Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

ANALISIS TINGKAT KESADARAN KEAMANAN SIBER TERHADAP ANCAMAN PHISHING MENGGUNAKAN TECHNOLOGY THREAT AVOIDANCE THEORY (TTAT) PADA MAHASISWA POLITEKNIK NEGERI BATAM

Ahmad Sopyan1 *, Hamdani Arif 2 **

Rekayasa Keamanan Siber, Teknik Informatika, Politeknik Negeri Batam
Jl. Ahmad Yani, Tlk. Tering, Kec. Batam Kota, Kota Batam, Kepulauan Riau 29461
ahmad.4332201009@students.polibatam.ac.id [1], hamdaniarif@polibatam.ac.id [2]

Article Info

Article history:

Received
…

Revised
…

Accepte
d …

Keyword:
Cybersecurity Awareness, Phishing, Technology Threat Avoidance Theory, University Students.

ABSTRACT

Phishing is one of the most common cybersecurity threats that exploits human vulnerabilities through social engineering techniques. As active users of digital technologies, university students are increasingly exposed to phishing attacks across various online platforms. This study aims to analyse Cybersecurity Awareness toward phishing threats among students of Polytechnic Negeri Batam using the *Technology Threat Avoidance Theory* (TTAT*)* approach. A quantitative method was employed through an online questionnaire distributed to 233 active students. The study examined the influence of Self-Efficacy, Avoidance Motivation, Avoidance Behaviour, and Behavioural Intention on Cybersecurity Awareness. Data were analysed using IBM SPSS Statistics through validity, reliability, descriptive, and multiple linear regression analyses. The results indicate that TTAT variables significantly influence students' Cybersecurity Awareness toward phishing threats. These findings emphasize the importance of strengthening Cybersecurity Awareness and phishing education programs within higher education institutions to enhance students' resilience against cyber threats.

I. PENDAHULUAN

Aktivitas akademik di perguruan tinggi saat ini sangat bergantung pada integrasi sarana digital. Mahasiswa memanfaatkan berbagai platform daring—seperti surat elektronik, jejaring sosial, perpesanan instan, hingga sistem informasi kampus—untuk menunjang kegiatan harian. Namun, tingginya adopsi teknologi ini berbanding lurus dengan eskalasi risiko siber, khususnya ancaman phishing. Serangan rekayasa sosial (social engineering) ini berupaya memanipulasi korbannya agar menyerahkan data sensitif dengan menyamar sebagai institusi resmi.

Kerentanan terhadap kejahatan phishing tidak semata-mata bersumber dari celah keamanan infrastruktur IT, melainkan dipicu oleh minimnya kesadaran siber pada tingkat pengguna. Pengguna akhir memegang peranan vital sebagai benteng pertahanan terdepan (human firewall) untuk memutus rantai serangan siber. Atas dasar tersebut, pembenahan Cybersecurity Awareness menjadi krusial dalam memitigasi insiden kebocoran data pribadi maupun institusi.

Untuk membedah dinamika psikologis pengguna dalam merespons risiko digital, penelitian ini melandaskan analisisnya pada kerangka Technology Threat Avoidance Theory (TTAT). Teori ini menjelaskan alur penghindaran ancaman yang digerakkan oleh efikasi diri (Self-Efficacy), dorongan motivasi (Avoidance Motivation), niat berperilaku (Behavioral Intention), hingga eksekusi tindakan proteksi nyata (Avoidance Behavior). Kerangka ini terbukti efektif memetakan sejauh mana individu mampu mengidentifikasi dan menangkal kejahatan phishing. Namun, penelitian mengenai tingkat kesadaran keamanan siber mahasiswa menggunakan pendekatan TTAT, khususnya di lingkungan perguruan tinggi vokasi, masih relatif terbatas.

Sebagai perguruan tinggi vokasi, Politeknik Negeri Batam mengintegrasikan ekosistem digital secara luas dalam kegiatan pembelajaran dan administrasi akademik. Ketergantungan ini berimplikasi pada tingginya potensi paparan serangan rekayasa sosial seperti phishing. Atas dasar kondisi tersebut, eksplorasi ini mengukur tingkat ketahanan siber pada 233 mahasiswa aktif—dengan penekanan pada rumpun ilmu non-komputer—menggunakan kerangka komprehensif TTAT (X_1, X_2, X_3, X_4) terhadap kesadaran siber (Y).

A. Rumusan Masalah dan Hipotesis Penelitian

Berdasarkan latar belakang tersebut, pertanyaan penelitian dalam studi ini dirumuskan sebagai berikut:

1. Seberapa besar pengaruh parsial dari *Self-Efficacy* (X_1), *Avoidance Motivation* (X_2), *Avoidance Behavior* (X_3), dan *Behavioral Intention* (X_4) terhadap *Cybersecurity Awareness* (Y)?
2. Apakah seluruh variabel dalam kerangka TTAT secara bersama-sama (simultan) memengaruhi *Cybersecurity Awareness* (Y) pada mahasiswa Politeknik Negeri Batam?

