عنوان مقاله:
مروری بر کاربرد رمزهای یک بار مصرف ترکیبی و حملات به ویژه فیشینگ

محل انتشار:
فصلنامه پژوهش در علوم رایانه, دوره 7, شماره 25 (سال: 1401)

تعداد صفحات اصل مقاله: 17

نویسنده:
سمیه نصیری - *فوق لیسانس مهندسی کامپیوتر گرایش نرم افزار، مدرس مدعو دانشگاه فرهنگیان پردیس الزهرا زنجان.*

خلاصه مقاله:
حملات فیشینگ گروهی از حملات هستند که امنیت کاربران و اطلاعات حیاتی آنها از جمله رمز عبور آنها را به خطر می اندازند و تاکنون راه حل های زیادی از جمله رمزهای یک بار مصرف برای جلوگیری از تهدیدات موجود ارائه شده است. علیرغم تلاش ها برای استفاده از رمزهای عبور یک بار مصرف برای جلوگیری از حملات فیشینگ، این هنوز یک چالش بزرگ است و تحقیقات بیشتری مورد نیاز است. بیشترین حمله برای جذب کاربران (با استفاده از تکنیک های مهندسی اجتماعی) به وب سایت های فیشینگ کاملا طراحی شده است که شبیه وب سایت های سازمان های هدف اصلی هستند تا با پر کردن برخی فرم ها، اطلاعات شخصی کاربران را دریافت کنند. فیشینگ، از جمله فیشینگ نیزه ای، به دلیل غیرقابل پیش بینی بودن، به یک مشکل جدی تبدیل شده است. این به نوبه خود به محققان و دست اندرکاران این امکان را می دهد تا راه حل هایی برای دفاع از آن یا حداقل آگاه ساختن کاربران از خطر این پدیده بیابند. کارایی روش پیشنهادی به صورت تحلیلی با استفاده از تعریف سناریو، مدل سازی و شبیه سازی محاسبه می شود و بر اساس معیار نرخ پیشگیری و همچنین ضریب پیچیدگی روش پیشنهادی اندازه گیری می شود که نشان دهنده بعید است که توسط مهاجمان حدس زده شود.

کلمات کلیدی:
فیشینگ، رمزیکبارمصرف.