BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah mengubah cara kita berinteraksi, berkomunikasi, dan berbagi informasi. Teknologi ini tidak hanya mempercepat proses komunikasi, tetapi juga memperluas jangkauan interaksi tanpa batasan geografis, memungkinkan orang untuk terhubung secara real-time di seluruh dunia. Namun, kemajuan tersebut juga memaksa masyarakat untuk beradaptasi dengan konsekuensi yang muncul, seperti meningkatnya ketergantungan terhadap teknologi dan risiko keamanan siber. Perkembangan teknologi informasi tersebut, menjadikan tak sedikit masyarakat yang harus mengikuti konsekuensi teknologi informasi tersebut (Nurudin, 2019). Masyarakat kini harus lebih bijak dalam menggunakan teknologi agar tidak terjerumus dalam ancaman digital, seperti penipuan online dan serangan siber lainnya. Seiring dengan itu, muncul kebutuhan akan literasi digital yang lebih baik agar pengguna dapat memanfaatkan teknologi secara aman dan efektif.

Aplikasi pesan instan telah menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari, memungkinkan orang untuk berkomunikasi dengan cepat, mudah, dan efisien. Dalam era digital ini, aplikasi seperti WhatsApp, Telegram, dan Line menjadi platform utama untuk berbagi pesan teks, gambar, video, hingga dokumen, menggantikan cara-cara tradisional seperti SMS atau telepon. Berdasarkan data dari Statista, pada tahun 2022, pengguna aplikasi pesan instan di seluruh dunia mencapai lebih dari 3 miliar orang, mencerminkan betapa pentingnya peran aplikasi ini dalam kehidupan modern. Selain itu, fleksibilitasnya dalam memungkinkan percakapan individu maupun kelompok menjadikannya alat komunikasi utama, baik untuk keperluan pribadi maupun profesional. Penggunaannya juga semakin meluas karena kemudahan akses dan fitur-fitur tambahan seperti enkripsi, panggilan video, dan berbagi lokasi secara real-time. Kehadiran aplikasi ini telah mengubah cara kita berinteraksi, membuat komunikasi lintas batas geografis menjadi lebih efisien dan terjangkau bagi banyak orang di seluruh dunia.

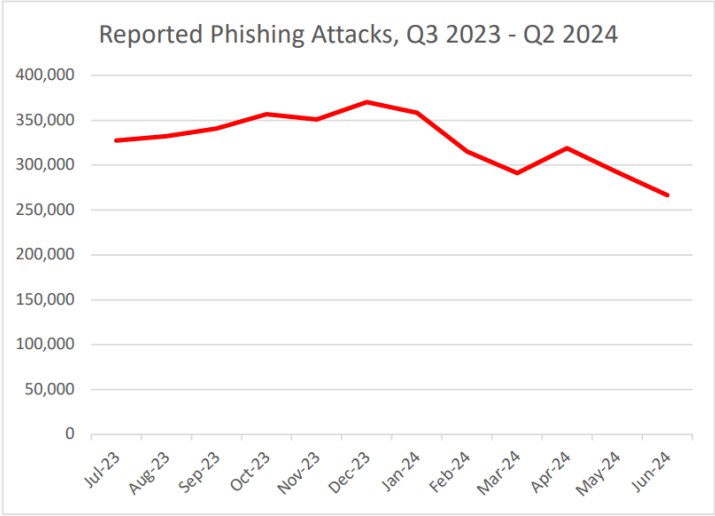
Salah satu aplikasi pesan instan yang paling banyak digunakan oleh masyarakat adalah Aplikasi WhatsApp. WhatsApp adalah salah satu *platform* yang mendominasi dalam hal tersebut. WhatsApp, dengan fitur-fiturnya yang canggih dan mudah digunakan, telah memungkinkan miliaran orang di seluruh dunia untuk terhubung satu sama lain dalam waktu

nyata tanpa batasan geografis. WhatsApp adalah salah satu aplikasi berbasis *mobile* yang paling populer. Popularitasnya meningkat karena fitur seperti harga terjangkau, privasi, dan kemampuan untuk mengirim pesan secara *real-time* ke individu atau sekelompok teman secara bersamaan (Cetinkaya, 2017).

