



ایمیل فیشینگ

دانشگاه فردوسی مشهد

مرکز فناوری اطلاعات و ارتباطات دانشگاه

تابستان 1398

## ایمیل فیشینگ<sup>۱</sup> چیست؟

یکی از قدیمی‌ترین و پرسودترین ابزارهای 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 راه‌های متداول نفوذ توسط هکرها یا سایر خلاف‌کاران اینترنتی است. با گذر زمان تکنیک‌های ایمیل فیشینگ و به‌طور کلی هک از طریق فیشینگ تغییر یافته است اما همچنان اساس کار استفاده از نا آگاهی کاربران در شبکه اینترنت است.

در عملیات‌های فیشینگ اتفاقی که رخ می‌دهد این است که کاربر فکر می‌کند که یک ایمیل عادی دریافت



کرده یا وارد یک صفحه عادی شده است. تقریباً همه چیز مشابه ایمیل یا صفحات عادی است. کاربران به این علت که به جزئیات دقت نمی‌کنند در دام هکرها خواهند افتاد و اطلاعات مهم نظیر نام کاربری و رمز عبور یا اطلاعات بانکی خود را در صفحه‌ای که در واقع به عنوان یک دام توسط هکرها ساخته شده وارد می‌کنند. در نتیجه مورد دستبرد یا کلاه برداری قرار می‌گیرند.

ایمیل فیشینگ از اواسط دهه 90 میلادی توسط مجرمین اینترنتی ایجاد شد. در این روش هکرها یا کلاه برداران سعی می‌کنند با فرستادن ایمیل‌های تقلبی مشابه ایمیل یک شرکت معروف و با محتوا و موضوع اغواءکننده مانند برنده شدن در قرعه‌کشی، کاربران را به دام بیندازند. سپس از آن‌ها می‌خواهند تا وارد یک لینک نا امن شوند یا یک بد افزار را دانلود کنند. با این که سالهاست که از این روش استفاده می‌شود اما همچنان طبق آخرین آمارها 48 درصد اینگونه ایمیل‌ها توسط کاربران باز می‌شود. همین موضوع سبب شده که کلاه برداران همچنان از این روش برای کار خود استفاده کنند.

---

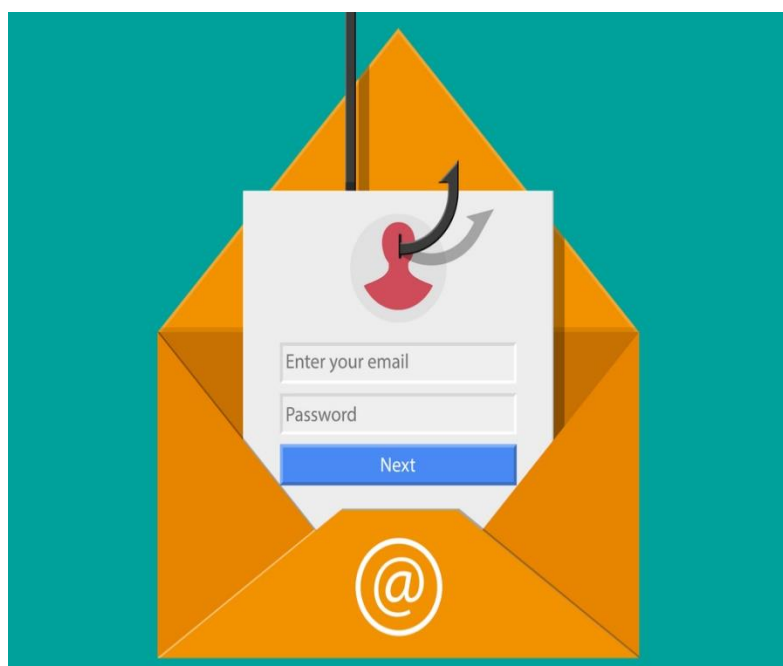
<sup>1</sup> Phishing

## 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.

- معمولاً کلاه برداران در فیشینگ 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 می‌توانند 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

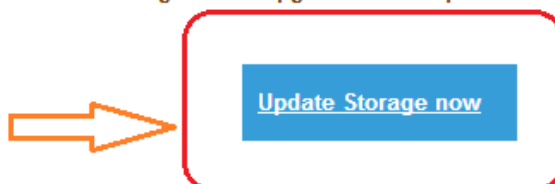
### 1. ایمیل درخواست افزایش فضای کاربر

شکل شماره‌ی 1 نمونه‌ای از ایمیل فیشینگ را نشان می‌دهد که به کاربر اعلام کرده 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.



### Incoming pending messages....(7)

Your mailbox @ferdowsi.um.ac.ir has reached its limit and you have (7) unread mails pending, Kindly click below to update your mail storage to our upgraded 80GB quota.



*If you're no longer interested in receiving account updates on your mailbox kindly ignore this message and click unsubscribe using the link below. You have few hours left to Update and avoid losing mail data*

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.

