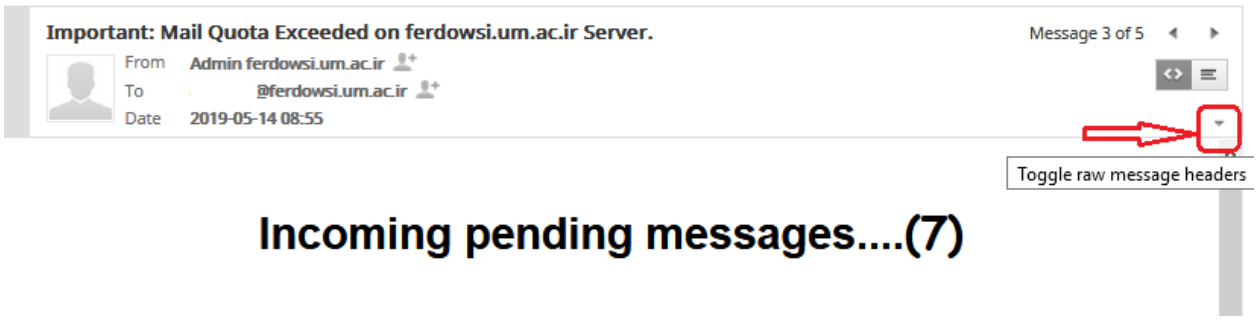
1. ایمیل درخواست افزایش فضای کاربر

شکل شماره‌ی 1 نمونه‌ای از ایمیل فیشینگ را نشان می‌دهد که به کاربر اعلام کره به دلیل پر شدن فضای ایمیل، امکان دریافت ایمیلهای جدید را نخواهد داشت. آدرس فرستنده‌ای که نشان داده، مطابق با دامنه دانشگاه است و در لینک Update مشخص شده، کاربر را ترغیب به کلیک بر روی آن و در نهایت دریافت شناسه و رمز کاربر می‌کند.



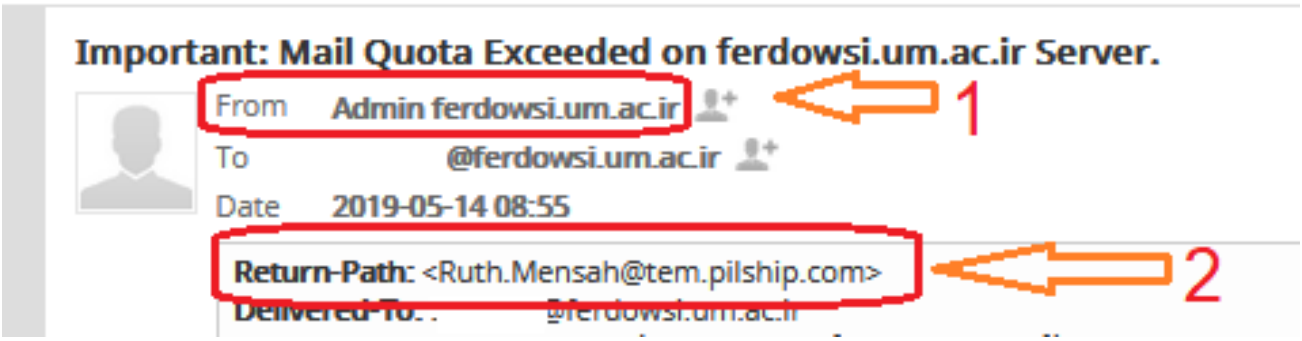
شکل (1)

برای تشخیص این نوع ایمیلها، شما ابتدا باید از صحت آدرس فرستنده مطمئن شوید. بدین منظور بر روی علامتی که در شکل شماره 2 مشخص شده کلیک نمایید تا به هدر ایمیل دسترسی پیدا کنید.



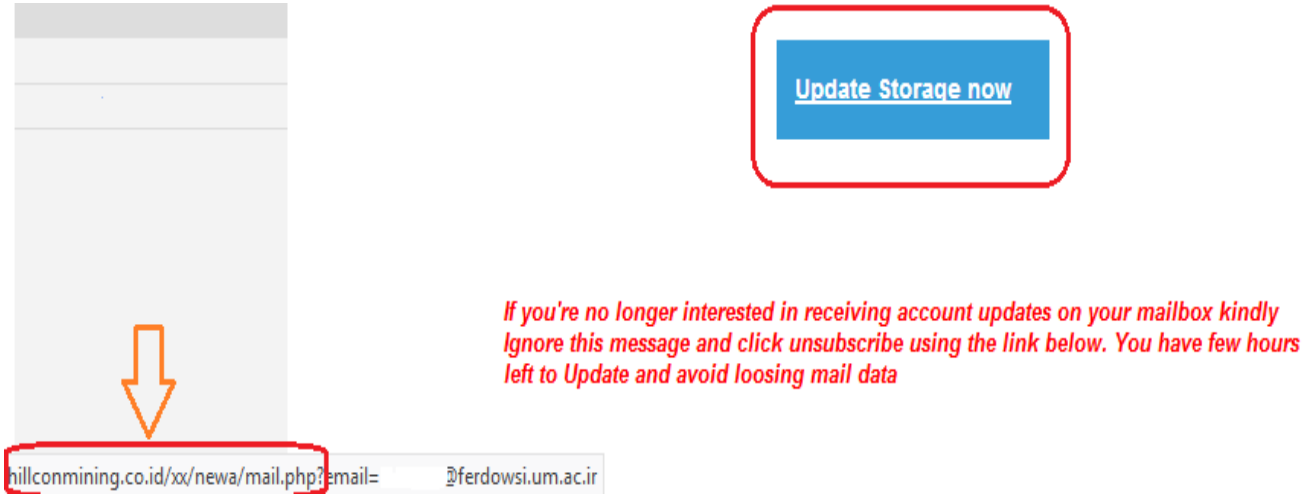
شکل (2)

با باز کردن هدر ایمیل متوجه آدرس ارسال کننده اصلی ایمیل خواهید شد. در شکل شماره 3 ، آدرس فرستنده‌ای که کاربر می‌بیند با شماره‌ی 1 نشان داده شده و آدرس اصلی فرستنده، با شماره 2 مشخص شده است. با بررسی آدرس فرستنده اصلی متوجه خواهید شد این ایمیل مربوط به دامنه دانشگاه نیست.