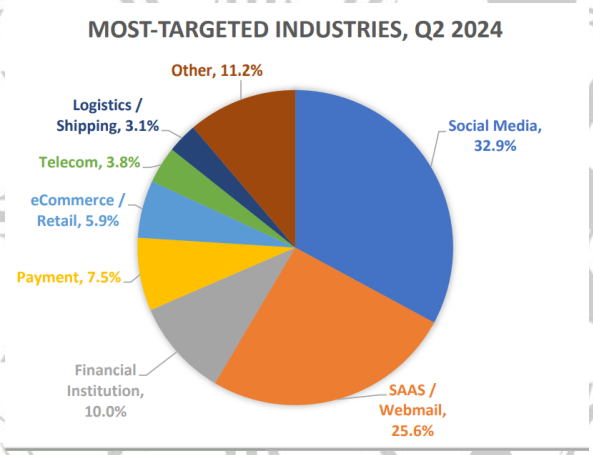
Aplikasi ini memfasilitasi pertukaran pesan teks, suara, gambar, video, dan berbagai jenis file lainnya. Pengguna WhatsApp dapat berkomunikasi dengan teman, keluarga, rekan kerja, dan berbagai kelompok sosial dengan cepat dan efisien. Dilansir dari databoks.katadata.co.id, Aplikasi WhatsApp sendiri merupakan aplikasi pesan instan yang menguasai pasar global pada tahun 2020. Aplikasi tersebut mampu menggaet 2 miliar pengguna aktif. Adanya hal tersebut membuktikan bahwa WhatsApp merupakan aplikasi yang cukup populer di kalangan Masyarakat (Purparisa, 2021).

Seiring dengan berbagai manfaat yang ditawarkan oleh WhatsApp, seperti kemudahan berkomunikasi dan fitur keamanan berupa enkripsi end-to-end, platform ini juga menjadi sasaran empuk bagi para penjahat siber yang memiliki niat jahat. Popularitas WhatsApp, dengan lebih dari 2 miliar pengguna aktif, menjadikannya target menarik bagi pelaku kejahatan siber yang memanfaatkan kelemahan atau ketidaktahuan pengguna. Salah satu ancaman yang sering terjadi adalah serangan phishing, di mana penjahat siber mencoba mencuri informasi pribadi seperti kata sandi, nomor kartu kredit, atau data sensitif lainnya dengan menyamar sebagai entitas tepercaya melalui pesan palsu. WhatsApp juga sering menjadi media penyebaran malware melalui file atau tautan yang dikirimkan dalam pesan, yang jika diakses oleh korban dapat merusak perangkat atau mencuri data pribadi. Dengan perkembangan teknologi yang semakin canggih, ancaman-ancaman ini juga semakin kompleks, memaksa pengguna untuk lebih waspada dan meningkatkan literasi digital guna melindungi diri dari risiko tersebut.

Salah satu metode yang paling banyak digunakan dalam kejahatan siber adalah teknik phishing. Phishing adalah tindakan kriminal yang menggunakan teknik rekayasa sosial. Pelaku phishing berusaha mendapatkan informasi pribadi seperti nama pengguna, kata sandi, dan detail kartu kredit yang dapat digunakan untuk pencurian identitas (Vadila & Pratama, 2021). Berdasarkan website *Anti-Phishing Working Group* (APWG), telah mencatat data gambar sebagai berikut:



Gambar 1



Gambar 2

Gambar 1 menunjukkan aktivitas ancaman phishing di kuarter tiga tahun 2023 hingga kuarter dua di tahun 2024. Sebanyak 350.000 lebih ancaman phishing yang terjadi di dunia hingga puncaknya pada Desember 2023 dengan 350.000 lebih ancaman phishing dan mulai turun di Maret 2024 dengan angka ancaman phishing 300.000. Angka tersebut masih terbilang banyak.

Gambar 2 menunjukkan industri-industri yang paling banyak ditargetkan oleh pelaku phising. Paling tinggi 32,9% yaitu sosial media. Posisi tertinggi kedua yaitu SAAS/Webmail dengan 25,6% perbandingan cukup lumayan sangat tipis dengan sosial media. Sisanya yaitu

shipping, *telecom, e-commerce, retail, payment*, dan lainnya. Disini menunjukkan bahwasannya sosial media menunjukkan angka tinggi dengan adanya ancaman phishing.

Serangan phishing semakin canggih seiring dengan perkembangan teknologi internet dan layanan online, kejahatan semacam ini menimbulkan ancaman terhadap keamanan internet. Akibatnya, phishing telah menjadi salah satu masalah paling sulit untuk diatasi (Alwanain, 2020). Dengan teknik-teknik baru seperti spear-phishing, yang menargetkan individu atau organisasi tertentu dengan pesan yang sangat personal, pelaku dapat mencuri informasi berharga pengguna. Kejahatan semacam ini menimbulkan ancaman serius terhadap keamanan internet, karena phishing tidak hanya mempengaruhi individu tetapi juga perusahaan besar dan instansi pemerintah yang menyimpan data dalam jumlah besar. Para penjahat siber terus mengembangkan metode mereka, seperti menggunakan domain palsu yang sangat mirip dengan yang asli atau mengirimkan tautan yang tampak sah tetapi berisi malware. Sumber-sumber ancaman phishing melalui literatur phishing berdasarkan survey, yaitu email, website, dan malware. Hal ini membuat phishing menjadi salah satu masalah paling sulit untuk diatasi, karena meskipun ada peningkatan dalam teknologi keamanan siber, teknik phishing terus beradaptasi dan berevolusi (Alwanain, 2020). Dalam banyak kasus, faktor manusia menjadi titik lemah, di mana kurangnya kesadaran atau kewaspadaan membuat pengguna lebih rentan terhadap jebakan digital ini. Karena kompleksitas dan sifat serangan yang terus berubah, upaya untuk mengatasi phishing membutuhkan kombinasi antara teknologi yang lebih canggih dan edukasi berkelanjutan bagi pengguna internet.

