BAB III

METODOLOGI PENELITIAN DAN PERANCANGAN

3.1 Metodologi Penelitian

Dalam perancangan ini, penulis menggunakan metode campuran (*mixed method*) yang mengintegrasikan berbagai pendekatan penelitian untuk menciptakan pemahaman yang komprehensif. Menurut Creswell (2018), pendekatan penelitian mixed method terdiri atas pengambilan data dengan metode kuantitatif, kualitatif, dan campuran.

3.1.1 Metode Kualitatif

Dalam perancangan ini, penulis menggunakan metode kualitatif untuk memahami pengalaman subjektif individu dan cara pandang mereka terhadap suatu isu. Menurut Leavy (2017), pendekatan kualitatif dapat memberikan wawasan yang mendalam tentang topik tertentu dengan mengumpulkan data deskriptif. Metode yang digunakan penulis untuk mengumpulkan beberapa informasi dan data adalah wawancara, studi eksisting dan studi referensi.

3.1.1.1 Wawancara

Penulis melakukan wawancara dengan ahli keamanan siber untuk mendapatkan pandangan profesional tentang fenomena phising. Selain itu, penulis juga melakukan wawancara dengan individu yang pernah menjadi salah satu korban phising untuk memahami kronologi kejadian phising.

1) *Interview* kepada Muhammad Faisal Qomarudin

Pada tanggal 20 Februari 2024, penulis mengadakan wawancara online dengan narasumber pada jam 20.00 – 21.00 WIB melalui GoogleMeet setelah mendapat persetujuan dari narasumber karena perbedaan lokasi antara Jakarta (penulis) dan Klaten (narasumber). Muhammad Faisal Qomarudin merupakan seorang lulusan Sistem Informasi yang saat ini bekerja sebagai Pengelola Sistem Jaringan DISDUKCAKPIL Kabupaten Klaten. Selama

wawancara, beliau mengungkapkan bahwa rendahnya kesadaran anak muda terhadap aktivitas phising telah menyebabkan anak muda menjadi korban. Menurut beliau, phising bisa dilakukan dengan mudah tanpa peralatan rumit, hanya dengan nomor telepon korban saja. Beliau juga menjelaskan berbagai teknik phising, termasuk yang kini marak dilakukan yaitu mengirimkan malware melalui pesan WhatsApp dengan menyamar sebagai undangan pernikahan atau resi pengiriman yang sering terjadi mengingat online shopping kini menjadi salah satu dari kebiasaan masyarakat sehari-hari.

Kurangnya kewaspadaan korban dimanfaatkan oleh pelaku phising untuk mencuri data pribadi korban, termasuk informasi keuangan seperti email, password, nomor rekening, pin, hingga KTP. Beliau menyampaikan terdapat beberapa cara untuk mengenali tanda pencurian data sedang berlangsung setelah korban mengklik malware yang dikirimkan melalui file ekstensi .apk tersebut, seperti perangkat terasa lambat atau sulit digerakkan. Untuk menghentikan proses pencurian data, korban dapat menyalakan mode pesawat dan mematikan perangkat untuk sebelum akhirnya menghapus aplikasi mencurigakan yang terunduh pada *handphone* korban. Selain itu, Beliau juga menyoroti kasus phising yang terjadi pada saudaranya yang masih duduk di bangku SMP dimana phising terjadi saat korban *login* pada website E-commerce palsu. Hal ini menyebabkan pelaku kemudian menggunakan akunnya untuk berbelanja dengan Shopee Paylater sebesar Rp6000.000. Beliau menekankan pentingnya memeriksa setiap informasi yang diterima dengan teliti dan memperhatikan seluruh domain website yang hendak dikunjungi.

Beliau juga memberikan saran kepada generasi muda untuk mengurangi risiko phising dengan tidak mengunggah informasi

sensitif secara terbuka, seperti tiket perjalanan, serta untuk berhati-hati dan merusak kertas alamat yang tertera pada paket untuk mencegah phising yang dilakukan dengan Teknik COD. Untuk mengatasi phising, beliau menyarankan pemasangan antivirus dan pelaporan website mencurigakan kepada KOMINFO untuk diblokir. Meskipun demikian, beliau mengakui bahwa pihak KOMINFO tidak dapat menghapus domain website yang mencurigakan, namun hanya bisa memblokirnya untuk mencegah korban baru terjebak disebabkan domain tersebut bukan miliknya sehingga tidak dapat website tidak dapat dihapuskan.

Gambar 3.1 Bukti Wawancara dengan Muhammad Faisal Qomarudin

2) Interview kepada Aziz Zulhakim Putra Chriswan

Pada tanggal 26 Februari 2024, penulis melakukan wawancara dengan Aziz Zulhakim dari Fakultas Bisnis Internasional, Universitas Binus. Wawancara dilakukan secara online melalui platform Zoom sesuai permintaan narasumber dikarenakan keterbatasan waktu. Pertemuan tersebut dijadwalkan pada pukul 12:00-13.00 WIB. Aziz dipilih sebagai narasumber untuk membagikan pengalamannya terkait kasus phishing yang dialaminya saat masih berada di SMA 1.

Kronologi kejadian dimulai ketika Aziz menerima panggilan telepon dari pelaku yang mengaku sebagai perwakilan resmi Gojek. Pelaku tersebut menyampaikan bahwa Aziz telah memenangkan hadiah saldo Go-Pay senilai Rp15.000.000. Meskipun merasa curiga karena nominal hadiah yang sangat besar, kecurigaannya menurun saat pelaku tidak memaksa, melainkan menanyakan ketersediaan Aziz untuk menerima hadiah. Apabila Aziz memutuskan untuk menerima hadiah tersebut, pelaku akan mengirimkan sebuah kode OTP kepada *handphone* miliknya. Penyampaian yang terkesan santai dari pelaku mengurangi kecurigaan Aziz terhadap situasi tersebut. Tanpa curiga, Aziz memberikan kode OTP kepada pelaku.

