ANALISIS PENIPUAN TAUTAN UNDANGAN WHATSAPP DI ERA DIGITAL BERBASIS PMT

Rensia Aurora[1)] **, Chandra Kirana** [2)]

[1,2)] *Teknik Informatika ISB Atma Luhur Pangkalpinang*
email : 2311500055@mahasiswa.atmaluhur.ac.id[1)] , chandra.kirana@atmaluhur.ac.id[2)]

Abstraksi

Perkembangan komunikasi digital melalui aplikasi WhatsApp telah meningkatkan risiko kejahatan siber, khususnya penipuan berbasis tautan undangan palsu yang memanfaatkan rekayasa sosial untuk mencuri data pribadi dan mengambil alih akun pengguna. Fenomena ini semakin meningkat seiring rendahnya literasi keamanan digital masyarakat serta tingginya intensitas penggunaan WhatsApp sebagai media komunikasi utama. Penelitian ini bertujuan untuk menganalisis modus penipuan tautan undangan WhatsApp dan menjelaskan perilaku protektif pengguna berdasarkan Protection Motivation Theory (PMT). Penelitian menggunakan metode studi literatur dengan pendekatan kualitatif deskriptif. Data dikumpulkan melalui penelaahan jurnal ilmiah, artikel akademik, laporan keamanan siber, dan penelitian terdahulu yang relevan pada rentang tahun 2020–2025. Literatur dipilih berdasarkan kesesuaian topik, relevansi terhadap phishing WhatsApp, dan keterkaitan dengan aspek perilaku pengguna digital. Analisis dilakukan menggunakan teknik content analysis untuk mengidentifikasi tema utama yang kemudian dipetakan ke dalam konstruk PMT, yaitu perceived severity, perceived vulnerability, response efficacy, dan self-efficacy. Hasil penelitian menunjukkan bahwa penipuan tautan undangan WhatsApp berhasil memanfaatkan rendahnya persepsi kerentanan pengguna, tingginya kepercayaan sosial terhadap pesan personal, serta terbatasnya kemampuan pengguna dalam mengenali indikasi phishing digital. Selain itu, pengguna yang memiliki literasi keamanan digital dan efikasi diri yang baik cenderung lebih mampu melakukan tindakan protektif, seperti memverifikasi identitas pengirim dan menghindari tautan mencurigakan. Penelitian ini memberikan kontribusi konseptual dalam memahami hubungan antara faktor psikologis pengguna dan ancaman phishing digital, sekaligus menjadi dasar pengembangan edukasi keamanan digital berbasis perilaku pengguna.

Kata Kunci :
penipuan digital, phishing WhatsApp, Protection Motivation Theory, keamanan digital, literasi digital

Abstract

The rapid development of digital communication technology has increased the use of WhatsApp as a primary communication platform, but it has also intensified the spread of cybercrime, particularly phishing scams through fake invitation links. These scams commonly exploit social engineering techniques to deceive users into clicking malicious links that may lead to personal data theft, account hijacking, and financial loss. This phenomenon continues to grow due to the low level of digital security literacy and users' limited awareness of cybersecurity threats. This study aims to analyze the modus operandi of WhatsApp invitation link scams and examine users' protective behavior using the Protection Motivation Theory (PMT) approach. The research employed a descriptive qualitative approach through a literature review method. Data were collected from scientific journals, academic articles, cybersecurity reports, and previous studies published between 2020 and 2025 that are relevant to phishing attacks, WhatsApp scams, and digital user behavior. The collected data were analyzed using content analysis techniques and categorized into the main PMT constructs, namely perceived severity, perceived vulnerability, response efficacy, and self-efficacy. The findings indicate that WhatsApp phishing scams are highly dependent on users' low perceived vulnerability, strong social trust toward personal messages, and limited capability in identifying phishing indicators. In addition, users with higher digital security literacy and stronger self-efficacy tend to demonstrate better protective behavior, such as verifying message sources and avoiding suspicious links. This study contributes conceptually to understanding the relationship between psychological factors and digital phishing threats, while also serving as a reference for developing user-based digital security education strategies.

Keywords **:**
Digital fraud, WhatsApp phishing, Protection Motivation Theory, digital security, cybersecurity behavior.