Berdasarkan permasalahan tersebut, 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 (Wibowo & Fatimah, 2017). Malware, atau malicious software, adalah program komputer yang dirancang secara khusus untuk menyusup, merusak, atau mencuri data dari perangkat pengguna tanpa sepengetahuan atau izin mereka. Jenis-jenis malware sangat beragam, mulai dari virus, worm, trojan, hingga spyware, dan biasanya disebarkan melalui file atau aplikasi yang tampak sah. Dalam konteks phishing, malware sering kali disisipkan dalam file.apk, yang jika diunduh dan diinstal oleh pengguna, dapat memberi akses kepada pelaku untuk mencuri informasi pribadi, seperti kredensial login, nomor kartu kredit, hingga data pribadi lainnya (Wibowo & Fatimah, 2017). Malware juga dapat menyebabkan kerusakan serius pada perangkat, memperlambat kinerja

sistem, atau bahkan mengunci data pengguna dengan ransomware, yang meminta tebusan untuk memulihkan akses. Dengan meningkatnya ancaman ini, analisis terhadap bagaimana phishing melalui malware menyebar dan berdampak pada pengguna aplikasi pesan instan, seperti WhatsApp, menjadi penting untuk memahami cara pencegahan yang efektif.

Di antara berbagai bentuk serangan phishing, serangan phishing yang melibatkan "file.apk" telah menjadi semakin umum dalam beberapa tahun terakhir, seiring dengan meningkatnya penggunaan perangkat mobile dan aplikasi berbasis Android. File.apk, yang merupakan format file instalasi untuk sistem operasi Android, sering kali digunakan oleh penjahat siber sebagai media penyebaran malware. Para pelaku phishing biasanya menyamar sebagai entitas tepercaya seperti yang telah dijelaskan sebelumnya, mulai dari penyedia layanan hingga institusi resmi, dan mengirimkan format file.apk melalui email, pesan instan, atau situs web palsu yang dirancang untuk menipu pengguna. Pengguna yang kurang berhati-hati atau tidak memiliki pengetahuan yang cukup mengenai risiko ini, sering kali tanpa sengaja mengunduh dan menginstal file.apk tersebut, tanpa menyadari bahwa file tersebut telah disusupi malware. Setelah diinstal, malware ini dapat memberikan akses ke perangkat pengguna, memungkinkan penjahat siber untuk mencuri informasi pribadi seperti kata sandi, data keuangan, dan informasi sensitif lainnya. Selain itu, malware yang terkandung dalam file.apk juga dapat mengakibatkan kerusakan pada perangkat, mengubah pengaturan, atau bahkan memata-matai aktivitas pengguna tanpa mereka sadari.

Bahkan, mahasiswa seringkali menjadi target utama dalam serangan phishing, terutama karena mereka seringkali kurang memiliki pengalaman atau pengetahuan yang memadai tentang keamanan siber. Menurut laporan dari Cybersecurity and Infrastructure Security Agency (CISA), sekitar 60% mahasiswa melaporkan telah mengalami serangan phishing selama periode studi mereka. Selain itu, studi dari Anti-Phishing Working Group (APWG) mencatat bahwa sektor pendidikan, termasuk mahasiswa, menjadi salah satu target utama phishing, dengan 25% dari semua insiden phishing melibatkan institusi pendidikan. Data dari Verizon’s 2023 Data Breach Investigations Report juga menunjukkan bahwa serangan phishing merupakan salah satu metode utama dalam pelanggaran data di sektor akademis, mempengaruhi sekitar 30% dari total insiden di lingkungan pendidikan. Angka-angka ini menunjukkan tingginya risiko yang dihadapi oleh mahasiswa, menggarisbawahi perlunya pendidikan dan kesadaran yang lebih baik tentang keamanan siber di kalangan mereka.

