Jitu: Jurnal Informatika Utama
Vol. 3, No. 1 Mei 2025
e-ISSN 2988-7631
Hal: 82-93

ANALISIS KESADARAN ANCAMAN PHISING DI SOCIAL MEDIA TERHADAP GEN Z DI INDONESIA RENTANG UMUR 12-27 TAHUN MENGGUNAKAN METODE LIKERT

Putri Wijiastuti[1], Hana Azahro[2], Achmad Edward[3]
Sistem Informasi Fakultas Ilmu Komputer Universitas Pamulang, Tangerang Selatan
E-mail : ptrputriastuti29@gmail.com

Abstrak

Penelitian ini menganalisis kesadaran ancaman phishing di media sosial terhadap generasi Z (Gen Z) di Indonesia dengan rentang usia 12-27 tahun menggunakan metode Likert. Media sosial menjadi platform utama interaksi Gen Z, namun sekaligus meningkatkan risiko serangan phishing yang bertujuan mencuri data pribadi melalui manipulasi psikologis. Survei yang melibatkan 101 responden mengungkap bahwa meskipun sebagian besar Gen Z memahami phishing dan dapat mengenali tautan berbahaya, kesadaran ini belum sepenuhnya tercermin dalam praktik keamanan digital seperti penggantian kata sandi rutin dan penggunaan autentikasi dua faktor. Penggunaan media sosial yang tinggi meningkatkan eksposur terhadap ancaman phishing, namun edukasi formal terkait keamanan siber masih minim. Metode Likert membantu mengukur persepsi, pengalaman, dan sikap Gen Z terhadap phishing secara kuantitatif, meskipun terdapat tantangan berupa bias responden dan keterbatasan skala ordinal dalam menangkap perilaku sebenarnya. Hasil penelitian ini menegaskan pentingnya peningkatan literasi dan edukasi keamanan siber yang interaktif dan relevan untuk melindungi Gen Z dari ancaman phishing yang semakin kompleks di era digital. Temuan ini juga dapat menjadi dasar pengembangan kebijakan keamanan siber yang lebih efektif dan terarah untuk generasi muda Indonesia.

Kata Kunci: phishing, media sosial, generasi Z

Abstract

This study analyzes the awareness of phishing threats on social media among Generation Z (Gen Z) in Indonesia aged 12-27 using the Likert method. Social media is the primary platform for Gen Z interactions but also increases the risk of phishing attacks aimed at stealing personal data through psychological manipulation. A survey of 101 respondents revealed that although most Gen Z understand phishing and can recognize suspicious links, this awareness is not fully reflected in digital security practices such as routine password changes and two-factor authentication use. High social media usage increases exposure to phishing threats, yet formal cybersecurity education remains limited. The Likert method helps quantitatively measure Gen Z's perceptions, experiences, and attitudes toward phishing, despite challenges such as respondent bias and the ordinal scale's limitations in capturing actual behavior. The findings highlight the importance of enhancing interactive and relevant cybersecurity literacy and education to protect Gen Z from increasingly complex phishing threats in the digital era. These results also provide a foundation for developing more effective and targeted cybersecurity policies for Indonesia's youth.

Keywords: *phishing, social media, Generation Z*

Creative Commons Attribution 4.0 International License

PENDAHULUAN

Kemajuan teknologi informasi dan komunikasi telah memberikan dampak besar dalam berbagai aspek kehidupan manusia, termasuk dalam cara berinteraksi dan berbagi informasi. Media sosial menjadi salah satu produk teknologi yang sangat populer di kalangan generasi muda, terutama Gen Z, yang lahir pada rentang tahun 1997 hingga 2012. Kelompok ini, dengan rentang usia 16-25 tahun, dikenal sebagai digital natives, yaitu generasi yang tumbuh bersama perkembangan teknologi digital. Penggunaan media sosial bagi Gen Z tidak hanya menjadi sarana komunikasi, tetapi juga sebagai ruang untuk mencari informasi, hiburan, dan mengekspresikan diri.

Namun, tingginya intensitas penggunaan media sosial di kalangan Gen Z juga meningkatkan risiko mereka terhadap ancaman keamanan siber, salah satunya adalah phishing.(Sutabri, 2023) Phishing adalah salah satu bentuk kejahatan siber yang dilakukan dengan tujuan mencuri informasi pribadi atau data sensitif pengguna melalui metode manipulasi psikologis.

Para pelaku phishing sering memanfaatkan platform media sosial sebagai sarana untuk menjebak korban, mengingat media ini memiliki populasi pengguna yang sangat besar dan sering kali kurang memiliki kesadaran keamanan siber yang memadai. Modus phishing di media sosial biasanya melibatkan pembuatan akun palsu, pengiriman pesan berisi tautan berbahaya, atau penyebaran informasi palsu untuk mendapatkan data pribadi, seperti kata sandi, informasi kartu kredit, atau nomor telepon.

