BAB II
KERANGKA TEORI

2.1 Kesadaran Pengguna

Kesadaran pengguna (*user awareness*) adalah tingkat pemahaman dan perhatian yang dimiliki oleh individu terhadap isu-isu tertentu, yang dalam konteks ini berkaitan dengan keamanan siber dan praktik phishing. Kesadaran ini mencakup kemampuan pengguna untuk mengenali, memahami, dan merespons ancaman siber yang mereka hadapi dalam penggunaan teknologi informasi sehari-hari, termasuk aplikasi pesan instan seperti WhatsApp. Kesadaran terhadap ancaman siber merupakan aspek penting dari perilaku aman dalam dunia digital, yang dapat membantu mengurangi risiko serangan dan dampak dari ancaman tersebut (Tzuo & Towndrow, 2015).

Kesadaran pengguna tidak hanya sebatas pengetahuan teknis, tetapi juga mencakup sikap dan perilaku pengguna dalam mengelola informasi dan menjaga privasi. Hal ini penting karena meskipun pengguna mungkin memiliki pengetahuan tentang ancaman siber, tanpa sikap yang benar dan perilaku yang sesuai, mereka tetap dapat menjadi korban serangan.

Kesadaran pengguna terhadap risiko penggunaan teknologi sangat penting untuk meminimalkan dampak negatif dari berbagai ancaman yang mungkin muncul. Kesadaran ini melibatkan pemahaman pengguna tentang potensi bahaya yang terkait dengan teknologi digital, termasuk risiko keamanan siber, privasi, serta kerugian finansial.

Salah satu tantangan utama dalam penggunaan teknologi adalah bagaimana risiko tersebut seringkali tidak terlihat atau dipahami dengan baik oleh pengguna umum. Sebagai contoh, perangkat Internet of Things (IoT) seperti kamera pintar atau perangkat rumah tangga cerdas, meskipun menawarkan kenyamanan, dapat menjadi target serangan siber jika tidak dilindungi dengan baik. Penjahat siber dapat mengeksploitasi celah keamanan pada perangkat IoT untuk mengakses jaringan pribadi atau bahkan mencuri informasi sensitif

Selain itu, dalam lingkungan bisnis, risiko-risiko terkait teknologi terus berkembang, seperti gangguan pada rantai pasokan digital, serangan malware, serta pencurian identitas. Organisasi perlu mengembangkan strategi pengelolaan risiko yang komprehensif, tidak hanya untuk melindungi data, tetapi juga untuk menjaga keberlanjutan operasional mereka. Meskipun demikian, kesadaran pengguna akan risiko ini masih sering kali rendah, terutama

dalam hal pengetahuan akan langkah-langkah pencegahan seperti penggunaan autentikasi dua faktor atau pengelolaan kata sandi yang kuat.

Menurut sebuah survei global oleh PwC, hanya 37% organisasi merasa sangat terekspos pada risiko siber, meskipun 60% di antaranya menganggap teknologi digital dan AI sebagai peluang (PwC, 2023). Hal ini menunjukkan adanya kesenjangan antara pemanfaatan teknologi dan kesadaran akan risiko yang mengikutinya. Untuk menghadapi tantangan ini, pengguna, baik individu maupun institusi, perlu terus meningkatkan literasi digital mereka, memahami risiko yang mengancam, serta mengadopsi praktik-praktik keamanan yang tepat guna melindungi diri dan data mereka.

Kesadaran pengguna dalam konteks digital, khususnya dalam menghadapi ancaman seperti *phishing*, adalah topik yang penting untuk dibahas dalam era teknologi informasi saat ini. Dalam kajian literatur, kesadaran dapat didefinisikan sebagai kemampuan seseorang untuk mengetahui, memahami, dan merespons informasi yang diterima secara efektif. Dalam konteks keamanan digital, kesadaran ini berkaitan dengan kemampuan pengguna untuk mengenali dan menghindari potensi ancaman, termasuk upaya *phishing* melalui platform komunikasi seperti WhatsApp.

Kesadaran (*awareness*) adalah bagian penting dari proses kognitif seseorang yang memungkinkan mereka untuk mengidentifikasi situasi berisiko dan mengambil tindakan pencegahan. Kesadaran ini berkaitan erat dengan teori pemrosesan informasi, yang menyatakan bahwa manusia mengolah informasi yang masuk secara berurutan, mulai dari perhatian, penyimpanan dalam memori, hingga pengambilan keputusan. Dalam menghadapi ancaman *phishing*, pengguna WhatsApp yang memiliki kesadaran tinggi akan lebih cenderung mampu mengenali pola-pola pesan mencurigakan dan mengambil langkah untuk menghindarinya.

Secara etimologis, istilah "kesadaran" berasal dari kata "sadar," yang dalam bahasa Indonesia mengacu pada kemampuan seseorang untuk memahami dan merespons lingkungannya. Kesadaran pengguna di dunia digital tidak hanya mencakup pengetahuan mengenai fitur aplikasi, tetapi juga mencakup pemahaman tentang ancaman yang mungkin terjadi, seperti penyebaran malware melalui *phishing*.

Menurut Noel Burch, kesadaran pengguna dapat dikategorikan ke dalam beberapa tingkatan, mulai dari *unconscious incompetence*, di mana seseorang tidak menyadari ancaman

dan tidak memiliki keterampilan untuk menanganinya, hingga *conscious competence*, di mana seseorang mengetahui ancaman dan tahu cara untuk menanganinya (Peel & Nolan, 2015) Pada tingkatan tertinggi, yaitu *unconscious competence*, pengguna secara otomatis dapat mengenali dan mengatasi ancaman tanpa memerlukan banyak pertimbangan kognitif.

Kesadaran pengguna terhadap ancaman dapat dikategorikan ke dalam empat tingkatan berdasarkan model Conscious Competence. Pertama, *unconscious incompetence*, di mana pengguna tidak menyadari ancaman dan juga tidak memiliki kemampuan untuk menghadapinya. Pada tahap ini, pengguna bahkan tidak tahu bahwa mereka tidak memiliki keterampilan yang dibutuhkan untuk menangani situasi tertentu, sehingga masih dalam kondisi tidak kompeten tanpa kesadaran diri

Selanjutnya, pengguna bergerak ke tahap *conscious incompetence*, di mana mereka mulai sadar akan ancaman dan ketidakmampuan mereka. Meskipun mereka belum menguasai keterampilan yang diperlukan, kesadaran ini menjadi awal untuk belajar dan memperbaiki diri. Pengguna di tahap ini sering mengalami frustrasi karena menyadari keterbatasan mereka, namun ini adalah fase penting untuk pengembangan

Pada tahap *conscious competence*, pengguna mulai menguasai keterampilan yang diperlukan untuk mengatasi ancaman, tetapi masih harus secara aktif berpikir dan berusaha untuk melakukannya dengan benar. Pada titik ini, keterampilan telah diperoleh melalui latihan yang konsisten, namun pengguna masih perlu memberikan perhatian pada tugas yang mereka hadapi

Tingkat tertinggi adalah *unconscious competence*, di mana pengguna dapat mengenali dan menangani ancaman secara otomatis tanpa perlu banyak pertimbangan kognitif. Pada tahap ini, keterampilan telah menjadi otomatis, memungkinkan pengguna untuk bertindak secara efektif tanpa harus berpikir keras tentang apa yang harus dilakukan

Kesadaran ini menjadi kunci dalam pencegahan kejahatan digital, terutama karena praktik *phishing* semakin canggih dan sering kali menyasar pengguna yang memiliki literasi digital rendah. Seiring dengan meningkatnya literasi digital, diharapkan kesadaran pengguna juga meningkat, sehingga mereka dapat lebih efektif dalam melindungi diri dari ancaman-ancaman yang ada di dunia maya (Hastjarjo, 2005).

