TeknoIS: Jurnal Ilmiah Teknologi Informasi dan Sains
Volume 16 Number 2, July 2026 Page. 187-193
Journal Homepage: https://teknois.unbin.ac.id/index.php/JBS/
Received: June 2026; Accepted: July 2026; Published: July 2026

Strategi Mitigasi Terhadap Ancaman *Malware Social Engineering* pada Perangkat *Mobile*

Laksmi Kartika Santhi[1*], Indriyani[2]
[1,2]Program Studi Teknologi Informasi, Institut Teknologi dan Bisnis STIKOM Bali
[1]Email: laksmi230040159@gmail.com
[2]Email: indriyani@stikom-bali.ac.id

*) *Corresponding Author*

ABSTRACT

This research explores the growing threat of malware that exploits social engineering techniques on mobile devices. The objective of this study is to formulate an effective mitigation strategy for users to combat psychological manipulation. This study employs a Systematic Literature Review (SLR) method, analyzing academic publications from the last ten years. The findings reveal that human factors remain the weakest link in cybersecurity. Therefore, reliance on technical defenses alone is insufficient. This study proposes a human-centric defense framework that integrates technical approaches, such as Endpoint Detection and Response (EDR), with intensive digital behavioral interventions, specifically real-time security nudging. This hybrid strategy bridges the gap between system security and user awareness, offering a more resilient defense against modern, AI driven social engineering attacks.

Keywords*: Malware, Social Engineering, Mobile Security, Mitigation.*

ABSTRAK

Penelitian ini menguraikan masalah mengenai ancaman malware yang memanfaatkan teknik rekayasa sosial (*social engineering*) pada perangkat *mobile*. Tujuan penelitian ini adalah untuk merumuskan strategi mitigasi yang efektif bagi pengguna dalam menghadapi manipulasi psikologis. Metode yang digunakan adalah studi literatur sistematis terhadap publikasi institusi akademik dalam sepuluh tahun terakhir. Hasil penelitian menunjukkan bahwa faktor manusia tetap menjadi rantai terlemah dalam keamanan siber, sehingga pendekatan teknis harus dikombinasikan dengan edukasi perilaku digital yang intensif.

Kata Kunci*: Malware*, Rekayasa Sosial, Keamanan Mobile, Mitigasi Siber.

A. PENDAHULUAN

Transformasi digital telah menempatkan perangkat seluler sebagai repositori utama data kredensial dan finansial [1]. Namun, peningkatan fungsi ini tidak berbanding lurus dengan tingkat literasi keamanan penggunanya [2]. Permasalahan utama yang muncul adalah kerentanan terhadap malware yang didistribusikan melalui rekayasa sosial (*social engineering*) [3]. Berbeda dengan serangan teknis murni, metode ini mengeksploitasi aspek psikologis manusia seperti rasa takut atau penasaran untuk mengelabui pengguna agar mengabaikan sistem pertahanan perangkat [4]. Hal ini menciptakan celah keamanan yang sulit dideteksi oleh perangkat lunak keamanan standar karena serangan diawali dengan persetujuan sadar dari pengguna yang termanipulasi[5].

Wawasan dalam penelitian ini memandang bahwa perlindungan siber tidak lagi cukup hanya dengan mengandalkan sistem teknis (*hardware/software*). Dibutuhkan pendekatan dua arah yang mencakup penguatan sisi teknis dan optimalisasi perilaku pengguna [6]. Rencana pemecahan masalah yang diusulkan adalah pengembangan strategi mitigasi berlapis (*defense-in-depth*) [7]. Hal ini meliputi implementasi teknologi deteksi dini berbasis perilaku aplikasi serta program edukasi

literasi digital secara kontinu untuk membangun pertahanan psikologis pengguna terhadap berbagai modus penipuan siber [8].

Kebaruan (*novelty*) dari penelitian ini terletak pada pengintegrasian strategi mitigasi yang tidak hanya bersifat statis-edukatif, tetapi juga adaptif terhadap evolusi ancaman terkini seperti rekayasa sosial berbasis kecerdasan buatan (*Generative AI*) [9]. Di saat penelitian sebelumnya banyak berfokus pada pelatihan kesadaran pasif, penelitian ini menawarkan kerangka kerja intervensi waktu-nyata (*real-time security nudging*) yang dirancang untuk menjembatani celah antara pengetahuan teoretis pengguna dan tindakan praktis saat menghadapi serangan yang bersifat persuasif dan otomatis [10].