Adapun hipotesis yang diuji mencakup:

1. $H_1 - H_4$: Masing-masing variabel *Self-Efficacy* (X_1), *Avoidance Motivation* (X_2), *Avoidance Behavior* (X_3), dan *Behavioral Intention* (X_4) berkonstelasi positif dan signifikan secara parsial terhadap *Cybersecurity Awareness* (Y)
2. H_5: Variabel *Self-Efficacy*, *Avoidance Motivation*, *Avoidance Behavior*, dan *Behavioral Intention* secara komposit/simultan berkonstelasi signifikan terhadap *Cybersecurity Awareness* (Y).

B. Tujuan Penelitian

Penelitian ini dilaksanakan dengan tujuan utama untuk:

1. Menganalisis besaran kontribusi parsial dari masing-masing dimensi TTAT—meliputi efikasi diri, motivasi penghindaran, perilaku pencegahan, dan niat berperilaku—terhadap tingkat kesadaran siber mahasiswa
2. Mengukur pengaruh komposit (simultan) dari seluruh variabel dalam model TTAT terhadap kesadaran siber mahasiswa Politeknik Negeri Batam.

C. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi teoretis maupun praktis sebagai berikut:

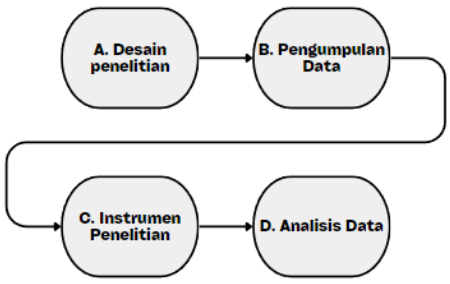
1. Manfaat Teoretis: Memperkaya literatur akademik di bidang keamanan informasi, khususnya mengenai penerapan kerangka *Technology Threat Avoidance Theory* (TTAT) pada aspek *human factor* pengguna akhir (*end-user*) di lingkungan perguruan tinggi vokasi.

2. Manfaat Praktis:

1) Kontribusi Institusional**:** Menyajikan pijakan empiris bagi manajemen Politeknik Negeri Batam dalam merumuskan kebijakan siber dan kurikulum pelatihan keamanan yang terukur, khususnya bagi mahasiswa rumpun keilmuan non-komputer.
2) Kontribusi Bagi Mahasiswa**:** Membekali pengguna akhir dengan pemahaman taktis mengenai indikator serangan sosial, serta mendorong pembiasaan prosedur pencegahan seperti validasi tautan URL, verifikasi sertifikat SSL, dan aktivasi Two-Factor Authentication (2FA).

II. METODE

Studi ini mengimplementasikan pendekatan kuantitatif berbasis paradigma positivisme untuk menguji hipotesis secara empiris, terstruktur, dan terukur. Metode survei diterapkan dengan menyebarkan kuesioner terstruktur guna mengumpulkan data primer dari responden mahasiswa aktif Politeknik Negeri Batam. Berikut adalah alur penelitian kuantitatif:



Gambar 1. Penelitian Kuantitatif

A. Desain Penelitian

Eksplorasi kuantitatif ini mengaplikasikan strategi survei eksplanatori untuk memetakan kesadaran siber mahasiswa terhadap manipulasi phishing. Pengumpulan data primer dilakukan melalui penyebaran instrumen kuesioner terstruktur berbasis

jaringan (*online*) kepada responden aktif di lingkungan Politeknik Negeri Batam.

Model penelitian terdiri dari empat variabel independen, yaitu *Self-Efficacy* (X1), *Avoidance Motivation* (X2), *Avoidance Behaviour* (X3), dan *Behavioral Intention* (X4), serta satu variabel dependen yaitu *Cybersecurity Awareness* (Y). Hubungan antar variabel dianalisis untuk mengetahui pengaruh masing-masing variabel terhadap tingkat kesadaran keamanan siber mahasiswa dalam menghadapi ancaman *phishing.*

TABEL 1 TABEL PEMBANDING PENELITIAN TERDAHULU

Peneliti & Tahun	Metode & Sampel	Temuan Utama	Kebaruan
Sari et al., 2023	Kuantitatif TTAT, 100 Mahasiswa	Variabel TTAT berpengaruh signifikan pada kesadaran siber.	Mengadopsi instrumen [1], namun menambah analisis bias rumpun keilmuan (Non-Teknis vs Teknis) & Action Plan.
Liang & Xue (2009) [1]	Kuantitatif TTAT, Pengguna IT	Mengembangkan kerangka dasar TTAT pada teknologi informasi.	Menerapkan model TTAT terkompresi pada ancaman spesifik phishing di lingkungan perguruan tinggi vokasi.
Darem 2021)	Kuantitatif Survei, Mahasiswa	Metode penyampaian kesadaran menentukan efektivitas pencegahan.	Mengintegrasikan hasil survei kuesioner dengan pengukuran eksperimental pre-test/post-test pelatihan teknis.

Model penelitian ini mengadopsi struktur TTAT terkompresi dengan mengeliminasi dimensi *Threat Appraisal* (Perceived Susceptibility dan Severity) untuk memfokuskan pengujian pada transisi kapabilitas internal (Self-Efficacy), motivasi, serta komitmen perilaku terhadap kesadaran siber. Penempatan Cybersecurity Awareness sebagai variabel terikat (Y) didasarkan pada Self-Perception Theory, di mana tindakan pencegahan nyata (X3) dan niat terencana (X4) yang dilakukan secara konsisten akan merefleksikan dan memperkuat tingkat kesadaran siber individu secara menyeluruh.