Selama proses pencurian data, Aziz tetap tidak curiga karena pelaku terus berbicara dengan dirinya melalui panggilan telepon sambil menjelaskan prosedur yang seharusnya dilakukan. Setelah berhasil mendapatkan kode OTP dari Aziz, pelaku menginformasikan bahwa pencairan dana Go-Pay membutuhkan waktu sekitar 2-3 hari. Aziz menyetujui dan mengakhiri panggilan tersebut. Beberapa jam kemudian, Aziz memeriksa saldo akun Gojeknya dan menyadari bahwa saldo sebesar Rp150.000 telah hilang. Aziz kemudian mencoba menghubungi pelaku namun tidak berhasil dan memperkitakan bahwa nomor miliknya telah diblokir pelaku. Setelah menyadari bahwa dirinya telah menjadi korban phising, Aziz tidak menghubungi pihak resmi Gojek karena ia merasa tidak yakin akan mendapatkan solusi dari pihak resmi dimana kesalahan terjadi karena kelalaiannya sendiri.

Gambar 3.2 Bukti Wawancara dengan Muhammad Faisal Qomarudin

3.1.1.2 Observasi

Penulis juga menerapkan pendekatan kualitatif dengan melakukan observasi secara non-partisipatif, di mana penulis hanya mengamati konten-konten yang diunggah oleh pengguna media sosial terkait pengalaman mereka dengan *phising*. Tujuannya adalah untuk memahami teknik-teknik yang sedang populer digunakan. Observasi ini terfokus pada *postingan* media sosial, salah satunya adalah melalui platform X dengan menggunakan kata kunci "penipuan" dan *"phising*". Saat ini, salah satu teknik phising yang sedang marak adalah penipuan dengan mengirimkan *pop-up* transaksi kepada korban. *Pop-up* tersebut mengonfirmasi pembayaran dengan jumlah tertentu, menyerupai *pop-up* layanan pembayaran digital. Apabila korban kurang waspada dan bingung, korban cenderung akan langsung mengklik *pop-up* untuk mengecek informasi tersebut. Dalam beberapa kasus, korban dihadapkan pada serangkaian *pop-up* yang mengharuskan mereka untuk menyetujui, akibatnya saldo korban akan disedot oleh pelaku. Hal ini memungkinkan pelaku untuk mengakses data dan akun korban serta memperoleh uang dari hasil phising *pop-up*.

Gambar 3.3 *Phising Metode Notifikasi Pop-Up*
Sumber: Twitter, 2024

Selain metode *pop-up,* metode phising yang sedang populer dan telah merugikan banyak orang adalah metode phising pengiriman paket COD. Penipuan ini terjadi saat paket dikirim atas nama orang lain ke alamat korban. Tujuannya adalah agar korban mengira bahwa salah satu anggota rumah telah memesan paket tersebut, sehingga korban kemudian membayar paket atas nama orang yang sebenarnya tidak terkait.

Gambar 3.4 *Phising dengan Metode COD*
Sumber: Twitter, 2024

Penulis juga melakukan observasi terhadap kejahatan yang serupa atau memiliki kemiripan dengan *phising*, yaitu *scamming.* Berdasarkan observasi yang dilakukan oleh penulis, *Scamming* dan *phishing* adalah dua jenis penipuan *online,* tetapi mereka memiliki perbedaan dalam metode dan tujuan. *Scamming* adalah tindakan penipuan umum yang mencakup berbagai teknik, seperti menjual barang palsu, skema investasi palsu, lotere palsu, atau memanfaatkan

simpati korban dengan cerita-cerita yang dibuat-buat. Tujuan utama *scamming* adalah untuk mencuri uang atau harta benda dari korban.

Di sisi lain, menurut SafeComputing, *phising* adalah jenis penipuan yang lebih spesifik di mana penipu menggunakan teknik rekayasa sosial untuk mendorong korban memberikan informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya. Ini biasanya dilakukan melalui email, pesan teks, atau situs web palsu yang tampak sah. Tujuan utama *phising* adalah untuk mencuri informasi sensitif dari korban, yang kemudian dapat digunakan untuk akses tidak sah ke akun atau sistem, atau untuk pencurian identitas.

3.1.1.3 Studi Eksisting

Penelitian eksisting telah dilakukan penulis terhadap beberapa media informasi berbasis website interaktif yang berfokus pada tema phishing yang telah ada sebelumnya. Dari penelitian ini, penulis dapat memahami jenis informasi yang perlu disampaikan, serta mengevaluasi kelebihan dan kekurangan dari masing-masing media tersebut untuk digunakan sebagai referensi dalam proses perancangan. Berikut adalah hasil penelitian eksisting terhadap *Website So Safe, The Phisherman,* dan *Spot the Phish:*

1) **The Pisherman**

"*The Phisherman*" adalah permainan berbasis *web* dengan tema bawah laut di mana pelaku phising digambarkan dengan karakter "*Phisherman".* Permainan ini melibatkan menjawab pertanyaan terkait *phishing* untuk mengalahkan pelaku *phising*. Pertanyaan-pertanyaan ini mensimulasikan berbagai situasi *phishing,* seperti mengidentifikasi keaslian email, mengenali panggilan palsu, dan menghindari jebakan iklan *pop-up*.