(Simanungkalit et al., 2024) Gen Z, yang cenderung lebih aktif di media sosial dan memiliki tingkat kepercayaan yang tinggi terhadap teknologi, menjadi salah satu kelompok yang rentan terhadap ancaman ini. Phishing telah menjadi salah satu ancaman keamanan siber yang signifikan, terutama di era media sosial. Dengan semakin canggihnya teknik manipulasi psikologis, phishing memanfaatkan kelemahan manusia dalam mengenali ancaman. Ancaman ini sering kali mencakup interupsi, intersepsi, modifikasi, dan fabrikasi yang dapat menyebabkan kerugian integritas data dan privasi pengguna (Salman Farizy, 2022) Sebuah survei global menunjukkan bahwa lebih dari 80% pengguna media sosial pernah menerima tautan atau pesan yang mencurigakan.

Di Indonesia, tingginya tingkat penetrasi internet dan penggunaan media sosial juga memperbesar peluang terjadinya kejahatan phishing. Laporan dari Kementerian Komunikasi dan Informatika menyebutkan bahwa kasus penipuan digital, termasuk phishing, meningkat secara signifikan dalam beberapa tahun terakhir.(Iskandar, 2024) Namun, meskipun ancaman ini semakin berkembang, tingkat kesadaran dan pengetahuan Gen Z tentang phishing masih relatif rendah.

Hal ini sering kali diperburuk oleh kurangnya pendidikan atau pelatihan khusus mengenai keamanan siber di tingkat sekolah atau perguruan tinggi. Dalam konteks ini, penting untuk melakukan analisis lebih mendalam tentang ancaman phishing di media sosial terhadap Gen Z.

Penelitian ini bertujuan untuk mengidentifikasi sejauh mana ancaman phishing memengaruhi pengguna media sosial berusia 16-25 tahun, serta untuk mengukur tingkat kesadaran dan sikap mereka terhadap ancaman tersebut. Dengan menggunakan metode Likert, penelitian ini akan mengevaluasi persepsi,

Creative Commons Attribution 4.0 International License

pengalaman, dan respons Gen Z terhadap phishing di media sosial. Metode ini dipilih karena memungkinkan pengukuran data kualitatif dalam bentuk skala numerik, sehingga memberikan gambaran yang lebih jelas tentang pola pikir dan sikap kelompok tersebut terhadap ancaman phishing. (Firdausiah Ersa et al., 2024)Penelitian ini memiliki signifikansi penting, baik secara akademis maupun praktis.

Secara akademis, penelitian ini diharapkan dapat memberikan kontribusi terhadap literatur keamanan siber, khususnya yang berkaitan dengan ancaman phishing di media sosial. Secara praktis, hasil penelitian ini dapat digunakan sebagai dasar untuk mengembangkan program edukasi dan kebijakan keamanan siber yang lebih efektif, terutama bagi kelompok Gen Z. Dengan demikian, penelitian ini tidak hanya bertujuan untuk mengidentifikasi ancaman, tetapi juga memberikan solusi untuk meningkatkan kesadaran dan perlindungan terhadap ancaman phishing di kalangan generasi muda.

1. Phising Sebagai Ancaman Siber

Phishing merupakan salah satu bentuk kejahatan siber yang bertujuan untuk mencuri informasi sensitif, seperti kata sandi, nomor kartu kredit, atau data pribadi, melalui manipulasi psikologis. Menurut (Hamim et al., 2023) Phishing adalah teknik rekayasa sosial yang memanfaatkan kepercayaan pengguna terhadap media komunikasi tertentu untuk menjebak korban. Ancaman phishing semakin berkembang seiring dengan meningkatnya adopsi teknologi digital dan media sosial, yang menjadi platform ideal bagi pelaku untuk menargetkan korban secara masif. Studi dari (Simanungkalit et al., 2024) menunjukkan bahwa media sosial, seperti Instagram, Facebook, dan Twitter, sering kali digunakan oleh pelaku phishing karena sifatnya yang interaktif dan kemudahan berbagi informas.

Phishing merupakan salah satu bentuk kejahatan siber yang bertujuan untuk mencuri informasi sensitif, seperti kata sandi, nomor kartu kredit, atau data pribadi, melalui manipulasi psikologis.Menurut (Fatmala Putri & Ratna Sari, 2023) phishing adalah teknik rekayasa sosial yang memanfaatkan kepercayaan pengguna terhadap media komunikasi tertentu untuk menjebak korban. Ancaman phishing semakin berkembang seiring dengan meningkatnya adopsi teknologi digital dan media sosial, yang menjadi platform ideal bagi pelaku untuk menargetkan korban secara masif. (Fatmala Putri & Ratna Sari, 2023)menunjukkan bahwa media sosial, seperti Instagram, Facebook, dan Twitter, sering kali digunakan oleh pelaku phishing karena sifatnya yang interaktif dan kemudahan berbagi informasi.