B. Pengumpulan Data

Target populasi mencakup seluruh mahasiswa aktif di lingkungan Politeknik Negeri Batam. Penentuan sampel memanfaatkan teknik convenience sampling (bagian dari non-probability sampling) guna menjangkau responden secara fleksibel melalui borang kuesioner digital (Google Form). Dari proses diseminasi instrumen, berhasil dihimpun sebanyak 233 sampel valid yang memenuhi kriteria pengujian. Responden yang bersedia mengisi kuesioner dan memenuhi kriteria penelitian dapat berpartisipasi dalam penelitian ini.

Proses diseminasi instrumen berhasil menghimpun 233 sampel valid dari beragam program studi. Data primer tersebut diolah secara inferensial untuk menganalisis kontribusi relatif variabel-variabel TTAT terhadap kesadaran siber pengguna akhir.

Instrumen penelitian berupa kuesioner yang disusun berdasarkan konstruk *Technology Threat Avoidance Theory* (TTAT). Pemilihan total 30 butir pernyataan dalam penelitian ini dilakukan secara eksplisit untuk memenuhi representasi seluruh indikator empiris dari model TTAT, yang diadopsi dan diadaptasi dari instrumen penelitian terdahulu yang valid[1]. Adapun sebaran operasional dari ke-30 butir pernyataan tersebut disajikan pada Tabel Klasifikasi berikut:

TABEL 2 SEBARAN BUTIR INSTRUMEN PENELITIAN

Variabel Penelitian	Kode Butir Pernyataan	Total Butir
Self-Efficacy (X1)	P1, P2, P3, P4, P5, P6	6 Butir
Avoidance Motivation (X2)	P1, P2, P3, P4, P5, P6	6 Butir
Avoidance Behaviour (X3)	P1, P2, P3, P4, P5, P6	6 Butir
Behavioral Intention (X4)	P1, P2, P3, P4, P5, P6	6 Butir
Cybersecurity Awareness (Y)	P1, P2, P3, P4, P5, P6	6 Butir
TOTAL BUTIR PERNYATAAN	P1 s.d P30	30 BUTIR

Skala Likert lima poin digunakan untuk menilai setiap pernyataan: Sangat Tidak Setuju (1), Tidak Setuju (2), Netral (3), Setuju (4), dan Sangat Setuju (5).

D. Analisis Data

Pengolahan data kuantitatif diproses menggunakan perangkat lunak IBM SPSS Statistics. Tahapan pengujian instrumen dan hipotesis disusun dalam lima tingkatan analisis:

1) *Evaluasi Validitas:*
Mengukur ketepatan tiap indikator melalui teknik korelasi *Pearson Product-Moment*. Indikator dinyatakan valid apabila koefisien korelasi hitung melampaui nilai kritis tabel ($r_{\text{hitung}} > 0{,}129$) pada taraf signifikansi 5% ($\alpha = 0{,}05$).

2) *Evaluasi Reliabilitas:*
Menilai konsistensi internal instrumen ukur menggunakan uji *Cronbach's Alpha*. Konstruk variabel dikategorikan andal apabila koefisien α yang dihasilkan berada di atas ambang batas $0{,}60$.

3) *Analisis Statistik Deskriptif:*
Pemetaan distribusi jawaban responden yang mencakup pemusatan data (skor minimum, maksimum, dan rerata) serta persebaran data (*standard deviation*).

4) *Model Regresi Linear Berganda:*
Persamaan regresi dirumuskan sebagai berikut:

$$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + \varepsilon$$

Di mana Y merepresentasikan tingkat *Cybersecurity Awareness*, β_0 merupakan intersep konstanta, serta β_1 hingga β_4 mewakili bobot koefisien regresi untuk prediktor efikasi diri (X_1), motivasi penghindaran (X_2), perilaku pencegahan (X_3), dan niat berperilaku (X_4), dengan ε sebagai pengganggu acak (*residual error*)

a) Uji t
Mengukur kontribusi individual tiap variabel independen terhadap variabel dependen (Sig. $< 0{,}05$)

b) Uji F
Menilai kelayakan model regresi secara keseluruhan pada taraf nyata $\alpha = 0{,}05$.

c) Koefisien Determinasi (R^2)
Mengukur proporsi varians Y yang mampu dijelaskan oleh kombinasi variabel X
.

E. Perancangan Artefak Keamanan Siber

Sebagai bentuk kontribusi rekayasa keamanan siber (cybersecurity engineering), penelitian ini merancang artefak teknis berupa cetak biru (blueprint) skenario simulasi spear-phishing terkontrol serta modul edukasi interaktif pada ekosistem layanan digital publik/korporat. Skenario simulasi merancang pengujian terhadap dua teknik manipulasi psikologis *end-user,* yaitu rekayasa urgensi akun melalui formulir verifikasi palsu dan manipulasi domain (typosquatting & SSL deception). Sementara itu, modul edukasi dirancang secara interaktif untuk memperkuat tindakan pencegahan nyata (Avoidance Behaviuor) melalui panduan praktis inspeksi visual header email, verifikasi sertifikat SSL/TLD, serta konfigurasi Multi-Factor Authentication (MFA/TOTP) guna mencegah pengambilalihan akun saat kredensial utama terkompromi.

