Jurnal Kreativitas Teknologi dan Komputer Vol. 15 No. 4, Apr 2024

PENGEMBANGAN WEBSITE PHISING UNTUK MENGANALISIS PENGARUH ANCAMAN PHISING DI KALANGAN MAHASISWA

Vannes Cristian[1], Jusia Amanda Ginting[2]
Universitas Bunda Mulia
E-mail: s32200037@student.ubm.ac.id[1],
jginting@bundamulia.ac.id[2]

Abstrak

Serangan phishing yang menyerang pengguna media sosial menimbulkan ancaman yang semakin serius. Penelitian ini bertujuan untuk mengukur tingkat kesadaran mahasiswa terhadap serangan phishing, khususnya melalui implementasi website palsu Instagram. Latar belakang penelitian ini dari kebutuhan untuk memahami sejauh mana mahasiswa dapat mengenali website phishing Instagram serta faktor-faktor yang memengaruhi tingkat kesadaran mereka. Metode penelitian melibatkan pengambilan data awal dengan kuesioner untuk menilai kesadaran mahasiswa terkait phishing. Berdasarkan hasil tersebut, dipilih target website phishing Instagram sebagai fokus implementasi.Analisis data dilakukan dengan membandingkan tampilan website phishing dan asli Instagram melalui dua kuesioner berbeda. Kuesioner pertama menilai UI tanpa menampilkan URL, sementara kuesioner kedua menampilkan URL. Hasil pengambilan data menunjukkan bahwa mahasiswa memiliki tingkat kesadaran keamanan rendah terhadap tampilan website phishing tanpa link, dengan mayoritas responden setuju bahwa tampilan tersebut sesuai dengan website resmi Instagram, namun kepercayaan tersebut mengalami penurunan sekitar 22% setelah melihat URL pada tampilan website palsu. Kesimpulan dari penelitian ini adalah bahwa kesadaran mahasiswa terhadap ancaman phishing butuh ditingkatkan melalui edukasi dan peringatan terkait URL phishing. Penelitian ini memberikan wawasan tentang tingkat keberhasilan serangan phishing dan faktor-faktor yang dapat memperngaruhi tingkat kesadaran keamanan mahasiswa. Pemahaman yang lebih baik terhadap ancaman ini diharapkan dapat meningkatkan keamanan pengguna Instagram dan mengurangi risiko jatuhnya korban dalam serangan phishing.

Kata Kunci — Phishing, Kesadaran Keamanan, Media Social, Instagram.

Abstract

Phishing attacks that attack social media users pose an increasingly serious threat. This study aims to measure the level of awareness of university students towards phishing attacks, specifically through the implementation of Instagram's fake website. The background of this research is from the need to understand the extent to which college students can recognize Instagram phishing websites as well as the factors that influence their level of awareness. The research method involved collecting baseline data with a questionnaire to assess students' awareness of phishing. Based on the results, the target Instagram phishing website was chosen as the focus of implementation.Data analysis was conducted by comparing the appearance of the phishing website and the original Instagram through two

different questionnaires. The first questionnaire assessed the UI without displaying the URL, while the second questionnaire displayed the URL. The results of the data collection show that students have a low level of security awareness of the phishing website display without a link, with the majority of respondents agreeing that the display is consistent with the official Instagram website, but the trust has decreased by about 22% after seeing the URL on the fake website display. The conclusion of this study is that students' awareness of phishing threats needs to be increased through education and warnings regarding phishing URLs. This study provides insights into the success rate of phishing attacks and the factors that may influence the security awareness level of college students. A better understanding of this threat is expected to improve the security of Instagram users and reduce the risk of falling victim to phishing attacks.

Keyword *— Phishing,Security Awareness,Social Media,Instagram.*

1. PENDAHULUAN

A) Latar Belakang

Internet merupakan interkoneksi dari satu jaringan ke jaringan yang lain yang menyebabkan hilangnya penghalang untuk berkomunikasi. Dunia pendidikan juga tidak bisa terlepas dari penggunaan teknologi ini. Penggunaan internet dan perangkat digital telah menjadi bagian penting di kehidupan sehari-hari terutama di kalangan mahasiswa.Mahasiswa sering menggunakan internet untuk berbagai tujuan, termasuk belajar, berkomunikasi, dan mencari hiburan. Terlepas dari keuntungan yang di miliki , internet mempunyai banyak sekali ancaman dan serangan untuk mendapatkan informasi dan keuntungan pribadi.

Salah satu serangan yang paling sering di jumpai adalah serangan phising. Phising adalah serangan yang berfokus pada pencurian informasi pribadi dengan memanfaatkan website atau email palsu yang tampak meyakinkan dan sering digunakan oleh pengguna atau user. Kegiatan phising bertujuan memancing orang untuk memberikan informasi pribadi secara sukarela tanpa disadari. Menurut laporan dari Anti-Phishing Working Group (APWG) pada tahun 2022 mencatat lebih dari 4,7 juta serangan sejak awal tahun 2019, jumlah serangan phishing telah meningkat lebih dari 150% per tahun.

