E-ISSN: 3025-0994
Halaman 4962-4974
Volume 4 Nomor 3 Tahun 2026

Pengaruh Cybersecurity Awareness Terhadap Kerentanan Mahasiswa Universitas Muhammadiyah Bandung Dalam Menghadapi Penipuan Digital

Ai Karlina[1], Nadia Azzahra Fadhilah[2], Shidqi Rafially[3], Meutia Anilfa Fajariah[4],Arina Shabrina[5]

[1,2,3,4,5] Program Studi Psikologi, Fakultas Sosial dan Humaniora, Universitas Muhammadiyah Bandung
e-mail: karlinasutiana45@gmail.com

Abstrak

Perkembangan media digital telah meningkatkan kemudahan akses informasi dan aktivitas daring, tetapi juga diikuti oleh meningkatnya risiko penipuan digital yang menyasar berbagai kalangan, termasuk mahasiswa. Cybersecurity awareness diduga berperan penting dalam memengaruhi kerentanan individu terhadap penipuan digital, namun penelitian yang secara khusus menguji hubungan tersebut pada konteks mahasiswa masih terbatas. Penelitian ini bertujuan menganalisis pengaruh cybersecurity awareness terhadap kerentanan mahasiswa Universitas Muhammadiyah Bandung (UMB) dalam menghadapi penipuan digital. Penelitian menggunakan pendekatan kuantitatif dengan desain korelasional terhadap 107 mahasiswa aktif UMB yang dipilih melalui teknik convenience sampling. Data dikumpulkan menggunakan kuesioner daring yang terdiri atas 13 aitem skala Cybersecurity Awareness dan 15 aitem skala Kerentanan terhadap Penipuan Digital. Kedua instrumen dinyatakan valid (r-hitung > r-tabel 0,190) dan reliabel (Cronbach's Alpha = 0,773 dan 0,838). Data dianalisis menggunakan uji korelasi Pearson dan regresi linear sederhana. Hasil menunjukkan hubungan positif yang kuat dan signifikan antara cybersecurity awareness dan kerentanan terhadap penipuan digital ($r = 0,798$; $p < 0,001$), dengan cybersecurity awareness menyumbang 63,7% variasi skor kerentanan ($R^2 = 0,637$; $F = 184,59$; $p < 0,001$). Arah hubungan yang positif mengindikasikan bahwa peningkatan pengetahuan keamanan siber tidak serta-merta menurunkan kerentanan apabila belum diikuti oleh perilaku pencegahan yang konsisten. Temuan ini menegaskan pentingnya program literasi keamanan siber di perguruan tinggi yang tidak hanya berorientasi pada peningkatan pengetahuan, tetapi juga pada penguatan keterampilan perilaku dalam menghadapi modus penipuan digital yang terus berkembang.

Kata Kunci: Cybersecurity Awareness; Keamanan Siber; Kerentanan; Mahasiswa; Penipuan Digital

Abstract

The rapid growth of digital media has increased ease of access to information and online activity, but has also been followed by a rising risk of digital fraud targeting various groups, including university students. Cybersecurity awareness is presumed to play an important role in shaping individuals' vulnerability to digital fraud, yet research specifically examining this relationship among university students remains limited. This study aims to analyze the influence of cybersecurity awareness on digital-fraud vulnerability among students at Universitas Muhammadiyah Bandung (UMB). A quantitative correlational design was employed involving 107 active UMB students selected through convenience sampling. Data were collected using an online questionnaire consisting of 13 items measuring Cybersecurity Awareness and 15 items measuring Vulnerability to Digital Fraud. Both instruments were valid (r-count > r-table 0.190) and reliable (Cronbach's Alpha = 0.773 and 0.838, respectively). Data were analyzed using Pearson correlation and simple linear regression. Results revealed a strong, significant positive relationship between cybersecurity awareness and vulnerability to digital fraud ($r = 0.798$; $p < 0.001$), with cybersecurity awareness accounting for 63.7% of the variance in vulnerability scores ($R^2 = 0.637$; $F = 184.59$; $p < 0.001$). The positive direction of this relationship indicates that increased cybersecurity knowledge does not automatically reduce vulnerability unless accompanied by consistent preventive behavior. These findings underscore the importance of cybersecurity literacy programs in higher education that focus not only on knowledge enhancement but also on strengthening behavioral skills in facing evolving digital-fraud tactics.

