ایمیل های نامعتبر

ایمیل نامعتبر (Fake Email) چیست؟

ایمیل های نامعتبر یکی از راه های متداول نفوذ توسط هکرها یا سایر خلاف کاران اینترنتی است. در عملیات نفوذ و سرقت اطلاعات 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.

به طور کلی ارسال کننده این گونه ایمیل ها، با ایجاد یک ایمیل جعلی و شبیه سازی آن با ایمیل هایی معتبر و ایمن نظیر ایمیل های بانک و شرکت های مرتبط با کارت اعتباری، بستری برای کلاه برداری ایجاد می کنند. این ایمیل ها به صورت معمول با فریب کاری در تلاش هستند که شما اطلاعات مهم و حساس خود را از قبیل نام کاربری، پسورد و اطلاعات کارت اعتباری را برای آنها ارسال نمایید، یکی از راه های آنها به عنوان مثال تهدید برای غیر فعال سازی کارت اعتباری شما در صورت عدم ارسال اطلاعات در موعد مقرر می باشد.

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. 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، 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 ۴۸ 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.

بر اساس گزارش های موجود روزانه حدود ۵۰۰ میلیون ایمیل نامعتبر تاثیرگذار ارسال می شود. در هر دقیقه حدود ۲۵۰ کامپیوتر هک می شود. این مشکلات و رخنه ها که منجر به سرقت اطلاعات محرمانه کاربران و شرکت ها می شود، بالغ بر ۳۸۸ میلیارد دلار در سال برای آنها هزینه به همراه دارد.(البته با توجه به عدم گزارش صحیح شرکت های مورد حمله این اطلاعات کاملا دقیق نیست)

ساختار یک ایمیل نامعتبر

- ایمیل های ارسال شده از میل سرور های عمومی.
- فایل های پیوست شده نامشخص و مشکوک
- مخاطب قرار دادن افراد به صورت عمومی (بدون ذکر اسم و فامیل شما)
- مشکلات نحوی و نگارشی (املایی و گرامری)
- ارجاع به سایت های نامشخص و یا سایت هایی با نگارش مشابه سایت های مطرح
- تهدید و یا فریبکاری برای انجام کاری ناخواسته
- شماره تلفن رایگان ناهمخوان با شماره های شناخته شده در ایمیل های مشکوک

راهکارهای پیشنهادی

- 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.
- نشانگر موس را بروی لینک های داخل ایمیل نگه دارید تا بتوانید مقصد نهایی لینک را مشاهده کنید، حتی در ایمیلهایی که از منابع آشنا ارسال می شوند.
- بهتر است بجای اینکه بروی لینک ها کلیک نمایید آنها را به صورت دستی در مرورگر تایپ نمایید.
- به شماره تلفن های موجود در ایمیل مشکوک باشید و هرگز با شماره های مشکوک تماس نگیرید.

سخن پایانی

برای بررسی و تحلیل اطلاعات و تشخیص ایمیل های جعلی، می بایست به هدر (header) ایمیل دریافتی مراجعه نمایید:

۱- بعداز لاگین به ایمیل اکانت مورد تظر به بخش inbox (در پنجره سمت چپ) مراجعه نموده و در پنجره سمت راست برروی ایمیل مورد تظر دابل کلیک نمایید تا محتوای ایمیل در پنجره ی جدید نمایش داده شود.

۲- جهت مشاهده اطلاعات هدر ایمیل مربوطه کافیست در صفحه لود شده برروی ایکون View Headers در سمت راست صفحه کلیک نمایید.

٪۹۱ از حملات فضای مجازی با یک ایمیل نامعتبر شروع می شوند.

٪۹۴ از ایمیل های نامعتبر دارای فایل های مخرب به صورت پیوست می باشند.