

Optimalisasi Kesadaran Keamanan Digital Untuk Mencegah Praktik Social Engineering Di Media Sosial Pada Ormas Oi Tangerang Selatan

Gigih Amrillah Ibnurhus¹, Syaeful Machfud², Okky Prasetya³

^{1,2,3}Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pamulang, Kota Tangerang Selatan, Indonesia

Email: : ¹*dosen02838@unpam.ac.id, ²dosen202836@unpam.ac.id, ³dosen02837@unpam.ac.id

(* : coresponding author)

Abstrak - Transformasi digital yang pesat mendorong organisasi kemasyarakatan (ormas), termasuk Ormas Oi, memanfaatkan media sosial secara intensif tanpa diimbangi literasi keamanan digital yang memadai, sehingga membuka celah bagi praktik social engineering yang mengeksploitasi kerentanan psikologis manusia. Penelitian ini bertujuan mengukur tingkat kesadaran keamanan digital anggota Ormas Oi Tangerang Selatan sebelum dan sesudah intervensi edukasi, serta menganalisis signifikansi perbedaannya sebagai indikator efektivitas pencegahan social engineering di media sosial. Penelitian menggunakan pendekatan kuantitatif dengan desain quasi-experimental one-group pretest-posttest terhadap 25 anggota aktif yang dipilih secara purposive sampling, dengan data dianalisis menggunakan paired sample t-test. Hasil menunjukkan skor edukasi keamanan digital meningkat dari rata-rata 10,76 menjadi 16,32, dan kesadaran pencegahan social engineering meningkat dari 16,12 menjadi 23,96, dengan nilai signifikansi $p < 0,05$ dan effect size sangat besar, namun N-Gain didominasi kategori sedang. Temuan ini membuktikan edukasi terstruktur efektif mengubah pola kognitif anggota dari kepercayaan sosial pasif menjadi kewaspadaan reflektif sebagai human firewall. Disimpulkan bahwa intervensi edukasi berdampak signifikan, namun perlu dilakukan secara berkelanjutan dengan simulasi kasus nyata, serta penelitian lanjutan disarankan menggunakan kelompok kontrol dan pengukuran longitudinal.

Kata Kunci: Edukasi Digital, Kesadaran Keamanan, Media Sosial, Ormas Oi, Social Engineering

Abstract - Oi, to intensively utilize social media without adequate digital security literacy, creating vulnerabilities exploited through social engineering that targets human psychological weaknesses. This study aims to measure the level of digital security awareness among members of Ormas Oi South Tangerang before and after an educational intervention, and to analyze the significance of the difference as an indicator of the effectiveness of preventing social engineering practices on social media. This research employed a quantitative approach with a quasi-experimental one-group pretest-posttest design involving 25 active members selected through purposive sampling, with data analyzed using a paired sample t-test. Results showed that digital security education scores increased from an average of 10.76 to 16.32, and social engineering prevention awareness increased from 16.12 to 23.96, with a significance value of $p < 0.05$ and a very large effect size, although N-Gain scores were predominantly in the moderate category. These findings confirm that structured education effectively shifted members' cognitive patterns from passive social trust toward reflective vigilance as a human firewall. It is concluded that the educational intervention had a significant impact, though it should be conducted continuously with real-case simulations, and future research is recommended to employ control groups and longitudinal measurements.

Keywords: Digital Education, Digital Security Awareness, Ormas Oi, Social Engineering, Social Media

1. PENDAHULUAN

Transformasi digital yang berlangsung pesat di Indonesia telah mengubah pola interaksi sosial masyarakat, termasuk organisasi kemasyarakatan (ormas), yang kini banyak memanfaatkan media sosial sebagai sarana komunikasi, konsolidasi anggota, dan penyebaran informasi organisasi. Namun, intensitas penggunaan media sosial yang tinggi ini tidak diimbangi dengan tingkat literasi keamanan digital yang memadai, sehingga membuka celah bagi praktik *social engineering*, yaitu manipulasi psikologis yang mengeksploitasi kelemahan manusia seperti rasa percaya, rasa takut, dan keinginan menolong untuk memperoleh akses maupun informasi rahasia secara tidak sah (Tyas Darmaningrat et al., 2022). Temuan empiris menunjukkan bahwa *social engineering* merupakan ancaman siber yang paling sulit ditangani karena tidak menasar celah teknis sistem, melainkan sisi kerentanan manusia sebagai elemen terlemah dalam rantai keamanan informasi (Chetioui et al., 2021). Penelitian yang dilakukan pada 508 pegawai di berbagai organisasi juga membuktikan bahwa tingkat kesadaran terhadap taktik *social engineering* masih tergolong rendah, sehingga intervensi

berupa edukasi dan pelatihan terstruktur terbukti mampu meningkatkan kewaspadaan secara signifikan (Almutairi & Alghamdi, 2022).