Gambar 3.5 Tampilan Gim Phiserman Berbasis *Website*
Sumber: https://barefootgames.org/the-phisherman?ref=https://www.barefootcomputing.org/

Sebelum memulai permainan, pemain diberikan informasi edukatif, termasuk definisi, jenis, karakter, dan cara menghindari phishing untuk meningkatkan pengetahuan mereka. Permainan ini menggunakan sistem poin di mana pemain mendapatkan poin tambahan untuk jawaban yang benar. Jawaban yang salah mengakibatkan pengurangan poin, disertai dengan pesan *feedback* korektif untuk membantu pemain menghindari jatuh ke dalam teknik phishing dalam kehidupan nyata.

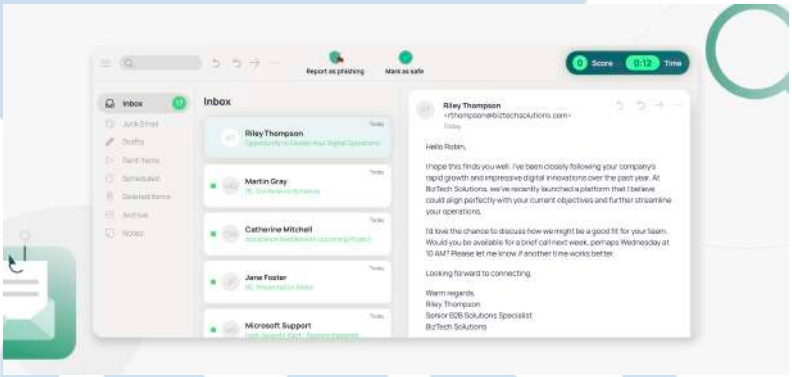
Tabel 3.1 Tabel Analisis SWOT The Pisherman

Strength	1) Memiliki alur cerita yang menarik dan cukup mudah untuk dipahami 2) Memberikan penjelasan sebelum memulai permainan 3) Banyak menggunakan elemen visual yang interaktif 4) Memberikan sifat personalisasi kepada user melalui pemilihan karakter, jawaban hingga level 5) Memiliki fitur audio
Weakness	1) Tidak dapat memulai atau melihat informasi sesuai pilihan 2) Tidak memiliki tombol back

Opportunity	1) Sangat menarik sebagai media informasi yang ditujukan bagi anak-anak 2) Dapat memperbanyak variasi jenis dan Teknik phising 3) Dapat menambahkan animasi menarik
Threat	1) Banyak media informasi yang lebih mudah dan praktis untuk diakses

2) So Safe

So Safe merupakan sebuah *website* yang dibuat dengan gamifikasi yang tinggi, berisi tes dengan beberapa pernyataan yang dibuat dengan tujuan untuk mengetahui apabila *user* dapat mengidentifikasi aktivitas *phising.*



Gambar 3.6 Tampilan *Website* Interaktif SoSafe
Sumber: https://sosafe-awareness.com/phishing-game/#

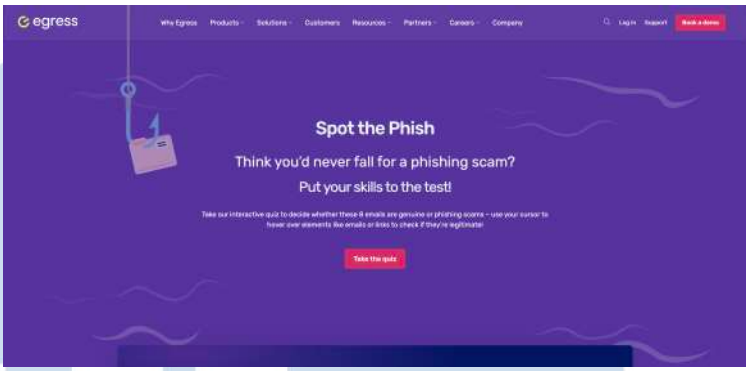
Pernyataan dibuat dalam bentuk email berisikan pesan dimana pemain harus menentukan apakah email tersebut aman atau tidak dengan memperhatikan komponen-komponen pada email. Setelah membaca, *user* dapat menentukan pilihan apakah pernyataan tersebut terdapat kesalahan mencurigakan yang menandakan adanya *phising.* Penentuan ini dilakukan dengan menekan salah satu dari dua *button* yang tersedia. Namun, pada *web So Safe*, hasil akhir tidak menyertakan penjelasan kesalahan dan langkah-langkah yang dapat

dilakukan untuk mengidentifikasi ataupun menghindari aktivitas *phising*.

Tabel 3.2 Tabel Analisis SWOT So Safe

Strength	1) Memiliki tujuan dan misi yang jelas dan cukup sederhana 2) Memberikan kebebasan bagi pengguna untuk mengerjakan tanpa urutan tertentu 3) Memberikan *user* pengalaman realistis untuk mengidentifikasi tanda-tanda phising 4) Memiliki tingkat kesulitan yang cukup beragam
Weakness	1) Tidak memberikan perkenalan terhadap topik yang diangkat 2) Tidak memberikan evaluasi kesalahan terhadap jawaban yang telah dipilih oleh *user* 3) Membahas jenis *phising* yang cukup terbatas (*email & link*) 4) Letak *button* yang janggal
Opportunity	1) Dapat menambahkan beberapa jenis pertanyaan dengan teknik phising yang berbeda 2) Dapat menambahkan informasi mengenai topik diawal ataupun evaluasi kesalahan di akhir permainan.
Threat	1) *Website* monoton sehingga kurang meninggalkan kesan bagi user 2) Beberapa informasi menyuguhkan dengan cara yang lebih menarik dan lebih lengkap

3) Spot the Phish



Gambar 3.7 Tampilan Website Spot the Phish
Sumber: https://www.egress.com/blog/phishing/spot-the-phish

Spot the Phis*h* adalah sebuah situs web yang memiliki kesamaan dalam mekanisme dengan So Safe, di mana kedua situs tersebut menampilkan serangkaian pertanyaan untuk menguji kemampuan pengguna dalam mengidentifikasi aktivitas *phishing*. Perbedaannya terletak pada cara hasil tes disajikan. Pada *web* Spot the Phish, setelah pengguna menjawab pertanyaan, hasil tes disertai dengan penjelasan tentang di mana kesalahan pengguna terletak, serta informasi tentang karakteristik *phising* dalam email, pesan, atau *link*. Namun, saat awal permainan, Spot the Phish tidak memberikan informasi atau penjelasan mengenai ciri atau karakteristik aktivitas *phising*.