Keywords : Cybersecurity Awareness; Keamanan Siber; Kerentanan; Mahasiswa; Penipuan Digital

LATAR BELAKANG

Perkembangan teknologi digital yang semakin pesat telah membawa perubahan besar dalam kehidupan sehari-hari, khususnya di kalangan mahasiswa. Aktivitas akademik, komunikasi, transaksi keuangan, hingga hiburan kini banyak dilakukan melalui platform digital. Di satu sisi, kemajuan ini memberikan kemudahan dan efisiensi; di sisi lain, meningkatnya ketergantungan terhadap teknologi digital diikuti oleh berbagai risiko, salah satunya maraknya penipuan digital.

Fenomena ini tercermin dari data Indonesia Anti-Scam Center (IASC) yang mencatat 432.637 laporan penipuan digital hingga Januari 2026, meningkat dari 418.462 laporan pada bulan sebelumnya, atau rata-rata sekitar 1.000 kasus per hari, angka yang disebut tiga hingga empat kali lebih tinggi dibandingkan negara lain yang umumnya hanya mencatat 150 hingga 400 kasus harian [1]. OJK bersama IASC juga melaporkan total kerugian akibat penipuan online yang melampaui Rp2,6 triliun hingga Mei 2025 [2]. Survei APJII terhadap 8.700 responden menemukan bahwa penipuan online menjadi kasus keamanan digital paling banyak dialami pengguna internet Indonesia, mencapai 22,12% [3], sementara survei GoodStats terhadap responden yang didominasi Generasi Z mencatat 26,7% pernah

mengalami penipuan online, dengan modus dominan berupa peniruan identitas pihak resmi dan tekanan psikologis agar korban bertindak cepat tanpa berpikir panjang [4].

Mahasiswa merupakan kelompok yang aktif dan intens menggunakan internet serta media digital, sehingga menjadi target potensial bagi pelaku penipuan digital. Penelitian Wijaya dan Nurnawati terhadap mahasiswa di Yogyakarta menemukan bahwa tingkat kesadaran mahasiswa terhadap modus phishing pada layanan online banking masih bervariasi dan banyak yang belum mampu mengenali ciri-ciri tautan atau pesan palsu [5]. Temuan serupa dilaporkan oleh Tan dkk. pada mahasiswa di Kota Batam, yang menunjukkan bahwa tingkat kesadaran keamanan siber mahasiswa cenderung bervariasi antarwilayah dan antarprogram studi [6]. Studi terbaru oleh Gwenhure dkk. terhadap mahasiswa di Yogyakarta menggunakan health belief model turut menegaskan bahwa mahasiswa tetap rentan terhadap serangan phishing melalui e-mail meskipun telah memiliki pemahaman dasar mengenai risiko siber [7]. Wahyuni dkk. dalam analisis kerentanan kejahatan online phishing juga menunjukkan bahwa berbagai modus phishing berbasis tools otomatis dapat dengan mudah mengeksploitasi kelengahan pengguna untuk mencuri kredensial akun maupun data pribadi [8]. Modus-modus penipuan digital yang berkembang saat ini pun semakin beragam, mulai dari tautan phishing yang menyamar sebagai notifikasi resmi, penipuan transaksi jual-beli daring, hingga rekayasa sosial melalui pesan yang menimbulkan rasa panik atau iming-iming hadiah [9].

Salah satu faktor penting dalam menghadapi risiko tersebut adalah cybersecurity awareness, yaitu tingkat pengetahuan dan kesadaran individu terhadap berbagai ancaman keamanan siber serta cara berperilaku aman dalam penggunaan teknologi informasi, mencakup kemampuan mengenali risiko, memahami dampak ancaman siber, dan menerapkan praktik keamanan yang tepat [10]. Parsons dkk. menyatakan bahwa cybersecurity awareness terdiri atas aspek pengetahuan, sikap, dan perilaku pengguna dalam menjaga keamanan informasi, yang berperan penting dalam mencegah insiden keamanan siber akibat human error [11]. Furnell dan Thomson menegaskan bahwa perkembangan kajian cybersecurity awareness telah bergeser dari sekadar penyampaian pengetahuan (culture) menuju pembentukan perilaku aman yang konsisten (behaviour) [12]. Rendahnya cybersecurity awareness sering menjadi faktor utama terjadinya serangan siber seperti phishing, malware, dan kebocoran data, akibat penggunaan kata sandi yang lemah dan pengabaian prosedur keamanan [13]. Von Solms dan Von Solms menekankan bahwa keamanan informasi yang efektif tidak hanya bergantung pada teknologi, tetapi juga pada kesadaran dan budaya keamanan pengguna [14].