Berdasarkan identifikasi masalah tersebut, penelitian ini bertujuan untuk menganalisis mekanisme manipulasi psikologis dalam penyebaran *malware* pada perangkat *mobile* [11], merumuskan kerangka strategi mitigasi yang menggabungkan solusi teknis dengan penguatan aspek perilaku pengguna, serta memberikan rekomendasi praktis bagi pengguna dalam mendeteksi dan menghindari ancaman rekayasa sosial di ekosistem digital.

Kajian teoritik dalam penelitian ini berpijak pada prinsip dasar keamanan informasi yang dikenal sebagai CIA Triad (*Confidentiality, Integrity, Availability*) [7]. **Clark** [12] menyatakan bahwa serangan rekayasa sosial secara langsung mengancam kerahasiaan dan integritas data melalui manipulasi informasi. Selain itu, landasan teori mengenai perilaku keamanan siber dari **Mitnick** [5] mempertegas bahwa manusia seringkali menjadi "titik terlemah" dalam rantai keamanan. Oleh karena itu, teori *protection motivation* diterapkan untuk memahami sejauh mana kesadaran akan ancaman dapat mempengaruhi tindakan preventif pengguna perangkat seluler [13].

B. METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif melalui metode Systematic Literature Review (SLR). Pendekatan ini dipilih karena mampu memberikan pemahaman yang komprehensif terhadap fenomena ancaman malware yang tidak hanya bersifat teknis, tetapi juga melibatkan dimensi psikologis pengguna sebagai target utama serangan [11], [4]. Kajian awal terhadap literatur menunjukkan adanya kecenderungan penelitian sebelumnya yang lebih menitikberatkan pada pengembangan mekanisme deteksi malware berbasis sistem, seperti analisis perilaku aplikasi dan pemanfaatan algoritma komputasi cerdas [14]. Di sisi lain, studi mengenai rekayasa sosial umumnya berfokus pada pola serangan dan teknik manipulasi [4], tanpa diikuti dengan formulasi strategi mitigasi yang aplikatif bagi pengguna perangkat mobile. Kondisi ini menunjukkan adanya kesenjangan antara pendekatan teknis dan pendekatan perilaku dalam penelitian keamanan siber. Oleh karena itu, penelitian ini menghadirkan kebaruan dalam bentuk perumusan strategi mitigasi terpadu yang mengombinasikan kedua pendekatan tersebut dalam kerangka defense-in-depth berbasis human-centric security [10], sehingga mampu memperkuat perlindungan tidak hanya pada sistem, tetapi juga pada pengguna sebagai titik kritis dalam rantai keamanan [5].

Tabel 1. Kriteria Inklusi dan Eksklusi Seleksi Literatur

Kriteria	Parameter Inklusi	Parameter Eksklusi
Rentang Waktu	Publikasi 10 tahun terakhir (2014 - 2024)	Publikasi sebelum tahun 2014
Fokus Kajian	Malware mobile, social engineering, literasi digital, real-time nudging	Serangan siber murni pada hardware PC/Server tanpa unsur psikologis
Jenis Sumber	Jurnal akademik peer-reviewed, laporan industri kredibel (NIST, ENISA, Kaspersky)	Artikel opini, blog tidak resmi, laporan tanpa validasi metodologis

Data yang digunakan dalam penelitian ini merupakan data sekunder yang diperoleh dari berbagai sumber ilmiah yang kredibel, seperti jurnal internasional terindeks, publikasi lembaga keamanan

siber [3], [1], serta buku referensi yang relevan dengan topik malware dan rekayasa sosial [11]. Literatur yang dikaji dibatasi pada publikasi dalam kurun waktu sepuluh tahun terakhir agar tetap mencerminkan perkembangan terkini dalam ancaman dan strategi mitigasi keamanan mobile. Proses seleksi dilakukan secara ketat dengan mempertimbangkan relevansi topik, kejelasan metodologi, serta kontribusi terhadap pembahasan mengenai interaksi antara malware, social engineering, dan perilaku pengguna. Pengumpulan data dilakukan melalui tahapan systematic literature review yang mengacu pada prosedur yang dikemukakan oleh **Kitchenham** (2004) [15]. Tahapan ini dimulai dari penentuan kata kunci yang sesuai dengan fokus penelitian, dilanjutkan dengan penelusuran literatur pada berbagai basis data akademik, kemudian dilakukan proses penyaringan berdasarkan kesesuaian isi dan kualitas penelitian. Literatur yang terpilih selanjutnya dianalisis secara mendalam untuk mengekstraksi informasi terkait karakteristik malware mobile [8], [1], teknik rekayasa sosial yang digunakan [9], serta bentuk mitigasi yang telah diusulkan dalam berbagai studi sebelumnya [6].