2. Media Sosial dan Kerentanannya terhadap Phishing

Serangan phishing sering menggunakan metode social engineering untuk menipu pengguna melalui pesan atau tautan palsu yang dirancang menyerupai sumber terpercaya. Social engineering adalah teknik yang mengandalkan manipulasi psikologis untuk mendapatkan akses tidak sah atau data sensitif. Phishing, sebagai bagian dari metode ini, merupakan salah satu bentuk ancaman keamanan siber yang paling banyak dilaporkan pada platform digital sedangkan media sosial telah menjadi bagian integral dari kehidupan Gen Z. Studi oleh (khaidir Laksamana, 2024)mengungkapkan bahwa lebih dari 90% Gen Z menggunakan media sosial setiap hari, dengan rata-rata waktu penggunaan

Creative Commons Attribution 4.0 International License

mencapai 3-4 jam per hari. Platform seperti Instagram, TikTok, dan Twitter sering digunakan untuk komunikasi, hiburan, hingga berbisnis.

Namun, tingginya intensitas penggunaan media sosial ini juga meningkatkan eksposur terhadap ancaman phishing (Ahmad Sari,2020). menunjukkan bahwa modus phishing di media sosial biasanya melibatkan tautan berbahaya yang disamarkan dalam bentuk pesan pribadi, komentar, atau promosi diskon palsu. Kerentanan Gen Z terhadap phishing di media sosial dipengaruhi oleh beberapa faktor, seperti tingkat kepercayaan yang tinggi terhadap platform digital, kurangnya pengetahuan tentang keamanan siber, serta minimnya kesadaran terhadap tanda-tanda phishing. Studi dari Prasetyo dan Dewi (2019) mencatat bahwa banyak pengguna media sosial, termasuk Gen Z, sering kali gagal mengenali tautan berbahaya atau akun palsu, sehingga menjadi korban phishing.

3. Gen Z dan Kesadaran Keamanan Siber

Gen Z, yang lahir di era digital, sering kali dianggap memiliki kemampuan teknologi yang lebih baik dibandingkan generasi sebelumnya. Namun, penelitian menunjukkan bahwa keahlian ini tidak selalu diiringi dengan kesadaran terhadap ancaman keamanan siber. Menghadapi ancaman phishing memerlukan penerapan langkah-langkah preventif seperti penggunaan firewall, enkripsi, serta pembaruan perangkat lunak secara berkala. Langkah-langkah ini bertujuan untuk mencegah akses tidak sah, menjaga kerahasiaan informasi, dan meningkatkan ketahanan sistem terhadap serangan siber (Farizy & Eriana, 2022). Sedangkan menurut laporan dari (Dyah Pawestri, 2021)hanya 35% dari Gen Z yang benar-benar memahami risiko keamanan di dunia maya, termasuk phishing.

Rendahnya tingkat kesadaran ini sering kali diperburuk oleh kurangnya edukasi formal tentang keamanan siber di tingkat sekolah dan perguruan tinggi(Anastasiah & Pandia, 2024). Gen Z juga cenderung lebih mudah terpengaruh oleh manipulasi psikologis, terutama jika phishing dilakukan melalui metode yang terlihat personal dan relevan dengan minat mereka. Penelitian oleh (Fatmala Putri & Ratna Sari, 2023)menemukan bahwa pesan phishing yang dirancang dengan memanfaatkan data pribadi atau kebiasaan pengguna cenderung lebih efektif dalam menjebak korban dari kalangan Gen Z.

4. Metode Likert dalam Penelitian Phishing

Metode Likert sering digunakan untuk mengukur sikap, persepsi, dan tingkat kesadaran individu terhadap suatu fenomena. Dalam konteks penelitian phishing, metode ini memberikan gambaran kuantitatif tentang respons pengguna terhadap ancaman tertentu. Studi oleh (Ukkas Irwan Mohammad, 2017)menunjukkan bahwa skala Likert sangat efektif untuk mengukur kesadaran dan persepsi pengguna terhadap ancaman phishing, karena memungkinkan pengumpulan data yang terstruktur dan mudah dianalisis. Penelitian dengan metode Likert biasanya melibatkan penyusunan kuesioner dengan serangkaian pernyataan yang menggambarkan sikap atau persepsi responden. Pernyataan ini dikategorikan dalam skala ordinal, mulai dari "sangat tidak setuju" hingga "sangat setuju." Metode ini tidak hanya membantu memahami tingkat kesadaran pengguna, tetapi juga mengidentifikasi faktor-faktor yang memengaruhi kerentanan terhadap phishing, seperti pengalaman, pengetahuan, dan sikap terhadap keamanan siber.