Meskipun kajian mengenai *social engineering* telah banyak dilakukan pada konteks perusahaan, institusi perbankan, dan lembaga pendidikan, penelitian yang secara khusus menyoroti organisasi kemasyarakatan berbasis komunitas seperti Ormas Oi masih sangat terbatas. Kesenjangan (*gap*) ini semakin relevan mengingat karakteristik anggota ormas yang heterogen dari sisi usia, latar belakang pendidikan, dan tingkat literasi digital, sehingga pendekatan intervensi generik belum tentu efektif diterapkan pada kelompok tersebut (Huwaidi & Destya, 2022). Kebaruan (*novelty*) dari penelitian ini terletak pada penerapan desain *quasi-experimental* dengan model *one-group pretest-posttest* untuk mengukur secara terukur efektivitas program optimalisasi kesadaran keamanan digital sebagai upaya preventif terhadap praktik *social engineering* di media sosial, khususnya pada komunitas Ormas Oi Tangerang Selatan yang belum pernah menjadi subjek kajian serupa sebelumnya.

Berdasarkan uraian tersebut, rumusan masalah penelitian ini adalah bagaimana tingkat kesadaran keamanan digital anggota Ormas Oi Tangerang Selatan sebelum dan sesudah diberikan intervensi edukasi, serta apakah terdapat perbedaan signifikan pada tingkat kesadaran tersebut sebagai indikator efektivitas pencegahan praktik *social engineering* di media sosial. Tujuan penelitian ini adalah untuk mengukur tingkat kesadaran keamanan digital anggota Ormas Oi Tangerang Selatan sebelum dan sesudah intervensi, serta menganalisis signifikansi perbedaan hasil *pretest* dan *posttest* guna menilai efektivitas program edukasi dalam mencegah praktik *social engineering* di media sosial. Manfaat penelitian ini terbagi menjadi manfaat teoretis dan praktis. Secara teoretis, penelitian ini diharapkan memperkaya literatur keilmuan komunikasi dan keamanan siber, khususnya terkait efektivitas intervensi edukatif pada komunitas non-formal. Secara praktis, hasil penelitian dapat menjadi acuan bagi pengurus Ormas Oi dan pemangku kepentingan terkait dalam merancang program literasi keamanan digital yang lebih tepat sasaran guna melindungi anggota dari ancaman rekayasa sosial di ranah media sosial.

2. METODE

2.1 Jenis dan Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan desain *quasi-experimental*, khususnya model *one-group pretest-posttest design*. Desain ini dipilih karena mampu mengukur perubahan variabel terikat melalui perbandingan hasil pengukuran sebelum (*pretest*) dan sesudah (*posttest*) pemberian perlakuan berupa edukasi kesadaran keamanan digital, tanpa melibatkan kelompok kontrol pembandingan (Hananto & Melini, 2023). Pendekatan ini relevan digunakan pada penelitian intervensi berskala kecil yang bertujuan menilai efektivitas suatu program edukatif secara terukur dan sistematis (Wang, 2026).

2.2 Populasi, Sampel, dan Teknik Sampling

Populasi penelitian ini adalah seluruh anggota aktif Ormas Oi wilayah Tangerang Selatan. Mengingat keterbatasan sumber daya dan karakteristik desain eksperimen semu berskala kecil, penelitian ini menetapkan sampel sebanyak 20 hingga 30 responden yang dipilih menggunakan teknik *purposive sampling*, dengan kriteria anggota aktif berusia minimal 17 tahun dan memiliki serta menggunakan minimal satu akun media sosial secara rutin. Jumlah sampel tersebut dianggap memadai untuk desain *one-group pretest-posttest* pada penelitian eksperimen semu berskala terbatas, karena penekanan utama terletak pada kedalaman intervensi dan ketepatan pengukuran perubahan, bukan pada generalisasi populasi besar.

2.3 Definisi Operasional Variabel

Variabel penelitian terdiri atas variabel bebas, yaitu program edukasi kesadaran keamanan digital, dan variabel terikat, yaitu tingkat kesadaran anggota dalam mencegah praktik *social engineering* di media sosial. Definisi operasional disusun agar setiap variabel dapat diukur secara konsisten melalui instrumen kuesioner berskala *Likert*.