Pendahuluan

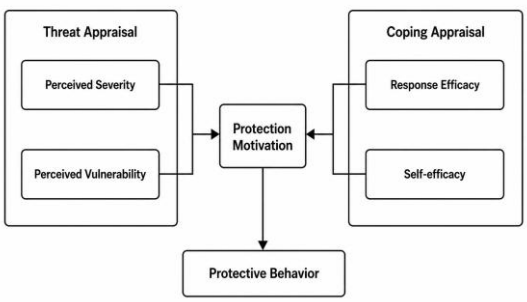
Perkembangan teknologi informasi dan komunikasi telah mendorong penggunaan aplikasi pesan instan secara masif dalam kehidupan masyarakat modern. Salah satu aplikasi yang paling banyak digunakan adalah WhatsApp karena menawarkan kemudahan Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis modus penipuan

tautan undangan WhatsApp di era digital menggunakan pendekatan Protection Motivation Theory (PMT). Penelitian difokuskan pada analisis literatur mengenai phishing WhatsApp, perilaku komunikasi, kecepatan pertukaran informasi, serta aksesibilitas yang tinggi. Namun, meningkatnya penggunaan WhatsApp juga diikuti oleh berkembangnya ancaman kejahatan siber, khususnya penipuan digital berbasis tautan atau link phishing yang dikirim melalui pesan pribadi maupun grup percakapan[1]. Modus penipuan melalui tautan undangan WhatsApp saat ini menjadi salah satu bentuk phishing yang paling sering ditemukan di Indonesia. Pelaku umumnya menyebarkan tautan palsu yang menyerupai undangan pernikahan digital, surat tilang elektronik, dokumen PDF, maupun pemberitahuan resmi lainnya untuk memancing korban mengklik tautan tersebut. Setelah tautan dibuka, korban dapat diarahkan menuju situs palsu, diminta mengunduh file berbahaya, atau tanpa sadar memberikan akses terhadap data pribadi dan perangkat digital mereka [2]Fenomena ini tidak hanya menimbulkan kerugian finansial, tetapi juga berdampak terhadap kebocoran data pribadi, penyalahgunaan identitas digital, pengambilalihan akun media sosial, serta gangguan psikologis korban akibat hilangnya rasa aman dalam berkomunikasi digital. Rendahnya literasi keamanan digital masyarakat menjadi salah satu faktor utama yang menyebabkan penipuan berbasis tautan WhatsApp masih terus berkembang. Selain itu, lemahnya kesadaran masyarakat terhadap keamanan data pribadi turut meningkatkan risiko penyalahgunaan informasi pengguna di era komunikasi digital [3]

Penelitian sebelumnya sebagian besar membahas phishing WhatsApp dari sisi teknis, keamanan sistem, maupun regulasi hukum siber [4]Penelitian lain juga menyoroti pentingnya edukasi keamanan digital dalam menekan peningkatan kejahatan siber berbasis media komunikasi instan [5] Namun, kajian yang membahas perilaku pengguna dan faktor psikologis dalam merespons ancaman phishing masih relatif terbatas. Padahal, keberhasilan penipuan digital tidak hanya dipengaruhi oleh kecanggihan teknologi pelaku, tetapi juga dipengaruhi oleh cara pengguna menilai ancaman dan mengambil keputusan ketika menerima tautan mencurigakan. Dalam konteks tersebut, Protection Motivation Theory (PMT) menjadi pendekatan yang relevan untuk menjelaskan perilaku protektif pengguna terhadap ancaman digital. PMT menjelaskan bahwa tindakan perlindungan seseorang dipengaruhi oleh dua proses utama, yaitu threat appraisal dan coping appraisal. Threat appraisal berkaitan dengan bagaimana individu menilai tingkat ancaman dan kerentanan terhadap risiko, sedangkan coping appraisal berkaitan dengan keyakinan individu terhadap efektivitas tindakan perlindungan dan kemampuan dirinya dalam menghadapi ancaman digitalUrgensi penelitian ini terletak pada meningkatnya kasus penipuan berbasis tautan WhatsApp yang memanfaatkan kelemahan perilaku pengguna digital. Selain itu, penelitian ini penting dilakukan karena memberikan perspektif psikologis terhadap fenomena phishing digital yang pengguna digital, dan faktor-faktor psikologis yang memengaruhi tindakan protektif pengguna terhadap ancaman siber.

