EVALUASI EFEKTIVITAS SIMULASI SERANGAN PHISHING TERHADAP KESADARAN KEAMANAN PENGGUNA MEDIA SOSIAL

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi *Teknik Komputer*

disusun oleh
HADAR SAMUDERA
22.83.0914

Kepada

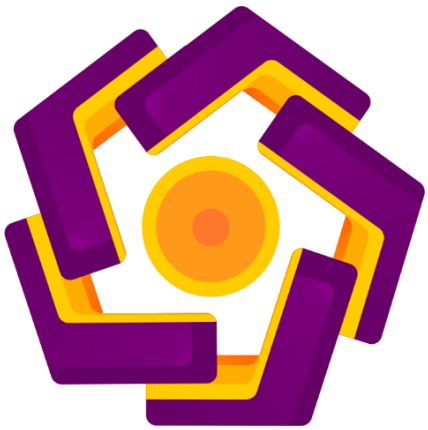
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2026

EVALUASI EFEKTIVITAS SIMULASI SERANGAN PHISHING TERHADAP KESADARAN KEAMANAN PENGGUNA MEDIA SOSIAL

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi *Teknik Komputer*



disusun oleh

HADAR SAMUDERA

22.83.0914

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2026

HALAMAN PERSETUJUAN

SKRIPSI

EVALUASI EFEKTIVITAS SIMULASI SERANGAN PHISING TERHADAP KESADARAN KEMANAN PENGGUNA MEDIA SOSIAL

yang disusun dan diajukan oleh

Hadar Samudera
22.83.0914

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 20 Januari 2026

Dosen Pembimbing,

Melwin Syafrizal, S.Kom., M.Eng., Ph.D.
NIK. 190302105

HALAMAN PENGESAHAN

SKRIPSI

EVALUASI EFEKTIVITAS SIMULASI SERANGAN PHISING TERHADAP KESADARAN KEMANAN PENGGUNA MEDIA SOSIAL

yang disusun dan diajukan oleh

Hadar Samudera
22.83.0914
Telah dipertahankan di depan Dewan Penguji
pada tanggal selasa, 20 Januari 2026

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Eko Pramono, S.Si, M.T. **NIK. 190302580**	
Wahid Miftahul Ashari, S.Kom., M.T. **NIK. 190302452**	
Melwin Syafrizal, S.Kom., M.Eng., Ph.D. **NIK. 190302105**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Januari 2026

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Hadar Samudera
NIM : 22.83.0914

Menyatakan bahwa Skripsi dengan judul berikut:

Evaluasi Efektivitas Simulasi Serangan Phising Terhadap Kesadaran Keamanan Pengguna Media Sosial

Dosen Pembimbing : Melwin Syafrizal, S.Kom., M.Eng., Ph.D.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 20 Januari 2026

Yang Menyatakan,

Hadar Samudera

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

INTISARI

Peningkatan penggunaan media sosial di kalangan usia muda diikuti dengan maraknya serangan phishing yang memanfaatkan rekayasa sosial untuk mencuri informasi sensitif pengguna. Kondisi ini menimbulkan risiko kebocoran data, pengambilalihan akun, dan kerugian lain karena banyak pengguna belum memiliki kesadaran keamanan siber yang memadai, seperti kebiasaan memeriksa URL maupun kewaspadaan terhadap tautan dan halaman login palsu. Penelitian ini bertujuan merancang dan mengevaluasi simulasi serangan phishing sebagai upaya edukasi untuk meningkatkan kesadaran keamanan pengguna media sosial. Metode yang digunakan berupa eksperimen semu dengan desain pre-test dan post-test terhadap responden pengguna aktif media sosial berusia 18–25 tahun. Responden terlebih dahulu mengisi kuesioner untuk mengukur tingkat kesadaran awal, kemudian mengikuti simulasi serangan phishing menggunakan SEToolkit dalam lingkungan terkontrol, disertai sesi edukasi singkat mengenai ciri-ciri phishing dan praktik aman di media sosial, selanjutnya simulasi serangan phishing menggunakan Zphisher, lalu mengisi kembali kuesioner untuk melihat perubahan tingkat kesadaran. Hasil pengukuran tingkat kesadaran keamanan siber menunjukan adanya peningkatan skor rata-rata responden antara pre-test dan post-test setelah diberikan edukasi tentang ciri-ciri phishing, praktik aman di media sosial, serta simulasi serangan phishing. Penelitian ini diharapkan dapat memberikan gambaran rancangan simulasi yang sistematis sebagai model pelatihan keamanan siber berbasis pengalaman langsung, sekaligus menjadi dasar bagi pengembangan program peningkatan kesadaran keamanan siber pada pengguna media sosial di lingkungan pendidikan maupun organisasi.

Kata kunci : phishing, SEToolkit, media sosial, Zphisher.

ABSTRACT

The rapid growth of social media use among young people has been followed by an increase in phishing attacks that exploit social engineering techniques to steal users' sensitive information. This situation creates risks of data breaches, account takeovers, and other losses because many users still lack adequate cybersecurity awareness, such as the habit of checking URLs and being cautious toward suspicious links and fake login pages. This study aims to design and evaluate a phishing attack simulation as an educational effort to improve the security awareness of social media users. The method used is a quasi-experimental design with pre-test and post-test involving active social media users aged 18–25 years. Respondents first completed a questionnaire to measure their initial level of awareness, then participated in a phishing attack simulation using SEToolkit in a controlled environment, accompanied by a brief educational session on phishing characteristics and safe practices on social media, followed by a phishing attack simulation using Zphisher, and finally completed the questionnaire again to observe changes in their awareness level. This study is expected to provide a structured simulation design as a cybersecurity training model based on direct experience, as well as a basis for developing security awareness programs for social media users in educational institutions and organizations.

***Keyword** : phishing, SEToolkit, social media, Zphisher*