Tabel 1. Definisi Operasional Variabel

Variabel	Definisi Operasional	Indikator	Skala
Edukasi Kesadaran Keamanan Digital (X)	Intervensi berupa sosialisasi dan pelatihan yang diberikan kepada anggota Ormas Oi untuk meningkatkan pemahaman terhadap ancaman siber	Pemahaman konsep keamanan digital, pengenalan modus phishing dan social engineering	Ordinal (Likert 1–5)
Kesadaran Pencegahan Social Engineering (Y)	Kemampuan anggota mengenali, menghindari, dan merespons secara tepat upaya manipulasi psikologis di media sosial	Kewaspadaan terhadap tautan mencurigakan, verifikasi identitas pengirim pesan, perlindungan data pribadi	Ordinal (Likert 1–5)

2.4 Teknik Pengumpulan Data dan Analisis Data

Pengumpulan data dilakukan melalui kuesioner tertutup berskala *Likert* yang disebarkan sebanyak dua kali, yaitu sebelum dan sesudah pemberian perlakuan edukasi. Sebelum digunakan, instrumen terlebih dahulu diuji validitas dan reliabilitasnya untuk memastikan ketepatan alat ukur. Data hasil *pretest* dan *posttest* selanjutnya dianalisis menggunakan uji normalitas sebagai prasyarat, dilanjutkan dengan uji beda berpasangan, yaitu *paired sample t-test* apabila data berdistribusi normal, atau uji *Wilcoxon signed-rank* apabila data tidak berdistribusi normal, guna menentukan signifikansi perubahan tingkat kesadaran keamanan digital anggota Ormas Oi Tangerang Selatan.

3. HASIL & PEMBAHASAN

3.1 Hasil

3.1.1 Gambaran Umum Responden

Responden penelitian berjumlah 25 anggota aktif Ormas Oi Tangerang Selatan yang dipilih secara purposive. Dari sisi usia, responden berkisar antara 17 hingga 41 tahun dengan rata-rata 27,1 tahun, didominasi kelompok usia 21-25 tahun (7 orang) dan 26-30 tahun (6 orang). Berdasarkan jenis kelamin, responden laki-laki lebih banyak (16 orang, 64%) dibanding perempuan (9 orang, 36%). Tingkat pendidikan terakhir didominasi jenjang S1 (14 orang), diikuti SMA/SMK (8 orang), D3 (2 orang), dan S2 (1 orang). Rata-rata lama penggunaan media sosial adalah 4,8 tahun, dengan platform utama yang paling banyak digunakan adalah WhatsApp (8 orang) dan Facebook (7 orang).

Tabel 2. Karakteristik Responden

Karakteristik	Kategori	Jumlah	Persentase
Jenis Kelamin	Laki-laki	16	64%
	Perempuan	9	36%
Pendidikan	SMA/SMK	8	32%
	D3	2	8%
	S1	14	56%
	S2	1	4%
Platform Utama	WhatsApp	8	32%
	Facebook	7	28%

	Instagram	4	16%
	Twitter/X	4	16%
	TikTok	2	8%

3.1.2 Deskripsi Skor Pretest dan Posttest

Hasil pengolahan menunjukkan peningkatan pada kedua variabel setelah intervensi edukasi diberikan. Skor variabel Edukasi Kesadaran Keamanan Digital (X) meningkat dari rata-rata 10,76 (SD 2,35) menjadi 16,32 (SD 2,27), sedangkan skor Kesadaran Pencegahan Social Engineering (Y) meningkat dari rata-rata 16,12 (SD 3,69) menjadi 23,96 (SD 4,00).

Tabel 3. Statistik Deskriptif Skor Pretest-Posttest

Variabel	Rata-rata Pretest	Rata-rata Posttest	Selisih (Gain)	N-Gain
X (Edukasi Keamanan Digital)	10,76	16,32	5,56	0,62 (Sedang)
Y (Kesadaran Pencegahan SE)	16,12	23,96	7,84	0,59 (Sedang)

Berdasarkan kategorisasi N-Gain, sebagian besar responden berada pada kategori peningkatan sedang, yaitu 15 orang untuk variabel X dan 14 orang untuk variabel Y, sementara 10 responden pada variabel X dan 9 responden pada variabel Y mencapai kategori tinggi. Hanya 2 responden pada variabel Y yang tergolong kategori rendah, konsisten dengan skor awal yang sudah relatif tinggi sebelum intervensi sehingga ruang peningkatannya lebih terbatas.

