فیشینگ(Phishing)

فیشینگ چیست و چگونه با آن مقابله کنیم؟ فیشینگ شایع ترین جرم سایبری محسوب می شود و در آن، فیشر سعی می کند اطالعات محرمانهی کاربر یا کاربران را سرقت کند.

فیشینگ(Phishing) به تلاش برای به دست آوردن اطاعاتی مانند نام کاربری یا گذرواژه یا اطلاعات حساب بانکی ازطریق جعل وب سایت و آدرس ایمیل و روش های متنوع دیگر گفته می شود. به بیان ساده تر، هنگامیکه شخصی تلاش میکند دیگری را فریب دهد تا اطلاعات شخصی اش را دراختیار بگیرد، حمله ی فیشینگ رخ میدهد .

انواع مختلف فیشینگ کدام است؟

فیشینگ انواع مختلفی دارد که به روش های مختلف تلاش میکنند به اطلاعات بانکی شما از طریق روش های متنوع مهندسی اجتماعی(Engineering Social)که در حوزه فیشینگ مانند ایمیل، تماس تلفنی، صفحات جعلی پرداخت، پیامک، انواع مدل های ربات های تلگرام و انواع روش های جدیدی که انتظار آن نمی رود، دست یابد.

برخی از معروف ترین روش های فیشینگ عبارت اند از :

فیشینگ با ایمیل های فریبنده

ارسال ایمیل جعلی(Email Fake) روشی ساده برای کلاهبرداری می باشد که توسط هکران و حتی افراد معمولی مورد سوء استفاده قرار می گیرد. در این روش کلاهبرداران با ارسال ایمیل های جعلی در قالب ایمیل اصلی افراد قربانی، باعث می شوند مشتریان شما بجای برقرار ارتباط با شما با هکر ها تبادل اطلاعات نمایند. این روش مخصوصا وقتی حائز اهمیت می باشد که اطلاعات مهمی نظیر اطلاعات بانکی، مدارک و سندهای مهم اداری، معاملات با شرکت های خارجی، تبادل ارز و... از طریق ایمیل ردوبدل شوند. لذا هکرها به راحتی امکان دریافت چنین اطلاعات ارزشمندی را خواهند داشت. ویا بعنوان مثالی دیگر در ایمیل های جعلی از آنها می خواهند که مبلغ را بجای واریز به شماره حساب های اصلی شرکت، به حساب مشخص شده در ایمیل جعلی واریز نمایند و یا با کلیک بر روی لینک آلوده رمز عبور اکانت را مجدد تغییر دهید و ....

به عنوان نمونه ای از ایمیل های جعلی لطفا به تصویر زیر توجه نمایید. این ایمیل از سمت فرستنده ای شناس و یا ناشناس (From: E-Mail Update Service [mailto:Mark.Abonyo@maersk.com]) ارسال شده است و ممکن است شما به اشتباه تصور کنید از سمت شرکت یا شخصی ارسال شده است و در نتیجه روی لینک آلوده کلیک نمایید.

From: E-Mail Update Service [mailto:Mark.Abonyo@maersk.com]
Sent: Wednesday, December 09, 2015 3:40 PM
To: [redacted]
Subject: Warning: Your E-mail[redacted]has been blacklisted/suspended

Dear

1969MB **2000**MB

We noticed your e-mail account has almost exceed it's limit. And you may not be able to send or receive messages any moment from now,
Click Here to renew your account.