Tinjauan Pustaka

Tinjauan pustaka dilakukan untuk mengidentifikasi penelitian terdahulu yang relevan terkait phishing WhatsApp, keamanan digital, serta penggunaan Protection Motivation Theory (PMT) dalam menganalisis perilaku pengguna terhadap ancaman siber. Penelitian yang dilakukan oleh [6]menyoroti berbagai modus phishing yang berkembang di WhatsApp, seperti penyebaran tautan palsu, file undangan, hingga situs tiruan yang bertujuan mencuri informasi pribadi pengguna. Studi tersebut mengungkapkan bahwa rendahnya literasi digital pengguna menyebabkan serangan phishing berkembang pesat dan sering kali tidak disadari hingga menimbulkan kerugian. Meskipun penelitian ini memberikan gambaran komprehensif mengenai teknik phishing, kajian tersebut belum mengeksplorasi aspek psikologis pengguna dalam merespons ancaman. Penelitian ini melengkapi celah tersebut dengan menggunakan Protection Motivation Theory (PMT) untuk menganalisis faktor kognitif yang memengaruhi kerentanan pengguna terhadap tautan undangan berbahaya. Selanjutnya, penelitian oleh [7] membahas penipuan digital melalui modus tilang daring yang marak di WhatsApp, di mana pelaku memanfaatkan rekayasa sosial untuk menciptakan rasa urgensi sehingga korban terdorong mengikuti instruksi yang diberikan. Penelitian tersebut menekankan pentingnya edukasi keamanan informasi dan peningkatan patroli siber, namun belum mengkaji bagaimana persepsi ancaman dan efikasi pengguna memengaruhi perilaku mereka dalam menghadapi tautan mencurigakan.Dalam penelitian ini, Protection Motivation Theory (PMT) digunakan untuk menjelaskan bagaimana pengguna menilai ancaman phishing digital dan membentuk perilaku protektif terhadap tautan mencurigakan di WhatsApp.

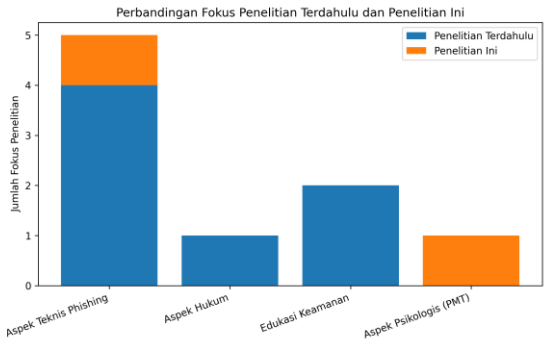


Gambar 1. Framework Protection Motivation Theory (PMT)
Sumber: Diolah Peneliti, 2026

