

**ANALISIS KEAMANAN PLATFORM *E-COMMERCE* DI INDONESIA  
TERHADAP RISIKO SERANGAN *PASSWORD HARVESTING FISHING*  
(*PHISHING*) DENGAN METODE *ACTION RESEARCH*  
MENGUNAKAN APLIKASI *SOCIAL ENGINEERING TOOLKIT (SET)***

Oleh

**Made Ody Gita Permana, NIM 2115051043**

**Pendidikan Teknik Informatika**

**ABSTRAK**

Jumlah pengguna *Internet* dan *E-Commerce* di Indonesia terus mengalami perkembangan, namun perkembangan ini juga membawa berbagai macam tantangan, terutama dalam hal keamanan. Salah satu contohnya adalah ancaman serangan *social engineering* dengan teknik *phishing*. Penelitian ini bertujuan untuk menganalisis keamanan *platform e-commerce* di Indonesia terhadap serangan *phishing* menggunakan metode *Action Research* yang terdiri dari 5 tahapan. Tahap *diagnosis* dimulai dengan mengidentifikasi masalah melalui studi literatur dan penentuan objek penelitian menggunakan teknik *purposive sampling*. Pada tahap *planning*, dilakukan penyusunan rencana terkait tindakan yang akan diambil dalam melakukan pengujian, seperti pemilihan *tools* dan menentukan prosedur pengujian. Pada tahap *action*, akan dilakukan pengujian dengan menggunakan *Social Engineering Toolkit (SET)* untuk mengetahui potensi atau celah keamanan pada masing-masing *platform*. Tahap *evaluation* mencakup pengklasifikasian *e-commerce* berdasarkan beberapa indikator. Pada tahap *learning*, akan dilakukan penarikan kesimpulan dan rekomendasi dari hasil pengujian yang telah dilakukan. Dari 31 *platform* yang diuji, ditemukan sebanyak 22 *platform* memiliki tingkat keamanan rendah karena dapat direplikasi dengan mudah untuk melakukan serangan *phishing*. Sebaliknya, 9 *platform* menunjukkan tingkat keamanan tinggi, karena menerapkan metode *Step-Wise Authentication* dan *Embedded Login*, yang terbukti efektif melindungi *platform* dari serangan *phishing*. Tingkat efektivitas aplikasi *SET* dalam melakukan pengujian tercatat sebesar 70,9%. Persentase tersebut termasuk dalam kategori tinggi, sehingga dapat disimpulkan aplikasi *SET* efektif dalam melakukan pengujian keamanan *platform e-commerce* terhadap risiko serangan *phishing*. Penelitian ini juga mengidentifikasi bahwa sebagian besar *platform* dengan keamanan rendah masih menggunakan metode *Single-Page Login* atau *URL* khusus untuk login, sehingga sangat rentan terhadap serangan *phishing*. Hasil penelitian ini memberikan panduan penting bagi pemilik *platform* untuk meningkatkan mekanisme keamanan, serta bagi pengguna sebagai referensi untuk memilih *platform e-commerce* yang lebih aman.

Kata Kunci: Keamanan *E-Commerce*, *Phishing*, *Social Engineering*, *Action Research*, Metode Autentikasi

**SECURITY ANALYSIS OF E-COMMERCE PLATFORM IN INDONESIA  
AGAINST THE RISK OF PASSWORD HARVESTING FISHING  
(PHISHING) ATTACKS WITH ACTION RESEARCH METHODS USING  
SOCIAL ENGINEERING TOOLKIT (SET) APPLICATION**

**By**

**Made Ody Gita Permana, NIM 2115051043**

**Informatics Engineering Education**

**ABSTRACT**

*The number of Internet and E-Commerce users in Indonesia continues to grow, but this development also brings various challenges, especially in terms of security. One example is the threat of social engineering attacks with phishing techniques. This research aims to analyze the security of e-commerce platforms in Indonesia against phishing attacks using the Action Research method which consists of 5 stages. The diagnosis stage begins with identifying problems through literature studies and determining research objects using purposive sampling techniques. In the planning stage, plans are made regarding the actions to be taken in conducting tests, such as selecting tools and determining test procedures. At the action stage, testing will be carried out using the Social Engineering Toolkit (SET) to determine the potential or security holes on each platform. The evaluation stage includes classifying e-commerce based on several variables. In the learning stage, conclusions and recommendations will be drawn from the test results that have been carried out. Of the 31 platforms tested, it was found that 22 platforms have a low level of security because they can be replicated easily to carry out phishing attacks. In contrast, 9 platforms showed a high level of security, as they implemented the Step-Wise Authentication and Embedded Login methods, which proved effective in protecting the platform from phishing attacks. The effectiveness rate of the SET application in conducting tests was recorded at 70.9%. This percentage falls into the high category, so it can be said that the SET application is effective in testing the security of e-commerce platforms against the risk of phishing attacks. This study also identified that most low-security platforms still use the Single-Page Login method or a special URL for login, making them very vulnerable to phishing attacks. The results of this study provide important guidance for platform owners to improve security mechanisms, as well as for users as a reference for choosing a more secure e-commerce platform.*

*Keywords: E-Commerce Security, Phishing, Social Engineering, Action Research, Authentication Method.*