2.2. Kesadaran Keamanan Siber

Kesadaran pengguna terhadap keamanan siber dapat dianalisis melalui beberapa dimensi yang meliputi:

a. Pengetahuan (*Knowledge*)

Pengetahuan mencakup pemahaman dasar pengguna mengenai ancaman siber, termasuk definisi phishing, cara kerja phishing, serta potensi risiko yang dihadapi ketika file.APK yang mencurigakan diunduh dan diinstal. Pengetahuan ini juga mencakup pengenalan terhadap tanda-tanda yang biasanya muncul dalam pesan phishing, seperti URL yang mencurigakan, permintaan informasi pribadi secara mendesak, atau tawaran yang tampak terlalu bagus untuk menjadi kenyataan (Parsons et al., 2013).

b. Persepsi Risiko (*Risk Perception*)

Persepsi risiko mengacu pada sejauh mana pengguna merasa bahwa mereka mungkin menjadi target atau korban dari serangan siber. Persepsi ini sangat dipengaruhi oleh pengalaman pribadi atau cerita dari orang lain mengenai insiden keamanan, serta bagaimana informasi mengenai risiko tersebut disampaikan. Pengguna dengan persepsi risiko yang tinggi cenderung lebih waspada dan berhati-hati dalam berinteraksi dengan file atau tautan yang diterima dari sumber yang tidak jelas (Woon, Tan, & Low, 2005).

c. Sikap (Attitude)

Sikap pengguna terhadap keamanan siber mencakup keyakinan dan nilai-nilai yang memengaruhi bagaimana mereka memandang pentingnya menjaga keamanan informasi. Sikap ini dapat dipengaruhi oleh pendidikan, budaya, dan lingkungan sosial. Pengguna dengan sikap positif terhadap praktik keamanan siber lebih cenderung mengambil tindakan pencegahan yang tepat, seperti memverifikasi sumber file sebelum mengunduh atau menggunakan aplikasi keamanan untuk memindai file (Ajzen, 1991).

d. Motivasi (Motivation)

Motivasi adalah dorongan internal yang memengaruhi tindakan pengguna terkait dengan keamanan siber. Motivasi dapat berasal dari kebutuhan untuk melindungi informasi pribadi, keinginan untuk menjaga reputasi online, atau bahkan peraturan dan kebijakan yang mengharuskan perilaku tertentu. Motivasi yang tinggi biasanya berbanding lurus dengan tindakan pencegahan yang lebih efektif terhadap ancaman siber (Pahnila, Siponen, & Mahmood, 2007).

e. Tindakan (Behavior)

Tindakan mengacu pada perilaku konkret yang diambil pengguna untuk melindungi diri dari ancaman siber. Ini bisa termasuk tidak mengklik tautan yang mencurigakan, mengabaikan atau melaporkan pesan yang tampak seperti phishing, menggunakan otentikasi dua faktor, dan memperbarui aplikasi secara teratur. Tindakan ini merupakan hasil akhir dari kombinasi pengetahuan, persepsi risiko, sikap, dan motivasi pengguna (Ng, Kankanhalli, & Xu, 2009).

f. Refleksi dan Evaluasi

Dimensi ini mencakup kemampuan pengguna untuk secara kritis mengevaluasi tindakan mereka terkait keamanan siber. Pengguna yang reflektif akan menganalisis pengalaman mereka dengan ancaman siber, belajar dari kesalahan, dan menyesuaikan perilaku mereka di masa depan untuk meningkatkan keamanan. Refleksi ini juga dapat mencakup evaluasi terhadap informasi baru yang mereka terima tentang ancaman siber dan bagaimana informasi tersebut mempengaruhi keputusan mereka (Kolb, 1984).

Kesadaran pengguna dapat dipengaruhi oleh berbagai faktor, diantaranya:

a. Tingkat Pendidikan

Pendidikan formal tentang keamanan siber atau teknologi informasi dapat meningkatkan pengetahuan dan sikap pengguna terhadap ancaman siber. Pengguna dengan latar belakang pendidikan di bidang teknologi lebih mungkin untuk mengenali dan menghindari ancaman seperti phishing.

b. Pengalaman Pribadi

Pengalaman langsung atau tidak langsung dengan serangan siber dapat meningkatkan kesadaran pengguna. Pengguna yang pernah menjadi korban atau mengetahui orang yang menjadi korban lebih cenderung waspada dan mengambil langkah-langkah pencegahan.

c. Sumber Informasi

Sumber informasi yang diakses oleh pengguna, seperti berita, media sosial, atau kampanye kesadaran, memainkan peran penting dalam membentuk kesadaran mereka. Informasi yang akurat dan relevan dapat meningkatkan pemahaman dan kewaspadaan pengguna.

d. Lingkungan Sosial

Norma sosial dan budaya di sekitar pengguna, termasuk praktik keamanan siber yang diterapkan di lingkungan kerja atau komunitas, juga mempengaruhi kesadaran mereka.

Lingkungan yang menekankan pentingnya keamanan siber dapat mendorong pengguna untuk lebih berhati-hati.

e. Teknologi dan Alat Keamanan

Ketersediaan dan penggunaan alat keamanan, seperti antivirus dan fitur keamanan di aplikasi, dapat meningkatkan kesadaran dan perlindungan pengguna. Pengguna yang terbiasa dengan teknologi ini lebih mungkin untuk mengenali dan menghindari ancaman.

Kesadaran pengguna terhadap keamanan siber dapat memiliki berbagai konsekuensi yang signifikan, baik positif maupun negatif, tergantung pada tingkat kesadaran tersebut. Beberapa akibat dari kesadaran pengguna meliputi:

a. Pengurangan Risiko Keamanan Siber

Pengguna dengan tingkat kesadaran yang tinggi cenderung lebih mampu mengenali dan menghindari ancaman siber, seperti phishing, malware, dan serangan social engineering. Akibatnya, risiko keamanan siber secara keseluruhan dapat berkurang. Pengguna yang waspada akan lebih selektif dalam mengklik tautan, mengunduh file, dan membagikan informasi pribadi, yang semuanya berkontribusi pada lingkungan digital yang lebih aman (Siponen, Pahnila, & Mahmood, 2010).

b. Peningkatan Perlindungan Data Pribadi

Kesadaran yang baik terhadap praktik keamanan siber mendorong pengguna untuk mengambil langkah-langkah yang lebih proaktif dalam melindungi data pribadi mereka. Misalnya, mereka lebih mungkin untuk menggunakan kata sandi yang kuat, mengaktifkan otentikasi dua faktor, dan memperbarui perangkat lunak secara teratur. Hal ini dapat mengurangi kemungkinan data pribadi disalahgunakan atau dicuri oleh pihak yang tidak berwenang (Hong, 2012).