Serangan phishing di dunia pendidikan juga telah menjadi perhatian khusus. Beberapa kasus serangan phishing terhadap mahasiswa telah terjadi, mengakibatkan kebocoran data pribadi. Hal ini menunjukkan bahwa mahasiswa merupakan kelompok yang rentan terhadap serangan ini di lingkungan pendidikan. Penelitian dengan judul “Analisis security awareness terhadap ancaman phising di kalangan mahasiswa” ini digunakan untuk mengukur tingkat awareness mahasiswa terhadap serangan phising.

B) Identifikasi Masalah

1. Bagaimana tingkat security awareness mahasiswa terhadap serangan phishing?
2. Bagaimana mengidentifikasi teknik phishing yang digunakan untuk mengelabui pengguna?

C) Tujuan Dan Manfaat Penelitian

Tujuan utama penelitian ini adalah untuk mengukur dan memahami sejauh mana mahasiswa memiliki kesadaran keamanan cyber terhadap serangan phishing. Hasil penelitian ini diharapkan dapat memberi kontribusi untuk meningkatkan pemahaman dan kesadaran mahasiswa terhadap ancaman phishing. Penelitian ini juga diharapkan bisa menjadi acuan bagi pihak universitas dalam mengembangkan program atau kebijakan yang bertujuan

meningkatkan security awareness di kalangan mahasiswa.

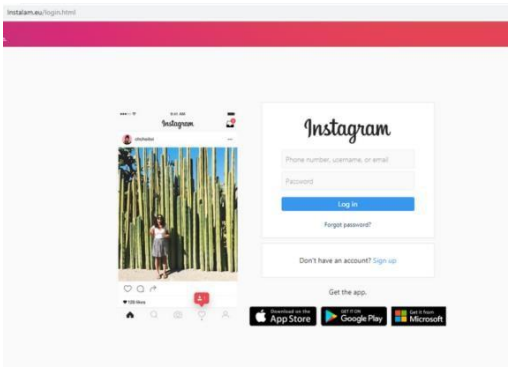
2. METODE PENELITIAN

1. Studi Literatur

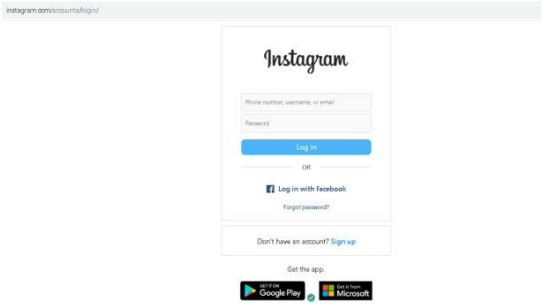
Metode penelitian mengumpulkan dan mengevaluasi penelitian terdahulu dari berbagai sumber literatur yang relevan untuk memberikan dasar teoretis yang kuat pada penelitian ini.

2. Pengambilan Data

Metode pengumpulan data menggunakan kuesioner untuk mengetahui website yang paling banyak diakses oleh sebagian mahasiswa dan platform apa yang paling sulit untuk di kenali sebagai website phishing. Kuesioner yang digunakan dalam penelitian ini disebarluaskan melalui media sosial seperti whatsapp, Line, & Instagram yang dibuat dengan bantuan Google Forms. Populasi penelitian untuk kuesioner ini merupakan mahasiswa aktif di kawasan Jakarta. Isi kuesioner yang di bagikan berupa pertanyaan mengenai website yang sering mereka akses dan beberapa pertanyaan terkait website-website phishing dimana narasumber diminta untuk memilih di antara 2 gambar website yang salah satu nya merupakan website phishing.



Gambar 1. Ancaman *Phishing*

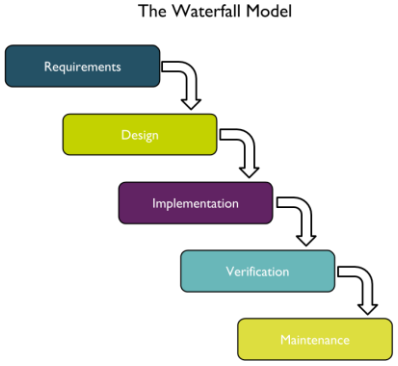


Gambar 2. Bukan Ancaman *Phishing*

setiap gambar yang diberikan ke narasumber, diberikan pilihan untuk memilih yang mana yang merupakan website phishing.

3. Waterfall

Metode pengembangan website phishing yang digunakan pada penelitian ini adalah metode waterfall.