Tabel 3.3 Tabel Analisis SWOT Spot the Phish

Strength	1) Tampilan sederhana menyebabkan informasi mudah dipahami 2) Penjelasan dan evaluasi yang cukup lengkap terhadap jawaban user 3) Tidak memakan waktu yang lama untuk pengerjaan
Weakness	1) Tampilan kurang menarik 2) Pertanyaan hanya terdiri atas 8 pertanyaan saja

	3) Hanya membahas *phising* yang terjadi pada email dan web 4) Minimnya interaksi dalam web
Opportunity	1) Dapat menambahkan variasi pertanyaan lainnya seputar phising 2) Menambahkan interaksi lainnya
Threat	1) Masih ada media yang lebih menarik 2) Informasi mengenai *phising* yang terlalu singkat dengan jenis dan teknik yang terbatas

3.1.1.4 Studi Referensi

Selain itu, penulis menemukan beberapa sumber yang dapat memberikan wawasan untuk merancang kampanye interaktif mengenai bahaya *phishing* dalam berbelanja *online.* Melalui penelitian ini, penulis ingin memahami jenis mekanisme situs *web* interaktif yang cocok untuk konten edukatif tentang phishing. Referensi penelitian mencakup Species in Pieces, Useless in London, *dan A* Tiny Adventure.

1) Species in Pieces

Gambar 3.8 Tampilan Website Species in Pieces
Sumber: http://species-in-pieces.com/

Species in Pieces adalah sebuah situs kampanye yang fokus untuk memberikan informasi mengenai hewan-hewan yang terancam punah. Oleh karena itu, keberadaan informasi yang komprehensif dengan statistik yang lengkap berdasarkan data menjadi sangat penting bagi situs ini. Presentasi informasi

ini diperkuat oleh penggunaan ilustrasi, grafik visual, animasi, dan interaksi yang menarik, yang dapat meningkatkan minat pengguna untuk menjelajahi situs *website* dan mempermudah pemahaman informasi. Situs ini menyajikan informasi dengan nada serius, namun tetap menyenangkan, dengan menggunakan warna-warna cerah dan gaya ilustrasi *flat design* yang mirip dengan gambar/bentuk asli dari binatang-binatang dalam *website* tersebut.

2) Violence Conjugale

Violence Conjugale merupakan sebuah *website* yang memiliki tujuan untuk mengedukasi pengguna mengenai kekerasan domestik yang sering kali dialami oleh wanita. Edukasi ini dibuat dengan bentuk interaktif dimana user berperan sebagai korban dan dapat berinteraski dengan pernyataan-pernyataan dari sebuah kasus kekerasan domestik.

Gambar 3.9 Tampilan website Violence Conjugale
Sumber: https://itsnotviolent.com/scenarios/4

Pada akhir kasus, *website* kemudian memberikan informasi lebih lengkap dengan meminta user untuk mengidentifikasi apakah kasus tersebut termasuk kekerasan domestik atau tidak.

3) Useless

Useless merupakan sebuah *website* kampanye interaktif yang bertujuan untuk memberikan edukasi tentang pentingnya

mengurangi penggunaan plastik serta mendorong perubahan kebiasaan masyarakat dengan menawarkan alternatif-alternatif barang dan tempat-tempat yang mendukung gerakan ini. *Website* ini menarik perhatian pengunjung dengan penggunaan warna-warna cerah dan kontras, serta ilustrasi yang sederhana namun mencolok.

Gambar 3.10 Tampilan *Website* Useless
Sumber: https://useless.london/

Penggunaan tipografi yang besar dan *layout* yang rapi tetapi menarik juga menarik perhatian dan memberikan kenyamanan dalam membaca informasi. Meskipun menyajikan banyak informasi, *website* ini tidak lupa mencantumkan *button* yang mengarahkan *user* ke tautan yang relevan untuk mengambil langkah-langkah perubahan menuju kebiasaan mengurangi plastik.

Tabel 3.4 Perbandingan Hasil Pengamatan *Website*

Aspek Penilaian	"Species in Pieces"	"Violence Conjugale"	"Useless"
Jenis *Website*	*Campaign* edukasi	*Campaign* edukasi	*Campaign* edukasi

Warna	*Colorful & simple*	Perpaduan warna gelap dengan *pop*	Warna kontras & *pop*
Typeface	*Display, textured all caps*	*Sans Serif*	Gabungan *display headline* & *sans serif body*
Ilustrasi	*Flat Design*	*Simple outline*	*Flat design,* vector
UI	Grafik, *bar indicators,*	*Menu hamburger, guidance*	*Hover color*, Ikon
UX	Fitur skip & save photo	*Animated, Download PDF*	*Hyperlink, Preloaders,*

3.1.1.4 Studi Literatur

1. Gen Z Financial Literacy

Menurut OECD/INFE (2020), pentingnya literasi keuangan adalah dalam mendorong inklusi keuangan, ketahanan keuangan, dan kesejahteraan keuangan. Menurut survei oleh UMN Consulting (2022), mayoritas responden Generasi Z (62,53%) menganggap diri mereka memiliki tingkat pengetahuan investasi yang sedang, yang menunjukkan bahwa mereka memiliki informasi yang cukup dan bersedia untuk berinvestasi dengan risiko rendah. Namun, tingkat literasi keuangan sesungguhnya Generasi Z, menurut informasi dari