III. HASIL DAN PEMBAHASAN

A. Karakteristik Responden

Deskripsi profil demografi disajikan untuk memberikan latar belakang komprehensif mengenai sebaran sampel 233 mahasiswa aktif Politeknik Negeri Batam. Data yang terhimpun mencakup variabel jenis kelamin, latar belakang jurusan, program studi, serta angkatan studi guna mendukung keandalan interpretasi temuan.

Penelitian ini melibatkan sebanyak 233 mahasiswa aktif Politeknik Negeri Batam yang berasal dari berbagai jurusan dan program studi. Penyajian karakteristik responden bertujuan untuk membantu memahami distribusi responden serta mendukung interpretasi hasil penelitian terkait tingkat kesadaran keamanan siber terhadap ancaman *phishing*.

1) Karakteristik Responden Berdasarkan Jenis Kelamin

TABEL 3 KARAKTERISTIK RESPONDEN BERDASARKAN JENIS KELAMIN

Jenis kelamin	Jumlah	Persentase
Laki – Laki	101	43,3%
Perempuan	132	56,7%
Total	233	100%

Ditinjau dari demografi gender, partisipasi mahasiswa perempuan mendominasi sampel dengan 132 responden (56,7%), sedangkan mahasiswa laki-laki tercatat sebanyak 101 orang (43,3%) dari total 233 sampel.

2) Karakteristik Responden Berdasarkan Jurusan

TABEL 4 KARAKTERISTIK RESPONDEN BERDASARKAN JURUSAN

Jurusan	Jumlah	Persentase
Manajemen Bisnis	144	61,8%
Teknik Informatika	67	28,8%
Teknik Elektro	22	9,4%
Total	233	100%

Proporsi responden terbanyak berasal dari Jurusan Manajemen Bisnis (144 mahasiswa atau 61,8%). Bidang keteknikan diwakili oleh Jurusan Teknik Informatika (28,8%) dan Teknik Elektro (9,4%).

3) Karakteristik Responden Berdasarkan Program Studi

TABEL 5 KARAKTERISTIK RESPONDEN BERDASARKAN PROGRAM STUDI

Program Studi	Jumlah	Persentase
Administrasi Bisnis dan Terapan	3	1,3%
Akuntansi Manajerial	88	37,8%
Animasi	21	9,0%
Logistik Perdagangan International	54	23,2%
Rekayasa keamanan Siber	41	17,6%
Teknik Rekayasa Perangkat Lunak	1	0,4%
Teknik Informatika	1	0,4%
Teknologi Rekayasa Multimedia	2	0,9%
Mekatronika	1	0,4%
Teknik Elektronika Manufaktur	21	9,0%
Total	233	100%

Sebaran sampel mencakup sepuluh program studi, dengan representasi terbesar dari Prodi Akuntansi Manajerial (37,8%), Logistik Perdagangan Internasional (23,2%), serta Rekayasa Keamanan Siber (17,6%). Porsi sisanya terdistribusi pada prodi vokasi teknis dan multimedia.

4) Karakteristik Responden Berdasarkan Angkatan

TABEL 6 KARAKTERISTIK RESPONDEN BERDASARKAN ANGKATAN

Angkatan	Jumlah	Persentase
2020	1	0,4%
2021	19	8,2%
2022	157	67,4%
2023	39	16,7%
2024	16	6,9%
2025	1	0,4%
Total	233	100%

Distribusi angkatan didominasi oleh mahasiswa angkatan 2022 (67,4%), diikuti angkatan 2023 (16,7%) dan 2021 (8,2%). Hal ini mencerminkan persepsi responden yang telah terbiasa berinteraksi dengan layanan digital akademik kampus.

B. Hasil Uji Validitas

Keabsahan instrumen diukur melalui korelasi skor butir terhadap total variabel pada kriteria $r_{\text{tabel}} = 0{,}129$ $(\alpha = 0{,}05)$. Hasil evaluasi pada Tabel 7 mengonfirmasi seluruh 30 indikator dinyatakan valid ($r_{\text{hitung}} > 0{,}129$). Namun, catatan perbaikan ditemukan pada indikator X_1-P_4 $(r = 0{,}154)$ yang berelasi paling lemah.