Gambar 3. Waterfall Model

metode waterfall (waterfall model) terdiri dari tahapan(1)Requirements,(2)Design, (3)Implementation, (4)Testing/verification , dan (5)Maintenance.

a) Requirement Analysis

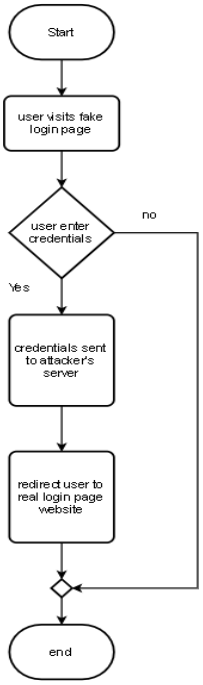
Pada tahapan requirement, pengambilan data menggunakan metode kuesioner dengan berbagai pertanyaan pilihan terkait gambar website phishing. Setelah melakukan pengambilan data di peroleh data-data seperti website yang mahasiswa sering akses dan website yang memiliki tingkat security awareness terendah.

b) Design

Tahap selanjutnya yaitu desain, setelah mengetahui website apa yang paling sering di akses oleh mahasiswa dan website yang memiliki tingkat security awanreness paling rendah maka kita dapat menentukan dan merancang desain website yang akan kita clone sebagai website phishing. Desain menggunakan low fidelity, mid fidelity dan high fidelity prototype. Berikut beberapa perancangan design diagram:

Flowchart sistem

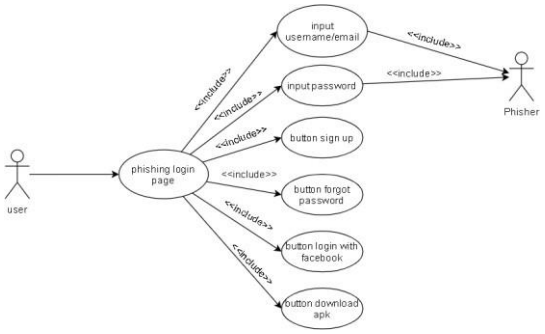
Flowchart adalah sebuah diagram yang menggambarkan alur proses atau alur logika suatu sistem.



Gambar 4. Flowchart sistem instagram phishing

Use Case Diagram

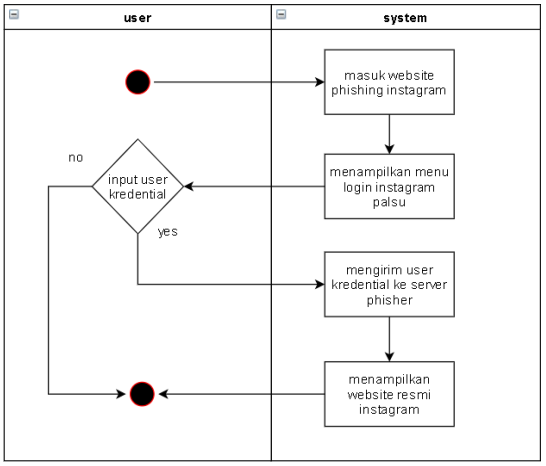
Use case diagram adalah interaksi antara aktor dengan sistem. Menunjukkan bagaimana aktor menggunakan sistem untuk mencapai tujuan tertentu.



Gambar 5. Use Case Diagram Instagram Phishing

Activity Diagram

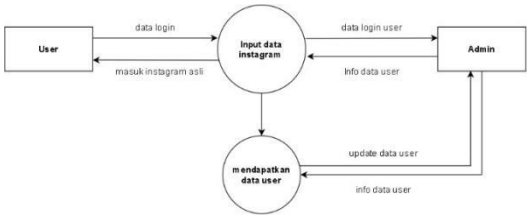
Activity diagram adalah diagram yang memodelkan proses-proses yang terjadi pada sebuah sistem. Activity diagram merupakan pengembangan dari Use Case yang memiliki alur aktivitas.



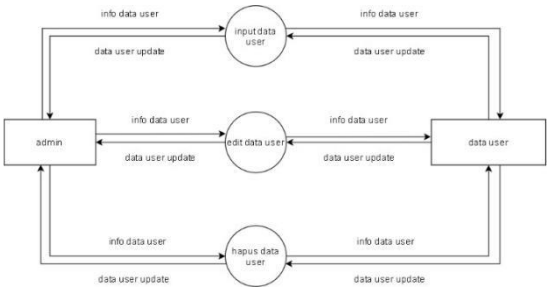
Gambar 6. Activity Diagram Instagram Phishing

Data Flow Diagram

Data Flow Diagram (DFD) adalah sebuah diagram yang digunakan untuk menggambarkan alur atau aliran data dalam suatu sistem. DFD merupakan alat visualisasi yang membantu dalam memodelkan proses- proses yang terjadi dalam suatu organisasi atau sistem.