Otoritas Jasa Keuangan (OJK) pada tahun 2022, hanya sebesar 44,04%, yang termasuk dalam kategori rendah karena di bawah 60%. Tingginya tingkat utang Generasi Z, seperti yang disampaikan oleh OJK pada tahun yang sama, tercermin dari data kepemilikan rekening dan jumlah pinjaman yang masih harus dibayar kepada fintech P2P lending. 62% dari rekening *fintech* pendanaan bersama dimiliki oleh individu usia 19-34 tahun, sementara 60% dari total pinjaman *fintech* pendanaan bersama disalurkan kepada kelompok usia yang sama. Ini menunjukkan dominasi Generasi Z dalam penggunaan *fintech* pendanaan.

2. Gen Z Media Consumption

Generasi Z adalah penduduk digital yang lahir dan besar dengan aktivitas seperti pendidikan, interaksi sosial, dan pekerjaan yang dilakukan secara *online.* Bagi sebagian besar dari mereka, keberadaan digital bukan hanya sekadar kemudahan, melainkan merupakan bagian yang tak terpisahkan dari identitas mereka. Mereka mengembangkan hubungan, mencari validasi, dan mencari tempat mereka di dunia melalui interaksi *online,* membentuk komunitas yang melintasi batas geografis. Berdasarkan survey oleh Indonesian Gen Z Report (2024), mayoritas dari 602 orang Generasi Z menghabiskan waktu sekitar 1–6 jam di media sosial setiap hari dan 14% mengakui bahwa mereka menggunakan media sosial selama 6–10 jam dan bahkan lebih dari 10 jam (5%).

Untuk penggunaannya sebagai media komunikasi, Generasi Z Indonesia dengan 92% responden mengkonfirmasi penggunaannya pada Whatsapp. Popularitas WhatsApp tidak hanya terbatas pada komunikasi pribadi, dengan banyak Generasi Z juga memanfaatkannya untuk kegiatan profesional dan komersial. Pada konsumsi konten, Generasi Z cenderung tertarik pada konten berbasis video singkat yang berlangsung dari beberapa detik hingga satu menit disebabkan kemudahan dalam berbagi dan konsumsi yang

cepat, terutama pada perangkat seluler. Sebanyak 29% dari Generasi Z mengklaim lebih suka menonton konten video, sementara hanya 7% yang lebih memilih artikel berbasis visual dan 3% lebih memilih membaca artikel dan 60% mengonsumsi gabungan antara ketiganya. Hal ini dibuktikan dengan tingginya penggunaan beberapa aplikasi seperti Youtube, Tiktok, dan Instagram Reels.

2. Gen Z *Financial Preferences*

Sebanyak 56% responden menyatakan bahwa pendapatan bulanan Generasi Z berada di bawah Rp 2,5 juta. Namun, pendapatan bulanan penduduk Indonesia sangat bergantung pada lokasi geografis mereka. Variasi dalam upah minimum ini tercermin dalam disparitas pendapatan antar wilayah. Sebagai Jakarta memiliki upah minimum tertinggi sebesar Rp 4,9 juta per bulan, sementara Jawa Tengah memiliki yang terendah sebesar Rp 1,9 juta per bulan. Dunia belanja online di Indonesia juga telah mengalami percepatan signifikan melalui situs *e-commerce* dan platform komersial sosial, terutama sejak munculnya pandemi COVID-19. Sebanyak 72% dari Generasi Z yang disurvei menyatakan preferensi mereka untuk berbelanja online di Shopee, dengan 11% pada platform *e-commerce* lokal Tokopedia dan 11% pada Tiktok Shop. Hal ini dibuktikan melalui data yang didapat dari kuesioner dimana 70% dari 102 Responden memilih aplikasi *e-commerce* sebagai tempat untuk berbelanja *online.*

Fenomena kepopuleran *e-commerce* di kalangan masyarakat dimanfaatkan oleh platform untuk memberikan diskon dan promosi substansial tanpa membebankan biaya platform. Hal ini mempengaruhi pembuatan keputusan pengguna terhadap aktivitas *online-shopping.* Selain itu, kenyamanan dan kemudahan berbelanja dari rumah, serta mudahnya dalam mencari dan membandingkan produk, membuat orang lebih memilih belanja *online.* Keterkaitan antara harga dan kenyamanan ini menunjukkan betapa pentingnya faktor-faktor tersebut dalam membentuk kebiasaan belanja *online.*

3. Gen Z *Shopping Behaviour*

Sesuai dengan pertumbuhan e-commerce, ekosistem pembayaran digital turut berkembang pesat di Indonesia. Para penyedia *fintech* memanfaatkan peluang tersebut untuk memperbesar penetrasi pasar. Berdasarkan survei yang dilakukan oleh Kredivo (2022), pembayaran digital yang paling umum banyak digunakan oleh konsumen ketika berbelanja online adalah *e-wallet* dan transfer bank. Metode pembayaran PayLater pun semakin diminati oleh konsumen. Berdasarkan survey oleh Kredivo (2022), terdapat 38% konsumen yang menggunakan PayLater saat berbelanja di *e-commerce* pada tahun 2022.

