علیرضا سلطانی نشان | 98111033302016

تکلیف دهم

تاریخ 26 اردیبهشت 00

عملیات فیشنیگ چیست؟

بطور کلی فیشینگ نوعی عملیاتی است که به هدف بدست آوردن اطلاعات حساس کاربران استفاده می‌شود، مانند username و password و دیگر اطلاعات مهمی که به طور خاص به هر یک از کاربران تخصیص یافته است مانند ای دی آنهاست که به صورت یونیک است.

کسی که عملیات فیشنیگ را پیاده سازی می‌کند خیلی باید دقت کند که سایت یا اپلیکیشنی که مینویسد دقیقا و صریحا همان نسخه کلون شده و تغلبی (Fake Page) سایت و اپلیکیشن رسمی و اصلی باشد در غیر این صورت کاربران متوجه عدم اصالت برنامه مورد نظر میشوند و از آن برنامه خارج خواهند شد.

این فیشینگ بایستی از هر نظر کاملا شبیه کلون خودش باشد، برای مثال سایتی را درنظر بگیرید که از یک آدرس URL استفاده می‌کند، کسی که قراراست عملیات فیشینگ خود را در سایت خودش انجام دهد باید این موضوع را هم در نظر بگیرد که دقیقا آدرس سایتش مانند آدرس سایت اصلی باشد، مانند سایت بانک ملت دات آی آر، چرا که بسیاری از کاربران در هنگام ورود به این سایت اصلا به نگارش خود در قسمت URL مرورگر خود توجه نمی‌کنند و فقط میخواهد به سمت اصلی سوق پیدا کنند، یعنی سایت اصلی بانک ملت که نگارش آدرس رسمی آن به این صورت است : mellat.ir، کسی که فیشینگ را در سایت خود که کلون شده سایت اصلی بانک ملت است و دقیقا همان UI را دارد، با آدرسی مانند melat.ir در سامانه ها و دامنه ها حضور میابد.

معمولا وبسایت های فیشینگ بخش Auth و احراز هویت آنها شبیه سایت اصلی است، به محض اینکه شما یوزر و پس خود را می‌زنید و وارد حساب می‌شوید دقیقا اطلاعات شما که کلید اصلی باز شدن در بانک برای شما بوده است، دست افرادی ناشناس خواهد افتاد. البته با آمدن راه هایی مانند Two Factor Authentication، یا رمز دو مرحله ای شما بایستی کدی که ارسال می‌شود را برای وبسایت مورد نظر وارد نمایید که البته آنهم میشود از طریق و شگرد های مهندسی اجتماعی به راحتی بدست آورد.