شکل (3)

همچنین با نگه داشتن موس بر روی لینک ایمیل، آدرس مقصد نهایی لینک، مطابق شکل شماره‌ی 4 نشان داده خواهد شد.

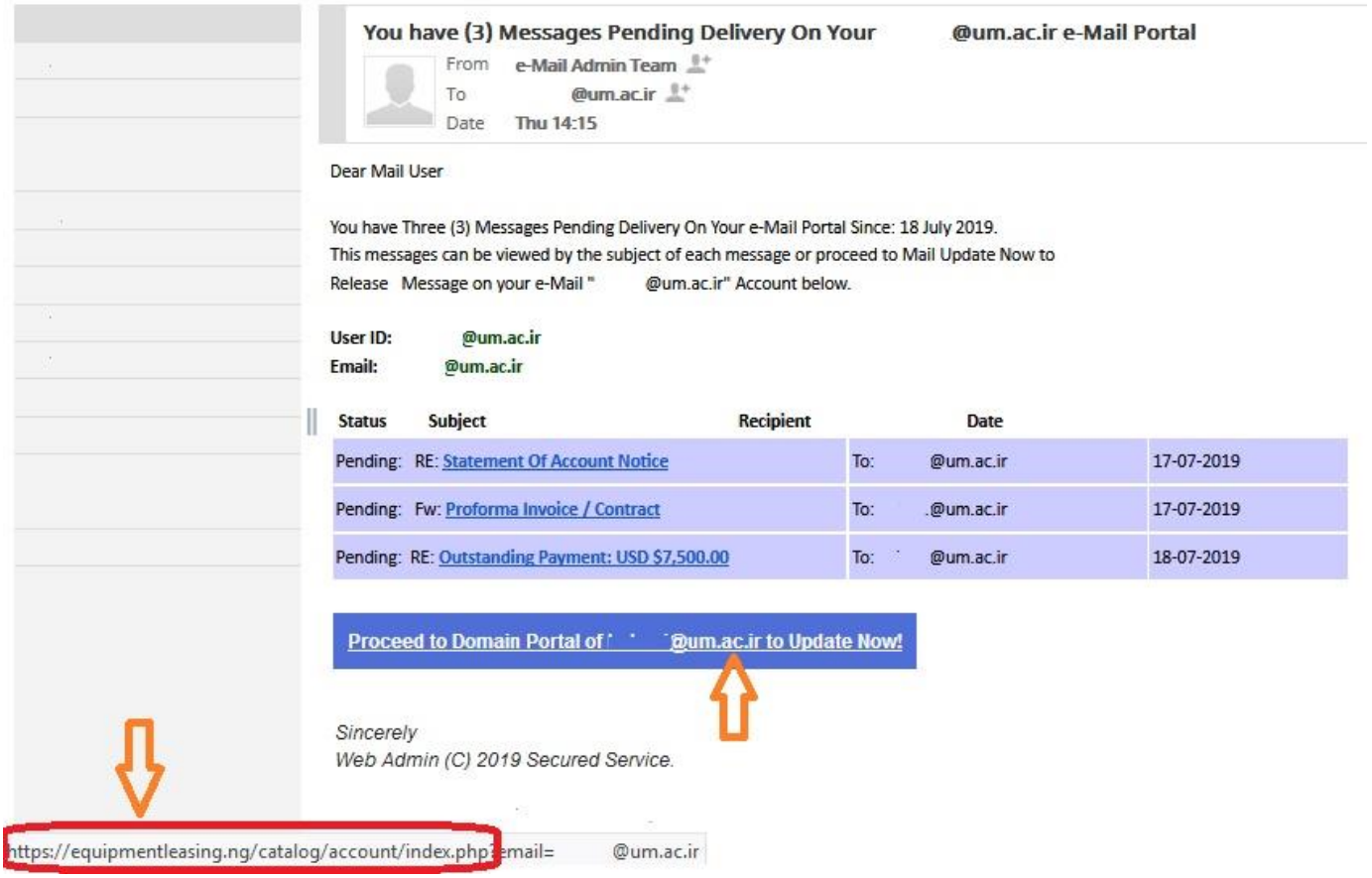


شکل (4)

همانطور که در لینک مشخص شده، آدرس لینک مربوط به دامنه دانشگاه نیست.

2. ایمیل درخواست آپدیت شناسه کاربر

نمونه دیگری از ایمیل فیشینگ در شکل شماره‌ی 5 مشخص شده که از کاربر خواسته به دلیل عدم دریافت تعدادی ایمیل نیاز به آپدیت شناسه دارد و کاربر را ترغیب به کلیک بر روی لینک می‌کند. در این ایمیل نیز با نگه داشتن موس بر روی لینک متوجه آدرس اصلی فرستنده که آدرسی غیر از دامنه um.ac.ir خواهید شد.



شکل (5)