Dalam dunia belanja *online,* ada perbedaan preferensi antara Generasi Z perempuan dan laki-laki. Perempuan Generasi Z lebih cenderung membeli pakaian dan produk kecantikan, menunjukkan perhatian pada penampilan pribadi dan ekspresi diri. Sementara itu, laki-laki Generasi Z lebih suka membeli barang-barang terkait hobi dan elektronik, menunjukkan minat dalam kegiatan rekreasi dan teknologi. Perbedaan preferensi berdasarkan jenis kelamin dalam belanja *online* ini menekankan variasi minat dan kebutuhan yang mempengaruhi perilaku konsumen di kalangan Generasi Z, yang juga berdampak pada berbagai barang dan layanan yang tersedia di pasar *e-commerce.*

Menurut survei yang dilakukan oleh Kredivo pada tahun 2022, terutama dalam kategori *gadget*, komputer, dan elektronik, generasi Z cenderung memiliki nilai transaksi yang lebih tinggi dibandingkan dengan kelompok usia lainnya. Konsumen berusia 18-25 tahun cenderung mengeluarkan lebih banyak uang untuk kebutuhan belajar dan pekerjaan. Pulsa dan voucher merupakan produk yang paling banyak dibeli oleh Generasi Z, yang menyumbang hampir sepertiga dari total transaksi. *Fashion,* aksesoris, serta produk kesehatan dan kecantikan juga merupakan produk yang umum dibeli oleh kelompok usia ini.

4. Target Audiens

Dalam melakukan penelitian ini, penulis menargetkan Generasi Z yang didasari oleh karakteristik dan perilaku mereka. Generasi Z menghabiskan banyak waktu online untuk pendidikan, hiburan, atau interaksi sosial dimana menurut Kredivo (2022), 85% dari transaksi *E-commerce* berasal dari Generasi Z dan milenial yang meningkatkan peluang mereka berinteraksi dengan konten phishing. Menurut studi oleh *Institute for the Public Understanding of Risk* (2022), generasi digital sangat bergantung pada internet sehingga kepercayaan yang tinggi pada teknologi membuat mereka sering menganggap platform digital adalah sesuatu yang sudah mereka kuasai dengan baik sehingga tidak ada kecurigaan, melainkan hanya kepercayaan diri bahwa mereka memiliki pengalaman yang cukup untuk dapat mengenali dan menghindari ancaman *phising.*

Penulis juga menargetkan Gen Z juga cenderung lebih terbuka dalam membagikan informasi pribadi di internet, yang dapat dimanfaatkan pelaku *phising* untuk membuat serangan lebih meyakinkan. Menurut Alves (2023), Generasi Z merupakan salah satu generasi yang *up-to-date* yang senang mengikuti tren terkini dan

dilibatkan dalam kegiatannya pada platform media sosial. Hal ini memberikan kemudahan bagi penulis dalam meningkatkan kesadaran dan asosiasi positif terkait mendorong perubahan kebiasaan untuk menghindari bahaya *phising.* Menurut Monteiro (2022), dengan penggunaan internet dan media sosial yang intens dan selalu menjadi bagian dari kehidupan mereka, generasi Z membentuk keterampilan dan perubahan gaya, kosakota dan keterampilan literasi dan bahasa baru/*slang* yang unik untuk membantu mereka mengekspresikan diri. Hal ini menjadi salah satu faktor penulis memilih penyampaian informasi dengan menggunakan Bahasa yang lebih lugas dan tidak formal agar terdengar lebih menarik dan mudah dipahami oleh target audiens.

Dengan kemampuannya yang menguasai teknologi, penulis memilih penyampaian pesan kampanye secara interaktif dengan melibatkan user dalam kegiatan simulasi pada *website*. Hal ini disebabkan preferensi gaya penyampaian yang digemari di kalangan Generasi Z dimana menurut hasil survei yang dilakukan oleh Ja'afar (2017) menunjukkan bahwa 61% siswa setuju bahwa aktivitas praktik langsung membantu mereka memahami pengajaran dengan lebih baik. Pembuatan *game* atau simulasi akan membantu memenuhi kriteria Generasi Z yang menyukai tantangan dan kepraktisan, seperti yang disebutkan oleh Thomas et al. (2017).

3.1.1.5 Kesimpulan

Phising merupakan ancaman serius yang telah menyebabkan banyak kerugian pada korban, terutama disebabkan oleh rendahnya kesadaran dan kewaspadaan terhadap teknik *phising* yang terus berkembang. Melalui wawancara, penulis mengetahui bahwa phising yang marak terjadi berhasil karena korban seringkali tanpa sadar mengklik *file* yang mencurigakan atau memberikan akses pada informasi keuangan, bahkan menerima paket yang mencurigakan tanpa menyadari tanda-tanda *phising* yang berpotensi menyebabkan

kerugian finansial yang signifikan. Dengan perkembangan teknologi, *phising* menjadi lebih mudah tersebar dan dilakukan secara digital, terutama jika korban kurang waspada. Namun, hal ini bisa dihindari jika korban memahami tanda-tanda aktivitas *phising,* berani melaporkan, dan selalu berhati-hati dalam menerima paket yang datang ke rumah.

3.1.2 Metode Kuantitatif

Dalam perancangan ini, penulis menggunakan metode kuantitatif untuk mengetahui kebiasaan target audiens dalam kegiatan *online shopping*. Menurut Sugiyono (2017, hal. 7), pendekatan kuantitatif merupakan sebuah metode penelitian yang didasarkan pada filsafat positivisme. Metode ini dianggap sebagai pendekatan ilmiah karena memenuhi prinsip-prinsip ilmiah yang konkret objektif, dapat diukur, rasional, dan terstruktur secara sistematis. Metode yang digunakan oleh penulis adalah kuesioner.