Berdasarkan Gambar 1, Protection Motivation Theory (PMT) terdiri dari dua komponen utama, yaitu threat appraisal dan coping appraisal. Threat appraisal mencakup perceived severity dan perceived vulnerability yang berkaitan dengan penilaian individu terhadap tingkat ancaman phishing digital. Sementara itu, coping appraisal terdiri dari response efficacy dan self-efficacy yang berkaitan dengan keyakinan individu terhadap efektivitas tindakan perlindungan dan kemampuan dirinya dalam menghadapi ancaman siber. Kedua komponen tersebut memengaruhi protection motivation yang kemudian membentuk protective behavior pengguna terhadap tautan mencurigakan di WhatsApp. Kekurangan ini menjadikan penelitian ini relevan, karena melalui pendekatan PMT dapat dianalisis bagaimana persepsi risiko dan kemampuan proteksi memengaruhi pengambilan keputusan individu saat menerima tautan undangan di WhatsApp. Penelitian oleh [8] menunjukkan bahwa komunikasi penipuan daring melalui WhatsApp memanfaatkan jaringan penyebaran tautan berbahaya, seperti file APK, PDF, dan tautan undangan palsu. Studi tersebut menjelaskan bahwa keberhasilan penipuan sangat bergantung pada kemampuan pelaku membangun kepercayaan dengan menyamar sebagai institusi resmi. Meskipun mampu memetakan pola jaringan komunikasi penipu, penelitian ini belum menjelaskan bagaimana evaluasi ancaman dalam diri pengguna memengaruhi keputusan untuk mengklik tautan yang diterima. Penelitian ini menawarkan kontribusi tambahan dengan mengintegrasikan PMT untuk menjelaskan bagaimana persepsi ancaman dan self-efficacy dapat mendorong atau mencegah tindakan klik terhadap tautan berbahaya. Menurut penelitian [9] ancaman phishing di WhatsApp terus meningkat seiring dengan maraknya penyebaran tautan palsu dan file undangan PDF yang dimodifikasi oleh pelaku untuk mencuri data pengguna. Penelitian tersebut berfokus pada analisis teknis serta rekomendasi manajemen keamanan informasi. Namun demikian, kajian ini belum menyoroti perilaku pengguna dari sisi motivasi dan persepsi keamanan yang memengaruhi keputusan membuka tautan. Oleh karena itu, penelitian ini memperluas temuan tersebut dengan memberikan perspektif perilaku berbasis PMT untuk menjelaskan mengapa sebagian pengguna tetap mengklik tautan meskipun telah mengetahui risiko phishing. Penelitian oleh [10] mengkaji penipuan phishing melalui modus tautan undangan pernikahan dari perspektif hukum pidana ekonomi dan menunjukkan bahwa regulasi kejahatan siber yang ada belum sepenuhnya mampu menekan maraknya penipuan melalui WhatsApp. Studi tersebut menekankan dampak ekonomi yang signifikan serta lemahnya mekanisme penegakan hukum. Meskipun memberikan kontribusi penting dari sisi legalitas, penelitian ini belum memandang perilaku pengguna sebagai faktor kunci keberlanjutan penipuan digital. Penelitian ini memperkuat kajian tersebut dengan menganalisis faktor psikologis pengguna berdasarkan PMT untuk memahami mengapa tautan undangan palsu masih efektif menjerat korban. Berdasarkan penelitian terdahulu tersebut, dapat disimpulkan bahwa sebagian besar penelitian masih berfokus pada aspek teknis, komunikasi, dan regulasi hukum terkait phishing digital di WhatsApp. Sementara itu, penelitian yang secara khusus mengaitkan perilaku protektif pengguna dengan pendekatan psikologis berbasis Protection Motivation Theory (PMT) masih relatif terbatas. Oleh karena itu, penelitian ini hadir untuk mengisi celah tersebut dengan menganalisis hubungan antara persepsi ancaman, efikasi diri, dan motivasi perlindungan pengguna terhadap penipuan tautan undangan WhatsApp di era digital.

Tabel 1. Peneliti Terdahulu

No	Penelitian	Ringkasan
1	Isadora, Kaela, Putri Aqila Nashwa	Penipuan tilang online WhatsApp berbasis rekayasa sosial.
2	F.Hafiz Rahmadani,H. Cahya Sutany, M. Ragil	Modus urgensi pada penipuan tilang online WhatsApp.
3	Wahyudin	Jaringan komunikasi penipuan melalui WhatsApp.
4	A.Trianurhamah dkk.	Ancaman phishing link dan file WhatsApp.
5	F. Hasna	Phishing link undangan pernikahan WhatsApp.

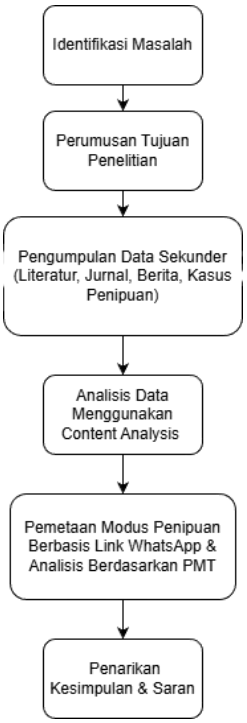


Gambar 2. Perbandingan Peneliti Terdahulu dan Saat ini

Grafik disajikan sebagai ilustrasi konseptual berdasarkan sintesis penelitian terdahulu