c. Dampak Positif pada Organisasi dan Komunitas

Di lingkungan organisasi atau komunitas, kesadaran pengguna yang tinggi dapat menciptakan budaya keamanan yang lebih kuat. Ketika individu lebih sadar akan ancaman siber dan berperilaku sesuai dengan praktik terbaik, organisasi dapat mengurangi insiden pelanggaran keamanan dan meningkatkan kepercayaan antara perusahaan dan pelanggannya. Ini juga dapat mengurangi biaya yang terkait dengan pemulihan dari serangan siber (Sommestad, Hallberg, Lundholm, & Bengtsson, 2014).

d. Peningkatan Ketahanan Digital

Dengan meningkatnya kesadaran pengguna, ketahanan digital suatu komunitas atau masyarakat terhadap serangan siber juga meningkat. Pengguna yang memiliki kesadaran tinggi cenderung lebih cepat dalam mendeteksi dan melaporkan ancaman, sehingga memungkinkan respon yang lebih cepat dan tepat. Ketahanan digital yang lebih baik membantu meminimalkan dampak dari serangan dan memungkinkan pemulihan yang lebih cepat (Ransbotham & Mitra, 2009).

e. Akibat Negatif dari Kesadaran yang Rendah

Sebaliknya, rendahnya kesadaran pengguna terhadap keamanan siber dapat menyebabkan konsekuensi yang merugikan. Pengguna yang tidak waspada cenderung menjadi target empuk bagi serangan siber, yang dapat menyebabkan pencurian identitas, kehilangan data, dan kerusakan finansial. Selain itu, kurangnya kesadaran dapat memicu penyebaran malware atau ransomware yang tidak disengaja melalui perangkat pengguna, yang berdampak pada individu lain atau bahkan jaringan organisasi secara keseluruhan (Dinev & Hu, 2007).

f. Konsekuensi Hukum dan Reputasi

Ketidakpatuhan terhadap praktik keamanan siber yang disebabkan oleh kurangnya kesadaran pengguna dapat mengakibatkan masalah hukum, terutama jika data pelanggan atau informasi sensitif lainnya terlibat. Hal ini dapat menyebabkan organisasi menghadapi tuntutan hukum atau denda. Selain itu, pelanggaran keamanan yang disebabkan oleh kelalaian pengguna dapat merusak reputasi organisasi atau individu, yang mungkin memerlukan waktu lama untuk dipulihkan (Herath & Rao, 2009).

Kesadaran atau *awareness* sendiri dapat disimpulkan dengan adanya kemampuan seseorang untuk menyadari ataupun mengenali hal-hal yang terjadi namun tidak ada tuntutan untuk keterlibatan dengan orang lain (individual). Kesadaran ini lebih merujuk ke pengamatan, perhatian, maupun pengalaman yang sedang dialami oleh diri sendiri (Vadila & Pratama, 2021)

Awareness yang tinggi dapat mengurangi risiko menjadi korban kejahatan phsihing file APK yang kerapkali terjadi saat ini. Ketika pengguna WhatsApp sadar dan mengetahui cara mengenali dan juga bagaimana merespon kejahatan phishing tersebut, maka pengguna sudah bisa melindungi informasi maupun data diri pribadi mereka (Alwanain, 2020)

2.3 Literasi Digital sebagai Salah Satu Kesadaran

Literasi digital sebagai salah satu kesadaran untuk mengantisipasi adanya phishing khususnya phishing file APK. Literasi digital sendiri merupakan sebuah kemahiran atau kecakapan dalam memanfaatkan adanya media digital seperti alat komunikasi digital dengan cermah dan juga bijak (Sihotang, 2022). Hal tersebut mencakup dengan adanya mengenali, memahami, hingga merespon suatu masalah. Alat komunikasi digital telah menggunakan proses yang didominasi dengan komunikasi yang tertulis seperti pesan jarak jauh (WhatsApp, Facebook, SMS, Mesengger, Email, dll). Kemampuan dalam literasi digital sangat perlu dilatih dan dibiasakan sedari dini agar penggunaannya bisa dengan bijak sehingga bisa mendorong produktivitas yang positif (Sihotang, 2022).

Mengenali phishing merupakan salah satu upaya kesadaran untuk mendeteksi adanya bahaya phishing file APK. Kemampuan mengenali ini merupakan langkah awal dari serangan siber khususnya phishing. Dalam literasi digital, lebih dituntut untuk kritis dengan adanya pesan-pesan yang kapan saja bisa menjadi serangan phsihing (Restianty, 2018)

Memahami terkait praktek phishing file APK menjadi salah satu tindakan edukasi terhadap adanya risiko kejahatan phishing file APK. Literasi digital tentu melibatkan dengan pemahaman-pemahaman yang lebih dalam terkait kejahatan siber termasuk phishing tersebut bekerja. Adanya pemahaman yang cukup seperti tahu akan modus hingga ciri-ciri phishing ini dapat disimpulkan bahwa pengguna lebih siap dengan adanya serangan phishing jika sewaktu-waktu menyerang di berbagai platform digital (Alwanain, 2020).

Merespon dengan bijak adanya tindakan siber khususnya phishing file APK dapat menyelamatkan dari kejahatan siber. Adanya literari digital yang cukup baik, pengguna dapat memverifikasi sebelum bertindak, hingga memeriksa kredibilitas suatu pesan phishing yang diterima. Literasi digital diciptakan untuk mendapatkan hingga menggunakan informasi dengan aman dan juga tepat (Wibowo & Fatimah, 2017).

2.4 WhatsApp sebagai Media Komunikasi

WhatsApp adalah aplikasi untuk mengirim pesan instan, jika dilihat dari tujuan utamanya, mirip dengan aplikasi SMS (Short Message Service) yang biasa digunakan di ponsel lama. Hanya saja, WhatsApp tidak menggunakan pulsa langsung seperti SMS, melainkan menggunakan layanan internet. Pengguna dapat mengirim pesan selama ponsel masih terhubung ke internet.

Selain itu, pengguna dapat mengirimkan file lunak dengan ekstensi PDF, dokumen, dan berbagai jenis dokumen lainnya (Pustikayasa, 2019).

WhatsApp merupakan aplikasi pesan instan yang memiliki fungsi untuk berkomunikasi jarak jauh atau secara tidak langsung. Sebagai media komunikasi, tentu WhatsApp juga berpotensi memiliki ancaman teknologi atau biasa disebut dengan *cybercrime*. Oleh karena itu, WhatsApp memiliki sistem keamanan *end to end*, sistem ini memungkinkan hanya antar pengirim dan penerima pesan saja yang dapat melihat juga membaca pesannya. Pihak WhatsApp dipastikan tidak dapat melihat dan membaca pesan tersebut.

Adanya sistem keamanan dan privasi dari WhatsApp, diharapkan pengguna mampu berkomunikasi secara aman. Sistem end to end mengamankan pesan-pesan yang dikirim dan diterima oleh pengguna dengan kode pengaman khusus yang dibuat oleh pengguna. (Pustikayasa, 2019).