Creative Commons Attribution 4.0 International License

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif untuk menganalisis ancaman phishing di media sosial terhadap Gen Z dengan rentang usia 16–25 tahun. Metode pengumpulan data dilakukan melalui survei dengan menggunakan kuesioner sebagai instrumen utama. Kuesioner dirancang menggunakan skala Likert 5 poin, di mana responden diminta untuk memberikan penilaian terhadap berbagai pernyataan terkait pengalaman, pengetahuan, serta persepsi mereka tentang ancaman phishing di media sosial.

Skala Likert digunakan untuk mengukur tingkat setuju atau tidak setuju responden terhadap pernyataan-pernyataan tersebut, sehingga memungkinkan penelitian ini mendapatkan data yang bersifat terukur dan dapat dianalisis secara statistik. Populasi penelitian adalah individu dalam rentang usia 16–25 tahun yang merupakan pengguna aktif media sosial. Teknik pengambilan sampel menggunakan metode *purposive sampling* untuk memastikan bahwa responden memiliki pengalaman yang relevan dengan fenomena phishing di media sosial. Jumlah sampel yang digunakan ditentukan berdasarkan perhitungan *sample size* yang memadai untuk analisis statistik, yaitu minimal 100 responden. Setelah data terkumpul, analisis dilakukan menggunakan metode statistik deskriptif untuk memberikan gambaran umum tentang persepsi dan pengetahuan responden.

Selain itu, analisis inferensial dilakukan untuk mengidentifikasi hubungan atau pengaruh antara variabel-variabel yang diukur, seperti tingkat pemahaman tentang phishing, frekuensi penggunaan media sosial, dan tingkat kewaspadaan terhadap ancaman phishing. Uji validitas dan reliabilitas kuesioner dilakukan terlebih dahulu untuk memastikan bahwa instrumen penelitian memenuhi standar keandalan dan akurasi dalam pengukuran.Hasil analisis ini diharapkan dapat memberikan wawasan yang mendalam tentang kerentanan Gen Z terhadap ancaman phishing di media sosial dan memberikan dasar bagi pengembangan strategi edukasi serta kebijakan keamanan digital yang lebih efektif.

Metode Likert digunakan dalam penelitian ini untuk mengukur persepsi, sikap, dan tingkat kesadaran Gen Z terhadap ancaman phishing di media sosial. Metode ini dipilih karena memberikan kemampuan untuk memperoleh data kuantitatif yang merepresentasikan sikap individu terhadap berbagai pernyataan atau indikator yang berkaitan dengan topik yang diteliti. Skala Likert memungkinkan peneliti menyusun serangkaian pernyataan yang mencerminkan aspek-aspek penting dari ancaman phishing, seperti kesadaran terhadap tanda-tanda phishing, tingkat kepercayaan terhadap media sosial, pengalaman sebelumnya sebagai korban phishing, dan perilaku keamanan siber yang dilakukan sehari-hari. Responden diminta untuk menunjukkan tingkat persetujuan mereka terhadap pernyataan-pernyataan tersebut menggunakan skala ordinal, mulai dari "sangat tidak setuju" hingga "sangat setuju." Dalam konteks penelitian ini, penggunaan metode Likert bertujuan untuk memahami sejauh mana Gen Z menyadari keberadaan dan bahaya phishing, (Michael Saputra & Lioe Valencia, 2024)serta bagaimana mereka bereaksi terhadap potensi ancaman tersebut. Data yang dikumpulkan melalui kuesioner Likert memungkinkan identifikasi pola-pola tertentu, seperti tingkat kesadaran yang rendah

Creative Commons Attribution 4.0 International License

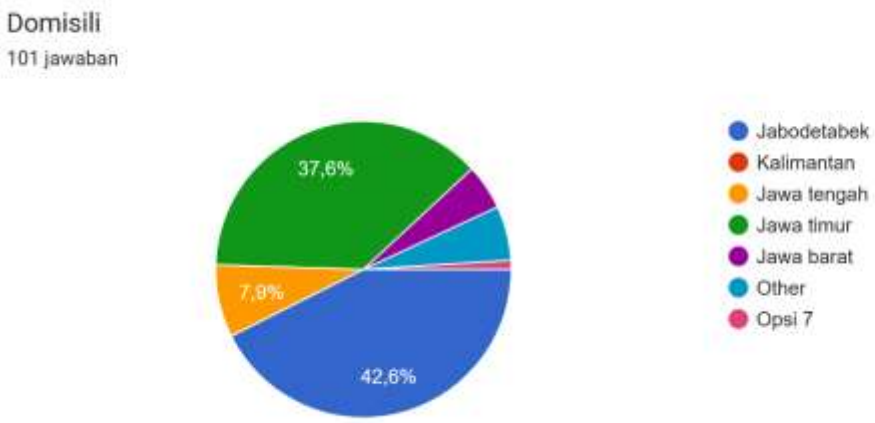
pada kelompok usia tertentu atau kecenderungan untuk mempercayai tautan yang dikirim melalui media sosial.