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi literatur (literature review). Pendekatan ini digunakan untuk memahami fenomena penipuan tautan undangan WhatsApp secara konseptual serta menganalisis perilaku protektif pengguna berdasarkan Protection Motivation Theory (PMT). Metode studi literatur dipilih karena mampu memberikan pemahaman yang sistematis terhadap fenomena kejahatan digital berdasarkan berbagai sumber ilmiah yang relevan [11]Data penelitian diperoleh dari berbagai sumber literatur sekunder berupa jurnal ilmiah nasional dan internasional, artikel akademik, laporan keamanan siber, prosiding penelitian, serta dokumen pendukung yang relevan dengan phishing WhatsApp dan keamanan digital. Literatur yang digunakan berasal dari publikasi tahun 2020–2025 agar sesuai dengan perkembangan ancaman phishing digital terkini. Pengumpulan data dilakukan melalui proses identifikasi topik penelitian, penelusuran literatur menggunakan kata kunci terkait phishing WhatsApp dan Protection Motivation Theory, seleksi sumber berdasarkan relevansi dan kualitas penelitian, serta pengelompokan literatur sesuai tema pembahasan. Selanjutnya, data dianalisis menggunakan teknik content analysis (analisis isi) untuk mengidentifikasi pola penipuan, strategi rekayasa sosial, faktor psikologis pengguna, serta hubungan antara ancaman digital dan motivasi perlindungan pengguna [12]Hasil analisis kemudian dipetakan ke dalam konstruk utama Protection Motivation Theory (PMT), yaitu perceived severity, perceived vulnerability, response efficacy, dan self-efficacy. Pendekatan ini digunakan untuk menjelaskan bagaimana pengguna menilai ancaman phishing dan membentuk perilaku protektif terhadap tautan mencurigakan di WhatsApp [13]Sebagai tahap akhir, hasil penelitian disusun secara sistematis melalui proses identifikasi masalah, pengumpulan literatur, analisis data, pemetaan berdasarkan PMT, hingga penarikan kesimpulan penelitian.

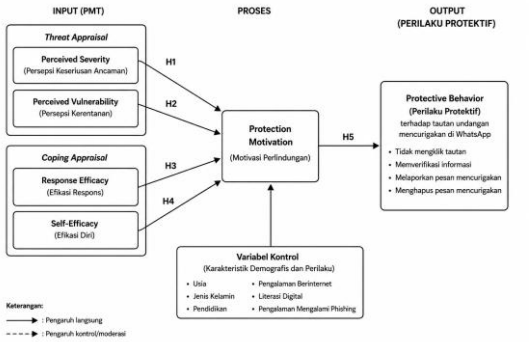


Gambar 3. Diagram Alir Langkah Penelitian

Hasil dan Pembahasan

Hasil Penelitian

Penelitian ini menganalisis modus penipuan melalui tautan undangan WhatsApp menggunakan pendekatan Protection Motivation Theory (PMT) yang mencakup konstruk perceived severity, perceived vulnerability, response efficacy, dan self-efficacy [14]



Gambar 4. Grafik Konsep Penelitian Berbasis PMT

Berdasarkan Gambar 4, penelitian ini menggunakan Protection Motivation Theory (PMT) sebagai dasar dalam menganalisis perilaku protektif pengguna terhadap penipuan tautan undangan WhatsApp. Konstruk threat appraisal terdiri dari perceived severity dan perceived vulnerability yang digunakan untuk mengukur persepsi ancaman pengguna terhadap phishing digital. Sementara itu, coping appraisal terdiri dari response efficacy dan self-efficacy yang digunakan untuk menjelaskan

kemampuan pengguna dalam menghadapi ancaman siber. Seluruh konstruk tersebut memengaruhi protection motivation yang kemudian membentuk perilaku protektif pengguna terhadap tautan mencurigakan di WhatsApp. Berdasarkan hasil sintesis literatur, penipuan berbasis tautan WhatsApp masih menjadi salah satu bentuk phishing digital yang efektif karena memanfaatkan faktor psikologis pengguna, seperti rasa penasaran, kepercayaan sosial, dan rendahnya kewaspadaan digital dalam komunikasi personal. Hasil kajian menunjukkan bahwa bentuk penipuan yang paling sering ditemukan meliputi tautan undangan pernikahan digital, file APK berkedok dokumen resmi, tautan tilang elektronik palsu, serta file PDF berbahaya yang dikirim melalui pesan WhatsApp. Pelaku umumnya menggunakan identitas yang menyerupai institusi resmi maupun kontak yang dikenal korban untuk meningkatkan tingkat kepercayaan pengguna terhadap pesan yang dikirim. Dari perspektif threat appraisal, pengguna pada umumnya memahami tingkat keparahan ancaman phishing digital, seperti pencurian data pribadi, pengambilalihan akun WhatsApp, hingga kerugian finansial. Namun demikian, persepsi kerentanan pengguna masih cenderung rendah karena sebagian besar individu merasa dirinya tidak akan menjadi korban penipuan digital. Selain itu, pada aspek coping appraisal ditemukan bahwa pengguna dengan tingkat literasi keamanan digital yang lebih baik cenderung memiliki kemampuan lebih tinggi dalam mengenali ciri-ciri phishing dan menghindari manipulasi sosial yang dilakukan pelaku. Temuan penelitian ini menunjukkan bahwa rendahnya literasi keamanan digital masih menjadi faktor utama yang menyebabkan pengguna rentan terhadap penipuan berbasis tautan WhatsApp. Oleh karena itu, peningkatan kesadaran keamanan siber dan kemampuan pengguna dalam mengenali ancaman digital menjadi langkah penting dalam mengurangi risiko phishing di era komunikasi digital.

