عنوان مقاله:
ارایه رویکردی به منظور شناسایی و پیش بینی وب سایت های فیشینگ به وسیله الگوریتم های کلاس بندی بر اساس مشخصه های صفحات وب

محل انتشار:
فصلنامه مدل سازی در مهندسی, دوره 14, شماره 47 (سال: 1395)

تعداد صفحات اصل مقاله: 15

نویسندگان:
مهدی دادخواه - *گروه مهندسی کامپیوتر و فناوری اطلاعات، موسسه آموزش عالی صنعتی فولاد، فولادشهر اصفهان*

محمد داورپناه جزی - *گروه مهندسی کامپیوتر و فناوری اطلاعات، موسسه آموزش عالی صنعتی فولاد، فولادشهر اصفهان*

مجید سعیدی مبارکه - *گروه کامپیوتر، واحد مبارکه، دانشگاه آزاد اسلامی، مبارکه، ایران*

خلاصه مقاله:
امروزه مهمترین ریسک و چالش مورد توجه در تجارت و بانکدارای الکترونیک، خطر کلاهبرداری آنلاین و حملات فیشینگ است. حملات فیشینگ همواره به عنوان یکی از ابزارهای پرکاربرد برای مهاجمان، به منظور سرقت کلمه های عبور و رمزهای الکترونیک کاربران در مبادلات الکترونیک بوده است. در این نوع کلاهبرداری، مهاجمان نامه های الکترونیک با ادعاهای مختلف به قربانی ارسال می کند و با تکنیکهای مختلفی قربانی را به صفحه های جعلی خود هدایت می کند سپس اقدام به سرقت اطلاعات حساس کاربران مانند رمزهای عبور می نماید. صفحات وب، نامه های الکترونیک و آدرسهای فیشینگ دارای ویژگی هایی هستند که از آنها می توان برای شناسایی این حملات استفاده کرد. در این مقاله رویکردی جهت شناسایی و پیش بینی وب سایتهای فیشینگ با استفاده از الگوریتمهای کلاس بندی بر اساس مشخصه های صفحات وب ارایه خواهد شد که نرخ خطای کمتری نسبت به سایر تکنیکهای مقابله با حملات فیشینگ، به خصوص تکنیکهای مشابه میتنی بر الگوریتمهای داده کاوی دارد. در رویکرد ارایه شده، ویژگی های قابل استفاده در شناسایی صفحات فیشینگ براساس میزان تاثیر در شناسایی این حملات وزن بندی شده سپس با اعمال الگوریتمهای کلاس بندی بر روی مجموعه داده های مرتبط، الگویی به منظور شناسایی این حملات استخراج می گردد که قادر به شناسایی حملات ژورنال فیشینگ بوده و نرخ خطای کمتری را نسبت به سایر روشهای مشابه پیشین نیز دارا می باشد.

کلمات کلیدی:
فیشینگ، دزدی الکترونیکی، امنیت تجارت الکترونیک، ژورنال فیشینگ، مدل سازی حملات، مشخصه صفحات وب