Kerentanan terhadap penipuan digital merujuk pada kecenderungan individu untuk menjadi korban berbagai modus penipuan berbasis teknologi, seperti phishing, rekayasa sosial, dan penyalahgunaan data pribadi. Wahyuni dkk. menunjukkan bahwa kerentanan ini banyak dipicu oleh kelengahan pengguna dalam mengenali tampilan situs atau pesan tiruan yang menyerupai layanan resmi [8]. Studi lain turut menunjukkan bahwa mahasiswa dengan pemahaman keamanan siber yang terbatas cenderung lebih sulit mengenali indikator phishing dan lebih rentan menjadi sasaran serangan [15]. Pada level kognitif, kerentanan turut dipengaruhi oleh bias optimisme, yaitu keyakinan individu bahwa dirinya kecil kemungkinan

menjadi korban, serta kecenderungan panik ketika menerima pesan mendesak yang mengatasnamakan pihak resmi [9].

Secara konseptual, semakin tinggi cybersecurity awareness seseorang, semakin besar kemampuannya mengenali dan menghindari ancaman penipuan digital, sehingga kerentanannya diharapkan menurun. Parsons dkk. menegaskan bahwa kesadaran keamanan informasi yang baik berperan sebagai faktor pelindung terhadap insiden keamanan siber [11]. Berdasarkan kajian teori tersebut, penelitian ini mengajukan hipotesis bahwa terdapat pengaruh cybersecurity awareness terhadap kerentanan mahasiswa Universitas Muhammadiyah Bandung dalam menghadapi penipuan digital.

Penelitian mengenai cybersecurity awareness dan penipuan digital telah banyak dilakukan, tetapi sebagian besar masih berfokus pada aspek phishing secara spesifik atau perilaku keamanan digital secara umum, dan sering kali dilakukan pada konteks kota atau kelompok mahasiswa tertentu di luar Jawa Barat. Penelitian yang secara khusus mengkaji pengaruh cybersecurity awareness terhadap kerentanan mahasiswa dalam menghadapi berbagai bentuk penipuan digital, tidak terbatas pada phishing semata, masih terbatas, khususnya pada konteks mahasiswa Universitas Muhammadiyah Bandung. Oleh karena itu, penelitian ini memiliki kebaruan (novelty) dengan menganalisis pengaruh cybersecurity awareness terhadap kerentanan mahasiswa terhadap penipuan digital secara lebih luas pada konteks perguruan tinggi di Bandung, sekaligus memberikan kontribusi teoretis bagi kajian keamanan siber pada populasi mahasiswa dan kontribusi praktis bagi pengembangan program literasi keamanan siber di lingkungan Universitas Muhammadiyah Bandung.

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk: (1) mengetahui tingkat cybersecurity awareness mahasiswa; (2) mengetahui tingkat kerentanan mahasiswa terhadap penipuan digital; dan (3) menganalisis pengaruh cybersecurity awareness terhadap kerentanan tersebut. Secara teoretis, penelitian ini diharapkan memperkaya kajian cybersecurity awareness dan kerentanan penipuan digital pada populasi mahasiswa; secara praktis, hasil penelitian diharapkan menjadi bahan pertimbangan bagi mahasiswa dalam meningkatkan kesadaran keamanan digital, bagi UMB dalam merancang program literasi siber, serta bagi peneliti selanjutnya sebagai rujukan penelitian sejenis.

METODE

Desain Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan desain korelasional untuk mengetahui hubungan antara *cybersecurity awareness* dan kerentanan terhadap penipuan digital. Data dianalisis menggunakan uji korelasi Pearson dan regresi linear sederhana, diolah melalui Microsoft Excel dan diverifikasi menggunakan JASP.

Variabel Penelitian

Variabel independen (X) adalah *cybersecurity awareness*, yaitu tingkat pengetahuan, pemahaman, dan kesadaran individu terhadap ancaman keamanan siber serta perilaku aman dalam penggunaan teknologi digital. Variabel dependen (Y) adalah kerentanan terhadap penipuan digital, yaitu tingkat kecenderungan individu untuk menjadi korban penipuan berbasis digital, seperti *phishing*, penipuan *online*, dan penyalahgunaan data pribadi.

