



چالش های امنیتی وب و جلوگیری از سرقت های اینترنتی

ابوذر نظری نیا

دانشجوی کارشناسی ارشد دانشگاه آزاد خرم آباد، abozarnazarynia@gmail.com

چکیده - حملات فیشینگ یا سرقت های اینترنتی یک چالش مهم در فضای مجازی و وب است و صفحات جعلی در این روش اطلاعات مهم کاربران را مورد سرقت قرار می دهد. صفحات جعلی با جعل هویت یک وبسایت دارای ظاهر شبیه به سایت اصلی بوده و از این طریق اعتماد کاربران را به خود جلب می نماید تا اطلاعات مهم آنها را سرقت نماید. در سرقت های آنلاین به طور معمول یک ایمیل جعلی از طرف هکر یا فیشر برای کاربران ارسال می شود و با روش های فریب آنها را ترغیب می نماید که بر روی لینک جعلی کلیک نموده و سپس به یک سایت جعلی وارد شوند که شبیه سایت قانونی بوده و از این طریق اطلاعات آنها مورد سرقت قرار گرفته شود. شناسایی این حملات باعث می شود تا زیان مالی آنها حداقل شود و اعتماد کاربران به تجارت الکترونیک افزایش داده شود و از طرفی امنیت فضای وب را افزایش دهد. در این مقاله چالش مرتبط با سرقت های آنلاین در اینترنت مورد توجه قرار گرفته شده و اهمیت شناسایی این حملات ارایه شده و تلاش شده تا با ارایه راهکارهای مفید صفحات جعلی وب تشخیص و شناسایی شوند.

کلید واژه - سرقت اطلاعات، جعل هویت، فیشینگ، وب سایت جعلی

تمام تلاش خود را بکار برده تا اطلاعات کاربردی کاربران وب را مورد سرقت قرار دهند و برای این منظور بیشتر از روش های فریب مانند مهندسی اجتماعی^۱ استفاده می نمایند. در این نوع از سرقتها یک سیکل مشاهده می شود که در ابتدا یک وبسایت قانونی جعل شده سپس لینک های آن برای کاربران ارسال شده و تلاش می شود تا اطلاعات مهم آن سرقت شوند. روش های مختلفی برای تشخیص حملات فیشینگ وجود دارد که بیشتر

۱- مقدمه

یکی از چالش های مهم وب وجود وبسایت های جعلی^۱ است که هویت سایت های قانونی^۲ را جعل نموده و ظاهر آنها بسیار شبیه به ظاهر وبسایت های قانونی بوده و برای فریب کاربران و سرقت اطلاعات آنها استفاده می شود [۱]. هکر و افراد سارق تحت وب^۳

^۱Fake websites

^۲Legal sites

^۳Phisher

^۴Social engineering