Aktivitas digital mereka yang tinggi, seperti sering menggunakan email, media sosial, serta aplikasi pesan instan untuk keperluan akademis dan sosial, menjadikan mereka rentan terhadap serangan ini. Phishing yang menyamar sebagai pesan dari institusi pendidikan, platform pembayaran, atau layanan umum sering kali berhasil menipu mahasiswa, karena terlihat sah dan relevan dengan kehidupan mereka. Selain itu, penggunaan perangkat mobile yang tidak selalu dilengkapi dengan perlindungan keamanan yang optimal memperbesar risiko ini. Dengan seringnya mahasiswa menerima pesan berisi tautan atau file yang tampak penting, banyak di antara mereka yang tanpa sengaja mengunduh malware atau memberikan informasi pribadi kepada pihak yang tidak bertanggung jawab. Kurangnya literasi digital yang memadai membuat kelompok ini menjadi sasaran empuk bagi penjahat siber yang memanfaatkan celah tersebut untuk mencuri data pribadi atau informasi keuangan mereka.

Kelompok kejahatan tersebut akan membuka jalan baru setiap kali pengguna WhatsApp sebagai korban melaporkan tindakan-tindakan kejahatan yang pernah ada. Sebelum adanya phishing apk, banyak jenis-jenis phishing yang telah dilakukan untuk meretas segala data korban. Phishing melalui SMS, melalui telefon, hingga phishing yang mengatasnamakan keluarga terdekat korban sehingga korban lebih cepat terperdaya oleh pelaku kejahatan siber.

Cara interaksi dan komunikasi masyarakat saat ini dalam kehidupan sehari-hari telah dipengaruhi oleh kemajuan teknologi informasi dan komunikasi, khususnya WhatsApp yang pada akhirnya membawa konsekuensi baru seperti ancaman keamanan siber yang telah dijelaskan diatas dapat dijelaskan lebih lanjut melalui teori pemrosesn informasi. Teori pemrosesan informasi dapat membantu kita memahami bagaimana seseorang akan sadar dengan tindakan interaksi yang terjadi hingga mendapatkan pembelajaran (Suryana, Lestari, & Harto, 2022).

Berdasarkan paparan diatas, penelitian ini akan diteliti dengan pendekatan kuantitatif. Peneliti akan menganalisis tingkat kesadaran masyarakat pengguna WhatsApp terhadap ancaman phishing “file.apk” dengan menggunakan teori pemrosesan informasi menurut Robert Mills Gagne dengan mengedepankan empat tahapan kesadadarn dengan objek mahasiswa ilmu komunikasi Universitas Muhammadiyah Malang.

1.2 Rumusan Masalah

1. Seberapa tinggi kesadaran pengguna WhatsApp akan bahaya phishing file APK?

1.3 Tujuan Penelitian

1. Untuk mengetahui seberapa tinggi kesadaran pengguna WhatsApp akan bahaya praktek phishing file APK

1.4 Manfaat Penelitian

Penelitian ini diharapkan memberikan berbagai manfaat, baik dari segi praktis, teoritis, maupun bagi peneliti:

1. Manfaat Praktis

   Penelitian ini akan membantu pengguna WhatsApp, khususnya mahasiswa, untuk lebih waspada terhadap ancaman phishing, terutama melalui file.apk. Dengan memahami cara kerja serangan phishing, pengguna dapat lebih bijaksana dalam berinteraksi di platform WhatsApp, sehingga dapat mengurangi risiko menjadi korban penipuan siber. Penelitian ini juga dapat menjadi panduan bagi pengguna aplikasi mobile dalam mengenali taktik phishing dan menjaga keamanan data pribadi.
2. Manfaat Teoritis

   Penelitian ini berkontribusi pada pengembangan literatur mengenai teori pemrosesan informasi, khussunya terkait seseorang yang akan bertindak atas kesadaran yang terjadi hingga mereka mendapatkan kesadaran terhadap ancaman keamanan siber seperti phishing. Selain itu, penelitian ini memperluas kajian mengenai ancaman phishing di media sosial, terutama WhatsApp, serta menawarkan sudut pandang baru dalam kaitannya dengan perkembangan teknologi dan keamanan siber di Indonesia.
3. Manfaat bagi Peneliti

   Penelitian ini menjadi sarana pembelajaran bagi peneliti dalam mendalami teori pemrosesan informasi dan implikasinya terhadap penggunaan teknologi sehari-hari. Peneliti juga mendapatkan pemahaman yang lebih mendalam mengenai teknik phishing dan cara-cara mencegahnya, serta memperluas wawasan dalam analisis data kuantitatif. Penelitian ini juga dapat menjadi acuan bagi peneliti dalam melanjutkan studi lebih lanjut mengenai ancaman siber dan dampaknya terhadap masyarakat.