Partisipan Penelitian

Populasi penelitian ini adalah seluruh mahasiswa aktif Universitas Muhammadiyah Bandung. Pengambilan sampel dilakukan dengan teknik *convenience sampling*, yaitu berdasarkan ketersediaan dan kemudahan akses peneliti terhadap responden yang bersedia mengisi kuesioner secara sukarela. Kriteria kelayakan *(eligibility criteria)* responden meliputi: (1) terdaftar sebagai mahasiswa aktif UMB (S1) pada tahun akademik berjalan; (2) berusia minimal 18 tahun; (3) merupakan pengguna aktif internet dan media sosial dalam kegiatan akademik maupun nonakademik; dan (4) bersedia mengisi kuesioner secara sukarela dan menyatakan persetujuan *(informed consent)*. Sampel penelitian berjumlah 107 mahasiswa yang memenuhi kriteria di atas. Karakteristik demografis sampel disajikan pada Tabel 1-3.

Tabel 1. Distribusi Responden Berdasarkan Jenis Kelamin

Jenis Kelamin	Jumlah	Persentase
Perempuan	68	63,6%
Laki-laki	39	36,4%
Total	107	100%

Tabel 2. Distribusi Responden Berdasarkan Angkatan

Angkatan	Jumlah	Persentase
2021	10	9,3%
2022	73	68,2%
2023	15	14,0%
2024	4	3,7%
2025	5	4,7%
Total	107	100%

Tabel 3. Distribusi Responden Berdasarkan Program Studi

Program Studi	Jumlah
Psikologi	31
Manajemen	28

Program Studi	Jumlah
Ekonomi Syariah	9
Farmasi	6
Ilmu Komunikasi	6
Administrasi Publik	5
Teknik Informatika	5
Akuntansi	4
Agribisnis	3
Lainnya	10

Instrumen Penelitian

Instrumen yang digunakan adalah kuesioner yang dikembangkan sendiri oleh tim peneliti, terdiri atas 28 aitem yang terbagi menjadi dua skala: (1) skala *Cybersecurity Awareness* (13 aitem, kode A1-A13), mengacu pada konsep Kruger dan Kearney [10] serta Parsons dkk. [11], mencakup pengetahuan mengenai keamanan kata sandi, keamanan e-mail dan lampiran, serta risiko mengunduh dan mengakses tautan; dan (2) skala Kerentanan terhadap Penipuan Digital (15 aitem, kode K3-K17), mengukur kesulitan mengenali tanda-tanda penipuan, kecenderungan panik atau percaya pada pesan mendesak, bias optimisme, serta riwayat pengalaman hampir menjadi korban penipuan digital. Dua aitem (K1 dan K2) yang semula termasuk dalam skala ini dihapus karena berbunyi protektif dan tidak searah dengan konstruk kerentanan yang diukur aitem-aitem lainnya. Kedua skala menggunakan skala Likert 5 poin: Sangat Tidak Setuju (1), Tidak Setuju (2), Netral (3), Setuju (4), Sangat Setuju (5). Kuesioner disebarkan secara daring melalui *Google Form*.

Uji Validitas Instrumen

Uji validitas menggunakan teknik *corrected item-total correlation*, dibandingkan dengan r-tabel untuk n=107 (df=105) pada taraf signifikansi 5% (dua arah) sebesar 0,190. Hasil uji validitas menunjukkan seluruh 13 aitem skala *Cybersecurity Awareness* (r-hitung 0,204-0,567) dan seluruh 15 aitem skala Kerentanan (r-hitung 0,302-0,553) memiliki r-hitung > r-tabel, sehingga seluruh 28 aitem dinyatakan valid (Tabel 4).

Tabel 4. Hasil Uji Validitas Instrumen

Skala	Jumlah Aitem	Rentang r-hitung	r-tabel	Keterangan
Cybersecurity Awareness (A1-A13)	13	0,204 – 0,567	0,190	Semua Valid
Kerentanan Penipuan Digital (K3-K17)	15	0,302 – 0,553	0,190	Semua Valid

Uji Reliabilitas Instrumen

Reliabilitas diuji menggunakan metode Cronbach's Alpha dengan kriteria reliabel apabila Alpha > 0,70 [16]. Hasil menunjukkan nilai Alpha 0,773 untuk skala *Cybersecurity Awareness* dan 0,838 untuk skala Kerentanan Penipuan Digital, sehingga kedua instrumen dinyatakan reliabel (Tabel 5).