Keamanan dan privasi WhatsApp tidak menjamin akan keamanan dan privasi data tiap penggunanya. Dalam konteks penggunaan WhatsApp, kebocoran data, penggunaan data pribadi untuk tujuan yang tidak diinginkan, serta serangan malware adalah beberapa ancaman untuk keamanan data saat pengguna menggunakan WhatsApp. Beberapa tindakan yang memungkinkan terjadinya kebocoran informasi pribadi yaitu, (1) berbagi informasi pribadi yang berlebihan seperti tanggal lahir hingga alamat, (2) membuka atau mengklik tautan yang tidak aman karena rentan mengalami serangan phishing atau pencurian data (Sari, Takariani, Pangaribuan, & Simatupang, 2023).

WhatsApp sebagai media komunikasi memiliki berbagai aspek yang menjadikannya salah satu platform komunikasi paling populer dan efektif di dunia. Salah satu keunggulan utama WhatsApp adalah aksesibilitasnya yang tinggi serta kemudahan penggunaannya. Aplikasi ini dirancang untuk dapat digunakan oleh semua kalangan, baik mereka yang terbiasa dengan teknologi digital maupun yang kurang terbiasa. WhatsApp tersedia secara gratis dan dapat diunduh serta digunakan di berbagai platform, termasuk smartphone Android, iOS, dan desktop melalui WhatsApp Web. Pengguna hanya perlu nomor telepon untuk mendaftar, yang menjadikan proses pengaturan akun sangat sederhana.

Selain itu, WhatsApp menawarkan fitur komunikasi yang komprehensif. Aplikasi ini tidak hanya memungkinkan pengguna untuk mengirim pesan teks, tetapi juga menyediakan fitur panggilan suara dan video dengan kualitas yang baik, baik secara individu maupun dalam grup.

Fitur pesan suara juga memungkinkan pengguna untuk merekam dan mengirim pesan audio, yang sangat berguna dalam situasi di mana mengetik tidak memungkinkan. Selain itu, WhatsApp mendukung pengiriman berbagai jenis file, termasuk gambar, video, dokumen, lokasi, dan kontak, menjadikannya alat yang sangat serbaguna untuk berbagi informasi. File tersebut sangat memudahkan pengguna untuk berkomunikasi lebih lanjut dan tidak hanya mengandalkan fitur chatting saja.

WhatsApp juga mendukung komunikasi kelompok melalui fitur grup chat, yang dapat mencakup hingga 1024 anggota. Fitur ini memungkinkan pengguna untuk berkomunikasi secara efektif dalam kelompok, baik itu untuk keluarga, teman, tim kerja, maupun komunitas yang lebih besar. Dengan adanya fitur-fitur tambahan seperti polling, penjadwalan acara, dan berbagi file, grup chat di WhatsApp mendukung kolaborasi yang efisien.

Keamanan dan privasi juga menjadi salah satu aspek utama yang ditawarkan oleh WhatsApp. Aplikasi ini menggunakan enkripsi end-to-end untuk semua komunikasi, yang berarti bahwa hanya pengirim dan penerima yang dapat melihat konten pesan, panggilan suara, dan video. WhatsApp sendiri tidak memiliki akses ke data pengguna, yang memastikan privasi komunikasi. Meskipun demikian, pengguna tetap perlu berhati-hati terhadap risiko keamanan lainnya seperti phishing, malware, dan kebocoran data.

WhatsApp juga memiliki fitur Status, yang mirip dengan fitur "Stories" pada platform lain seperti Instagram dan Facebook. Pengguna dapat berbagi foto, video, teks, dan GIF yang akan hilang setelah 24 jam, memungkinkan ekspresi diri yang lebih kreatif dan cara berinteraksi yang berbeda dengan kontak. Selain itu, WhatsApp memungkinkan komunikasi lintas batas secara global tanpa biaya tambahan, selama pengguna memiliki koneksi internet. Ini menjadikannya alat yang sangat kuat untuk berkomunikasi dengan teman, keluarga, dan rekan bisnis yang berada di lokasi yang berbeda.

Integrasi WhatsApp dengan layanan lain seperti WhatsApp Pay dan WhatsApp Business juga menambah nilai bagi pengguna. WhatsApp Business menyediakan fitur tambahan seperti balasan otomatis, profil bisnis, katalog produk, dan label untuk mengelola pelanggan, yang sangat berguna untuk usaha kecil dan menengah. Melalui WhatsApp Business, perusahaan dapat mengirim pemberitahuan, memberikan dukungan pelanggan, dan bahkan menjual produk atau layanan langsung melalui chat.

WhatsApp juga memainkan peran penting dalam situasi darurat atau krisis. Aplikasi ini sering digunakan untuk komunikasi cepat dalam situasi darurat seperti bencana alam atau keadaan darurat kesehatan, di mana informasi penting dapat dengan cepat disebarkan kepada banyak orang melalui grup chat atau pesan broadcast. Namun, meskipun WhatsApp memiliki banyak keunggulan, platform ini juga menghadapi tantangan, seperti risiko keamanan data dan penyebaran informasi yang salah atau hoaks.

2.5 Kejahatan Media Teknologi Informasi dan Komunikasi

Perkembangan teknologi informasi dan komunikasi (TIK) yang pesat memberikan dampak besar dalam kehidupan sehari-hari, baik secara positif maupun negatif. Salah satu dampak negatif yang paling nyata adalah peningkatan kejahatan siber yang menggunakan media teknologi sebagai platform untuk melakukan tindakan kriminal. Kejahatan ini memanfaatkan jaringan internet dan perangkat teknologi untuk menyerang individu, perusahaan, dan bahkan pemerintah. Bentuk-bentuk kejahatan yang dilakukan sangat beragam, mulai dari pencurian data, penipuan daring, penyebaran malware, hingga *phishing* dan serangan *ransomware*.

Salah satu aspek kejahatan teknologi informasi yang paling umum adalah *cybercrime*, yang mencakup berbagai tindakan ilegal yang dilakukan melalui sistem komputer. Menurut Statista (2022), kejahatan siber di seluruh dunia telah menyebabkan kerugian finansial yang sangat signifikan, dengan prediksi kerugian global mencapai triliunan dolar pada tahun-tahun mendatang. Pelaku kejahatan siber biasanya menargetkan data-data sensitif, seperti informasi kartu kredit, identitas pribadi, serta data perusahaan yang bernilai tinggi.

Kejahatan media TIK juga dapat berupa serangan terhadap infrastruktur digital kritis, seperti sistem keuangan, transportasi, dan energi. Serangan semacam ini dapat mengakibatkan kerusakan besar-besaran pada skala nasional, termasuk penutupan layanan penting atau bahkan penghentian operasi bisnis secara permanen. Di Indonesia, serangan siber seperti ini semakin meningkat seiring dengan adopsi teknologi digital yang masif di berbagai sektor (Setiadi, 2021).

Selain itu, teknologi komunikasi juga menjadi sarana untuk menyebarkan konten-konten ilegal, seperti pornografi, ujaran kebencian, dan propaganda terorisme. Hal ini menciptakan tantangan besar bagi pemerintah dan penegak hukum untuk mengawasi dan menangani penyebaran informasi berbahaya tersebut di internet (Suryani, 2020).