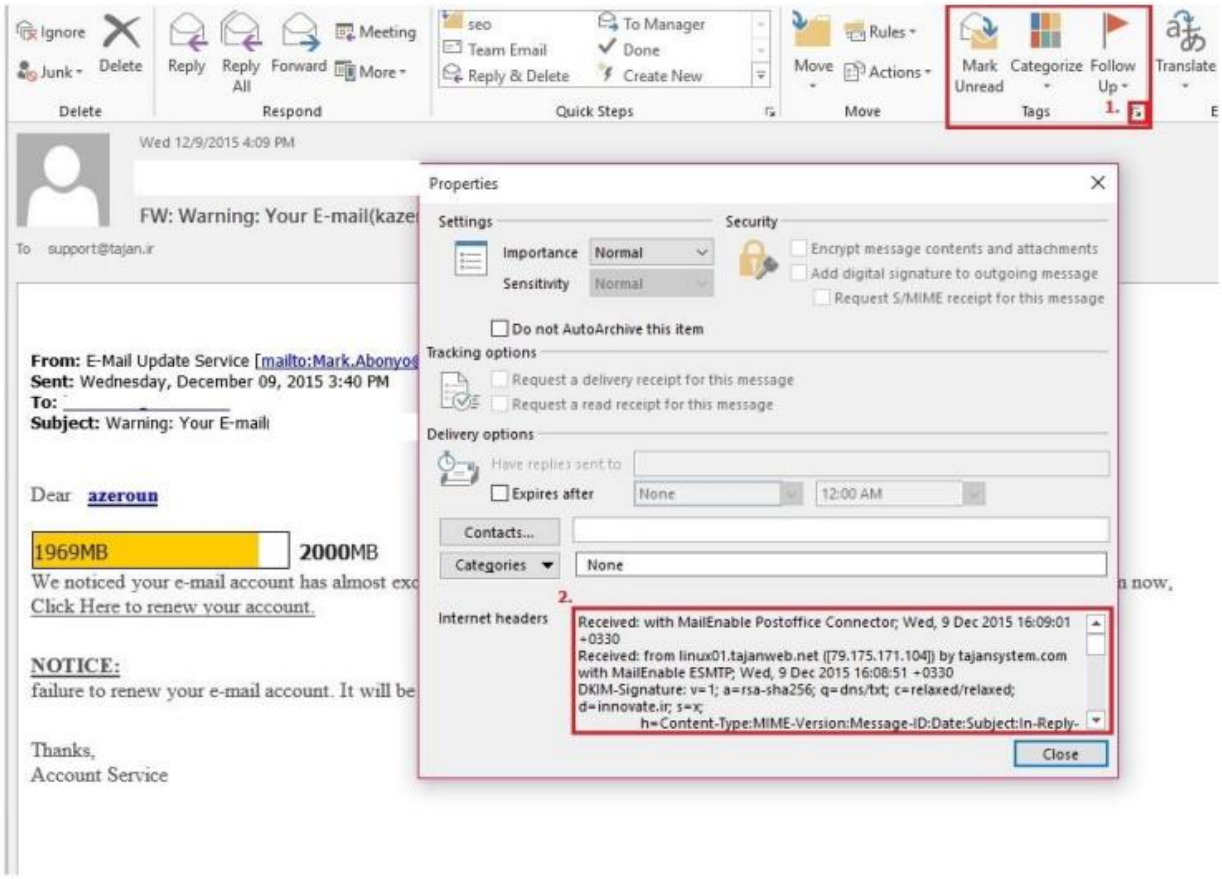
NOTICE:
failure to renew your e-mail account. It will be permanently disabled.

Thanks,
Account Service

جهت تشخیص ایمیل های جعلی، می بایست به هدر(header)ایمیل دریافتی مراجعه نمایید. جهت این کار به شرح زیر اقدام نمایید:

-مشاهده هدر ایمیل در آتلوک (:Outlook)

در آتلوک، بر روی ایمیل مورد نظر دابل کلیک کنید و آن را انتخاب کنید و سپس بر روی Options در نسخه ۲۰۰۷ و یا بر روی Tags در نسخه ۲۰۱۰ تا ۲۰۱۹ نرم افزار Outlook کلیک کرده و Options Messageرا انتخاب کنید و در قسمت Headers Internet می توانید اطلاعات مربوط به Header را مشاهده کنید.



به هیچ وجه ایمیلی به شکل فوق از مرکز فناوری اطلاعات دانشگاه ارسال نمی شود، و از کلیک بر روی لینک ارائه شده جداً خودداری فرمایید .

برای جلوگیری از هرگونه سو استفاده احتمالی این چند نکته امنیتی را در نظر داشته باشید :

۱. ایمیل هایی که از طرف افراد ناشناس ارسال می شوند و دارای فایل ضمیمه هستند و یا لینک های آلوده دارند را از روی سرور حذف نمایید و هرگز روی لینک مربوطه کلیک ننمایید. همچنین ممکن است فایل های ضمیمه دارای پسوندهای اجرایی نظیر. exe باشند که با باز کردن آن، کامپیوتر و یا شبکه شما را آلوده نمایند.

۲. در صورت دریافت ایمیلی از طرف دوست ، شرکت و ... که در آن بر انجام کاری تاکید شده است، نظیر واریز وجه به حساب حتما از طریق تلفن با فرد مقابل هماهنگ کنید. همچنین بهتر است از راه های دیگری غیر از ایمیل را نظیرفکس و... برای تبادل اطلاعات حساب های بانکی استفاده نمایید.

۳. در صورتی که ایمیلی برای پرداخت صورت حساب دریافت کردید، به هنگام مراجعه به درگاه پرداخت آنلاین دقت کنید که در اول آدرس سایت درگاه:// https ویا نماد اعتماد الکترونیکی وجود داشته باشد. در غیر اینصورت احتمال فیشینگ بالا می باشد !

۴. همیشه برای اکانت های ایمیل خود از پسورد های قوی شامل حروف بزرگ، حروف کوچک، اعداد و کاراکترهای خاص نظیر #، @و... همزمان استفاده نمایید .

۵. بطور مرتب از آنتی ویروس های معتبر و به روز جهت اسکن فایلها استفاده نمایید.

۶. ایمیل دریافتی را بررسی بیشتر به واحد امنیت و مانیتورینگ اطلاع رسانی نمایید .

حراست مرکز اورژانس پیش بیمارستانی و مدیریت حوادث دانشگاه علوم پزشکی بوشهر