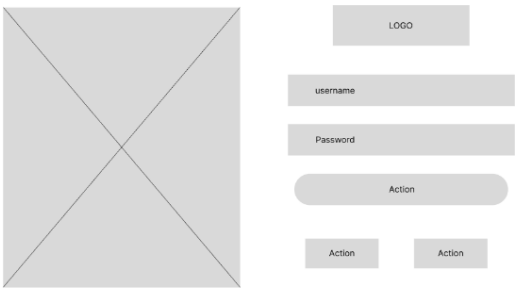
Gambar 7. Data Flow Diagram Instagram Phishing



Gambar 8. Data Flow Diagram data user

Low Fidelity Design

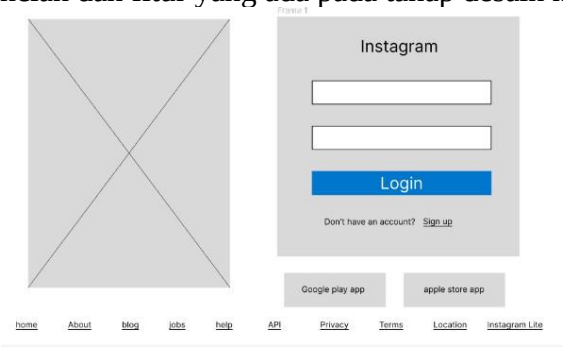
Low fidelity design adalah representasi konsep atau prototipe yang sederhana dan tidak memiliki detail visual atau fungsionalitas penuh.



Gambar 9. Low Fidelity Design Instagram Phishing

Medium Fidelity Design

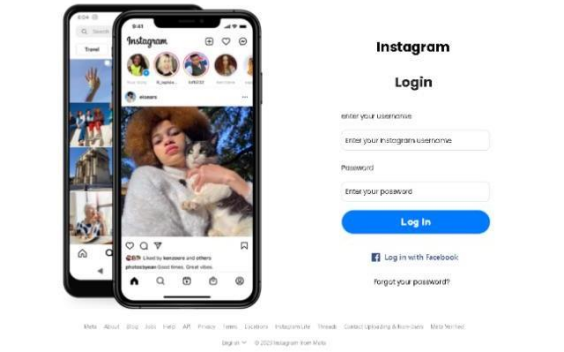
Medium-fidelity design adalah tahap dalam proses desain di mana desainer menciptakan prototipe desain dengan tingkat detail dan keterlibatan yang berada di tengah tengah antara desain low-fidelity dan desain high- fidelity. Medium-fidelity design bertujuan untuk memberikan gambaran yang lebih rinci tentang bagaimana sistem akan terlihat , tanpa harus menyertakan semua rincian dan fitur yang ada pada tahap desain high-fidelity.



Gambar 10. Medium Fidelity Design Instagram Phishing

High Fidelity Design

High-fidelity design adalah tahap dalam proses desain di mana desainer menciptakan prototipe atau representasi desain dengan tingkat detail yang sangat tinggi dan mendekati produk atau sistem final. Desain ini mencakup elemen visual, interaktif, dan fungsionalitas yang sangat rinci, memberikan gambaran yang akurat tentang bagaimana produk atau sistem akan terlihat dan berperilaku.



Gambar 11. High Fidelity Design Instagram Phishing

c) Implementation

Tahapan selanjutnya adalah mengimplementasikan desain menjadi program dengan bahasa pemrograman/coding. Pada perancangan website ini menggunakan bahasa pemrograman html , css dan php dengan microsoft visual studio code. Pada database untuk menyimpan data korban phishing menggunakan MySQL phpMyAdmin.

d) Verification/Testing

Tahap selanjutnya adalah tahapan testing untuk melihat apakah program atau wehsite dapat berfungsi dengan baik. Testing menggunakan black box testing untuk menguji apakah website phishing dapat berfungsi dengan baik dan dapat memanipulasi calon korban phishing.

e) Maintenance

Tahap selanjutnya yaitu pemeliharaan baru dilaksanakan apabila produk sudah dikeluarkan dan ada kesalahan yang ditemukan pada saat sistem digunakan langsung oleh user.

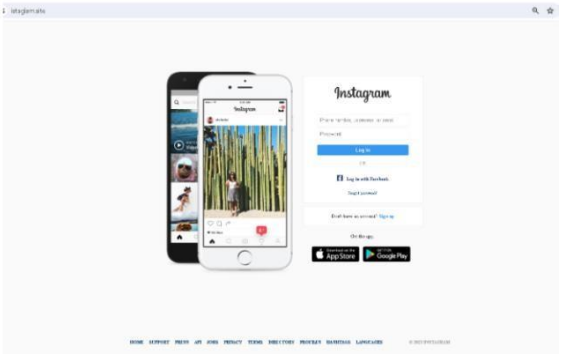
4. Analisis Data

Analisis di lakukan dengan melakukan perbandingan website instagram phishing dengan menampilkan URL dan tanpa URL menggunakan 2 kuesioner berbeda. Berdasarkan hasil pengambilan data menggunakan kuesioner dikumpulkan 50 responden. Berdasarkan jawaban responden. Perhitungan kuesioner akan dilakukan menggunakan perhitungan skala likert.