Dalam konteks kejahatan teknologi informasi dan komunikasi, kesadaran dan pemahaman pengguna terhadap potensi ancaman menjadi sangat penting. Pengguna yang kurang memahami

risiko kejahatan di dunia digital rentan menjadi korban serangan. Oleh karena itu, literasi digital harus ditingkatkan untuk meminimalkan risiko terpapar kejahatan media, dengan edukasi mengenai bagaimana mengidentifikasi ancaman siber dan cara melindungi diri dari serangan tersebut.

Masyarakat tentu sudah tidak mengalami kesulitan dalam mengakses informasi dari seluruh penjuru dunia. Pesatnya perkembangan teknologi informasi dan komunikasi ini tentu diiringi dengan oknum yang sengaja menyalahgunakan kemajuan teknologi. Biasa disebut kejahata siber, atau *cybercrime*. Kejahatan ini terjadi di dunia maya dan tentunya merugikan banyak pihak (Habibi, 2020).

Semakin majunya teknologi, semakin banyak dan berkembang pula jenis-jenis kejahatan siber di media. Salah satu contoh yang terbaru ialah praktik phishing file.apk. Phishing merupakan salah satu kejahatan di dunia digital yang cukup berbahaya. Phising sendiri merupakan upaya pencurian informasi pribadi pengguna, seperti kartu kredit dan debit, hingga data pribadi lainnya seperti alamat rumah (Alwanain, 2020).

Informasi pribadi mencakup beberapa hal yang penting untuk kehidupan seseorang yang harusnya hanya diketahui oleh individu masing-masing. Nama lengkap, tempat dan tanggal lahir, nomor induk kependudukan, hingga nomor telepon adalah data-data yang harus dilindungi. Jika tidak, dapat menyebabkan penyalahgunaan data dan kerugian, seperti penipuan, penyadapan, hingga peminjaman uang (Ramadhan, Alhafidh, & Firmansyah, 2022).

2. 6 Fenomena Phising

Phishing adalah suatu metode penipuan siber di mana pelaku berusaha untuk mendapatkan informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya dengan menyamar sebagai entitas yang tepercaya. Istilah "phishing" berasal dari kata "fishing" (memancing), yang menggambarkan upaya pelaku untuk "memancing" korban agar memberikan informasi mereka secara sukarela. Dalam konteks digital, phishing sering dilakukan melalui email, pesan teks, atau aplikasi pesan instan seperti WhatsApp, di mana pengguna diarahkan untuk mengunduh file atau mengklik tautan berbahaya yang tampak sah (Jagatic, Johnson, Jakobsson, & Menczer, 2007). Phishing berkembang menjadi berbagai bentuk yang lebih spesifik, seperti spear phishing, di mana serangan ditargetkan pada individu atau organisasi tertentu dengan menggunakan informasi yang dipersonalisasi, dan whaling, yang menargetkan individu dengan profil tinggi seperti eksekutif perusahaan. Meskipun metode dan targetnya mungkin berbeda,

tujuan akhir dari semua serangan phishing adalah untuk mengecoh korban agar memberikan informasi pribadi mereka.

Phishing dapat muncul dalam berbagai bentuk, dan pelaku seringkali menggunakan berbagai teknik untuk menipu korban. Beberapa bentuk dan teknik phishing yang umum meliputi:

a. Email Phishing

   Email phishing adalah bentuk paling umum dari phishing, di mana pelaku mengirimkan email yang tampak berasal dari sumber yang tepercaya seperti bank, perusahaan teknologi, atau layanan online. Email ini sering kali berisi tautan ke situs web palsu yang dirancang untuk meniru situs asli, atau berisi lampiran berbahaya yang dapat menginstal malware di perangkat korban (Hong, 2012).

b. Spear Phishing

   Spear phishing adalah serangan yang lebih terfokus dan dipersonalisasi, di mana pelaku menargetkan individu tertentu menggunakan informasi yang telah dikumpulkan sebelumnya. Serangan ini seringkali lebih sulit dikenali karena email atau pesan yang dikirim mungkin berisi informasi yang relevan dan spesifik tentang korban, seperti nama, posisi, atau hubungan profesional mereka (Symantec, 2018).

c. Whaling

   Whaling adalah bentuk spear phishing yang menargetkan individu dengan posisi penting atau profil tinggi, seperti CEO atau manajer senior. Serangan ini dirancang untuk menipu target agar mengungkapkan informasi yang sangat sensitif atau untuk melakukan transfer dana ke rekening pelaku (Harvey & Bray, 2015).

d. Vishing dan Smishing

   Vishing (voice phishing) melibatkan penggunaan panggilan telepon untuk menipu korban agar memberikan informasi pribadi, sementara smishing (SMS phishing) menggunakan pesan teks atau aplikasi pesan instan seperti WhatsApp untuk mencapai tujuan yang sama. Dalam kedua kasus ini, pelaku seringkali menyamar sebagai perwakilan resmi dari organisasi tepercaya (Dhamija, Tygar, & Hearst, 2006).

e. Phishing melalui File.APK

   File.APK adalah format file yang digunakan untuk mendistribusikan dan menginstal aplikasi pada perangkat Android. Dalam konteks phishing, pelaku dapat mengirimkan file.APK berbahaya yang tampak seperti aplikasi sah, tetapi sebenarnya berisi malware

yang dapat mencuri informasi pengguna atau mengendalikan perangkat mereka. Phishing melalui file.APK biasanya dilakukan melalui aplikasi pesan instan seperti WhatsApp, di mana pengguna menerima file yang tampak tidak berbahaya dari kontak yang dikenal atau dari sumber yang tidak dikenal (Almomani et al., 2013).

Mekanisme phishing terdiri dari beberapa tahap yang dirancang untuk menipu dan mengeksploitasi korban. Tahap-tahap ini meliputi:

a. Pengumpulan Informasi

   Sebelum meluncurkan serangan phishing, pelaku sering kali mengumpulkan informasi tentang target mereka. Informasi ini dapat mencakup data pribadi yang diperoleh dari media sosial, rekaman publik, atau kebocoran data. Pengumpulan informasi ini memungkinkan pelaku untuk menyesuaikan serangan mereka agar lebih efektif dan sulit dikenali oleh korban (Jakobsson & Myers, 2007).

b. Penyamaran

   Dalam tahap ini, pelaku menciptakan tampilan yang meyakinkan dengan menyamar sebagai entitas tepercaya. Ini bisa berupa email dengan alamat pengirim yang tampak sah, situs web palsu yang meniru desain dan URL dari situs asli, atau bahkan pesan WhatsApp yang tampaknya berasal dari kontak yang dikenal. Penyamaran ini adalah kunci keberhasilan phishing karena membuat korban percaya bahwa mereka berinteraksi dengan entitas yang sah (Dhamija et al., 2006).

c. Eksploitasi Psikologis

   Pelaku sering kali menggunakan teknik manipulasi psikologis untuk meningkatkan peluang keberhasilan serangan mereka. Teknik ini meliputi penciptaan rasa urgensi (misalnya, "Akun Anda akan diblokir jika tidak merespons dalam 24 jam"), ketakutan (misalnya, "Ada upaya login yang mencurigakan dari lokasi yang tidak dikenal"), atau ketertarikan (misalnya, "Anda memenangkan hadiah! Klik di sini untuk mengklaimnya"). Teknik-teknik ini dirancang untuk mendorong korban mengambil tindakan cepat tanpa berpikir panjang (Workman, 2008).