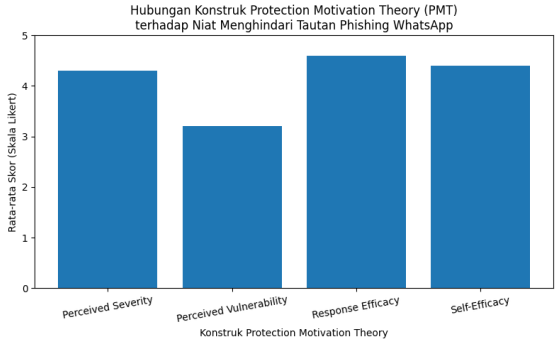
Pembahasan

Hasil penelitian menunjukkan bahwa keberhasilan penipuan berbasis tautan WhatsApp tidak hanya dipengaruhi oleh kecanggihan teknik pelaku, tetapi juga dipengaruhi oleh faktor psikologis pengguna digital. Protection Motivation Theory (PMT) menjelaskan bahwa individu akan terdorong melakukan tindakan protektif ketika memiliki persepsi ancaman yang tinggi dan keyakinan bahwa dirinya mampu melakukan perlindungan terhadap ancaman tersebut [15]Dalam konteks phishing WhatsApp, pengguna yang memiliki tingkat self-efficacy tinggi cenderung lebih kritis terhadap pesan digital dan tidak mudah terpengaruh oleh manipulasi emosional. Sebaliknya, pengguna dengan literasi keamanan digital rendah lebih rentan menjadi korban karena kurang memahami indikator phishing, seperti tautan mencurigakan, identitas pengirim palsu, maupun file berbahaya yang dikirim melalui aplikasi pesan instan. Temuan penelitian ini juga menunjukkan bahwa rekayasa sosial menjadi faktor utama keberhasilan phishing digital. Pelaku tidak hanya mengeksploitasi kelemahan teknis sistem, tetapi juga memanfaatkan kelemahan perilaku manusia, seperti rasa panik, rasa penasaran, dan kepercayaan sosial terhadap pesan personal. Kondisi tersebut menyebabkan pengguna sering kali mengabaikan proses verifikasi sebelum membuka tautan yang diterima. Selain itu, kesadaran terhadap ancaman digital belum tentu diikuti oleh perilaku pencegahan yang konsisten. Sebagian pengguna telah mengetahui risiko phishing, tetapi tetap membuka tautan karena merasa ancaman tersebut tidak akan berdampak langsung pada dirinya. Fenomena ini menunjukkan adanya optimism bias dalam perilaku pengguna digital, yaitu kecenderungan individu menganggap dirinya lebih aman dibandingkan orang lain terhadap ancaman siber. Dari sisi coping appraisal, penelitian ini menunjukkan bahwa peningkatan literasi keamanan digital memiliki peran strategis dalam membentuk perilaku protektif pengguna. Pengguna yang memahami langkah-langkah keamanan digital dan merasa mampu menerapkannya cenderung lebih berhati-hati dalam menerima pesan yang mengandung tautan atau file mencurigakan. Oleh karena itu, edukasi keamanan digital berbasis perilaku menjadi salah satu strategi penting dalam upaya mitigasi phishing WhatsApp. Secara akademik, penelitian ini memberikan kontribusi dengan mengintegrasikan Protection Motivation Theory dalam konteks penipuan tautan WhatsApp yang berbasis komunikasi personal dan relasi sosial. Pendekatan ini menunjukkan bahwa upaya pencegahan kejahatan siber tidak hanya memerlukan solusi teknis, tetapi juga memerlukan pemahaman terhadap faktor psikologis dan perilaku pengguna digital dalam menghadapi ancaman phishing di era komunikasi modern.

Kelebihan dan Kelemahan Penelitian

Kelebihan penelitian ini terletak pada penggunaan kerangka Protection Motivation Theory (PMT) yang mampu menjelaskan perilaku pengguna secara komprehensif dalam konteks penipuan berbasis pesan instan. Selain itu, penyajian hasil dalam bentuk grafik konseptual membantu mempermudah pemahaman hubungan antar konstruk PMT yang berkaitan dengan motivasi perlindungan pengguna.