3.1.3 Uji Normalitas dan Uji Beda Berpasangan

Uji normalitas Shapiro-Wilk terhadap selisih skor (gain) menunjukkan data berdistribusi normal, dengan nilai signifikansi variabel X sebesar 0,144 dan variabel Y sebesar 0,651 (keduanya lebih besar dari 0,05). Oleh karena itu, uji beda yang digunakan adalah paired sample t-test.

Tabel 4. Hasil Uji Paired Sample T-Test

Variabel	Nilai t	df	Sig. (2-tailed)	Keterangan
X (Edukasi Keamanan Digital)	18,51	24	0,000	Signifikan
Y (Kesadaran Pencegahan SE)	15,31	24	0,000	Signifikan

Hasil uji menunjukkan nilai signifikansi kedua variabel jauh di bawah 0,05, sehingga hipotesis nol ditolak dan terdapat perbedaan yang signifikan antara skor pretest dan posttest. Besaran effect size (Cohen's d) untuk variabel X sebesar 3,70 dan variabel Y sebesar 3,06, keduanya tergolong sangat besar, menunjukkan bahwa perubahan yang terjadi bukan sekadar signifikan secara statistik tetapi juga berdampak praktis yang substansial. Temuan ini menjawab rumusan masalah bahwa kesadaran keamanan digital anggota Ormas Oi meningkat nyata setelah intervensi, sekaligus membuktikan efektivitas program edukasi sebagai upaya preventif terhadap praktik social engineering di media sosial, sejalan dengan tujuan penelitian.

3.2 Pembahasan

Kenaikan skor yang konsisten pada seluruh indikator variabel X maupun Y tidak sekadar mencerminkan pertambahan angka statistik, melainkan menandakan pergeseran pola kognitif

anggota Ormas Oi dari kondisi *awareness* yang bersifat pasif menuju kesiapsiagaan yang lebih reflektif terhadap manipulasi psikologis di ranah digital. Rendahnya skor pretest, khususnya pada indikator verifikasi identitas pengirim pesan, mengindikasikan bahwa sebelum intervensi, anggota cenderung mengandalkan rasa percaya sosial sebagai dasar interaksi daring, sebuah kerentanan yang justru menjadi celah utama yang dieksploitasi pelaku *social engineering* karena serangan jenis ini menasar sisi psikologis manusia, bukan celah teknis sistem (Tsauri, 2025). Lonjakan skor posttest yang signifikan secara statistik memperkuat argumen bahwa edukasi terstruktur mampu mengubah pola pikir tersebut menjadi lebih kritis, sejalan dengan temuan bahwa program penguatan kesadaran memberi dampak nyata pada kemampuan mengenali indikasi manipulasi meskipun materi disampaikan dalam durasi terbatas (Alsulami et al., 2021).

Besaran *effect size* yang sangat tinggi pada kedua variabel menunjukkan bahwa efektivitas intervensi ini bukan sekadar signifikan secara uji statistik, tetapi juga bermakna secara substansial dalam konteks praktik pencegahan. Temuan ini relevan dengan gagasan bahwa peningkatan kesadaran keamanan tidak cukup diukur dari sisi pengetahuan semata, melainkan harus disertai perubahan sikap kewaspadaan yang berkelanjutan agar anggota mampu berperan sebagai *human firewall* dalam ekosistem komunikasi digital komunitasnya (Cletus et al., 2022). Namun demikian, kategori N-Gain yang didominasi tingkat sedang mengisyaratkan bahwa satu kali intervensi belum cukup membentuk kebiasaan keamanan yang otomatis, melainkan baru pada tahap pembentukan fondasi kognitif, sebagaimana ditegaskan bahwa efektivitas pelatihan keamanan siber sangat bergantung pada keberlanjutan dan pengulangan materi, bukan hanya pada intensitas satu sesi edukasi (Chetoui et al., 2021). Kondisi ini juga sejalan dengan pola pada kelompok usia muda dan pengguna nonformal lain, yang menunjukkan bahwa edukasi tunggal mampu mendongkrak pemahaman dasar secara tajam, tetapi penguatan berkelanjutan tetap diperlukan agar kewaspadaan tersebut tidak menurun seiring waktu (Agung, 2025). Dengan demikian, dapat disimpulkan bahwa intervensi edukasi terbukti efektif menjawab rumusan masalah penelitian, yakni mendorong perbedaan signifikan pada kesadaran keamanan digital anggota Ormas Oi sebagai langkah preventif terhadap praktik *social engineering* di media sosial, meski keberlanjutannya tetap menjadi variabel penentu jangka panjang.

