شنبه 01 اردیبهشت 1397 - 20:06

# کلاهبردای با ایمیل

چند مرحله ساده برای حفاظت از سرمایه گذاری الکترونیکی:

آیا می دانید چگونه می توانید از کلاهبرداریهایی که با ایمیل صورت می گیرد در امان باشید؟ با بیش از 75 میلیون ایمیل فیشینگ که هر روز ارسال می شوند اگر شما هم یکی از افراد دریافت کننده این ایمیل ها باشید نباید خیلی تعجب کنید. بر اساس آمار «جمعیت مبارزه با فیشینگ» معروف به APWG از میان 75 میلیون حمله که همه روزه انجام می گیرد بیش از 2000 قربانی ثبت شده در روز گرفتار می شوند و بیش از یک میلیون دلار سالانه از آنها دزدیده می شود.

فیشینگ یا Phishing در حقیقت یک جعل هویت است به طوریکه جاعل از طریق ایمیل های تقلبی دست به کار می شود. به عبارت دیگر وب سایت هایی هستند که توسط افراد کلاهبردار ساخته شده اند. این وب سایت ها به گونه ای طراحی شده اند که خود را به جای یک سرور ایمیل سر شناس مانند یاهو جا می زنند و وقتی قربانی به این آدرس هدایت می شود با صفحه ای کاملاً مشابه صفحه یاهو روبرو می شود و نام کاربری و کلمه عبور خود را وارد می کند و به این روش می توانند به اطلاعات حساس فرد (مانند اطلاعات حساس بانکی) دست پیدا کنند.

این کلاهبرداران وب سایتی شبیه به وب سایت یک کمپانب بزرگ و خوشنام مانند وب سایت بانک های بزرگ و کمپانی های سرمایه گذاری طراحی می کنند تا وب سایت خود را به جای آنها جا بزنند سپس تعداد زیادی ایمیل به قربانیان خود ارسال می کنند گویی این ایمیل از آن شرکت بزرگ ارسال شده است در این ایمیل حتی لوگوی آن کمپانی هم وجود دارد آنها معمولاً شرایط را اضطراری جلوه می دهند و مثلاً از شما می خواهند مراحلی را طی کنید در غیر این صورت حساب کاربری خود را از دست خواهید داد. و در این میان از شما حساب کاربری و رمز عبور را هم خواهند خواست. و همینطور تا حد امکان از شما اطلاعات بیشتری می گیرند.

حال که با مشکلات مربوط به امنیت ایمیل و حساب کاربری آشنا شدید بد نیست درباره راه های مقابله و حفاظت خود اطلاعاتی بدست آورید.

## نحوه حفاظت:

-1 هیچگاه اطلاعات کاربری خود را از طریق یک درخواست یا فرمی که با ایمیل دریافت کرده اید وارد نکنید.

-2 همیشه برای وارد کردن اطلاعات حساس کاربری یک صفحه جدید در مرورگر خود باز کنید و آدرس آن وب سایت را به صورت دستی وارد کنید. مثلا اگر از ebay پیغامی دریافت کردید که از شما خواسته بود وارد آن وب سایت شوید روی هیچ لینکی کلیک نکنید و فقط یک صفحه دیگر باز کنید آنگاه آدرس. www.ebay.com // :http را در آن وارد کنید. سپس می توانید اطلاعات کاربری خود را وارد کنید.

-3 هیچگاه در یک ایمیل مشکوک به فیشینگ روی لینکی کلیک نکنید.

-4 هیچگاه در یک ایمیل مشکوک به فیشینگ یا هر ایمیل ناشناخته دیگری فایل های ضمیمه ( Attachments ) را باز نکنید.

-5 برای وارد کردن اطلاعات حساس مانند رمز عبور و نام کاربری همیشه از وب سایت های ایمن که با https:// شروع می شوند استفاده کنید و به وب سایت هایی که آدرس اینترنتی آنها با http:// شروع می شوند برای وارد کردن اطلاعات حساس اعتماد نکنید.

-6 مرتبا فعالیت هایی که در حساب کاربری شما انجام می شود زیر نظر داشته باشید و ببینید کارهای مشکوکی انجام شده است یا خیر.

-7 مطمئن شوید مرورگر شما به روز یا Update شده است و همه وصله های امنیتی آن نصب شده است.

-8 کامپیوتر خود را بایک آنتی ویروس و آنتی اسپای ویر و یک فایروال مناسب و به روز محافظت کنید.

-9 شاید بخواهید یک ابزار ضد فیشینگ مانند Earth link Scam Blocker نصب کنید تا هنگام باز شدن یک صفححه مشکوک به شما گوشزد کند. این نرم افزار رایگان است و می توانید آنرا از اینترنت دانلود کنید.

همچنان که این کلاهبرداری ها در حال افزایش است بهتر است آگاهی خود را در این زمینه افزایش دهید تا بتوانید از اطلاعات محرمانه خود محافظت کنید.

## نوشته: لیزا اسمیت