TABEL 7 UJI VALIDITAS

Variabel	Pernyataan	sig	*Corrected item-Total Correlation* (r hitung)	r tabel	Keterangan
Self-Efficacy (X1)	P1	0.000	0.170	0.129	Valid
	P2	0.000	0.352	0.129	Valid
	P3	0.000	0.344	0.129	Valid
	P4	0.000	0.154	0.129	Valid
	P5	0.000	0.336	0.129	Valid
	P6	0.000	0.304	0.129	Valid
Avoidance Motivation (X2)	P1	0.000	0.606	0.129	Valid
	P2	0.000	0.639	0.129	Valid
	P3	0.000	0.621	0.129	Valid
	P4	0.000	0.601	0.129	Valid
	P5	0.000	0.491	0.129	Valid
	P6	0.000	0.586	0.129	Valid
Avoidance Behavior (X3)	P1	0.000	0.369	0.129	Valid
	P2	0.000	0.227	0.129	Valid
	P3	0.000	0.290	0.129	Valid
	P4	0.000	0.307	0.129	Valid
	P5	0.000	0.155	0.129	Valid
	P6	0.000	0.171	0.129	Valid
Behavioral Intention (X4)	P1	0.000	0.494	0.129	Valid
	P2	0.000	0.619	0.129	Valid
	P3	0.000	0.588	0.129	Valid
	P4	0.000	0.450	0.129	Valid
	P5	0.000	0.584	0.129	Valid
	P6	0.000	0.541	0.129	Valid
kesadaran keamanan siber (Y)	P1	0.000	0.372	0.129	Valid
	P2	0.000	0.588	0.129	Valid
	P3	0.000	0.173	0.129	Valid
	P4	0.000	0.608	0.129	Valid
	P5	0.000	0.571	0.129	Valid
	P6	0.000	0.620	0.129	Valid

Hasil evaluasi validitas pada Tabel 7 mengonfirmasi seluruh 30 indikator dinyatakan valid ($r_{\text{hitung}} > 0{,}129$). Meski demikian, indikator X_1-P_4 mencatatkan korelasi item-total paling rendah ($r =$

0,154), menandakan perlunya penajaman redaksi pernyataan untuk instrumen penelitian mendatang.

C. Hasil Uji Reliabilitas

Evaluasi keandalan instrumen menghasilkan nilai *Cronbach's Alpha* sebesar 0,889 (Tabel 9). Karena nilai koefisien ini melampaui standar kriteria 0,60, instrumen dinyatakan memiliki konsistensi internal yang sangat tinggi

TABEL 8 KRITERIA RELIABILITAS

No	Presentase	Keterangan
1.	81%-100%	Sangat baik
2.	61%-80%	Baik
3.	41%-60%	Cukup
4.	21%-40%	Kurang
5.	0%-20%	Kurang Sekali

Nilai Alpha Cronbach ditentukan sebesar 0,889 berdasarkan Tabel 6. Alat penelitian ini dianggap dapat diandalkan karena angka tersebut lebih besar dari 0,70. Selain itu, nilai *Cronbach's Alpha* berada pada kategori sangat baik, yang menunjukkan bahwa instrumen penelitian memiliki tingkat konsistensi internal yang tinggi dan layak digunakan untuk analisis lebih lanjut.

TABEL 9 DATA RELIABLE

Pertanyaan/ Butir Pernyataan	*Cronbach's Alpha*	Penjelasan
30	0.889	Reliabel/ Sangat Baik

D. Hasil Uji Statistik Deskriptif

Analisis statistik deskriptif dilakukan untuk memberikan gambaran umum mengenai distribusi data pada setiap variabel penelitian.

TABEL 10 HASIL UJI STATISTIK DESKRIPTIF

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Self_Efficacy	233	13.00	30.00	22.1717	3.34454
Avoidance_Motivation	233	6.00	30.00	24.6052	4.80197
Avoidance_Behavior	233	8.00	30.00	21.9013	3.45084
Behavioral_Intention	233	14.00	30.00	24.8455	4.51551
Cybersecurity_Awareness	233	14.00	30.00	24.3863	4.10384
Valid N (listwise)	233				

Rangkuman deskriptif pada Tabel 10 memperlihatkan seluruh variabel berada pada kategori sedang-tinggi. Variabel Behavioral Intention mencatatkan rerata tertinggi (24,8455), sementara Avoidance Behavior mencatatkan rerata relatif terendah di antara prediktor (21,9013 atau 3,65 dari skala 5). Temuan ini menunjukkan bahwa tindakan proteksi nyata masih menjadi aspek yang paling krusial untuk ditingkatkan.

E. Hasil Uji Regresi Linear Berganda

Pengujian regresi berganda dilakukan untuk membuktikan pengaruh simultan maupun parsial prediktor TTAT (X_1, X_2, X_3, X_4) terhadap variabel terikat (Y).

.

1) Uji Simultan (Uji F)
Hasil estimasi statistik pada Tabel 11 mencatatkan $F_{\text{hitung}} = 87{,}988$ dengan nilai signifikansi $p < 0{,}001$. Hasil ini membuktikan bahwa seluruh konstruk TTAT secara kolektif berkonstelasi signifikan dalam menentukan tingkat kesadaran siber mahasiswa. Rumus berikut dapat digunakan untuk mencari nilai tabel F:

$$F = (R^2/k)/((1 - R^2)/(n - k - 1))$$

Olah data ANOVA pada Tabel 11 menghasilkan $F_{\text{hitung}} = 87{,}988$ dengan p-value $< 0{,}001$. Karena nilai signifikansi jauh di bawah 0,05, terbukti bahwa kombinasi variabel *Self-Efficacy*, *Avoidance Motivation*, *Avoidance Behavior*, dan *Behavioral Intention* secara bersama-sama berpengaruh signifikan terhadap kesadaran siber mahasiswa.:

TABEL 11 UJI F

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2371.162	4	592.790	87.988	<,001[b]
	Residual	1536.074	228	6.737		
	Total	3907.236	232			

a. Dependent Variable: Cybersecurity_Awareness

b. Predictors: (Constant), Behavioral_Intention, Self_Efficacy, Avoidance_Behavior, Avoidance_Motivation