d. Pelaksanaan Serangan

   Setelah korban termanipulasi, pelaku meluncurkan serangan dengan mengarahkan korban ke situs web palsu, mengunduh file berbahaya, atau mengungkapkan informasi pribadi mereka. Dalam kasus phishing file.APK, serangan ini biasanya melibatkan korban yang

mengunduh dan menginstal file.APK berbahaya yang kemudian memberikan pelaku akses ke data atau kontrol atas perangkat korban (Jagatic et al., 2007).

e. Pengumpulan dan Eksploitasi Data

Setelah serangan berhasil, pelaku mulai mengumpulkan data yang telah dicuri, seperti kredensial login, informasi kartu kredit, atau data pribadi lainnya. Data ini kemudian dapat digunakan untuk tujuan yang lebih lanjut, seperti pencurian identitas, penipuan keuangan, atau dijual di pasar gelap. Dalam beberapa kasus, pelaku juga dapat menggunakan perangkat yang telah terinfeksi untuk meluncurkan serangan lebih lanjut atau sebagai bagian dari botnet (Hong, 2012).

Phishing memiliki dampak yang signifikan terhadap pengguna, baik secara individual maupun organisasi. Dampak ini meliputi:

a. Pencurian Identitas

Informasi pribadi yang dicuri melalui phishing dapat digunakan untuk mencuri identitas korban, yang dapat mengakibatkan kerugian finansial, reputasi yang rusak, dan masalah hukum bagi korban (Jagatic et al., 2007).

b. Kerugian Finansial

Phishing sering kali bertujuan untuk mendapatkan akses ke rekening bank atau kartu kredit korban, yang dapat mengakibatkan pencurian dana. Selain itu, biaya pemulihan dari serangan phishing, termasuk perlindungan identitas dan pemulihan akun, dapat menjadi beban finansial tambahan bagi korban (Harvey & Bray, 2015).

c. Kehilangan Privasi

Data pribadi yang diambil melalui phishing dapat digunakan oleh pelaku atau pihak ketiga untuk memantau, melacak, atau mengeksploitasi korban dalam berbagai cara. Ini mengakibatkan hilangnya privasi dan rasa aman bagi korban (Dhamija et al., 2006).

d. Kerusakan Reputasi

Bagi individu atau organisasi, menjadi korban phishing dapat merusak reputasi mereka. Misalnya, jika data pelanggan bocor karena serangan phishing, kepercayaan pelanggan terhadap organisasi tersebut dapat menurun drastis (Jakobsson & Myers, 2007).

Kejahatan Phishing sendiri merupakan tindakan mengancam hingga menjebak korbannya dengan konsep memancing korban. Jika korban tidak memiliki kesadaran yang tinggi adanya kejahatan phishing, informasi data privasi korban yang menjadi taruhannya. Banyak pengguna aplikasi yang

tidak menyadari adanya ancaman-ancaman kejahatan seperti phishing tersebut. Mereka menganggap sepele dan tidak perlu dipikir terlalu dalam. Namun, hingga saat ini banyak pengguna media sosial yang telah terjebak dalam phishing. Pelaku phishing tersebut melakukan kejahatannya dengan memberi link atau dokumen palsu dan mengirimkan ke media sosial korban. Jika korban tidak berhati-hati, pelaku dapat dengan mudah mengambil uang hingga data privasi korbannya (Wibowo & Fatimah, 2017).

Sumber-sumber ancaman phishing, yaitu email, website, dan malware. Peneliti akan menganalisis sumber phishing yang berasal dari malware. Malware sendiri merupakan suatu program komputer yang dibuat untuk merusak hingga mencuri data pengguna, biasanya berupa aplikasi. Penelitian ini membahas phishing di aplikasi WhatsApp yang merupakan dari sumber malware. Cara kerja phishing melalui malware ini yaitu dengan cara berpura-pura untuk meminta tolong korbannya mendownload file yang dikirim oleh pelaku. File tersebut dapat dengan cepat mencuri data korban jika korban tidak sadar akan adanya phishing (Wibowo & Fatimah, 2017).

"File.apk" merupakan salah satu modus phishing yang terjadi di aplikasi WhatsApp. "file.apk" ini berupa dokumen yang berjenis "APK". Tidak seperti dokumen yang dikirimkan pada umumnya yang berjenis PDF, WORD, hingga PPT, dokumen berjenis "APK" ini telah menjadi sarana phishing yang kerap kali ditemui. "file.apk" ini merupakan bentuk format aplikasi untuk smartphone berbasis android.

Penipuan yang menggunakan "file.apk" ini dikirimkan secara berurutan melalui chat atau ruang obrolan di sosial media WhatsApp dengan berbagai modus. Contoh modus yang kerap kali ditemukan ialah, modus surat undangan pernikahan, file cek resi paket, tagihan pembayaran, hingga surat tilang polisi. Akibatnya, setelah aplikasi ini diinstal, pelaku dapat dengan mudah menyadap data keamanan penting seperti kode *One Time Passwor*d (OTP), pin, *password,* hingga *e-wallet* korban. Setelah pelaku mendapatkan data keamanan korban tersebut, pelaku dapat menyalahgunakan untuk kepentingan pribadinya seperti mencuri seluruh saldo *m-banking* atau *e-wallet* korban (Sali & Sari, 2023).

Adanya isu terkait penipuan phishing "file.apk" di aplikasi pesan instan WhatsApp yang dapat mengambil data keamanan seseorang, maka diperlukan suatu kesadaran tiap individu yang memiliki aplikasi WhatsApp agar lebih waspada jika ada yang mengirim pesan berupa dokumen atau "file,apk".

2.7 Kesadaran terhadap Kejahatan Melalui Media Baru (Phishing file.apk di Aplikasi WhtasApp)

Banyaknya kejahatan siber disekitar kita, tentu menumbuhkan kewaspadaan bagi pengguna. Sebagai media baru, WhatsApp baru-baru ini digemparkan oleh adanya tindakan praktik phishing yang dapat mengambil data pribadi korban sebagai pengguna media WhatsApp.

Sebagai pengguna WhatsApp, perlu adanya kesadaran tinggi untuk mencegah terjadinya kebocoran data dan privasi pengguna. Kesadaran pengguna akan keamanan informasi tentu berpengaruh besar pada sikap individu untuk pembentukan perilaku peduli atau sadar keamanan informasi (Sari, Takariani, Pangaribuan, & Simatupang, 2023).

Pelaku kejahatan phishing dapat dengan mudah mengumpulkan, mengungkapkan, dan menggunakan data pribadi korban "file.apk" tanpa persetujuan korbannya. Kondisi ini tentu mengakibatkan hal yang tidak diinginkan oleh siapa saja. Jika informasi pribadi dengan mudah diakses tanpa izin, maka pengguna aplikasi WhatsApp harus semakin waspada dengan adanya tindakan kejahatan phishing berupa "file.apk".