Peneliti juga memanfaatkan metode ini untuk mengevaluasi hubungan antara variabel-variabel seperti tingkat pendidikan, intensitas penggunaan media sosial, dan pengalaman sebelumnya sebagai korban phishing dengan sikap terhadap keamanan siber. (Iskandar, 2024)Selain itu, metode Likert memberikan fleksibilitas dalam pengolahan data. Peneliti dapat menggunakan analisis statistik deskriptif untuk mendapatkan gambaran umum tentang persepsi responden, serta analisis inferensial untuk mengidentifikasi hubungan atau perbedaan signifikan di antara kelompok-kelompok tertentu dalam populasi Gen Z. Dalam studi ini, Likert juga membantu peneliti untuk mengukur seberapa efektif program edukasi keamanan siber atau kampanye anti-phishing yang telah dilakukan. Hasil penelitian yang menggunakan metode Likert tidak hanya memberikan wawasan yang mendalam tentang persepsi dan sikap Gen Z, tetapi juga berfungsi sebagai dasar untuk rekomendasi kebijakan atau intervensi yang lebih terarah untuk melindungi kelompok usia ini dari ancaman phishing yang semakin berkembang di media sosial.(Firdausiah Ersa et al., 2024)

HASIL PENELITIAN

Studi ini bertujuan untuk menganalisis kesadaran Gen Z di Indonesia (rentang umur 12-27 tahun) terhadap ancaman phishing di media sosial menggunakan skala Likert. Disini kami mengumpulkan data melalui kuisioner dan berikut data yang kami dapatkan:

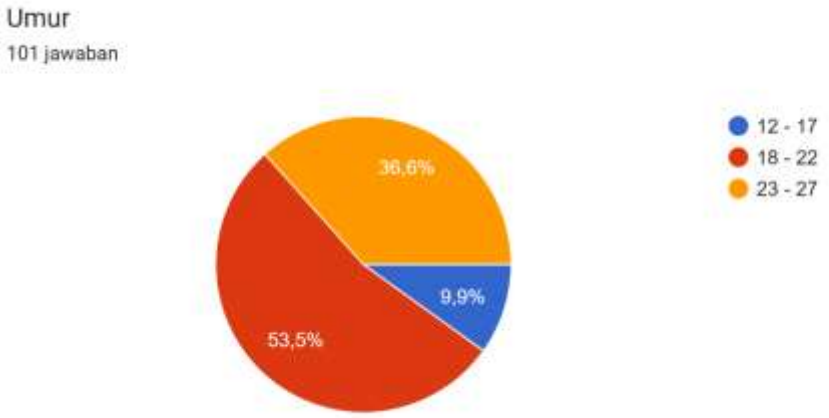
Data Domisili Responden Dimana pada hasil data tersebut disebutkan bahwa responden sebagian besar berdomisili pada Jabodetabek



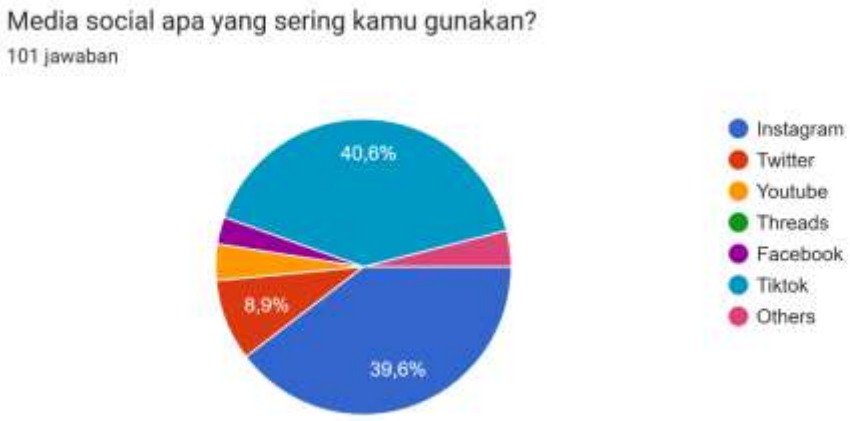
Gambar 1

Data umur Responden: Sebagian responden pada kuisioner inni Sebagian besar berumur 18-22 tahun Dan yang terakhir merupakan data media sosial yang digunakan adalah platform Tiktok dan Instagram.

Creative Commons Attribution 4.0 International License



Gambar 2.