3.1.2.1 Kuesioner

Kuesioner difokuskan pada pertanyaan yang berkaitan dengan pemahaman, kesadaran, perilaku, dan kebiasaan saat berbelanja *online,* serta langkah-langkah pencegahan terhadap aktivitas *phising* yang telah diambil oleh responden. Penulis menggunakan kuesioner ini dengan tujuan untuk mengevaluasi tingkat pengetahuan, kerentanan, dan kebiasaan target sasaran terhadap serangan *phising.*

Kuesioner tersebut disebarkan kepada masyarakat berusia 17 hingga 25 tahun di berbagai wilayah di Indonesia pada tanggal 20 Februari 2024. Penyebaran kuesioner dilakukan melalui tautan Google Forms dan berhasil mendapatkan total 102 responden. Semua peserta telah menyetujui untuk mengikuti kuesioner setelah membaca penjelasan mengenai tujuan penelitian. Setiap responden mengisi kuesioner secara individu yang terdiri dari sekitar 35 pertanyaan. Sebanyak 73 dari total 102 responden berasal dari wilayah Jabodetabek, sementara 19 responden berasal dari luar wilayah

tersebut, termasuk mahasiswa, pekerja, dan non-pekerja. Partisipan tersebar secara merata dalam hal jenis kelamin dan usia. Pengumpulan data dilakukan menggunakan metode *nonprobability* (tidak acak), dengan jumlah sampel yang ditentukan dengan rumus Slovin. Populasi pengguna internet di Indonesia pada awal 2024 berjumlah 221.563.479 jiwa berdasarkan data dari Asosiasi Penyelenggara Jasa Internet Indonesia (2023), sehingga sampel yang diperlukan adalah:

$$n = \frac{\mathbf{N}}{\mathbf{1+ Ne2}} = \frac{221.563.479}{1+ 221.563.479\ (0{,}1)2} = 99{,}99 \approx 100$$

Keterangan

N= Jumlah Populasi

n = Jumlah Sampel

e = Derajat Ketelitian (10%)

Tabel 3.5 Tabel Profil Responden

Variabel	Kategori	Presentase
Usia	17 – 19 tahun	10,8%
	20 – 23 tahun	44.1%
	24 – 25 tahun	44.1%
	>25 tahun	1%
Domisili	Jabodetabek	71,5%
	Luar Jabodetabek	18,5%
Pekerjaan	Siswa/Mahasiswa	28,4%
	Pekerja	70,7%
	Ibu Rumah Tangga	1%

1) Hasil Kuesioner

Kuesioner difokuskan pada responden dewasa dengan tujuan untuk mendalami pemahaman individu berusia 17—25 tahun

terhadap *feedback* dan preferensi responden mengenai penggunaan informasi dan pola belanja *online*. Selain itu, kuesioner bertujuan untuk mengidentifikasi sejauh mana pemahaman dan pengetahuan, serta kerentanan responden terhadap serangan phising.

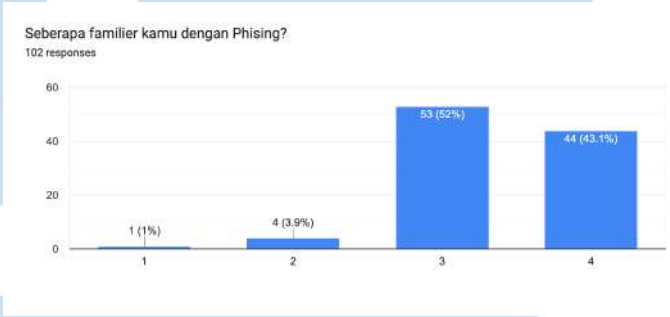
Gambar 3.11 Hasil Tes Apakah Responden Pernah Mengalami Penipuan

Pada pertanyaan apakah responden pernah mengalami penipuan saat berbelanja *online,* 66,7% menjawab tidak pernah mengalami penipuan saat berbelanja online, 23,5% menjawab pernah mengalami hal tersebut, dan 9,8% menjawab tidak yakin. Responden yang menjawab tidak pernah memiliki kemungkinan tidak mengenali tanda-tanda atau bagaimana kebiasaan mereka dapat mengekspos diri terhadap kegiatan phising.

Gambar 3.12 Hasil Tes Faktor Terjadinya Penipuan pada Responden

Pada pertanyaan mengenai bagaimana penipuan yang dialami oleh responden terjadi, sebanyak 9% mengatakan bahwa

produk yang tiba berbeda jauh/tidak sesuai dengan produk yang telah dibeli, sebanyak 3% mengklik *link* mencurigakan, dan sebanyak 2% tergiur oleh diskon dan harga murah, disusul dengan beberapa faktor penyebab pengalaman penipuan lainnya. Data diatas menampilkan beberapa faktor penyebab terjadinya *phising* yang dapat disebabkan oleh diri maupun faktor luar.



Gambar 3.13 Skala Familier terhadap Phising

Pada skala tingkat familier responden terhadap fenomena *phising,* sebanyak 52% menjawab sangat familier dengan fenomena *phising,* 43,1% menjawab cukup familier dengan *phising*, sedangkan sisanya sebanyak 3,9% dan 1% merasa cukup hingga belum familier.

Gambar 3.14 Frekuensi Responden mengecek link dengan teliti

Pada pertanyaan mengenai frekuensi responden untuk memperhatikan *link* yang diterima sebelum membukanya,

sebanyak 55,9% mengatakan cukup sering mengecek, 34,3% selalu mengecek sebanyak 9,8% cukup jarang mengecek link dengan teliti sebelum akhirnya mengklik *link* tersebut. Data ini menampilkan frekuensi pengecekan *link* secara teliti yang diterima responden yang berpengaruh terhadap tingkat kewaspadaan pada *link* yang hendak dibuka tersebut.

Gambar 3.15 Pemahaman Responden terhadap Ciri Situs Tidak Aman

Pada pertanyaan mengenai pemahaman ciri situs aman dan tidak aman dari ancaman siber, mayoritas responden mengatakan cukup paham (43,1%) dan sangat paham (38,2). Namun, 12,7% menyatakan kurang paham dan sisanya tidak paham mengenai ciri-ciri dari situs aman dan tidak aman dari ancaman siber.