Tindakan pencegahan diperlukan untuk mencegah penyebaran penipuan "file.apk" yang dapat menyadap data pribadi pengguna WhatsApp. Adanya kesadaran keamanan informasi pengguna WhatsApp, akan dapat mengurangi risiko penipuan phishing terkhususnya phishing "file.apk". Pengguna WhatsApp yang baik perlu memahami dengan seksama segala hal yang bisa saja terjadi dari mana saja. Umumnya terkait informasi pribadi yang memiliki risiko tinggi jika orang lain atau pelaku phishing tahu dan menggunakan untuk kejahatan lainnya (Alif & Pratama, 2020).

2.8 Teori Pemrosesan Informasi

Media komunikasi dapat berfungsi sebagai alat untuk memperluas dan memperkuat pengaruh mereka dalam pemikiran dan tindakan manusia. Dengan kata lain, setiap penemuan baru dalam teknologi komunikasi sedang dipertimbangkan untuk memperluas kemampuan manusia itu sendiri (Surahman, 2016). Jika sebagai individu tidak dapat dengan baik memanfaatkan teknologi komunikasi yang ada, maka hal-hal seperti kejahatan siber bisa terus terjadi tanpa henti. Pada hakikatnya, semakin hari maka teknologi semakin maju. Individu semakin pintar mencari celah guna melakukan kejahatan siber demi kepentingan pribadi.

Selanjutnya, terdapat pula teori pemrosesan informasi (*information processing theory*) oleh Robert Mills Gagne. Teori ini menyebutkan bahwa pemrosesan informasi dapat membantu

memahami terkait pembelajaran merupakan faktor yang penting serta mengingat kembali informasi yang dikontrol oleh otak. Perkembangan tersebut adalah hasil dari belajar yang terus berulang. Bagaimana seseorang merespon akan tindakan interaksi yang terjadi (kejadian phishing) hingga akhirnya dapat pembelajaran (Suryana, Lestari, & Harto, 2022)

Gagne memberikan empat fase dalam pemrosesan informasi, sebagai berikut:

1. Receiving the Stimulus Situation (Menerima Situasi Stimulus)

   Fase dimana seseorang akan dihadapkan dengan adanya situasi yang memicu pemrosesan informasi lebih lanjut. Tahapan ini sangat penting karena seseorang akan menganalis atau memperhatikan suatu kejadian. Dalam penelitian ini, pengguna WhatsApp akan dihadapi dengan ancaman seperti menerima pesan phishing dari nomor tidak dikenal maupun nomor yang dikenal. Selanjutnya pengguna akan masuk di tahap pemrosesan infromasi untuk menerka-nerka apakah pesan tersebut termasuk pesan phishing atau tidak.
2. Stage of Acquisition (Tahap Akuisisi)

   Fase ini merupakan tahapan dimana seseorang akan membentuk berbagai kumpulan antara informasi baru maupun informasi yang lama. Informasi-informasi tersebut akan digunakan sebagai rujukan dimana pengguna WhatsApp memiliki pengetahuan dan juga pemahaman terkait ancaman phishing file APK serta tahu akan cara menanggulanginya.
3. Storage (Penyimpanan)

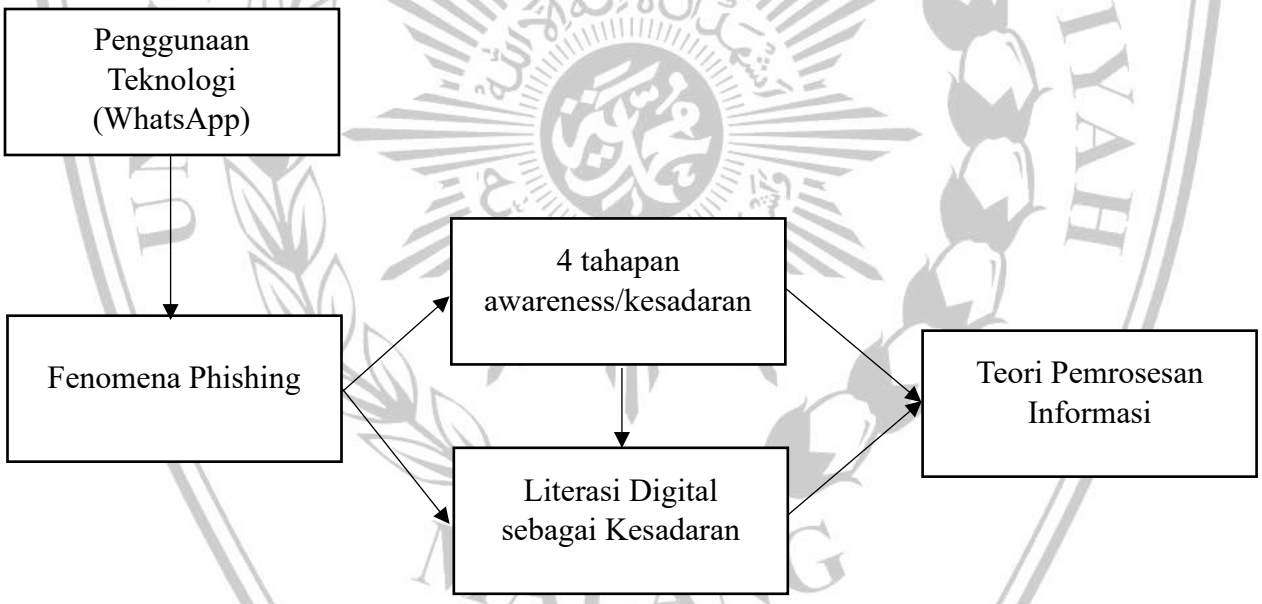
   Tahapan ini, seseorang akan menyimpan informasi yang telah dipelajari dalam memori mereka. Nantinya, jika pengguna WhatsApp akan dihadapkan dengan adanya pesan phishing, pengguna akan tahu apa yang harus dilakukan. Sehingga, tidak ada kerugian maupun kesalahan akibat tidak adanya informasi yang dimiliki.
4. Retriveal (Pengambilan Kembali)

   Fase ini merupakan fase mengingat kembali informasi yang ada di dalam memori. Kemampuan pengguna ini untuk mengambil informasi yang telah disimpan sehingga pengguna dapat dengan mudah mengenali dan juga menanggapi ancaman phishing dengan baik. Adanya retriveal ini dapat meningkatkan kesiapan pengguna WhatsApp dalam menghadapi situasi yang berbahaya utamanya kejahatan siber berupa phishing.

Teori tersebut dapat menjelaskan bahwa pemrosesan infromasi merupakan proses yang tidak akan terputus mengingat semuanya akan selalu belajar dari pengalaman yang bisa berulang. Pemahaman yang mendalam terkait adanya serangan siber khususnya phishing file APK ini diperoleh dari adanya edukasi dalam mengenali tanda-tanda phsihing. Tidak hanya meningkatkan kesadaran saja, tapi juga akan memperkuat kemampuan mereka untuk melindungi ancaman siber (Suryana, Lestari, & Harto, 2022)

2.9 Kerangka Pemikiran

Adapun kerangka pemikiran yang dibuat untuk mengetahui tingkat kesadaran mahasiswa ilmu komunikasi Universitas Muhammadiyah Malang sebagai pengguna WhatsApp terhadap ancaman phishing "file.apk" dan dengan adanya pesan WhatsApp yang tidak dikenal. Berikut konsep kerangka pemikiran penelitian tingkat kesadaran pengguna WhatsApp terhadap ancaman phishing "file.apk" dengan adanya pesan WhatsApp tidak dikenal.