Gambar 3

Perhitungan skala likert dilakukan dengan cara misalnya diberikan pernyataan yang dikemas dengan form kuisioner yang menggunakan skala Likert 5 poin untuk mengukur tingkat kewaspadaan Gen Z terhapan Ancaman Phising. Untuk menerjemahkan hasil skala likert adalah dengan analisis interval. Dan agar dapat dihitung dalam bentuk kuantitatif, jawaban dari responden diberi bobot atau skor. Didalam Kuisioner terdapat 12 pertanyaan dengan Skala yang terdiri dari 1 (Sangat Tidak Setuju) hingga 5 (Sangat Setuju).yang dibagi kedalam 4 garis besar.

Distribusi jawaban responden berdasarkan indikator skala disajikan dalam Tabel 1 berikut.

No	Indikator	Skor 1	Skor 2	Skor 3	Skor 4	Skor 5	Rata-rata
1	Saya mengetahui apa itu phishing dan bagaimana cara kerjanya	5	7	19	29	41	3,75
2	Saya dapat mengenali tautan berbahaya yang mencurigakan di media sosial	3	6	16	30	46	4,02

(cc) BY
Creative Commons Attribution 4.0 International License

3	Saya tahu cara melaporkan akun palsu di media sosial	4	9	17	25	46	3,93
4	Saya pernah menerima tautan atau pesan mencurigakan di media sosial	5	7	22	22	45	3,8
5	Saya pernah menjadi korban phishing di media sosial	40	25	15	9	12	2,51
6	Saya merasa penggunaan media sosial meningkatkan risiko keamanan data pribadi saya	6	8	19	36	32	3,64
7	Saya selalu memeriksa keaslian tautan sebelum mengkliknya	5	5	18	24	49	4,02
8	Saya rutin mengganti kata sandi media sosial saya	18	20	24	16	23	3,24
9	Saya mengaktifkan fitur keamanan tambahan seperti autentikasi dua faktor (2FA)	8	10	24	22	37	3,91
10	Saya merasa ancaman phishing di media sosial adalah masalah serius	0	2	10	29	60	4,52
11	Saya percaya bahwa edukasi tentang phishing dapat membantu melindungi pengguna dari ancaman ini	0	3	11	27	60	4,49
12	Saya merasa platform media sosial cukup aman untuk digunakan sehari-hari	5	9	34	23	30	3,51

Tabel 1

Berikut adalah temuan utama dari survei yang melibatkan 101 responden berdasarkan 4 point:

1. **Pengetahuan dan Kesadaran terhadap Phishing**
   - Sebagian besar responden menyatakan memahami phishing dan cara kerjanya, dengan rata-rata skor 3.75 dan median 4.

Creative Commons Attribution 4.0 International License

- Kemampuan untuk mengenali tautan berbahaya memiliki skor rata-rata tertinggi (4.02), menunjukkan bahwa mayoritas responden cukup mampu mengidentifikasi potensi ancaman.

2. **Pengalaman dan Kebiasaan Penggunaan Media Sosial**
   - Rata-rata skor pengalaman menerima tautan mencurigakan adalah 3.80, yang mengindikasikan bahwa mayoritas responden pernah menghadapi ancaman phishing secara langsung.
   - Meski demikian, hanya sedikit yang mengaku pernah menjadi korban phishing, dengan rata-rata skor 2.51.
   - Responden juga merasa risiko keamanan data pribadi meningkat akibat penggunaan media sosial (rata-rata skor 3.64).
3. **Perilaku Keamanan di Media Sosial**
   - Responden cukup berhati-hati dengan selalu memeriksa keaslian tautan sebelum mengkliknya (rata-rata 4.02).
   - Namun, kebiasaan mengganti kata sandi media sosial masih tergolong rendah dengan rata-rata skor 3.24.
   - Penggunaan fitur keamanan tambahan seperti autentikasi dua faktor (2FA) juga tergolong sedang, dengan rata-rata skor 3.91.
4. **Persepsi terhadap Ancaman Phishing dan Edukasi**
   - Responden sangat menyadari bahwa phishing merupakan ancaman serius, dengan rata-rata skor 4.52.
   - Edukasi tentang phishing dipandang sebagai langkah penting untuk melindungi pengguna, dengan rata-rata skor 4.49.
   - Meski ada kesadaran akan risiko, banyak yang merasa platform media sosial cukup aman untuk digunakan sehari-hari (rata-rata skor 3.51).

Berdasarkan file hasil survei, distribusi responden didominasi oleh pengguna media sosial aktif yang berada dalam kelompok usia 16–25 tahun. Sebagian besar responden menggunakan platform populer seperti Instagram dan TikTok, yang secara konsisten disebut sebagai media dengan risiko phishing tertinggi. Hal ini menguatkan relevansi penelitian dalam konteks media sosial yang sering digunakan Gen Z. Hasil ini sesuai dengan latar belakang penelitian yang menyoroti tingginya penetrasi media sosial di Indonesia, terutama di kalangan Gen Z. Sesuai literatur, platform seperti TikTok dan Instagram tidak hanya menjadi sarana komunikasi tetapi juga target utama bagi pelaku phishing. Studi ini menunjukkan bahwa meskipun kesadaran akan ancaman cukup tinggi, praktik keamanan digital seperti pembaruan kata sandi atau penggunaan 2FA belum diterapkan secara konsisten, mengindikasikan adanya gap antara kesadaran dan tindakan. Berdasarkan temuan, edukasi tentang tanda-tanda phishing dan cara menghadapinya perlu diperkuat. Platform media sosial bersama lembaga pendidikan dapat menjalankan kampanye yang menargetkan Gen Z dengan pendekatan yang interaktif dan relevan, seperti simulasi ancaman phishing atau gamifikasi edukasi keamanan digital.