3. HASIL DAN PEMBAHASAN

a) Implementasi Antarmuka

Dalam tahap implementasi antarmuka disajikan hasil pembuatan antarmuka website phishing instagram.



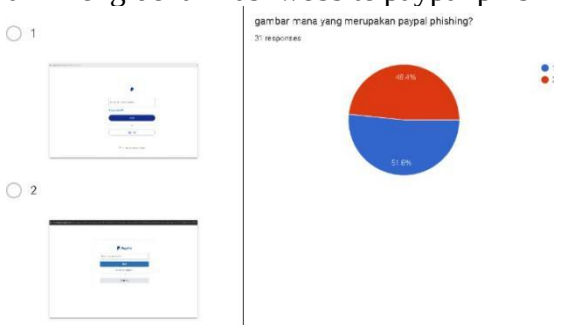
Gambar 12. Antarmuka website phishing instagram

b) Hasil Pengambilan Data Awal

Hasil pengambilan data awal menggunakan kuesioner untuk menentukan website yang akan dirancang dikumpulkan 31 responden. Beberapa website yang memiliki poin rendah sebagai berikut:

-Paypal

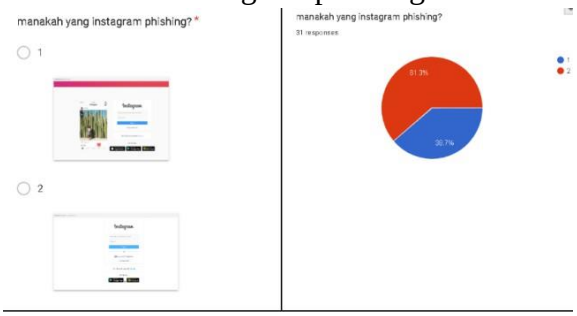
Pada platform paypal, responden cenderung seimbang di mana ada 51.6% /16 responden yang keliru dalam mengidentifikasi website paypal phishing



Gambar 13. diagram responden phishing paypal

-Instagram

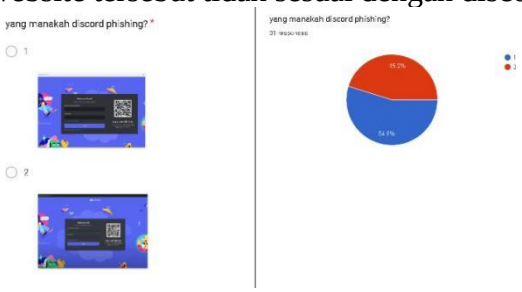
website instagram menjadi website yang paling sulit untuk di identifikasi sebagai website phishing. Terdapat 61.3% atau 19 dari 31 responden yang keliru dalam mengindentifikasi yang mana website instagram phishing.



Gambar 14. diagram responden phishing instagram

-Discord

Pada gambar kuisioner tersebut sekilas tidak ada perbedaan sama sekali dengan kedua website discord tersebut, namun jika di lihat lebih teliti gambar 2 merupakan discord phishing di mana link atau url dari website tersebut tidak sesuai dengan discord original.



Gambar 15. diagram responden Discord phishing

Dari data-data diatas, website phishing yang akan di implementasikan pada penelitian ini adalah website instagram.

c) Pengujian keberhasilan sistem website phishing

Pengujian dilakukan dengan metode black box testing untuk mengevaluasi fungsionalitas sistem dari website phishing instagram.

Tabel 1. pengujian keberhasilan sistem

No	Kegiatan testing	Input	Output	Hasil
1	Uji input kredential	Masukan usernane dan password	Username dan password user	sesuai
2	Uji tombol login	Klik button login	Memasukan kredential user ke database phisher dan menampilkan halaman website instagram resmi	sesuai
3	Uji tombol log in facebook	Klik button log in with facebook	Menampilkan halaman login facebook	sesuai
4	Uji tombol forgot password	Klik button forgot password	Menampilkan halaman forgot password instagram resmi	sesuai
5	Uji tombol sign up	Klik button sign up	Menampilkan halaman sign up instagram resmi	sesuai
6	Uji tombol get the app google play dan app store	Klik button google play dan apps store	Menampilkan halaman download aplikasi instagram	sesuai

d) Analisis Data

Analisis di lakukan dengan melakukan perbandingan website instagram phishing menggunakan 2 kuesioner berbeda yang dibagikan pada para mahasiswa di Jakarta. Kuesioner pertama hanya menampilkan UI atau tampilan dari website instagram phishing kemudian kuesioner kedua menampilkan link pada website untuk membandingkan bagaimana pendapat responden terhadap tampilan kuesioner website phishing tanpa link dan website phishing dengan menampilkan link nya. Berdasarkan hasil pengambilan data menggunakan kuesioner pertama dikumpulkan 50 responden. Berdasarkan jawaban responden, sebagian besar jenis kelamin sampel yang diperoleh adalah Laki-laki. Berdasarkan domisili di peroleh di dominasi jakarta Pusat.