Tabel 5. Hasil Uji Reliabilitas Instrumen

Skala	Jumlah Aitem	Cronbach's Alpha	Keterangan
Cybersecurity Awareness (A1-A13)	13	0,773	Reliabel
Kerentanan Penipuan Digital (K3-K17)	15	0,838	Reliabel

Teknik Pengumpulan dan Analisis Data

Data dikumpulkan secara daring melalui penyebaran tautan *Google Form* kepada mahasiswa UMB yang memenuhi kriteria kelayakan. Data yang terkumpul diperiksa kelengkapannya, diberi kode, dan diolah menggunakan Microsoft Excel (uji validitas, reliabilitas, statistik deskriptif, korelasi Pearson, regresi linear sederhana) serta diverifikasi menggunakan JASP.

HASIL DAN PEMBAHASAN

Pelaksanaan Penelitian

Penelitian dilaksanakan dengan menyebarkan kuesioner secara daring melalui *Google Form* kepada mahasiswa UMB. Diperoleh 107 responden dengan data lengkap dan layak dianalisis. Pemeriksaan kualitas data menunjukkan tidak ada nilai kosong *(missing)* dan seluruh nilai berada pada rentang skala Likert 1-5 yang valid.

Statistik Deskriptif

Tabel 6. Statistik Deskriptif Variabel Penelitian

Variabel	Mean	Std. Deviasi	N
Cybersecurity Awareness (X)	55,54	4,834	107
Kerentanan Penipuan Digital (Y)	64,62	5,858	107

Skor *Cybersecurity Awareness* memiliki rentang teoretis 13-65 dengan mean 55,54, mengindikasikan tingkat kesadaran keamanan siber mahasiswa yang cukup tinggi. Skor Kerentanan terhadap Penipuan Digital memiliki rentang teoretis 15-75 dengan mean 64,62, yang juga tergolong cukup tinggi, menunjukkan bahwa mahasiswa secara rata-rata masih cukup rentan terhadap penipuan digital.

Hasil Uji Korelasi Pearson

Tabel 7. Hasil Uji Korelasi Pearson (Signifikan pada taraf 0,01, dua arah)

Variabel	Cybersecurity Awareness (X)	Kerentanan Penipuan Digital (Y)
Cybersecurity Awareness (X)	1	0,798
Kerentanan Penipuan Digital (Y)	0,798	1

Diperoleh nilai koefisien korelasi r = 0,798 dengan signifikansi p < 0,001, menunjukkan hubungan positif yang kuat dan signifikan antara *cybersecurity awareness* dan kerentanan terhadap penipuan digital.

Hasil Analisis Regresi Linear Sederhana

Tabel 8. Ringkasan Model Regresi

Model	R	R Square	Adjusted R Square	Std. Error
1	0,798	0,637	0,633	3,544

Nilai R *Square* sebesar 0,637 menunjukkan bahwa 63,7% variasi skor kerentanan terhadap penipuan digital dapat dijelaskan oleh *cybersecurity awareness*, sedangkan 36,3% dipengaruhi faktor lain di luar penelitian.

Tabel 9. Hasil Uji ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	2318,49	1	2318,49	184,59	0,000
Residual	1318,80	105	12,56		
Total	3637,29	106			

Nilai F = 184,59 dengan signifikansi 0,000 (p < 0,05) menunjukkan bahwa model regresi yang digunakan signifikan secara statistik dan layak digunakan untuk memprediksi kerentanan berdasarkan *cybersecurity awareness*.

Tabel 10. Koefisien Regresi Linear Sederhana

Variabel	B	Std. Error	Beta	t	Sig.
Konstanta	10,876	3,969	-	2,740	0,007
Cybersecurity Awareness	0,968	0,071	0,798	13,587	0,000

Nilai koefisien regresi B = 0,968 dengan signifikansi 0,000 menunjukkan bahwa *cybersecurity awareness* berpengaruh signifikan terhadap kerentanan mahasiswa terhadap penipuan digital. Persamaan regresi yang terbentuk adalah: $\hat{Y}$ = 10,876 + 0,968X.