Penggunaan teknologi (WhatsApp) menjadi titik awal untuk mempengaruhi berbagai faktor psikologis dan sosial yang berkontribusi terhadap kesadaran phishing pengguna. Sebagai teknologi komunikasi instan yang sangat populer, WhatsApp menawarkan banyak kemudahan kepada penggunanya dalam bertukar informasi, namun juga meningkatkan risiko paparan ancaman dunia maya seperti phishing melalui file.APK. Pemanfaatan teknologi ini tidak hanya bersifat

pasif, namun juga membentuk perilaku pengguna melalui pola interaksi dan paparan risiko yang ada di dunia digital.

Pengguna yang memiliki sikap positif terhadap perlindungan data pribadi akan lebih berhati-hati dalam membuka pesan atau file yang mencurigakan. Pengalaman pengguna dengan WhatsApp dan paparan terhadap risiko-risiko digital akan memengaruhi bagaimana mereka menilai pentingnya menjaga keamanan, yang pada akhirnya meningkatkan atau mengurangi kesadaran mereka terhadap ancaman phishing.

Lebih lanjut, dalam diagram ini, norma subjektif berperan sebagai variabel mediasi yang menghubungkan penggunaan WhatsApp dengan persepsi pengguna terhadap ancaman siber. Norma subjektif mengacu pada tekanan sosial yang dirasakan pengguna dari lingkungannya, seperti keluarga, teman, dan rekan kerja. Tekanan ini dapat mempengaruhi keputusan pengguna apakah akan merespons pesan yang berisi file APK, terutama jika pesan tersebut berasal dari sumber yang dikenal.

Dalam konteks ini, norma subjektif menjadi penting karena menunjukkan bahwa keputusan untuk membuka file berbahaya tidak hanya dipengaruhi oleh kesadaran individu tentang keamanan, tetapi juga oleh ekspektasi sosial yang mereka rasakan. Misalnya, seseorang mungkin merasa perlu membuka file yang dikirim oleh seorang teman, meskipun mereka ragu tentang keamanannya, karena adanya tekanan sosial untuk merespons pesan dari kontak yang dikenal.

Persepsi kontrol perilaku juga berperan penting dalam memengaruhi persepsi pengguna terhadap ancaman phishing. Kontrol perilaku yang dirasakan mengacu pada keyakinan pengguna tentang kemampuan mereka mengendalikan situasi dan melindungi diri dari ancaman dunia maya. Pengguna yang merasa memiliki kendali lebih besar atas perangkatnya karena pengetahuan teknis atau pengalaman menghadapi ancaman dunia maya cenderung terhindar dari serangan phishing.

Pengguna ini akan lebih waspada dalam mengevaluasi file.APK yang mencurigakan dan cenderung mengambil langkah preventif seperti tidak mengunduh atau membuka file dari sumber yang tidak dikenal. Persepsi kontrol perilaku ini menunjukkan bahwa keyakinan individu terhadap kemampuan mereka dalam menghadapi ancaman siber sangat berpengaruh terhadap kesadaran mereka terhadap phishing.

2. 10 Penelitian Terdahulu

Identitas Penelitian	Hasil Penelitian	Perbedaan Penelitian
Judul: "Analisis Faktor-faktor yang Mempengaruhi Kesadaran Pengguna terhadap Keamanan Informasi pada Aplikasi WhatsApp" Penulis: Andi Wijaya, Siti Nurjanah Jurnal: Jurnal Sistem Informasi, Vol. 12, No. 3, 2021	Penelitian ini menemukan bahwa faktor pengetahuan tentang keamanan informasi, pengalaman sebelumnya dengan serangan siber, dan kepercayaan terhadap aplikasi berperan signifikan dalam meningkatkan kesadaran pengguna terhadap ancaman keamanan, termasuk phishing, di WhatsApp.	Penelitian ini berfokus pada faktor-faktor internal pengguna seperti pengetahuan dan pengalaman, sedangkan penelitian yang sedang saya lakukan lebih menekankan pada bagaimana pengguna bereaksi terhadap ancaman phishing secara spesifik, termasuk perilaku yang dapat mengurangi risiko serangan.
Judul: "Pengaruh Sosialisasi Digital terhadap Pencegahan Phishing pada Pengguna Media Sosial di Indonesia" Penulis: Ahmad Fauzi, Rini Marlina Jurnal: Jurnal Komunikasi dan Informatika, Vol. 8, No. 2, 2020	Penelitian ini menunjukkan bahwa sosialisasi digital yang dilakukan oleh pihak berwenang atau organisasi non-profit memiliki efek signifikan dalam meningkatkan kesadaran dan pencegahan terhadap phishing di kalangan pengguna media sosial.	Sementara penelitian ini menekankan peran sosialisasi dari pihak eksternal, penelitian saya lebih fokus pada respons individu terhadap ancaman phishing secara langsung dalam konteks penggunaan WhatsApp.
Judul: "Studi Tentang Kesadaran Keamanan Informasi pada Pengguna Smartphone di Kalangan Mahasiswa" Penulis: Dian Prasetyo, Nurul Hidayah	Penelitian ini menemukan bahwa kesadaran tentang keamanan informasi di kalangan mahasiswa masih rendah, terutama terkait dengan ancaman seperti malware dan phishing,	Penelitian ini berfokus pada kesadaran umum terhadap keamanan informasi di kalangan mahasiswa, sementara penelitian saya lebih spesifik pada kesadaran terhadap praktik phishing di aplikasi WhatsApp.

Jurnal: Jurnal Teknologi Informasi dan Komputer, Vol. 9, No. 1, 2021	meskipun penggunaan smartphone sangat tinggi.	
Judul: "Tingkat Kesadaran Pengguna WhatsApp di Indonesia Terhadap Ancaman Phishing: Sebuah Survei Nasional" Penulis: Rahmat Hidayat, Lina Kartika Jurnal: Jurnal Keamanan Siber, Vol. 6, No. 4, 2022	Survei ini menemukan bahwa sebagian besar pengguna WhatsApp di Indonesia tidak sepenuhnya sadar akan ancaman phishing yang menyebar melalui pesan dan file berbahaya. Selain itu, tingkat pendidikan dan usia pengguna berhubungan dengan kesadaran terhadap ancaman ini.	Penelitian ini memberikan data kuantitatif yang luas tentang kesadaran phishing, sementara penelitian saya akan mengkaji lebih dalam tentang faktor-faktor yang memengaruhi perilaku spesifik terhadap phishing.
Judul: "Strategi Pencegahan Phishing pada Aplikasi Pesan Instan Berbasis Smartphone" Penulis: Yuliana Sari, Budi Santoso Jurnal: Jurnal Teknologi dan Keamanan, Vol. 7, No. 2, 2022	Penelitian ini mengusulkan beberapa strategi pencegahan phishing, termasuk pengembangan fitur keamanan yang lebih canggih pada aplikasi pesan instan seperti WhatsApp, serta pentingnya pendidikan pengguna tentang bahaya phishing.	Penelitian ini lebih fokus pada solusi teknis dan kebijakan untuk mencegah phishing, sementara penelitian saya lebih mengarah pada pemahaman perilaku pengguna dan kesadaran terhadap ancaman phishing.