Tabel 2. Ringkasan Literatur Utama

Penulis (Tahun)	Fokus Penelitian	Kontribusi Terhadap Penelitian Ini
Park & Kim (2024) [10]	Real-time behavioral nudging	Landasan konsep intervensi waktu-nyata untuk pengguna perangkat mobile.
Jones & Ahmad (2024) [9]	AI-driven social engineering	Identifikasi tren evolusi serangan yang semakin terotomatisasi.
Souri & Hosseini (2018) [14]	Malware detection via data mining	Dasar pendekatan teknis dan analisis perilaku aplikasi pada sistem.
Hadnagy (2018) [4]	Sains rekayasa sosial	Kerangka teori mengenai taktik psikologis (human hacking).

Analisis data dalam penelitian ini dilakukan menggunakan pendekatan analisis tematik. Melalui proses ini, data yang telah dikumpulkan diidentifikasi, diklasifikasikan, dan diinterpretasikan untuk menemukan pola-pola utama yang berkaitan dengan kerentanan pengguna serta strategi mitigasi yang efektif. Hasil analisis kemudian disintesiskan untuk membangun suatu kerangka strategi mitigasi yang bersifat terpadu, yang mengintegrasikan aspek teknis seperti deteksi perilaku aplikasi dengan aspek non-teknis berupa peningkatan kesadaran dan literasi keamanan pengguna [2]. Untuk memperkuat landasan teoritis, hasil sintesis tersebut juga dikaitkan dengan prinsip dasar keamanan informasi seperti CIA Triad [7] serta teori *Protection Motivation* yang menjelaskan hubungan antara persepsi ancaman dan perilaku preventif pengguna [13]. Secara keseluruhan, proses penelitian ini dilakukan secara sistematis mulai dari identifikasi permasalahan, pengumpulan dan seleksi literatur, analisis tematik, hingga penyusunan kerangka strategi mitigasi yang diusulkan. Pendekatan ini diharapkan mampu menghasilkan kontribusi ilmiah yang tidak hanya bersifat konseptual, tetapi juga memberikan implikasi praktis dalam meningkatkan ketahanan pengguna perangkat mobile terhadap ancaman malware berbasis rekayasa sosial.

C. HASIL DAN PEMBAHASAN

1. HASIL

1) Pola Utama Serangan Social Engineering pada Mobile

Ekstraksi literatur menunjukkan tiga pola utama yang paling dominan digunakan dalam menyebarkan malware ke perangkat pengguna mobile pada era modern.

TeknoIS: Jurnal Ilmiah Teknologi Informasi dan Sains
Volume 16 Number 2, July 2026 Page. 187-193
Journal Homepage: https://teknois.unbin.ac.id/index.php/JBS/
Received: June 2026; Accepted: July 2026; Published: July 2026

Tabel 3. Pola Serangan Social Engineering pada Perangkat Mobile

Vektor Serangan	Mekanisme Distribusi Malware	Faktor Psikologis yang Dieksploitasi
Smishing (SMS Phishing) & Chat Apps	Pengiriman tautan berbahaya melalui SMS atau aplikasi pesan instan dengan dalih paket kurir atau peringatan bank palsu.	Urgensi, kepanikan, dan kepercayaan terhadap otoritas
Trojanized/Fake Apps	Penyisipan malware ke dalam aplikasi yang tampak sah (misalnya aplikasi edit foto, PDF reader) di app store pihak ketiga.	Keingintahuan, pencarian fitur gratis/premium tanpa bayar.
AI-Generated Scams	Penggunaan Generative AI (Deepfake audio/teks) untuk menciptakan profil palsu atau tiruan suara figur otoritatif [9].	Empati, ketakutan, serta ilusi legitimasi yang sangat tinggi

2) Strategi Mitigasi Berdasarkan Literatur

Hasil pemetaan menunjukkan bahwa strategi perlindungan secara garis besar terbagi ke dalam dua domain yaitu sistemik (teknis) dan kognitif perilaku (non-teknis).

Tabel 4. Pemetaan Strategi Mitigasi Teknis dan Non-Teknis

Pendekatan	Metode Perlindungan	Fungsi Utama
Teknis (Sistemik)	Behavioral Application Analysis [14]	Mendeteksi anomali pada aktivitas perangkat lunak secara otomatis.
Teknis (Sistemik)	Endpoint Detection & Response (EDR) [7]	Karantina malware otomatis di tingkat kernel seluler.
Perilaku (Non-Teknis)	Pelatihan Kesadaran Keamanan (Security Awareness) [2]	Meningkatkan pengetahuan kognitif dasar pengguna.
Perilaku (Non-Teknis)	Real-time Security Nudging [10]	Memberikan peringatan kontekstual saat pengguna hendak melakukan aksi berisiko tinggi.