Penggunaan metode Likert dalam analisis ancaman phishing terhadap Gen Z memiliki kelebihan yang signifikan, namun juga menghadapi berbagai tantangan yang perlu diatasi agar hasil penelitian dapat diinterpretasikan secara valid dan reliabel. Salah satu tantangan utama adalah bias jawaban responden. Responden cenderung memberikan jawaban yang "aman" dengan memilih nilai tengah, seperti

Creative Commons Attribution 4.0 International License

"netral," untuk menghindari komitmen terhadap pilihan yang lebih ekstrem. Hal ini dapat mengurangi keakuratan data, terutama jika responden merasa kurang percaya diri atau tidak memahami dengan baik konteks phishing yang disajikan dalam pernyataan. Tantangan lain adalah kemungkinan kurangnya pemahaman responden terhadap ancaman phishing.

Gen Z memiliki latar belakang pengalaman dan pemahaman yang bervariasi mengenai keamanan siber. Jika responden tidak cukup memahami konsep phishing atau tidak mengenali risiko yang terlibat, mereka mungkin memberikan jawaban yang tidak konsisten atau kurang informatif. (Yesba Rianus Parindingan & Fathirah, 2024)Hal ini bisa berdampak pada validitas data, terutama jika kuesioner tidak dirancang dengan contoh atau deskripsi yang jelas. Selanjutnya, kesulitan dalam mengukur aspek kompleks dari phishing melalui skala ordinal juga menjadi tantangan. Phishing tidak hanya mencakup ancaman teknis, tetapi juga faktor psikologis dan perilaku, seperti tingkat kepercayaan, intuisi, dan reaksi terhadap situasi tertentu.

Metode Likert, meskipun efektif untuk mengukur sikap, memiliki keterbatasan dalam menangkap dimensi-dimensi perilaku atau tindakan nyata yang dilakukan responden. Kelemahan dalam analisis data Likert juga dapat menjadi hambatan. Data dari skala Likert bersifat ordinal, sehingga penggunaan analisis statistik yang tidak sesuai (seperti penghitungan rata-rata) dapat menimbulkan interpretasi yang kurang valid. Peneliti harus memastikan bahwa metode analisis yang digunakan sesuai dengan sifat data, seperti analisis frekuensi, chi-square, atau regresi logistik ordinal, untuk menghindari penyimpulan yang salah.

Selain itu, tantangan logistik dan teknis dalam penyebaran kuesioner juga tidak dapat diabaikan. Mengingat Gen Z adalah kelompok yang sangat bergantung pada media digital, pengumpulan data sering dilakukan secara daring.(Iskandar, 2024) Namun, pendekatan ini dapat menimbulkan tantangan seperti rendahnya tingkat partisipasi, kesulitan menjangkau responden dengan tingkat pendidikan atau pemahaman yang rendah, serta potensi manipulasi data oleh responden yang tidak serius. Terakhir, keberagaman latar belakang Gen Z menambah kompleksitas analisis. Gen Z memiliki variasi yang luas dalam hal pendidikan, pengalaman teknologi, dan penggunaan media sosial.

KESIMPULAN

Penelitian ini memberikan wawasan yang mendalam tentang ancaman phishing di media sosial yang dihadapi oleh generasi Z (Gen Z) dengan rentang usia 16–25 tahun. Sebagai kelompok yang sangat aktif menggunakan media sosial, Gen Z menjadi sasaran empuk bagi pelaku phishing yang memanfaatkan platform digital untuk mencuri informasi pribadi atau data sensitif melalui teknik manipulasi psikologis. Penelitian ini mengungkap bahwa rendahnya tingkat kesadaran keamanan siber, minimnya pendidikan formal tentang ancaman phishing, serta tingginya tingkat kepercayaan terhadap teknologi menjadikan Gen Z lebih rentan terhadap ancaman tersebut. Melalui penggunaan metode Likert, penelitian ini berhasil mengevaluasi persepsi, pengalaman, dan tingkat kesadaran Gen Z terhadap phishing. Hasil menunjukkan bahwa sebagian besar responden memiliki pemahaman yang terbatas tentang tanda-tanda phishing, seperti tautan berbahaya atau akun