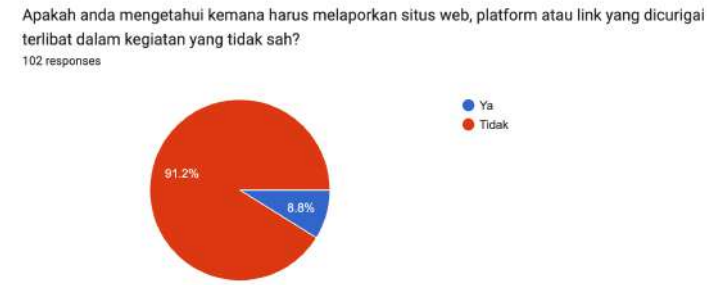
Gambar 3.16 Hasil Tes Identifikasi Phising oleh Responden

Untuk menguji hal tersebut, penulis memberikan pilihan yang dapat menjadi tanda-tanda phising dimana beberapa pilihan

bukan merupakan tanda-tanda *phising* untuk mengetahui apakah responden dapat mengidentifikasi dengan benar. Mayoritas telah memilih jawaban dengan benar, namun beberapa responden masih memilih salah mengidentifikasi tanda-tanda *phising* dengan memilih pilihan tidak ada kebijakan pengembalian (23,5%) dan *link* berbentuk https (25,5%).

Gambar 3.17 Langkah yang Diambil saat Menemukan Link Mencurigakan

Ketika menemukan *link* mencurigakan, sebanyak 43% responden memutuskan untuk hanya melewati *link* tersebut. Sebanyak 39% responden memilih untuk melaporkan situs agar situs dapat diblokir, dan 10% memberitahukan informasi mengenai situs mencurigakan kepada kerabat dan orang disekitarnya. Sisa dari responden mengatakan memastikan situs melalui web terpercaya, memasang keamanan tambahan, mengecek namun tetap berhati-hati.



Gambar 3.18 Pemahaman Responden mengenai Pelaporan Phising

Meskipun Sebagian besar responden mengetahui keberadaan *link* mencurigakan, mayoritas responden (91,2%) tidak mengetahui kemana harus melaporkan situs web, platform atau *link* mencurigakan yang terlibat dalam kegiatan yang tidak sah. Beberapa responden (8,8%) menyebutkan *link* dan situs *web* ataupun platform mencurigakan dapat dilaporkan melalui *web* resmi yang bertanggung jawab.

2) Kesimpulan

Berdasarkan hasil kuesioner tersebut, dapat disimpulkan bahwa sebagian besar individu Gen Z di Indonesia, baik yang pernah mengalami penipuan maupun yang tidak, mengaku familiar dengan aktivitas phishing dan telah berusaha untuk lebih berhati-hati dalam mengakses berbagai hal. Meskipun mereka telah meningkatkan kewaspadaan, masih ada kebiasaan tertentu yang tanpa disadari dapat membuat mereka rentan terhadap aktivitas phishing. Sebagian dari mereka telah mengambil langkah-langkah perlindungan diri terhadap aktivitas *phishing*, namun masih banyak yang tidak bisa mengenali tanda-tanda *phishing* dan tidak tahu cara atau di mana melaporkan aktivitas tersebut.

b. Metodologi Perancangan

Dalam perancangan media kampanye mengenai bahaya phising, penulis menggunakan metode Design Thinking oleh Hasso-Plattner yang dijelaskan Institute of Design at Stanford atau lebih dikenal dengan d.school. Menurutnya, fase design thinking terbagi menjadi 5 tahapan, yaitu:

3.2.1 Emphatize

Empathize merupakan sebuah langkah yang dilakukan untuk memahami target sasaran. Tahap ini perlu dilakukan untuk mendapatkan

insight masalah yang mereka hadapi dan kebutuhan akan solusi tanpa adanya asumsi pribadi. Tahap ini dapat dilakukan dengan observasi dan *interview*/wawancara.

3.2.2 Define

Selanjutnya, berdasarkan informasi yang diperoleh pada tahap empati, penulis kemudian mengolahnya untuk mengidentifikasi dan mendefinisikan masalah tersebut dari sudut pandang penulis. Dalam menentukan masalah ini, penulis perlu mempertimbangkannya dari sudut pandang audiens. Tahap ini dapat dilakukan dengan membuat persona, *empathy map.*

3.2.3 Ideate

Ideate merupakan tahapan peralihan dari identifikasi masalah untuk menciptakan sebuah solusi terhadap permasalahan tersebut. Pada tahap ini, penulis akan untuk mencari dan menemukan sebuah ide. Ide didapat berdasarkan informasi dan data yang telah didapatkan pada tahap *emphatize* dan *define*. Tahap *ideate* dilakukan menggunakan beberapa cara seperti *brainstorming*, *mindmapping* dan *sketching*

3.2.4 Prototype

Prototype merupakan fase uji coba desain untuk menemukan solusi terbaik. Berdasarkan ide yang telah diperoleh, tahap ini dapat dilakukan dengan menggambarkannya secara visual sebelum akhirnya diuji kepada *user* untuk mengetahui interaksi *user* terhadap solusi yang ditawarkan.

3.2.5 Test

Test merupakan fase akhir dalam proses desain, meskipun desainer dapat kembali menyesuaikan langkah-langkah sebelumnya. Tahap ini bertujuan untuk mendapatkan *feedback* dari *user* yang kemudian digunakan untuk meningkatkan solusi dari masalah desain. Pada tahap ini, penulis perlu memahami *user* dan mengembangkan solusi potensial berdasarkan hasil dari *test* yang telah diuji.