Tabel 2. responden berdasarkan jenis kelamin

Jenis Kelamin

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	PRIA	33	66.0	66.0	66.0
	WANITA	17	34.0	34.0	100.0
	Total	50	100.0	100.0	

Tabel 3. responden berdasarkan Domisili

Domisili

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Jakarta Barat	5	10.0	10.0	10.0
	Jakarta Pusat	30	60.0	60.0	70.0
	Jakarta Selatan	4	8.0	8.0	78.0
	Jakarta Timur	8	16.0	16.0	94.0
	Jakarta Utara	3	6.0	6.0	100.0
	Total	50	100.0	100.0	

Tabel 4. responden berdasarkan semester

semester

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	2	4.0	4.0	4.0
	3	6	12.0	12.0	16.0
	4	9	18.0	18.0	34.0
	5	9	18.0	18.0	52.0
	6	11	22.0	22.0	74.0
	7	9	18.0	18.0	92.0
	8	4	8.0	8.0	100.0
	Total	50	100.0	100.0	

Untuk perhitungan penyelesaian akhir didapatkan dengan rumus berikut:

$$indeks(\%) = \frac{\text{total skor}}{Y} * 100$$

Total skor = Jumlah dari perkalian total responden dan nilai skala likert.

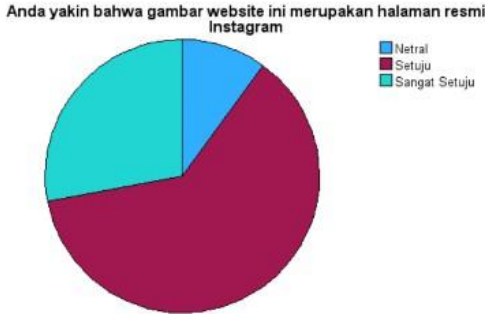
Y = Jumlah dari hasil perkalian antara Jumlah responden menjawab dan skor tertinggi likert.

Kuesioner 1

Tabel 5. responden kuesioner 1

Anda yakin bahwa gambar website ini merupakan halaman resmi Instagram

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Netral	5	10.0	10.0	10.0
	Setuju	31	62.0	62.0	72.0
	Sangat Setuju	14	28.0	28.0	100.0
	Total	50	100.0	100.0	



Indeks pertanyaan

$$indeks(\%) = \frac{209}{250} * 100 = 83{,}6\% \quad \text{——}$$

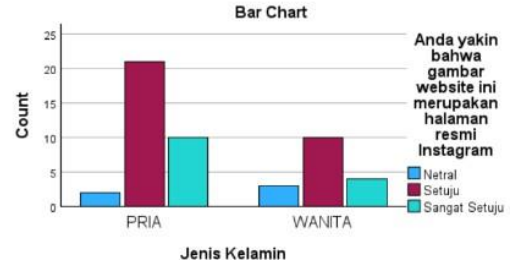
Diagram di atas menunjukan 62% setuju bahwa gambar website tersebut adalah website resmi instagram, 28% sangat setuju website tersebut adalah website resmi dan 10% netral terhadap gambar website tersebut.

Tabel 6. perbandingan responden kuesioner 1 berdasarkan jenis kelamin

Jenis Kelamin * Anda yakin bahwa gambar website ini merupakan halaman resmi Instagram Crosstabulation

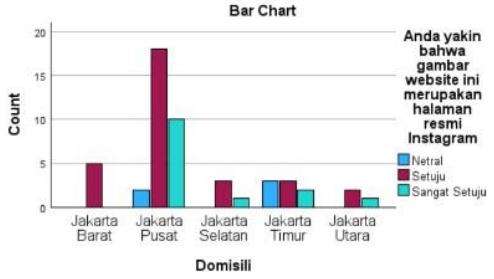
Count

		Anda yakin bahwa gambar website ini merupakan halaman resmi Instagram			
		Netral	Setuju	Sangat Setuju	Total
Jenis Kelamin	PRIA	2	21	10	33
	WANITA	3	10	4	17
Total		5	31	14	50



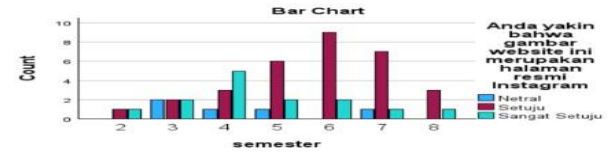
Tabel 7. perbandingan responden kusioner