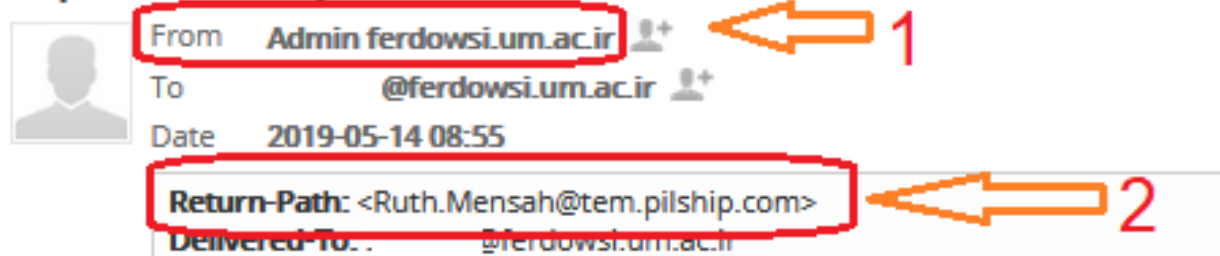


### Incoming pending messages....(7)

شکل (2)

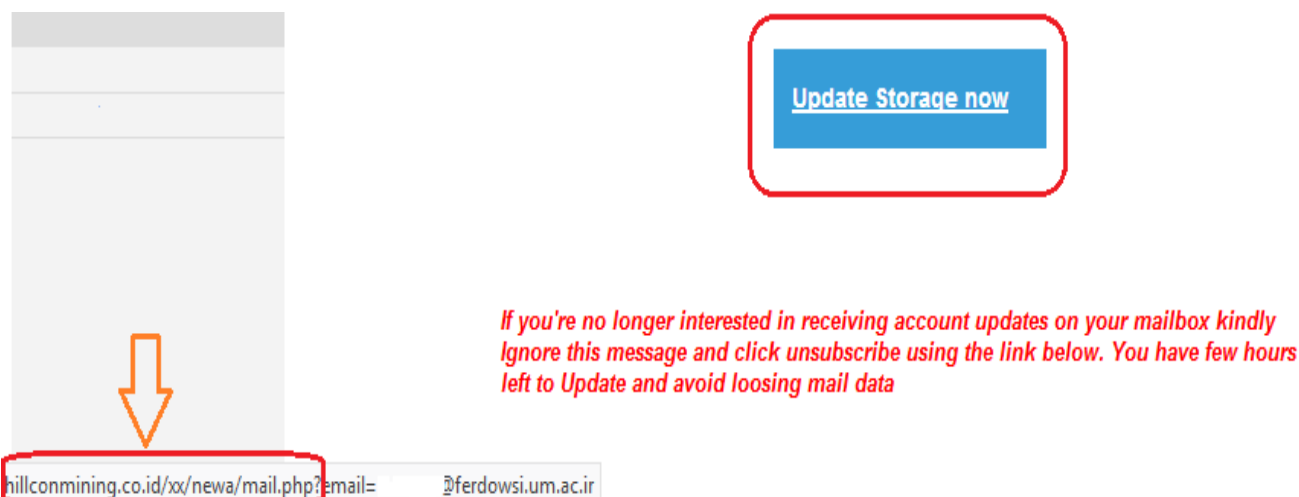
با باز کردن هدر ایمیل متوجه آدرس ارسال کننده اصلی ایمیل خواهید شد. در شکل شماره 3 ، آدرس فرستنده‌ای که کاربر می‌بیند با شماره‌ی 1 نشان داده شده و آدرس اصلی فرستنده، با شماره 2 مشخص شده است. با بررسی آدرس فرستنده اصلی متوجه خواهید شد این ایمیل مربوط به دامنه دانشگاه نیست.

### Important: Mail Quota Exceeded on ferdowsi.um.ac.ir Server.



شکل (3)

همچنین با نگر 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 شماره 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 نگره داشتن موس بر روی لینک متوجه آدرس اصلی فرستنده که آدرسی غیر از دامنه um.ac.ir خواهید شد.

**You have (3) Messages Pending Delivery On Your @um.ac.ir e-Mail Portal**

From: e-Mail Admin Team  
To: @um.ac.ir  
Date: Thu 14:15

Dear Mail User

You have Three (3) Messages Pending Delivery On Your e-Mail Portal Since: 18 July 2019.  
This messages can be viewed by the subject of each message or proceed to Mail Update Now to Release Message on your e-Mail " @um.ac.ir" Account below.

User ID: @um.ac.ir  
Email: @um.ac.ir

Status	Subject	Recipient	Date
Pending	RE: <a href="#">Statement Of Account Notice</a>	To: @um.ac.ir	17-07-2019
Pending	Fw: <a href="#">Proforma Invoice / Contract</a>	To: @um.ac.ir	17-07-2019
Pending	RE: <a href="#">Outstanding Payment: USD \$7,500.00</a>	To: @um.ac.ir	18-07-2019

[Proceed to Domain Portal of @um.ac.ir to Update Now!](#)

Sincerely  
Web Admin (C) 2019 Secured Service.

<https://equipmentleasing.ng/catalog/account/index.php?email=@um.ac.ir>

شکل (5)