Adapun kelemahan penelitian ini terletak pada penggunaan metode studi literatur yang bergantung pada temuan penelitian terdahulu, sehingga analisis yang dihasilkan bersifat konseptual dan belum didukung oleh data empiris secara langsung. Oleh karena itu, penelitian selanjutnya disarankan untuk mengombinasikan pendekatan berbasis perilaku dengan metode empiris, seperti survei atau analisis forensik digital, agar diperoleh pemahaman yang lebih komprehensif mengenai ancaman penipuan berbasis tautan di platform WhatsApp.



Gambar 5. Grafik Hubungan Konstruk PMT terhadap Niat Menghindari Tautan Phishing WhatsApp

Grafik disajikan sebagai ilustrasi konseptual berdasarkan sintesis hasil penelitian terdahulu, bukan hasil pengukuran empiris langsung.

Kesimpulan dan Saran

Berdasarkan hasil studi literatur yang telah dilakukan, dapat disimpulkan bahwa penipuan melalui tautan undangan WhatsApp merupakan bentuk phishing digital yang berkembang melalui strategi rekayasa sosial dan pemanfaatan kepercayaan pengguna dalam komunikasi personal. Modus penipuan ini tidak hanya menimbulkan kerugian finansial, tetapi juga menyebabkan kebocoran data pribadi, pengambilalihan akun digital, serta meningkatnya risiko penyalahgunaan identitas pengguna. Analisis menggunakan Protection Motivation Theory (PMT) menunjukkan bahwa perilaku protektif pengguna dipengaruhi oleh dua faktor utama, yaitu threat appraisal dan coping appraisal. Pada aspek threat appraisal, pengguna umumnya memahami tingkat keparahan ancaman phishing, tetapi masih memiliki persepsi kerentanan yang rendah sehingga merasa dirinya tidak mudah menjadi korban penipuan digital. Sementara itu, pada aspek coping appraisal, pengguna yang memiliki literasi keamanan digital dan self-efficacy tinggi cenderung lebih mampu mengenali dan menghindari tautan mencurigakan. Hasil penelitian juga menunjukkan bahwa keberhasilan phishing WhatsApp tidak hanya dipengaruhi oleh faktor teknis, tetapi juga dipengaruhi oleh aspek psikologis dan perilaku pengguna digital. Oleh karena itu, peningkatan literasi keamanan digital, kesadaran ancaman siber, dan kemampuan pengguna dalam menerapkan langkah protektif menjadi faktor penting dalam upaya pencegahan penipuan digital. Penelitian ini memberikan kontribusi konseptual dengan mengaitkan Protection Motivation Theory terhadap fenomena penipuan berbasis tautan WhatsApp. Namun, penelitian ini masih memiliki keterbatasan karena menggunakan metode studi literatur sehingga belum didukung oleh data empiris secara langsung.

SARAN

Berdasarkan hasil penelitian, diperlukan peningkatan literasi keamanan digital masyarakat sebagai upaya mengurangi risiko penipuan berbasis tautan WhatsApp. Edukasi mengenai ciri-ciri phishing, pentingnya verifikasi tautan, serta kesadaran terhadap ancaman rekayasa sosial perlu dilakukan secara berkelanjutan melalui institusi pendidikan, media digital, maupun platform komunikasi. Selain itu, pengembang aplikasi pesan instan diharapkan dapat meningkatkan sistem keamanan dan deteksi tautan berbahaya untuk meminimalkan penyebaran phishing digital. Penelitian selanjutnya disarankan menggunakan metode kuantitatif atau survei langsung terhadap pengguna WhatsApp agar diperoleh data empiris yang lebih mendalam mengenai perilaku protektif pengguna terhadap ancaman siber.

Daftar Pustaka

[1] A. P. M. C. Sitorus and A. Astono, "Arus Jurnal Sosial dan Humaniora (AJSH)," *Arus J. Sos. dan Hum.*, vol. 4, no. 1, pp. 157–162, 2024, doi: https://doi.org/10.57250/ajsh.v4i1.

[2] A. Desi, T. Ambodo, and A. Tohawi, "Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia," *Islam. Law J. Siyasah*, vol. 9, no. 2, pp. 118–131, 2024, doi: 10.53429/iljs.v9i2.858.

