عنوان مقاله:
بررسی راهکارهایی در برابر حملات فیشینگ

محل انتشار:
چهاردهمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات (سال: 1400)

تعداد صفحات اصل مقاله: 10

نویسندگان:
فاطمه سلمانوندی - *دانشجوی دپارتمان مهندسی کامپیوتر ، آموزشکده فنی وحرفه ای دختران اهواز ،دانشگاه فنی و حرفه ای استان خوزستان،ایران*

منیژه نوری - *مدرس دپارتمان مهندسی کامپیوتر ، آموزشکده فنی و حرفه ای دختران اهواز ،دانشگاه فنی و حرفه ای استان خوزستان ،ایران*

خلاصه مقاله:
فیشینگ به معنای دزدی رمزعبور از طریق طعمه گذاری میباشد. فیشینگ به عنوان یک جرم مهندسی اجتماعی شناخته می شود، که از جعل هویت و بازی کردن در نقش دیگری برای دستیابی به اطلاعات شخصی افراد استفاده می کند و امنیت کاربران وب را به مخاطره می اندازد.[۱] در عمل، به صورت ایجاد کپی دقیق رابط گرافیکی یک تارگاه معتبر مانند: بانکها انجام می شود . ابتدا کاربر از طریق پست الکترونیکی و یا آگهی های تبلیغاتی تارگاه های دیگر به این صفحه جعلی راهنمایی میشود .سپس از کاربر درخواست میشود تا اطلاعات کارت یا حساب خود را وارد نماید و به این صورت، کلاهبرداران به اطلاعات اصلی حساب یا کارت افراد دسترسی پیدا میکنند.[۲] اغلب راه حل های ضد-فیشینگ دارای دو محدویت ، نیاز به زمان دسترسی سریع برای یک محیط زمان-واقعی و نیاز به نرخ (سرعت) تشخیص بالا است.[۳] لذا در این مقاله قصد داریم به مروری بر راهکارهایی در برابر حملات فیشینگ که توسط پژوهشگران پیشین انجام شده ، بپردازیم.

کلمات کلیدی:
حملات فیشینگ، مهندسی اجتماعی، پست الکترونیکی، رابط گرافیکی