2. PEMBAHASAN

Data yang tersaji pada bagian hasil menunjukkan bahwa pendekatan keamanan tradisional tidak lagi relevan dalam menghadapi serangan rekayasa sosial modern. Evolusi serangan, terutama dengan hadirnya *AI generated scams* [9], membuat manipulasi psikologis semakin sulit dibedakan dengan komunikasi asli. Hal ini sejalan dengan teori *Protection Motivation* [13], di mana pengguna sering kali gagal mengambil tindakan pencegahan bukan karena tidak tahu (kurang edukasi), melainkan karena beban kognitif (cognitive load) yang dimanfaatkan oleh serangan secara instan.

Berbeda dengan penelitian terdahulu seperti **Souri** dan **Hosseini** (2018) [14] yang menitikberatkan deteksi data mining secara teknis di latar belakang, hasil sintesis ini menekankan keharusan konsep *Human-Centric Defense*. Kebaruan (*novelty*) utama dari penelitian ini terletak pada integrasi intervensi perilaku waktu-nyata (*real-time security nudging*) dengan sistem deteksi teknis. Berbeda dengan pendekatan tradisional yang bersifat statis dan pasif, real-time nudging secara proaktif menginterupsi 'mode otomatis' kognitif pengguna saat berhadapan dengan manipulasi psikologis, memberikan jeda waktu kritis sebelum eksekusi instruksi berbahaya. Integrasi ini menjembatani celah fundamental antara keamanan sistem murni dan kerentanan psikologis pengguna, menciptakan perlindungan

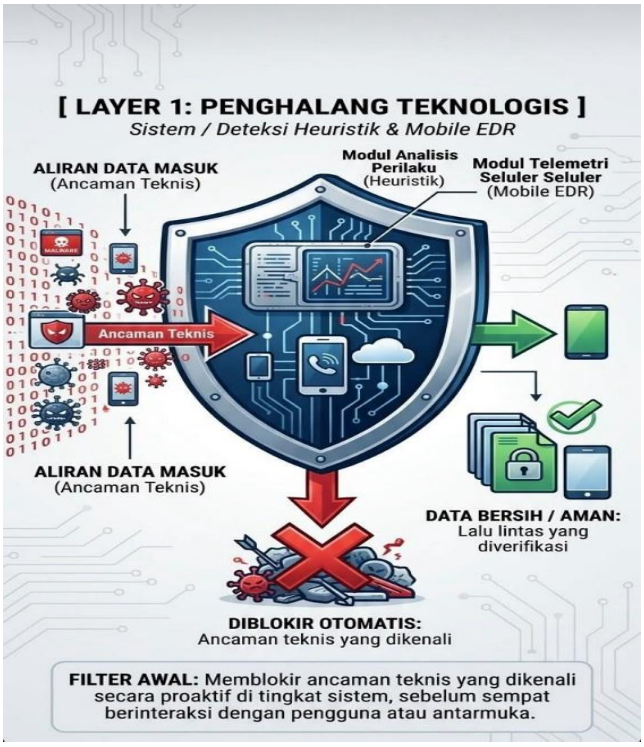
TeknoIS: Jurnal Ilmiah Teknologi Informasi dan Sains
Volume 16 Number 2, July 2026 Page. 187-193
Journal Homepage: https://teknois.unbin.ac.id/index.php/JBS/
Received: June 2026; Accepted: July 2026; Published: July 2026

komprehensif yang adaptif terhadap ancaman modern. Oleh karena itu, penelitian ini mengusulkan kerangka strategi terpadu yang secara langsung menjembatani celah antara teknis dan perilaku.

Lapisan Pertahanan	Elemen Kunci	Mekanisme Kerja
Layer 1: Technological Barrier	Deteksi Heuristik & EDR Mobile	Memblokir malware yang diketahui secara langsung tanpa interaksi pengguna. Memantau izin aplikasi secara ketat.
Layer 2: Real-time Nudging (Novelty)	Intervensi UI Dinamis Berbasis AI	Jika sistem mencurigai anomali namun butuh input user, UI akan memunculkan "jeda kognitif" (contoh: peringatan detik mundur sebelum mengunduh dari sumber tidak dikenal).
Layer 3: Continuous Cognitive Defense	Literasi Digital Terstruktur	Pelatihan berkala menggunakan simulasi ancaman mutakhir (termasuk simulasi *AI-scam*) untuk mempertahankan persepsi ancaman di level ideal.

