فیشینگ(Phishing) چیست؟

در اصطلاح رایانه، فیشینگ عملی مجرمانه در جهت دسترسی غیر قانونی به اطلاعات حساس و مهم همچون نام کاربری، رمز عبور افراد و جزئیات کارتهای اعتباری از طریق قابل اعتماد نشان دادن ارتباط الکترونیکی است. فیشینگ به طور معمول از طریق ایمیل و پیام کوتاه صورت می گیرد و کاربر را به سوی وارد کردن اطلاعات در یک پایگاه اینترنتی جعلی سوق می دهد.

آسیب های فیشینگ:

کمترین ضرری که می توان در نظر گرفت دسترسی به ایمیل است، به عنوان مثال سارق با استفاده از ایمیل افراد اقدام به ارسال spam می کند. بیشترین ضرر فیشینگ، بلاک کردن سرور ایمیل دانشگاه، عدم ارسال ایمیل به دانشگاه های معتبر جهان، عدم دسترسی به پایگاه های علمی معتبر و ...

این نگرانی نیز وجود دارد که سارق اطلاعات بدست آمده از افراد مختلف را تغییر دهد و با درست کردن حساب جعلی به اسم یکی از قربانیان از اعتبار او سوء استفاده نموده شهرت او را لکه دار کند.

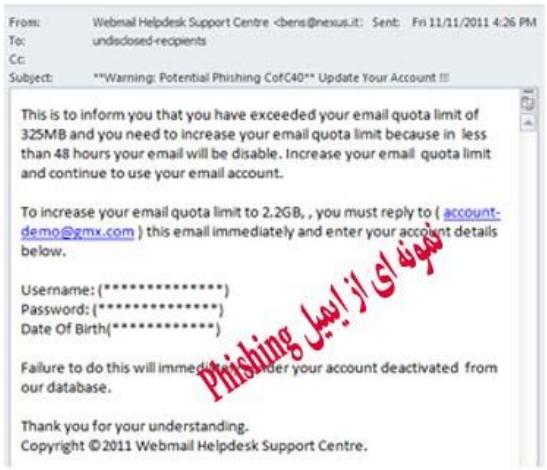
در مرحله اول شخص سارق در اینترنت ایمیل افراد قربانی را از صفحات وب استخراج می کند.

در مرحله دوم سارق به کاربران ایمیل ارسال کرده و به طرق مختلف از آنها درخواست اطلاعات کاربری شامل نام کاربری و کلمه عبور می نماید.

در مرحله سوم سارق با استفاده از اطلاعات استخراج شده عملیات مورد نظر خود را انجام می دهد.

- افرادی که تا به حال به ایمیل های مشکوک پاسخ داده اند باید اقدام به تغییر پسورد خود نمایند.
- مرکز فناوری اطلاعات هیچ گونه نیازی به دریافت اطلاعات کاربری، کاربران از طریق ایمیل ندارد

به محض دریافت ایمیل حاوی درخواست اطلاعات هویتی فوراً آن را پاک نمایید.



نمونه ای از ایمیل phishing

فیشینگ چگونه اتفاق می افتد؟

فیشینگ طی سه مرحله اتفاق می افتد در مرحله اول شخص سارق در اینترنت ایمیل افراد قربانی را پیدا پیدا می کند، بنابراین بهتر است افراد از قرارد دادن ایمیل خود به صورت واضح در صفحات وب جلوگیری کنند و ایمیل خود را در قالب عکس و یا به صورت کد شده در صفحات قرار دهند. سارق بعد از استخراج ایمیل به کاربران ایمیل ارسال می کند.

ایمیل های فیشینگ انواع گوناگونی دارد، در تعدادی از آنها فایلی پیوست شده است که دانلود آن فایل ممکن است خطرناک باشد. در دسته دیگر از کاربر درخواست می کند که به ایمیل پاسخ دهد که در صورت پاسخ اطلاعات فرد قربانی برای سارق ارسال می گردد. در دسته دیگر ایمیل های فیشینگ لینکی قرار گرفته شده که از فرد قربانی درخواست می کند روی لینک کلیک کند و با کلیک کردن بر روی لینک اطلاعات حساب برای سارق ارسال می گردد.

مهاجمان به منظور فریب کاربران از روش های متعددی استفاده می نمایند

- استفاده از logo و سایر علائم تجاری شناخته شده و معتبر، ساختار و طراحی email تقلبی مشابه وب سایت واقعی است، بگونه ای که در اولین مرحله تشخیص جعلی بودن آن برای بسیاری از کاربران غیرممکن است.
- بخش from نامه الکترونیکی ارسالی، مشابه ارسال یک email معتبر، از شرکت مربوطه است. در متن email ممکن است فرمی تعبیه شده باشد که از کاربران خواسته شود به دلایل خاصی(مثلا" account شما در معرض تهدید است و ممکن است مورد سوء استفاده قرار گیرد، فضای inbox شما پر شده است، ما در حال بروز رسانی سرور هستیم و نیاز به اطلاعات شما داریم و یا تهدید قطع ایمیل شما درصورت پاسخ ندادن)،شما رامجبور به وارد کردن اطلاعات خود در فرم مندرج در ایمیل و یا با کلیک بر روی لینک موجود در ایمیل نمایند. در شکل روبرو یک نمونه email جعلی نشان داده شده است .