Pembahasan

Penelitian ini bertujuan menganalisis pengaruh *cybersecurity awareness* terhadap kerentanan mahasiswa Universitas Muhammadiyah Bandung dalam menghadapi penipuan digital. Hasil uji korelasi Pearson menunjukkan nilai r = 0,798 (p < 0,001), mengindikasikan hubungan positif yang kuat antara kedua variabel. Hasil analisis regresi menunjukkan R *Square* sebesar 0,637, artinya *cybersecurity awareness* menjelaskan 63,7% variasi skor kerentanan penipuan digital.

Temuan ini menunjukkan hubungan positif yang kuat dan signifikan antara *cybersecurity awareness* dan kerentanan terhadap penipuan digital, berbeda dengan asumsi teoretis yang menyatakan bahwa peningkatan *cybersecurity awareness* seharusnya menurunkan kerentanan individu terhadap ancaman siber. Perbedaan ini diduga berkaitan dengan karakteristik instrumen yang digunakan. Skala kerentanan tidak hanya mengukur kemungkinan menjadi korban penipuan digital, tetapi juga mengukur kesadaran responden terhadap pengalaman serta potensi risiko yang pernah atau mungkin mereka alami. Dengan demikian, responden dengan *cybersecurity awareness* lebih tinggi cenderung lebih mampu mengenali berbagai bentuk ancaman digital sehingga memberikan skor kerentanan yang lebih tinggi.

Arah hubungan yang ditemukan adalah positif, semakin tinggi skor *cybersecurity awareness*, semakin tinggi pula skor kerentanan, sehingga perlu diinterpretasikan secara hati-

hati. Secara konseptual, ada beberapa penjelasan yang mungkin: (1) mahasiswa yang lebih sadar terhadap ancaman siber justru lebih banyak terpapar informasi tentang modus penipuan, sehingga lebih banyak pula yang menyadari bahwa mereka pernah hampir menjadi korban; (2) skala kerentanan ini mengukur kombinasi antara refleksi kognitif atas risiko dan pengalaman konkret, sehingga responden yang lebih sadar secara digital justru lebih jujur mengenali kerentanan mereka; atau (3) terdapat hubungan timbal balik, yaitu pengalaman hampir menjadi korban justru mendorong mahasiswa lebih aktif meningkatkan *awareness*-nya. Bada dan Nurse dalam tinjauan sistematis mengenai dampak sosial dan psikologis *cybersecurity awareness* turut menegaskan bahwa kesadaran keamanan siber berkaitan erat dengan pengalaman emosional individu terhadap ancaman digital, sehingga responden yang lebih sadar risiko juga cenderung lebih reflektif dalam melaporkan kerentanannya sendiri[17].

Temuan ini relevan dengan konteks fenomena penipuan digital yang semakin masif di Indonesia, dengan IASC mencatat lebih dari 432 ribu laporan penipuan per Januari 2026, dengan modus yang terus berkembang dan semakin sulit dibedakan dari komunikasi resmi [1]. Kondisi ini menegaskan bahwa kesadaran kognitif saja belum cukup untuk sepenuhnya mencegah kerentanan, dan diperlukan pendekatan pendidikan yang tidak hanya meningkatkan pengetahuan *(knowledge)*, tetapi juga melatih respons perilaku konkret dalam menghadapi modus penipuan terkini.

Temuan ini sejalan dengan penelitian Alqahtani yang menyatakan bahwa *cybersecurity awareness* merupakan konsep yang dipengaruhi oleh berbagai faktor, seperti pengalaman menggunakan teknologi, kebiasaan berinternet, serta perilaku keamanan digital [18]. Oleh karena itu, peningkatan pengetahuan mengenai keamanan siber tidak selalu diikuti oleh penurunan tingkat kerentanan apabila belum diwujudkan dalam perilaku keamanan yang konsisten. Hong dkk. juga menjelaskan bahwa individu dengan tingkat kesadaran keamanan siber yang baik masih dapat melakukan perilaku berisiko, seperti membuka tautan yang tidak dikenal atau mengabaikan prosedur keamanan karena dipengaruhi oleh kebiasaan, rasa percaya diri yang berlebihan, maupun tekanan situasional [19].

Di sisi lain, penelitian Ruzaili dkk. menunjukkan bahwa pengetahuan mengenai *phishing* belum tentu mampu memprediksi perilaku pencegahan secara optimal [20]. Hasil tersebut memperkuat temuan penelitian ini bahwa peningkatan *cybersecurity awareness* saja belum cukup untuk menurunkan kerentanan terhadap penipuan digital. Diperlukan kemampuan menerapkan pengetahuan tersebut dalam bentuk perilaku nyata, seperti memverifikasi identitas pengirim, memeriksa keaslian tautan, menggunakan autentikasi multifaktor, serta menghindari pengambilan keputusan secara terburu-buru ketika menerima pesan yang bersifat mendesak.