		Anda yakin bahwa gambar website ini merupakan halaman resmi Instagram			
		Netral	Setuju	Sangat Setuju	Total
Domisili	Jakarta Barat	0	5	0	5
	Jakarta Pusat	2	18	10	30
	Jakarta Selatan	0	3	1	4
	Jakarta Timur	3	3	2	8
	Jakarta Utara	0	2	1	3
Total		5	31	14	50



Tabel 8. perbandingan responden kuesioner 1 berdasarkan semester

		Anda yakin bahwa gambar website ini merupakan halaman resmi Instagram			
		Netral	Setuju	Sangat Setuju	Total
semester	2	0	1	1	2
	3	2	2	2	6
	4	1	3	5	9
	5	1	6	2	9
	6	0	9	2	11
	7	1	7	1	9
	8	0	3	1	4
Total		5	31	14	50



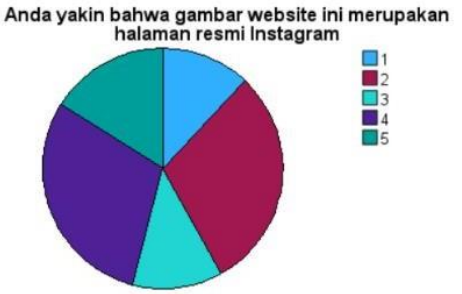
Berdasarkan data-data diatas dapat disimpulkan bahwa 83,6% responden setuju bahwa tampilan website instagram pada kuesioner merupakan website instagram resmi.

Kuesioner 2

Tabel 9. responden kuesioner 2

Anda yakin bahwa gambar website ini merupakan halaman resmi Instagram

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	6	12.0	12.0	12.0
	2	15	30.0	30.0	42.0
	3	6	12.0	12.0	54.0
	4	15	30.0	30.0	84.0
	5	8	16.0	16.0	100.0
	Total	50	100.0	100.0	



Indeks pertanyaan

$$indeks(\%) = \frac{154}{250} * 100 = 61{,}6\%$$

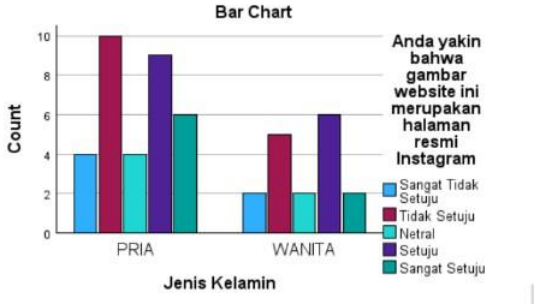
Diagram di atas menunjukan 16% responden sangat setuju bahwa website phishing ini merupakan website resmi, 30% responden setuju , 12% responden netral , 30% sangat tidak setuju dan 12% sangat tidak setuju. Hal ini menunjukan penurunan kepercayaan responden terhadap website tersebut setelah melihat url atau link website tersebut.

Tabel 10. perbandingan responden kuesioner 2 berdasarkan jenis kelamin

Jenis Kelamin * Anda yakin bahwa gambar website ini merupakan halaman resmi Instagram Crosstabulation

Count

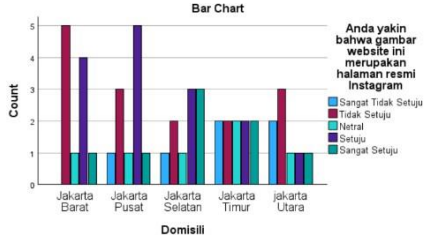
		Jenis Kelamin		
		PRIA	WANITA	Total
Anda yakin bahwa gambar website ini merupakan halaman resmi Instagram	Sangat Tidak Setuju	4	2	6
	Tidak Setuju	10	5	15
	Netral	4	2	6
	Setuju	9	6	15
	Sangat Setuju	6	2	8
Total		33	17	50



Tabel 11. perbandingan responden kusioner 2 berdasarkan domisili

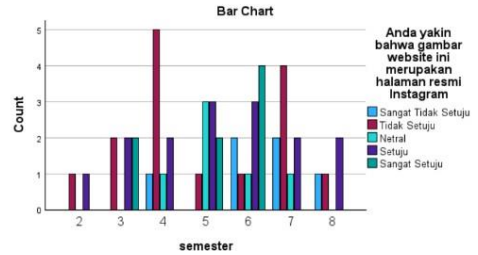
Anda yakin bahwa gambar website ini merupakan halaman resmi Instagram

		Sangat Tidak Setuju	Tidak Setuju	Netral	Setuju	Sangat Setuju	Total
Domisili	Jakarta Barat	0	5	1	4	1	11
	Jakarta Pusat	1	3	1	5	1	11
	Jakarta Selatan	1	2	1	3	3	10
	Jakarta Timur	2	2	2	2	2	10
	jakarta Utara	2	3	1	1	1	8
Total		6	15	6	15	8	50