2) Uji Parsial (Uji t) & Diagnostik Model
Pengujian parsial pada Tabel 12 mengonfirmasi bahwa *Avoidance Motivation* ($\beta = 0{,}335; p < 0{,}001$), *Avoidance Behavior* ($\beta = 0{,}094; p = 0{,}047$), dan *Behavioral Intention* ($\beta = 0{,}423; p < 0{,}001$) terbukti menjadi faktor pendorong

yang signifikan. Sementara itu, *Self-Efficacy* ($\beta = 0{,}086; p = 0{,}062$) tidak menunjukkan pengaruh signifikan. Pengujian multikolinearitas memastikan model terbebas dari multikolinearitas (Tolerance $>$ 0,10 dan VIF $<$ 10,0). Rumus berikut dapat digunakan untuk menentukan nilai tabel-t:

$$t = b_i / Sb_i$$

Uji t pada Tabel 12 membuktikan tiga prediktor berpengaruh positif dan signifikan terhadap kesadaran siber, yaitu *Avoidance Motivation* ($\beta = 0{,}335; p < 0{,}001$), *Avoidance Behavior* ($\beta = 0{,}094; p = 0{,}047$), dan *Behavioral Intention* ($\beta = 0{,}423; p < 0{,}001$). Sebaliknya, *Self-Efficacy* ($\beta = 0{,}086; p = 0{,}062$) tidak menunjukkan pengaruh signifikan secara parsial. Evaluasi diagnostik multikolinearitas mengonfirmasi seluruh variabel bebas memiliki nilai *Tolerance* $>$ 0,10 dan VIF $<$ 10,0, sehingga model terbebas dari masalah multikolinearitas:

TABEL 12 UJI T

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardized Coefficients Beta	t	Sig.
1	(Constant)	3.020	1.453		2.078	.039
	Self_Efficacy	.105	.056	.086	1.873	.062
	Avoidance_Motivation	.286	.056	.335	5.135	<,001
	Avoidance_Behavior	.111	.056	.094	2.000	.047
	Behavioral_Intention	.385	.056	.423	6.831	<,001

a. Dependent Variable: Cybersecurity_Awareness

Capaian $R^2 = 0{,}607$ pada Tabel 13 menunjukkan daya jelaskan model TTAT sebesar 60,7% terhadap variasi *Cybersecurity Awareness*, sedangkan 39,3% sisa variansi dipengaruhi prediktor lain di luar model..

TABEL 13 SUMMARY

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.779[a]	.607	.600	2.59561

a. Predictors: (Constant), Behavioral_Intention, Self_Efficacy, Avoidance_Behavior, Avoidance_Motivation

F. Pembahasan

Menggunakan hasil analisis regresi linier multivariat untuk mengevaluasi dampak berbagai faktor dalam *Technology Threat Avoidance Theory* (TTAT) terhadap kesadaran keamanan siber terhadap ancaman *phishing* pada mahasiswa Politeknik Negeri Batam. Data yang dianalisis mencakup variabel bebas yaitu *Self-Efficacy* (X1), *Avoidance Motivation* (X2), *Avoidance Behaviour* (X3), dan *Behavioral Intention* (X4), serta variabel terikat yaitu *Cybersecurity Awareness* (Y).

1) Pembuktian secara simultan mengonfirmasi bahwa variabel *Technology Threat Avoidance Theory* (TTAT) secara kolektif berpengaruh signifikan terhadap kesadaran siber mahasiswa ($p < 0{,}001$). Dengan nilai $R^2 = 0{,}607$, model ini mampu menerangkan 60,7% variasi kesadaran siber, sedangkan 39,3% sisanya dipengaruhi faktor luar seperti tingkat literasi digital dan rekam jejak terpapar serangan.

2) Secara parsial, dorongan motivasi (*Avoidance Motivation*), tindakan nyata (*Avoidance Behavior*), serta niat berperilaku (*Behavioral Intention*) terbukti menjadi determinan utama yang meningkatkan kesadaran siber. Sebaliknya, variabel efikasi diri (*Self-Efficacy*) menunjukkan anomali dengan tidak adanya pengaruh signifikan ($p = 0{,}062 > 0{,}05$).

3) Penjelasan empiris atas anomali ini terungkap melalui *Independent Samples t-Test* antara mahasiswa rumpun non-teknis (61,8%) dan teknis (38,2%). Kelompok non-teknis mencatatkan rerata keyakinan diri yang lebih tinggi secara signifikan ($p < 0{,}05$), namun tidak diimbangi dengan kebiasaan proteksi nyata. Fenomena ini membuktikan adanya *False Sense of Security* (rasa aman semu), di mana rasa percaya diri harian mahasiswa non-teknis belum didasari oleh kapabilitas teknis yang memadai untuk menangkal peretasan phishing.

IV. KESIMPULAN

A. Kesimpulan

Studi ini membuktikan bahwa kerangka *Technology Threat Avoidance Theory* (TTAT) secara simultan mampu memprediksi ketahanan dan kesadaran siber mahasiswa Politeknik Negeri Batam terhadap kejahatan phishing ($R^2 = 60{,}7\%$). Secara parsial, niat proteksi dan motivasi penghindaran memegang peranan paling dominan dalam membentuk kesadaran siber.

Pembuktian empiris mengidentifikasi keberadaan fenomena *False Sense of Security* pada kelompok mahasiswa non-teknis, di mana keyakinan diri intuitif tidak berbanding lurus dengan kebiasaan proteksi teknis nyata. Oleh karena itu, intervensi edukasi siber di perguruan tinggi vokasi harus mengedepankan pelatihan teknis terapan (seperti validasi SSL dan konfigurasi MFA) untuk membangun perilaku proteksi yang efektif..

Untuk meningkatkan pengetahuan siswa mengenai phishing, dapat disimpulkan bahwa penelitian ini dapat dijadikan landasan bagi penelitian atau pertimbangan di masa mendatang. Selain itu, diharapkan penelitian ini dapat meningkatkan kesadaran siswa akan pentingnya keamanan siber.

B. Keterbatasan Penelitian

Peneliti menyadari bahwa penelitian ini memiliki beberapa keterbatasan yang dapat menjadi perhatian bagi penelitian selanjutnya:

1) Bias Komposisi Jurusan: Sampel dalam penelitian ini didominasi oleh mahasiswa dari Jurusan Manajemen Bisnis (61,8%), sehingga hasil kesimpulan mengenai kesadaran keamanan siber ini lebih mencerminkan perspektif mahasiswa non-teknis dan berpotensi menimbulkan bias jika digeneralisasikan untuk seluruh populasi mahasiswa Politeknik Negeri Batam secara makro.

2) Risiko Self-Selection Bias: Penggunaan teknik convenience sampling non-probabilistik melalui penyebaran Google Form secara daring memiliki risiko self-selection bias. Responden yang berpartisipasi secara sukarela cenderung merupakan mahasiswa yang lebih aktif secara digital, sehingga berpotensi belum menangkap secara utuh kondisi mahasiswa yang memiliki tingkat literasi digital lebih rendah.

C. Saran

Sebagai bentuk kontribusi praktis dari hasil penelitian ini dalam memitigasi rendahnya perilaku pencegahan mahasiswa, peneliti merekomendasikan adanya tindakan diseminasi edukasi secara langsung. Sebagai wujud komitmen tersebut, peneliti telah menyusun rancangan program kerja beserta instrumen edukasi berupa Online Sharing Session yang ditujukan bagi mahasiswa Politeknik Negeri Batam, yang secara mendetail dipaparkan pada Lampiran 1 di akhir naskah ini.

DAFTAR PUSTAKA

[1] Y. Xue, “R ESEARCH A RTICLE A VOIDANCE OF I NFORMATION T ECHNOLOGY T HREATS :,” vol. 33, no. 1, pp. 71–90, 2009.

[2] N. A. G. Arachchilage and S. Love, “Security awareness of computer users: A phishing threat avoidance perspective,” *Comput. Human Behav.*, vol. 38, pp. 304–312, 2014, doi: 10.1016/j.chb.2014.05.046.

[3] Person, “Information Security Awareness Level Measurement Using Multiple Criteria Decision Analysis (Mcda),” *J. Penelit. dan Pengemb. Komun. dan Inform.*, vol. 5, no. 1, p. 122371, 2014.

[4] K. Saidi and Y. Prayudi, “Analisis Indikator Utama Dalam Information Security - Personality Threat Terhadap Phishing Attack,” *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 6, no. 1, pp. 21–30, Jun. 2021, doi: 10.32528/JUSTINDO.V6I1.3801.

[5] M. Zulfahmi, H. #1, and S. Destya, “Mencegah Serangan Rekayasa Sosial dengan Human Firewall,” *JUSTIN (Jurnal Sist. dan Teknol. Informasi)*, vol. 10, no. 1, pp. 107–112, Jan. 2022, doi: 10.26418/JUSTIN.V10I1.44280.

[6] N. Vadila and A. R. Pratama, “Analisis Kesadaran Keamanan Terhadap Ancaman Phishing,” *Automata*, vol. 2, no. 2, pp. 1–4, 2021.

[7] S. Destya, “Pengukuran Tingkat Kesadaran Keamanan Informasi Berdasarkan Behavior Dan Offence Scale,” *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 5, no. 2, pp. 236–240, Jul. 2020, doi: 10.24114/CESS.V5I2.18206.

[8] D. Irawan and S. Kom, “MENCURI INFORMASI PENTING DENGAN MENGAMBIL ALIH AKUN FACEBOOK DENGAN METODE PHISING,” *JIKI (Jurnal Ilmu Komput. dan Inform.*, vol. 1, no. 1, pp. 43–46, Jul. 2020, doi: 10.24127/JIKI.V1I1.671.

[9] H. Wijayanto, A. H. Muhammad, and D. Hariyadi, “Analisis Penyalahgunaan Data Pribadi Dalam Aplikasi Fintech Ilegal Dengan Metode Hibrid,” *J. Ilm. SINUS*, vol. 18, no. 1, p. 1, Jan. 2020, doi: 10.30646/sinus.v18i1.433.

[10] F. Baso and M. R. Ramadan, "Hubungan Tingkat Kesadaran Pengguna terhadap Cybercrime dan Pengaplikasian Fitur Peringatan Phishing dan Malware Pada Google Browser," *J. Embed. Syst. Secur. Intell. Syst.*, pp. 269–273, Nov. 2024, doi: 10.59562/JESSI.V5I3.5527.