Berdasarkan temuan tersebut, penelitian ini memberikan implikasi bahwa program literasi keamanan siber di lingkungan perguruan tinggi tidak cukup berfokus pada peningkatan pengetahuan semata, tetapi juga perlu mengembangkan keterampilan praktis melalui simulasi *phishing* berbasis gamifikasi yang terbukti efektif meningkatkan kewaspadaan pengguna terhadap serangan *phishing* [21], pelatihan pengambilan keputusan, serta pembiasaan perilaku keamanan digital. Efektivitas program semacam ini perlu dievaluasi secara berkala menggunakan kerangka evaluasi yang sistematis [22], agar dampaknya terhadap penurunan kerentanan dapat diukur secara objektif. Dengan demikian, mahasiswa tidak hanya

memahami ancaman siber secara konseptual, tetapi juga mampu menerapkan langkah-langkah pencegahan dalam kehidupan sehari-hari.

Keterbatasan Penelitian

Keterbatasan penelitian ini meliputi: (1) desain *cross-sectional* yang tidak dapat menyimpulkan hubungan kausal; (2) teknik *convenience sampling* yang membatasi generalisasi; (3) pengukuran berbasis *self-report* yang rentan terhadap bias sosial-desirabilitas; dan (4) kemungkinan adanya variabel ketiga (misalnya intensitas penggunaan internet atau pengalaman menjadi korban sebelumnya) yang menjelaskan korelasi yang ditemukan.

SIMPULAN

Berdasarkan hasil penelitian terhadap 107 mahasiswa Universitas Muhammadiyah Bandung, dapat disimpulkan bahwa: (1) instrumen penelitian yang digunakan (28 aitem: 13 Cybersecurity Awareness + 15 Kerentanan Penipuan Digital) dinyatakan valid (semua r-hitung > r-tabel 0,190) dan reliabel (α=0,773 dan α=0,838); (2) terdapat hubungan positif yang kuat dan signifikan antara cybersecurity awareness dan kerentanan terhadap penipuan digital ($r = 0,798$; $p < 0,001$); dan (3) cybersecurity awareness berpengaruh signifikan terhadap kerentanan mahasiswa, dengan kontribusi sebesar 63,7% terhadap variasi skor kerentanan ($R^2 = 0,637$; $F = 184,59$; $p < 0,001$).

SARAN

Bagi penelitian selanjutnya, disarankan menambahkan variabel mediator atau moderator seperti pengalaman menjadi korban, intensitas penggunaan internet, atau faktor kepribadian, untuk memperoleh gambaran yang lebih komprehensif mengenai dinamika kerentanan digital. Penting pula untuk mengembangkan intervensi pendidikan siber yang tidak hanya meningkatkan pengetahuan, tetapi secara khusus melatih kemampuan mahasiswa mengenali dan merespons modus penipuan digital yang spesifik dan terus berkembang, misalnya melalui pendekatan gamifikasi [21] yang dievaluasi efektivitasnya secara berkala [22]. Penelitian selanjutnya juga disarankan menggunakan teknik random sampling agar temuan dapat digeneralisasi ke seluruh populasi mahasiswa UMB.

DAFTAR PUSTAKA

[1] I. A.-S. C. (IASC), “Penipuan Digital di Indonesia Meledak 4 Kali Lipat,” 2026, *Suara.com*. [Online]. Available: https://www.suara.com/tekno/2026/03/25/135918/

[2] K. I. Center, “Penipuan Belanja Online, Modus Scam Terbanyak di Indonesia,” 2025. [Online]. Available: https://databoks.katadata.co.id

[3] APJII, “Survei Penetrasi Internet dan Segmentasi Pasar ISP 2025,” 2025. [Online]. Available: https://data.goodstats.id/statistic/22-pengguna-internet-indonesia-alami-penipuan-online-qHAgN

[4] G. Data, “26% Publik RI Jadi Korban Penipuan Online 2025,” 2025. [Online]. Available: https://data.goodstats.id/statistic/26-publik-ri-jadi-korban-penipuan-online-2025-2jeLQ

[5] L. Wijaya and E. K. Nurnawati, “Analisis Kesadaran Mahasiswa Yogyakarta Tentang Phishing Pada Online Banking,” *J. Din. Inform.*, vol. 11, no. 2, 2022.