Tabel 12. perbandingan responden kuesioner 2 berdasarkan semester

		Anda yakin bahwa gambar website ini merupakan halaman resmi Instagram					
		Sangat Tidak Setuju	Tidak Setuju	Netral	Setuju	Sangat Setuju	Total
semester	2	0	1	0	1	0	2
	3	0	2	0	2	2	6
	4	1	5	1	2	0	9
	5	0	1	3	3	2	9
	6	2	1	1	3	4	11
	7	2	4	1	2	0	9
	8	1	1	0	2	0	4
Total		6	15	6	15	8	50



Berdasarkan data-data diatas terdapat penurunan kepercayaan yang cukup signifikan hingga 22% ketika responden melihat website phishing instagram dengan tampilan link yang tidak familiar.

4. KESIMPULAN

Penelitian ini menggambarkan serangan phishing terhadap pengguna Instagram melalui website palsu. Berdasarkan hasil penelitian, dapat disimpulkan:

1. Kesadaran rendah terhadap Tampilan Website Phishing Tanpa Link (Kuesioner1): Mahasiswa menunjukkan tingkat kesadaran yang rendah terhadap tampilan website phishing ketika tidak ada URL atau link yang ditampilkan. Mayoritas setuju bahwa tampilan tersebut sesuai dengan website resmi Instagram.
2. Pengaruh Link pada Kesadaran Mahasiswa (Kuesioner2): Penggunaan link pada tampilan website phishing berpengaruh signifikan terhadap kesadaran mahasiswa. Setelah melihat link, sebagian responden menunjukkan penurunan kepercayaan terhadap keaslian website tersebut.
3. Teknik Phishing yang Digunakan: Penelitian mengidentifikasi teknik phishing yang digunakan, termasuk tautan palsu dan situs web palsu yang meniru tampilan Instagram resmi untuk mengecoh pengguna.

DAFTAR PUSTAKA

[1] Vadila, N. and Pratama, A. R. (2021) ‘Analisis Kesadaran Keamanan Terhadap Ancaman Phishing’, Automata, 2(2), pp. 1–4.

[2] Hayati, M. and Fata, D. (2021) ‘Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phising’, Djtechno Jurnal Teknologi Informasi, 2(1), pp. 21–28. doi: 10.46576/djtechno.v 2i1.1252.

[3] Setiyawan, G. P. B., Helilintar, R. and Wulanningrum, R. (2022) ‘Sistem Informasi Survey Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Metode Multiple Criteria Decision Analisys (MCDA)’, Seminar Nasional Inovasi Teknologi, pp. 73–80.

[4] Sulaeman, A. et al. (2023) ‘Aplikasi Monitoring Smart Charger Android Berbasis Mikrokontroler Esp8266 Menggunakan Flutter Monitoring Application of Smart Charger

Android Based on Microcontroller Esp8266 Using Flutter', 16(1). Available at:https:// journal.ubm.ac.id/index.php/jiems.
[5] Theodorus Yagoyamu (2020) 'Pengembangan Sitem informasi Berbasis Web Menggunakan Waterfall Method Untuk Memperkenalkan Kebudayaan, dan Pariwisata Suku Asmat', Unes Repository, pp. 22–24.
[6] Hadi Ramadhan, I. and Kumalasari Nurnawati, E. (2022) 'Analisis Ancaman Phishing Dalam Layanan E-Commerce', Prosiding Snast, (November), pp. E31-41. doi: 10.34151/ prosidingsnast.v 8i1.4169
[7] Fadlika, R. et al. (2023) 'Employee Information Security Awareness in the Power Generation Sector of PT ABC', International Journal of Advanced Computer Science and Applications, 14(4), pp.594–603. doi: 10.14569/IJACSA.2023.0140465.
[8] ADITYA, M. (2021) 'Penerapan Komunikasi Pemasaran Digital di Masa Pandemi COVID-19: Studi Kasus di Perusahaan Penyedia Layanan Web Hosting Niagahoster Periode April …', (September 2020), pp. 2020–2021. Availableat:http:// etd.repository.ugm.ac.id/penelitian/detail/204408.
[9] Batmetan, J. R. et al. (2018) 'Tingkat Kesadaran Privasi Atas Masalah Keamanan Informasi', p. 4. doi: 10.31219/OSF.IO/CAHZR.
[10] Akraman, R., Candiwan, C. and Priyadi, Y. (2018) 'Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia', Jurnal Sistem Informasi Bisnis, 8(2), p. 115. doi: 10.21456/vol8iss2pp115-122.
[11] APWG Quarter (2022) 'Phising Activity Trend Report', (December). Available at: https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf.