



**ANALISIS TINGKAT KESADARAN DAN PENGETAHUAN  
MAHASISWA UPN “VETERAN” JAKARTA TERHADAP *MAIL  
PHISHING***

**SKRIPSI**

**MUHAMMAD TAUFIQURAHMAN  
NIM. 1910511010**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA  
2023**



**NALISIS TINGKAT KESADARAN DAN PENGETAHUAN MAHASISWA  
UPN “VETERAN” JAKARTA TERHADAP *MAIL PHISHING***

**SKRIPSI**

**Diajukan sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana  
Komputer**

**MUHAMMAD TAUFIQURAHMAN  
NIM. 1910511010**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA  
2023**

## LEMBAR PERSETUJUAN

Yang bertanda tangan di bawah ini:

Nama : Muhammad Taufiqurahman  
NIM. : 1910511010  
Program Studi : ~~Informatika/Sistem Informasi Program Sarjana Diploma 3~~  
(\*Coret yang tidak perlu)  
Judul Skripsi/TA. : Analisis Tingkat Kesadaran dan Pengetahuan  
Mahasiswa UPN "Veteran" Jakarta Terhadap *Mail Phising*

Dinyatakan telah memenuhi syarat dan menyetujui untuk mengikuti ujian sidang skripsi.

Jakarta, 6 Juni 2023

Mengetahui,  
Ketua Program Studi,

  
Dr. Widya Cholil, M.I.T.

Menyetujui,  
Dosen Pembimbing,

  
Henki Bayu Seta, S.Kom, MTI.

## PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Muhammad Taufiqurahman  
NIM : 1910511010  
Tanggal : 17 Juli 2023

Bilamana dikemudian hari ditemukan ketidaksamaan dengan pernyataan ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 17 Juli 2023

Yang Menyatakan,



Muhammad Taufiqurahman

# PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan dibawah ini :

Nama : Muhammad Taufiqurahman  
NIM : 1910511010  
Fakultas : Ilmu Komputer  
Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul :

## ANALISIS TINGKAT KESADARAN DAN PENGETAHUAN MAHASISWA UPN "VETERAN" JAKARTA TERHADAP MAIL PHISHING

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 17 Juli 2023

Yang Menyatakan,



Muhammad Taufiqurahman

## LEMBAR PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama : Muhammad Taufiqurrahman  
NIM : 1910511010  
Program Studi : S1 Informatika  
Judul Tugas Akhir : Analisis Tingkat Kesadaran Dan Pengetahuan Mahasiswa UPN "Veteran" Jakarta Terhadap Mail Phishing

Telah berhasil dipertahankan dihadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Jayanta, S.Kom., M.Si  
Penguji I



Ruth Mariana Bunga Wadu S.Kom., MMSI  
Penguji II



Henki Bayu Seta, S.Kom, MTI.  
Pembimbing



Dr. Ermatita, M.Kom  
Dekan



Dr. Widya Cholil, M.IT  
Kepala Program Studi

Ditetapkan di : Jakarta  
Tanggal Ujian : 03 Juli 2023



# ANALISIS TINGKAT KESADARAN DAN PENGETAHUAN MAHASISWA UPN “VETERAN” JAKARTA TERHADAP *MAIL PHISHING*

MUHAMMAD TAUFIQURAHMAN

## ABSTRAK

Perkembangan teknologi yang pesat dapat menimbulkan masalah, diantaranya kejahatan internet (*cybercrime*) sebagai salah satu media yang digunakan untuk pencurian data oleh individu, organisasi dan pemerintah. Jenis kejahatan yang sering terjadi adalah *phishing*. *Phishing* merupakan salah satu metode *cybercrime* yang mengiringi perkembangan teknologi digital. Kejahatan digital ini berupa pencurian informasi dan data pribadi melalui *email*, panggilan telepon, pesan teks, dan tautan yang meniru lembaga tertentu. Berdasarkan Laporan Tahunan Monitoring Keamanan Siber pada tahun 2021, terdapat 262 *website* terdampak *phishing* di Indonesia. Lalu, berdasarkan data pada tahun 2022 di kuartal I, Indonesia Anti-*Phishing* Data Exchange (IDADX) mencatat total sebanyak 3.169 laporan *phishing* dan pada kuartal II 2022 mendapatkan sebanyak total 5.579 laporan di Indonesia. Penelitian ini bertujuan untuk memberi pengetahuan mengenai *phishing* untuk kalangan mahasiswa UPN “Veteran” Jakarta dan untuk memberi masukan kepada UPT TIK UPN “Veteran” Jakarta untuk mengevaluasi berdasarkan sampel yang digunakan pada penelitian ini. Penelitian ini menggunakan metode eksperimental dengan tools Visual Studio Code dan Firebase serta metode kuesioner dengan menggunakan tools Microsoft Office Excel dan Statistical Package for the Social Sciences (SPSS). Berdasarkan hasil penelitian ini, ditemukan bahwa tingkat kesadaran mahasiswa di UPN “Veteran” Jakarta dari tiga angkatan yang terdiri dari 1500 sampel menunjukkan tingkat yang relatif tinggi pada uji metode eksperimental. Hal ini menunjukkan bahwa mahasiswa di UPN “Veteran” Jakarta memiliki tingkat kesadaran yang baik terhadap *email phishing* yang diterima. Namun, ketika penelitian ini melihat tingkat pengetahuan mahasiswa berdasarkan sampel 385 mahasiswa dengan menggunakan metode kuesioner, ditemukan hasil rata-rata yang menunjukkan tingkat netral. Ini berarti, dalam hal pengetahuan tentang *email phishing*, mahasiswa cenderung memiliki pemahaman yang seimbang atau tidak memiliki kecenderungan yang kuat. Secara keseluruhan, hasil penelitian ini menyatakan bahwa mahasiswa di UPN Veteran Jakarta memiliki tingkat kesadaran yang relatif tinggi, namun masih terdapat kecenderungan netral dalam tingkat pengetahuan.

**Kata Kunci:** *cybercrime, phishing, mail phishing, kesadaran, pengetahuan*

# **ANALYSIS OF THE LEVEL OF AWARENESS AND KNOWLEDGE OF UPN "VETERAN" JAKARTA STUDENTS AGAINST MAIL PHISHING**

**MUHAMMAD TAUFIQURAHMAN**

## ***ABSTRACT***

*Rapid technological advancements can create problems, including internet crime (cybercrime) as one of the means used for data theft by individuals, organizations, and governments. One common type of crime is phishing, which is a cybercrime method that accompanies the development of digital technology. This digital crime involves stealing information and personal data through email, phone calls, text messages, and links that imitate specific institutions. According to the Annual Report on Cyber Security Monitoring in 2021, there were 262 phishing-affected websites in Indonesia. Furthermore, based on data from the first quarter of 2022, Indonesia Anti-Phishing Data Exchange (IDADX) recorded a total of 3,169 phishing reports, and in the second quarter of 2022, it received a total of 5,579 reports in Indonesia. This research aims to provide knowledge about phishing for students at UPN "Veteran" Jakarta and to provide input to the ICT Center of UPN "Veteran" Jakarta for evaluation based on the sample used in this study. The research adopts an experimental method using Visual Studio Code and Firebase as tools, as well as a questionnaire method using Microsoft Office Excel and the Statistical Package for the Social Sciences (SPSS) as tools. Based on the findings of this research, it was discovered that the awareness level of students at UPN "Veteran" Jakarta from three academic cohorts, comprising 1,500 samples, showed a relatively high level in the experimental method test. This indicates that students at UPN "Veteran" Jakarta have a good level of awareness regarding received phishing emails. However, when examining the students' knowledge level based on a sample of 385 students using a questionnaire method, the average results indicated a neutral level. This means that in terms of knowledge about email phishing, students tend to have a balanced understanding or no strong inclination. Overall, the results of this research indicate that students at UPN Veteran Jakarta have a relatively high level of awareness, but there is still a neutral tendency in terms of knowledge level.*

**Keywords:** *cybercrime, phishing, email phishing, awareness, knowledge*



## KATA PENGANTAR

Puji dan syukur dipanjatkan atas kehadiran Allah SWT. karena atas karunia-Nya peneliti dapat menyelesaikan Tugas Akhir dengan baik.

Dalam penyelesaian Tugas Akhir ini tidak lepas dari bantuan banyak pihak yang telah memberikan bantuan dan dukungan. Untuk itu peneliti mengucapkan banyak terima kasih kepada:

1. Dr. Ermatita, M.Kom., selaku dekan Fakultas Ilmu Komputer.
2. Dr. Widya Cholil, M.I.T. selaku Ketua Program Studi Sarjana Jurusan Informatika.
3. Henki Bayu Seta, S.Kom, MTI. selaku Dosen Pembimbing.
4. UPT TIK UPN Veteran Jakarta, yang telah membantu dan memberi izin dalam penelitian ini
5. Kedua orang tua dan kedua kakak yang telah memberikan dukungan baik secara moral maupun materil.
6. Amelia Andani, Amelia Monica, Gito Putro Wardana, Nio Dimas Radityo, Abril Muhammad Fikar, Alvin Daniswara, Fauzan Alhafizh, Muhammad Fathurrahman, Jamie Saviola, Viryal Nada, Wahyu Miftahul Aflah, Fajran Khalis, Felicia Griselda, Tania Larasati, Nisyanti Yahya yang telah memberikan dukungan dan semangat dalam penyelesaian skripsi ini.
7. Rafif Priyambodo Prakoso, Raihan Kemmy, dan Ajeng Arifa yang memberi dukungan serta pengetahuan dalam perbaikan penulisan.
8. Keluarga besar UKM Veteran Jakarta *E-sports* sebagai tempat tumbuh dan berkembang dalam mengembangkan *softskill* maupun relasi yang dimiliki.
9. Dan semua pihak yang tidak dapat peneliti sebutkan satu persatu tanpa mengurangi rasa hormat.

Peneliti menyadari bahwa masih banyaknya kekurangan secara materi maupun teknik penulisan dari Tugas Akhir ini, mengingat kurangnya pengetahuan dan pengalaman peneliti. Oleh karena itu, kritik dan saran yang membangun akan sangat berarti bagi peneliti.

Jakarta, 6 Juni 2022

Peneliti,

Muhammad Taufiqurahman

## DAFTAR ISI

	Halaman
LEMBAR JUDUL .....	ii.
LEMBAR PERSETUJUAN.....	iii
PERNYATAAN ORISINALITAS .....	iv
PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS .....	v
LEMBAR PENGESAHAN .....	vi
ABSTRAK .....	vii
<i>ABSTRACT</i> .....	viii
KATA PENGANTAR .....	ix
DAFTAR ISI.....	xi
DAFTAR TABEL.....	xiv
DAFTAR GAMBAR .....	xv
BAB 1 PENDAHULUAN .....	1
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	4
1.3. Tujuan Penelitian .....	5
1.4. Manfaat Penelitian .....	5
1.5. Ruang Lingkup.....	5
1.6. Luaran yang Diharapkan .....	6
1.7. Sistematika Penulisan .....	6
BAB 2 TINJAUAN PUSTAKA .....	7
2.1. Kesadaran dan Pengetahuan.....	7
2.2. Definisi <i>Phishing</i> .....	7
2.3. Teknik <i>Phishing</i> .....	8
2.4. Sistem Informasi Akademik.....	10
2.5. <i>Cloning Website</i> .....	10
2.6. <i>Firebase Realtime Database</i> .....	10
2.7. Populasi dan Sampel .....	12
2.7.1. Populasi .....	12

2.7.2.	Sampel .....	12
2.8.	Uji Instrumen Penelitian .....	13
2.8.1.	Uji Validitas .....	13
2.8.2.	Uji Reliabilitas.....	14
2.9.	Metode Analisis Data.....	15
2.9.1.	Analisis Statistik Deskriptif.....	15
2.9.2.	Rumus Analisis Deskriptif Interval.....	16
2.9.3.	Rumus Perhitungan Rata-Rata .....	17
2.10.	Penelitian Terdahulu .....	18
<b>BAB 3 METODOLOGI PENELITIAN.....</b>		<b>23</b>
3.1.	Tahapan Penelitian .....	23
3.2.	Alur Penelitian .....	23
3.2.1.	Identifikasi Masalah .....	23
3.2.2.	Studi Literatur.....	24
3.2.3.	Pengumpulan Data .....	24
3.2.4.	Pengolahan Data.....	27
3.2.5.	Analisis Data .....	27
3.2.6.	Kesimpulan.....	28
3.3.	Alat dan Bahan Penelitian.....	28
3.3.1.	Perangkat Keras ( <i>Hardware</i> ).....	28
3.3.2.	Perangkat Lunak ( <i>Software</i> ).....	28
3.4.	Tahapan Kegiatan.....	29
<b>BAB 4 HASIL DAN PEMBAHASAN.....</b>		<b>30</b>
4.1.	Hasil Perhitungan Populasi dan Sampel .....	30
4.2.	Hasil Uji Instrumen Penelitian.....	30
4.2.1.	Uji Validitas .....	30
4.2.2.	Uji Reliabilitas.....	31
4.3.	Pengujian Metode Eksperimental .....	32
4.4.	Pengujian Metode Kuesioner .....	41
4.5.	Analisis Deskriptif Variabel Penelitian.....	42
4.5.1.	Analisis Deskriptif Kesadaran.....	42
4.5.2.	Analisis Deskriptif Pengetahuan .....	47

BAB 5 PENUTUP .....	58
5.1. Kesimpulan .....	58
5.2. Saran.....	59
DAFTAR PUSTAKA .....	60
RIWAYAT HIDUP.....	63
LAMPIRAN.....	65
LAMPIRAN 1. SURAT IZIN PENELITIAN .....	65
LAMPIRAN 2. PAKTA INTEGRITAS PENELITIAN.....	66
LAMPIRAN 3. REFERENSI R TABEL .....	67
LAMPIRAN 4. KUESIONER .....	68
LAMPIRAN 5. HASIL UJI VALIDITAS .....	71
LAMPIRAN 6. HASIL UJI RELIABILITAS .....	72
LAMPIRAN 7. <i>SOURCE CODE</i> PROGRAM.....	73
LAMPIRAN 8. HASIL TURNITIN .....	76

## DAFTAR TABEL

	Halaman
Tabel 2.1. Penilaian Analisis Deskriptif .....	17
Tabel 2.2. Penelitian Terdahulu .....	18
Tabel 3.1. Skala <i>Likert</i> .....	25
Tabel 3.2. Kuesioner Pengetahuan <i>Mail Phishing</i> .....	26
Tabel 3.3. Penilaian Analisis Deskriptif .....	27
Tabel 3.4. Tahapan Kegiatan .....	29
Tabel 4.1. Hasil Uji Validitas.....	31
Tabel 4.2. Hasil Uji Reliabilitas .....	32
Tabel 4.3. Detail Sampel.....	42
Tabel 4.4. Mahasiswa yang Merespon <i>Email Phishing</i> .....	43
Tabel 4.5. Mahasiswa yang Merespon <i>Email Phishing</i> Berdasarkan Asal Fakultas .....	44
Tabel 4.6. Mahasiswa yang Tidak Merespon <i>Email Phishing</i> .....	46
Tabel 4.7. Hasil Analisis Deskriptif Pengetahuan .....	50

## DAFTAR GAMBAR

	Halaman
Gambar 1.1. Laporan <i>Monitoring</i> Keamanan Siber Tahun 2021 (Direktorat Operasi Keamanan Siber, 2021) .....	2
Gambar 1.2. Laporan <i>Phishing</i> Kuartal I Tahun 2022 (Indonesia Anti-Phishing Data Exchange, 2022) .....	3
Gambar 1.3. Laporan <i>Phishing</i> Kuartal II Tahun 2022 (Indonesia Anti-Phishing Data Exchange, 2022) .....	3
Gambar 2.1. Perbandingan Aplikasi Website Tradisional dengan <i>Firebase</i> (Biswas, 2022).....	12
Gambar 3.1. Tahapan Penelitian .....	23
Gambar 3.2. Metode Eksperimental .....	25
Gambar 4.1. <i>Source Code</i> Halaman Tampilan <i>Website</i> SIAKAD UPNVJ pada Elemen <i>Head</i> .....	32
Gambar 4.2. <i>Source Code</i> Halaman Tampilan <i>Website</i> SIAKAD UPNVJ pada <i>Form Login</i> .....	33
Gambar 4.3. <i>Source Code</i> Halaman Tampilan <i>Website</i> SIAKAD UPNVJ pada <i>Form Submit Login</i> .....	34
Gambar 4.4. <i>Source Code</i> Halaman Tampilan <i>Website</i> SIAKAD UPNVJ .....	35
Gambar 4.5. Tampilan <i>Website</i> Resmi SIAKAD UPNVJ .....	35
Gambar 4.6. Tampilan <i>Cloning Website</i> SIAKAD UPNVJ .....	36
Gambar 4.7. <i>Project Realtime Database</i> .....	37
Gambar 4.8. <i>Source Code</i> Fungsi Menulis dan Mendapatkan Hasil dari Penyerangan <i>Mail Phishing</i> .....	38
Gambar 4.9. <i>Source Code</i> untuk untuk Menyimpan Data Korban Penyerangan <i>Mail Phishing</i> .....	39
Gambar 4.10. Tampilan <i>Email</i> Administrator Palsu .....	40
Gambar 4.11. Pesan Penyerangan Tahap Pertama .....	40
Gambar 4.12. Pesan Penyerangan Tahap Kedua .....	41
Gambar 4.13. Korban <i>Mail Phishing</i> .....	41
Gambar 4.14. Hasil Jawaban Responden Berdasarkan Asal Fakultas .....	48

Gambar 4.15. Hasil Jawaban Responden Berdasarkan Tahun Angkatan .....49