[6] 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, 2024.

[7] A. K. Gwenhure, “University Students’ Security Behavior against Email Phishing Attacks: Insights from the Health Belief Model,” *J. Cybersecurity*, vol. 11, no. 1, p. Tyaf034, 2025, doi: 10.1093/cybsec/tyaf034.

[8] N. K. A. T. Wahyuni, P. P. Cahayani, I. G. N. Y. Wicaksana, and I. A. K. B. Wijayanti, “Analisis Kerentanan Kejahatan Online Phishing Menggunakan Tools Zphisher, Shellphish, dan Whphisher,” *J. Tek. Mesin, Elektro dan Ilmu Komput.*, vol. 3, no. 1, pp. 23–31, 2023.

[9] P. B. Polri, “Waspada SMS Phishing E-Tilang: Dari Modus Digital hingga Jerat Hukum,” 2026. [Online]. Available: https://pusiknas.polri.go.id/detail_artikel/waspada_sms_phising_e-tilang

[10] H. A. Kruger and W. D. Kearney, “A Prototype for Assessing Information Security Awareness,” *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006, doi: 10.1016/j.cose.2006.02.008.

[11] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, “The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies,” *Comput. Secur.*, vol. 66, pp. 40–51, 2017, doi: 10.1016/j.cose.2017.01.004.

[12] S. Hu, C. Hsu, and Z. Zhou, “Security Education, Training, and Awareness Programs: Literature Review,” *J. Comput. Inf. Syst.*, vol. 62, no. 4, pp. 752–764, 2022, doi: 10.1080/08874417.2021.1913671.

[13] M. A. Sasse, S. Brostoff, and D. Weirich, “Transforming the ‘Weakest Link’: A Human–Computer Interaction Approach to Usable and Effective Security,” *BT Technol. J.*, vol. 19, no. 3, pp. 122–131, 2001, doi: 10.1023/A:1011902718709.

[14] R. Von Solms and B. Von Solms, “From Policies to Culture,” *Comput. Secur.*, vol. 23, no. 4, pp. 275–279, 2004, doi: 10.1016/j.cose.2004.01.013.

[15] K. Okokpujie, C. G. Kennedy, K. Nnodu, and E. Noma-Osaghae, “Cybersecurity Awareness: Investigating Students’ Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment,” *Int. J. Sustain. Dev. Plan.*, vol. 18, no. 1, pp. 255–263, 2023, doi: 10.18280/ijsdp.180127.

[16] J. C. Nunnally, *Psychometric Theory*, 2nd ed. New York, NY: McGraw-Hill, 1978.

[17] A. Alzubaidi, “Measuring the Level of Cyber-Security Awareness for Cybercrime in Saudi Arabia,” *Heliyon*, vol. 7, no. 1, p. e06016, 2021, doi: 10.1016/j.heliyon.2021.e06016.

[18] M. A. Alqahtani, “Factors Affecting Cybersecurity Awareness among University Students,” *Appl. Sci.*, vol. 12, no. 5, p. 2589, 2022, doi: 10.3390/app12052589.

[19] W. C. H. Hong, C. Chi, J. Liu, Y. Zhang, V. N.-L. Lei, and X. Xu, “The Influence of Social Education Level on Cybersecurity Awareness and Behaviour,” *Educ. Inf. Technol.*, vol. 28, no. 1, pp. 439–470, 2023, doi: 10.1007/s10639-022-11121-5.

[20] H. Ruzaili, N. Katuk, K. Mohd Zaini, and W. Abdullah, “Phishing Awareness and Preventive Measures Among University Students: Knowledge, Behaviors, and Victimisation Perspectives,” *Millenium – J. Educ. Technol. Heal.*, no. 29, p. E43489, 2026, doi: 10.29352/mill0229.43489.

[21] M. Canham, C. Posey, and M. Constantino, “Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks,” *Front. Educ.*, vol. 6, p. 807277, 2022, doi: 10.3389/feduc.2021.807277.

[22] S. Baadel, F. Thabtah, and J. Lu, “Cybersecurity Awareness: A Critical Analysis of Education and Law Enforcement Methods,” *Informatica*, vol. 45, no. 3, pp. 335–345, 2021, doi: 10.31449/inf.v45i3.3328.