[3] A. N. Luthiya, B. Irawan, and R. Yulia, "Kebijakan Hukum Pidana Terhadap Pengaturan Pencurian Data Pribadi Sebagai Penyalahgunaan Teknologi Komunikasi Dan Informasi," *J. Huk. Pidana dan Kriminologi*, vol. 2, no. 2, pp. 1–10, 2021, doi: 10.51370/jhpk.v2i2.43.

[4] A. D. Wijaya and T. P. Anggriawan, "Perlindungan Hukum Terhadap Data Pribadi Dalam Penggunaan Aplikasi di Smartphone," *Inicio Legis*, vol. 3, no. 1, pp. 63–72, 2022, doi: 10.21107/il.v3i1.14873.

[5] D. A. Puanandini, A. S. R. Sapaat, M. R. P. Ramadhan, D. P. Punggawa, and D. I. Purnama, "Ham Perlindungan Data Pribadi Tantangan Dan," *MEDIA Akad.*, vol. 3, no. 7, 2025, doi: https://doi.org/10.62281/v3i7.2598.

[6] K. Isadora, N. P. Aqila, H. Gustina, A. Nabila, and Nurfitriana, "Analisis Modus Phising terhadap Whatsapp," *J. Akuntansi, Bisnis dan Ekon. Indones.*, vol. 3, no. 2, pp. 45–52, 2024, doi: https://doi.org/10.30630/jabei.v3i2.243.

[7] F. H. Rahmadani, H. C. Sutany, M. R. Aditya, M. A. Fajar, Y. U. Dari, and Fauziyah, "Cybercrime: Analisis Dan Mitigasi Resiko Penipuan Tilang Online Melalui Aplikasi WhatsApp (WA)," *J. Sist. Inf. Galuh*, vol. 3, no. 1, 2025, doi: 10.25157/jsig.v3i1.4124.

[8] Wahyuddin, L. F. Ersa, G. Aningsih, T. Hidayat, and A. F. Sonni, "Network Analysis of Online Fraud Communication Through Social Media Whatsapp Messenger," *J. Netnografi Komun. Vol.2*, vol. 2, no. 2, pp. 73–90, 2024, doi: https://doi.org/10.59408/jnk.v2i2.27.

[9] A. Trianurahmah, A. Fauzi, E. N. Tyas, M. A. Suryanto, M. Rizky, and P. Wibisono, "Analisis Ancaman Pishing Melalui Aplikasi WhatsApp: Studi Kasus Manajemen Sekuriti Waspadai Maraknya Kejahatan Phising Dengan Modus Berbasis Link," *Orbit J. Ilmu Multidisiplin Nusant.*, vol. 1, no. 2, pp. 60–74, 2024, doi: 10.63217/orbit.v1i2.81.

[10] F. Hasna, "Analisis Kejahatan Phising dengan Modus Link Undangan Pernikahan Pada Aplikasi," 2024, [Online]. Available: https://online-journal.unja.ac.id/Pampas/article/view/17704

[11] D. N. Ayman and N. Lucky, "Analisis Kejahatan Siber Sniffing Pada Media Sosial Whatsapp," *Anomie*, vol. 7, pp. 35–49, 2025, [Online]. Available: https://jom.fisip.budiluhur.ac.id/anomie/article/view/559%0Ahttps://jom.fisip.budiluhur.ac.id/anomie/article/download/559/289

[12] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, pp. 1–10, 2017, doi: 10.26555/jiteki.v3i1.6643.

[13] M. W. A. Prastya *et al.*, "Analisis Ancaman Pishing melalui Aplikasi WhatsApp: Review Metode Studi Literatur," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 7, no. 3, pp. 190–197, 2024, doi: 10.32672/jnkti.v7i3.7551.

[14] N. S. Sulaiman, M. A. Fauzi, S. Hussain, and W. Wider, "Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks," *Inf.*, vol. 13, no. 9, pp. 1–17, 2022, doi: 10.3390/info13090413.

[15] R. Rudi, "An Analysis of Phishing Susceptibility Through the Lens of Protection Motivation Theory," pp. 1–65, 2023, [Online]. Available: https://uia.brage.unit.no/uia-xmlui/handle/11250/3080484%0Ahttps://uia.brage.unit.no/uia-xmlui/bitstream/handle/11250/3080484/no.uia:inspera:143804570:36975082.pdf?sequence=1