Creative Commons Attribution 4.0 International License

palsu. Selain itu, intensitas tinggi penggunaan media sosial turut meningkatkan risiko Gen Z terhadap phishing, terutama ketika mereka kurang memiliki kewaspadaan terhadap pesan-pesan yang mencurigakan. Namun, penelitian ini juga mengidentifikasi tantangan dalam penggunaan metode Likert, termasuk bias responden, kurangnya pemahaman terhadap konsep phishing, dan keterbatasan skala ordinal dalam menangkap aspek perilaku. Meskipun demikian, metode ini memberikan data yang terstruktur dan memungkinkan analisis hubungan antara variabel, seperti pengalaman menjadi korban phishing dengan tingkat kesadaran keamanan siber. Secara keseluruhan, penelitian ini menegaskan pentingnya meningkatkan literasi keamanan digital di kalangan Gen Z melalui program edukasi dan kampanye yang lebih efektif. Kesadaran dan pemahaman yang lebih baik tentang phishing dapat membantu melindungi generasi muda dari ancaman siber yang semakin kompleks di era digital. Hasil penelitian ini juga memberikan kontribusi penting untuk pengembangan kebijakan keamanan siber yang lebih terarah, baik di tingkat individu maupun institusi.

DAFTAR PUSTAKA

Anastasiah, M., & Pandia, H. (2024). Analisis perilaku pengguna mobile banking terhadap keamanan informasi menggunakan metode Human Aspects of Information Security Questionnaire (HAIS-Q). *Journal of Social Science Research, 4*.

Dyah Pawestri, F. (2021). Korelasi antara information privacy concern dan perlindungan privasi pengguna Twitter di Indonesia. *ANUVA, 5*(2), 221–236.

Farizy, E. S. (2022). Keamanan sistem informasi. *Jurnal Pengabdian Ilmu Komputer*, 208.

Fatmala Putri, D., & Ratna Sari, W. (2023). Analisis perlindungan nasabah BSI terhadap kebocoran data dalam menggunakan digital banking. *Jurnal Ilmiah Ekonomi dan Manajemen, 1*(4), 173–181. https://doi.org/10.61722/jiem.v1i4.331

Firdausiah Ersa, L., Aningsih, G., Hidayat, T., & Febri Sonni, A. (2024). Analisis jaringan komunikasi penipuan daring melalui media sosial Whatsapp Messenger. *Jurnal Netnografi Komunikasi, 2*(2). http://netnografiikom.org/index.php/netnografi

Firmansyah, R., & Persada, G. N. (2024). Perancangan Sistem Pemesanan Produk pada Toko Merchandise. Id Berbasis Website Menggunakan Metode Prototype. *Jurnal Informatika Utama*, *2*(1), 1-13.

Hamim, N., Irwan, M., & Nasution, P. (2023). Analisis perlindungan hukum terhadap keamanan data privasi pada marketplace Shopee. *IJM: Indonesian Journal of Multidisciplinary, 1*. https://journal.csspublishing/index.php/ijm

Iskandar, O. (2024). *Analisis kejahatan online phishing pada masyarakat* (Vol. 1, Issue 2).

Laksamana, K. (2024). Analisis keamanan data terhadap penggunaan e-wallet sebagai alat transaksi digital untuk mencegah penipuan online.

Mohammad, U. I. (2017). Implementasi skala Likert pada metode perbandingan eksponensial untuk menentukan pilihan asuransi. *6*.

Parindingan, F. Y. R., & Fathirah, D. (2024). Strategi efektif untuk mengidentifikasi fraud di era digital.

Pugu, M. R., Riyanto, S., & Haryadi, R. N. (2024). *Metodologi Penelitian; Konsep, Strategi, dan Aplikasi*. PT. Sonpedia Publishing Indonesia.

Creative Commons Attribution 4.0 International License

Saputra, M., & Valencia, L. (2024). Analisis tingkat kesadaran risiko keamanan dan privasi dalam bermedia sosial berdasarkan gender dan generasi.

Simanungkalit, J. A. R., Hertadi, R., & Hosnah, A. U. (2024). Analisis tindak pidana penipuan online dalam konteks hukum pidana: Cara menanggulangi dan pencegahannya. *Jurnal Mahasiswa Humanis, 4*(2), 281–294.

Sutabri, T. (2023). Analisis kejahatan carding pada BNI 46. *Blantika: Multidisciplinary Journal, 2*(1). https://blantika.publikasiku.id/153

Zein, A. (2022). Evaluasi keamanan wireless LAN menggunakan ISSAF (Information System Security Assessment Framework). *Jurnal Sainstech*, 29–35.

Zein, A. (2024). Analisa penyerangan untuk cyber security social engineering. *Jurnal Teknik Informatika Unpam*, 642–648.

Creative Commons Attribution 4.0 International License