[11] A. Asyhary, J. Arsyad, U. Tamrin, J. P. Lande, and N. Umar, "Meningkatkan Kesadaran Remaja Terhadap Phishing Melalui Literasi Digital: Studi Kasus di SMK Darussalam Makassar," *J. Pengabdi. Literasi Digit. Indones.*, vol. 3, no. 2, pp. 60–71, Oct. 2024, doi: 10.57119/ABDIMAS.V3I2.122.

[12] D. Wina *et al.*, "The Importance of Security Awareness in Combating Phishing Attacks: A Case Study of Bank Rakyat Indonesia," *Soshum J. Sos. dan Hum.*, vol. 14, no. 3, pp. 207–214, Nov. 2024, doi: 10.31940/SOSHUM.V14I3.207-214.

[13] T. Tan, H. Sama, T. Wibowo, G. Wijaya, and O. E. Aboagye, "Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam," *J. Teknol. dan Inf.*, vol. 14, no. 2, pp. 163–173, Sep. 2024, doi: 10.34010/JATI.V14I2.12518.

[14] U. Negeri Makassar *et al.*, "Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar," *Vokatek J. Pengabdi. Masy.*, vol. 1, no. 1, pp. 28–33, Jan. 2023, doi: 10.61255/VOKATEKJPM.V1I1.29.

LAMPIRAN 1: PERENCANAAN DAN INSTRUMEN SOSIALISASI BERBASIS ONLINE SHARING SESSION (IMPLEMENTASI PENINGKATAN CYBERSECURITY AWARENESS)

Sebagai bentuk diseminasi hasil penelitian ilmiah dan implementasi dari kesepakatan sidang, disusun rencana aksi sosialisasi berupa edukasi interaktif daring (Online Sharing Session). Program ini dirancang secara spesifik untuk meningkatkan kesadaran siber sekaligus memitigasi titik lemah perilaku keamanan yang ditemukan pada objek penelitian.

A. Rencana Aksi Sosialisasi

1. Nama Program: Online Sharing Session "Cybersecurity Awareness: Mengubah Niat Menjadi Perilaku Aman dari Phishing".
2. Metode Eksekusi: Peneliti menyelenggarakan webinar interaktif menggunakan platform Microsoft Teams / Zoom internal Politeknik Negeri Batam. Undangan berupa tautan (link) acara disebarkan secara digital ke grup-grup komunikasi mahasiswa.
3. Waktu Pelaksanaan: Diadakan pada hari Sabtu (akhir pekan) dalam kurun waktu 1 bulan setelah naskah resmi disetujui.
4. Target Keberhasilan: Dihadiri oleh minimal 50 partisipan aktif mahasiswa Politeknik Negeri Batam, dengan fokus undangan utama pada rumpun mahasiswa non-teknis (Jurusan Manajemen Bisnis) guna memitigasi kerentanan siber yang terdeteksi di lapangan.

B. Susunan Acara

Waktu	Agenda	Deskripsi
15.00 - 15.05 WIB	Pembukaan oleh Moderator	Sambutan & Tata Tertib
15.05 - 15.20 WIB	Pemaparan Hasil Riset	Sosialisasi Temuan
15.20 - 15.45 WIB	Sesi Implementasi Aksi Keamanan (Cybersecurity Action)	Panduan Praktik Pencegahan *Phishing* (Avoidance Behaviour)
15.45 - 15.55 WIB	Sesi Diskusi & Tanya Jawab	Interaksi Respon Balik
15.55 - 16.00 WIB	Penutup & Dokumentasi	Foto Bersama & Absensi

C. Cetak Biru Materi Presentasi

Struktur materi dirancang tidak hanya sebatas teori, melainkan difokuskan pada implementasi taktik penghindaran ancaman (*Technology Threat Avoidance*) sesuai dengan hasil regresi penelitian:

1. Slide 1 & 2: Membedah Gap Antara Niat vs Tindakan Nyata (Fase Teori)
   Mengedukasi peserta mengenai temuan riset bahwa keyakinan diri (*Self-Efficacy*) yang tinggi tanpa dasar teknis justru memicu "rasa aman semu" (*false sense of security*). Menyadarkan peserta bahwa niat aman (*Behavioral Intention*) tidak cukup jika skor tindakan pencegahan nyata (*Avoidance Behaviour*) mereka terbukti masih sangat rendah.
2. Slide 3 & 4: Panduan Implementasi Pencegahan Phishing (Fase Aksi)
   Sebagai wujud implementasi dari *Cybersecurity Awareness*, peneliti mendemonstrasikan tindakan pencegahan (*Avoidance Behaviour*) konkret yang harus dipraktikkan peserta:
3. Visual *URL & SSL Checking*: Edukasi cara paling cepat memverifikasi keaslian struktur domain link akademik kampus dan mengecek status keamanan sertifikat pada browser.
4. Penguatan *Human Firewall (2FA)*: Panduan terarah bagi mahasiswa untuk mengaktifkan lapis keamanan tambahan *Two-Factor Authentication (2FA)* pada akun institusi sebagai benteng pertahanan utama saat kredensial bocor.