4. KESIMPULAN

Penelitian ini membuktikan bahwa edukasi keamanan digital secara signifikan meningkatkan kesadaran pencegahan *social engineering* anggota Ormas Oi Tangerang Selatan, dibuktikan hasil *paired sample t-test* ($p < 0,05$) dengan *effect size* besar serta N-Gain kategori sedang-tinggi. Temuan ini mengimplikasikan bahwa edukasi mampu mengubah pola kognitif dari kepercayaan sosial pasif menjadi kewaspadaan reflektif, menjadikan anggota berperan sebagai *human firewall*. Namun, penelitian ini memiliki limitasi berupa sampel kecil (25 responden), desain *one-group pretest-posttest* tanpa kelompok kontrol, serta pengukuran jangka pendek yang belum menggambarkan keberlanjutan efek secara *longitudinal*. Berdasarkan temuan tersebut, disarankan agar Ormas Oi dan organisasi sejenis menyelenggarakan edukasi keamanan digital secara berkelanjutan dan berkala, bukan hanya sekali, guna memperkuat retensi pengetahuan dan membentuk kebiasaan waspada yang otomatis dalam menghadapi *social engineering*. Materi edukasi sebaiknya diperkaya dengan simulasi kasus nyata dan praktik verifikasi identitas pengirim pesan. Bagi penelitian selanjutnya, disarankan menggunakan desain *quasi-experimental* dengan kelompok kontrol, jumlah sampel lebih besar dan representatif, serta pengukuran *longitudinal* untuk menguji keberlanjutan efek edukasi dalam jangka panjang secara lebih *robust*.

DAFTAR PUSTAKA

- Agung, H. (2025). Efektivitas Edukasi Cybersecurity dalam Meningkatkan Pengetahuan Siswa tentang Ancaman Digital pada Siswa Menengah Atas. *Jurnal Ilmu Komputer (JUIK)*, 5(2), 104. <https://doi.org/10.31314/juik.v5i2.4436>
- Almutairi, B. S., & Alghamdi, A. (2022). The Role of Social Engineering in Cybersecurity and Its Impact. *Journal of Information Security*, 13(04), 363–379. <https://doi.org/10.4236/jis.2022.134020>
- Alsulami, M. H., Alharbi, F. D., Almutairi, H. M., Almutairi, B. S., Alotaibi, M. M., Alanzi, M. E., Alotaibi, K. G., & Alharthi, S. S. (2021). Measuring awareness of social engineering in the educational sector in

- the kingdom of saudi arabia. *Information (Switzerland)*, 12(5), 1–13. <https://doi.org/10.3390/info12050208>
- Chetoui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2021). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, 198(2021), 656–661. <https://doi.org/10.1016/j.procs.2021.12.302>
- Cletus, A., Weyory, B., & Opoku, A. (2022). Improving social engineering awareness, training and education (SEATE) using a behavioral change model. *International Journal of Advanced Computer Science and Applications*, 13(5).
- Hananto, B. A., & Melini, E. (2023). Mengukur Tingkat Pemahaman Pelatihan Desain Karakter dengan Quasi-Experiment One Group Pretest-Posttest. *Jurnal Titik Imaji*, 6(2), 91–97. <http://journal.ubm.ac.id/index.php/titik-imaji/>
- Huwaiti, M. Z., & Destya, S. (2022). Mencegah serangan rekayasa sosial dengan human firewall. *JUSTIN (Jurnal Sistem Dan Teknologi Informasi)*, 10(1), 107–112.
- Tsauri, M. S. (2025). Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall. *Journal of Applied Informatics and Computing*, 9(4), 1127–1136. <https://doi.org/10.30871/jaic.v9i4.9585>
- Tyas Darmaningrat, E. W., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. *Sewagati*, 6(2). <https://doi.org/10.12962/j26139960.v6i2.92>
- Wang, Y. (2026). *Effects of Game-Based Learning on Piano Music Knowledge Among Elementary School Pupils: Pretest-Posttest Quasi-Experimental Study*. 14, 1–14. <https://doi.org/10.2196/80766>