1) Diagram Representasi Alur Kerja Mitigasi (*Defense-in-Depth Model*)

Sebagai bentuk visualisasi tambahan untuk memperkuat pemahaman terhadap Tabel 5, berikut adalah representasi struktural dari alur kerja mitigasi:



Gambar 1. Layer 1: Penghalang Teknologi

TeknoIS: Jurnal Ilmiah Teknologi Informasi dan Sains
Volume 16 Number 2, July 2026 Page. 187-193
Journal Homepage: https://teknois.unbin.ac.id/index.php/JBS/
Received: June 2026; Accepted: July 2026; Published: July 2026

Gambar 2. Layer 2: Intervensi Waktu-Nyata

Gambar 3. Layer 3: Pertahanan Kognitif Berkelanjutan

2) Implikasi dan Keterbatasan

Implikasi dari kerangka kerja ini adalah keharusan bagi pengembang sistem operasi mobile dan aplikasi keamanan untuk tidak sekadar menciptakan fitur pemblokiran pasif, tetapi merancang antarmuka (UI/UX) yang membimbing keputusan keamanan pengguna saat kritis (nudging). Meskipun kerangka ini menawarkan solusi komprehensif, studi ini memiliki keterbatasan karena masih berbasis Systematic Literature Review. Validitas operasional dari kerangka integrasi ini belum diuji melalui simulasi prototipe langsung pada perangkat seluler secara luas.

D. KESIMPULAN

Penelitian ini menyimpulkan bahwa ancaman malware di perangkat mobile yang digerakkan oleh rekayasa sosial terus beradaptasi, bergeser dari manipulasi dasar menjadi penipuan mutakhir berbasis AI. Untuk mengatasi hal tersebut, pertahanan keamanan siber tidak bisa lagi berjalan di jalur yang terpisah antara solusi teknis (sistem) dan non-teknis (edukasi). Strategi mitigasi yang paling efektif adalah pendekatan terpadu (*human-centric defense*) yang menempatkan intervensi langsung berbasis perilaku pengguna, seperti *real-time security nudging*, sebagai benteng utama. Untuk penelitian lanjutan, disarankan adanya eksperimen empiris atau pengembangan aplikasi prototipe yang menerapkan fitur nudging interaktif guna mengukur tingkat efektivitas penurunan klik berisiko oleh pengguna secara kuantitatif.

E. DAFTAR PUSTAKA

[1] Kaspersky, "Mobile Threat Report," 2023.

[2] D. P. Lestari, "Pengaruh Literasi Digital terhadap Keberhasilan Serangan Social Engineering," Jurnal Manajemen Informatika Universitas Negeri Surabaya, 2023.

[3] ENISA, "Threat Landscape Report," 2021.

[4] C. Hadnagy, Social Engineering: The Science of Human Hacking. Wiley, 2018.

[5] K. Mitnick, The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Stay Safe. Little, Brown and Company, 2017.

[6] H. Brawijaya dan R. Saputra, "Strategi Mitigasi Ancaman Ransomware pada Perangkat Mobile Menggunakan Framework NIST," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer Universitas Brawijaya, 2023.

[7] NIST, "Security and Privacy Controls for Information Systems," NIST Special Publication 800-53, 2020.

[8] R. A. G. Gultom, "Tantangan Keamanan Siber Nasional dalam Menghadapi Ancaman Malware Seluler," Jurnal Pertahanan dan Bela Negara (Universitas Pertahanan RI), 2022.

[9] S. L. Jones dan R. Ahmad, "The evolution of multi-channel social engineering in mobile ecosystems," Journal of Cybersecurity and Privacy, vol. 4, no. 1, hlm. 45-62, 2024.

[10] J. S. Park dan K. Kim, "Real-time behavioral nudging to mitigate mobile social engineering: A human-centric approach," Computers & Security, vol. 138, hlm. 103651, 2024.

[11] N. W. Utami, "Analisis Psikologis Korban Serangan Social Engineering di Media Sosial," Jurnal Komunikasi Universitas Gadjah Mada, 2022.

[12] L. Clark, "Why awareness alone is not enough," Network Security, vol. 2013, no. 11, hlm. 13-14, 2013.

[13] R. W. Rogers, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," 1983.

[14] A. Souri dan R. Hosseini, "A state-of-the-art survey of malware detection approaches using data mining techniques," Human-centric Computing and Information Sciences, vol. 8, no. 1, 2018.

[15] B. Kitchenham, "Procedures for Performing Systematic Reviews," Keele University, Tech. Rep., 2004.