Jurnal Pengabdian Literasi Digital Indonesia
E-ISSN. 2961-9440
Volume: 3, Nomor 2, Desember, **2024**, *Hal*: 60-71

Meningkatkan Kesadaran Remaja Terhadap Phishing Melalui Literasi Digital: Studi Kasus di SMK Darussalam Makassar

Andi Asyhary J. Arsyad[1*], Usman Tamrin[1], Janisa Pascawati Lande[1], Najirah Umar[2]

[1]*Universitas Pejuang Republik Indonesia*
andiasyhary001@gmail.com, usmangolrock@gmail.com, janisalande@gmail.com
[2]*Universitas Handayani Makassar*
najirah@handayani.ac.id

Abstrak

Serangan phishing adalah salah satu ancaman keamanan siber yang paling umum dan merusak, memanfaatkan kelemahan manusia seperti kurangnya kewaspadaan dan literasi digital. Penelitian ini bertujuan untuk mengidentifikasi strategi efektif dalam meningkatkan kesadaran terhadap serangan phishing melalui literasi digital di kalangan remaja. Penelitian ini dilaksanakan di SMK Darussalam Makassar dengan menggunakan metode kuantitatif deskriptif dan melibatkan 227 responden. Hasil penelitian menunjukkan bahwa 80% responden setuju bahwa literasi digital berperan penting dalam mengurangi dampak phishing. Literasi digital, yang mencakup pemahaman tentang teknologi, identifikasi ancaman, dan langkah-langkah perlindungan, terbukti efektif dalam melindungi siswa dari serangan phishing. Berdasarkan Teori Motivasi Perlindungan (PMT), kesadaran akan ancaman phishing dan efektivitas tindakan perlindungan meningkatkan motivasi siswa untuk melindungi diri. Penelitian ini merekomendasikan pengembangan program literasi digital yang berkelanjutan, kebijakan pengurangan penggunaan internet yang tidak perlu, serta pemblokiran akses ke situs web berbahaya. Dengan meningkatkan literasi digital, masyarakat, terutama remaja, akan lebih siap menghadapi ancaman siber dan menjaga keamanan informasi pribadi mereka.

Kata Kunci: *Phishing, Literasi Digital, Remaja*

DOI:
https://doi.org/10.57119/abdimas.v3i2.122
*Correspondensi: Andi Asyhary J. Arsyad
Email: andiasyhary001@gmail.com

Received: 30-07-2024
Accepted: 22-08-2024
Published: 26-10-2024

Abstract

Phishing attacks are among the most common and damaging cybersecurity threats, exploiting human vulnerabilities such as a lack of awareness and digital literacy. This study aims to identify effective strategies for increasing awareness of phishing attacks through digital literacy among teenagers. The research was conducted at SMK Darussalam Makassar using a descriptive quantitative method and involved 227 respondents. The findings indicate that 80% of respondents agree that digital literacy plays a significant role in reducing the impact of phishing. Digital literacy, which includes understanding technology, identifying threats, and taking protective measures, has proven effective in protecting students from phishing attacks. Based on the Protection Motivation Theory (PMT), awareness of phishing threats and the effectiveness of protective actions increase students' motivation to protect themselves. This study recommends the development of sustainable digital literacy programs, policies to reduce unnecessary internet usage, and the blocking of access to harmful websites. By improving digital literacy, the community, especially teenagers, will be better prepared to face cyber threats and safeguard their personal information.

Keywords **:** *Phishing, Digital Literacy, Teenagers*

I. PENDAHULUAN

Dalam era digital yang semakin berkembang pesat, internet telah menjadi bagian integral dari kehidupan sehari-hari. Dalam era digital yang semakin berkembang pesat, internet telah menjadi bagian integral dari kehidupan sehari-hari. Penggunaan internet yang luas telah membawa banyak manfaat, seperti

memfasilitasi komunikasi global, mempercepat akses informasi, dan meningkatkan efisiensi dalam berbagai sektor seperti pendidikan, bisnis, dan pemerintahan (Corradini & Nardelli, 2020) Namun, transformasi digital ini juga meningkatkan potensi risiko keamanan siber, termasuk serangan phishing. Phishing adalah metode penipuan yang menggunakan teknik rekayasa sosial untuk memperoleh informasi pribadi atau finansial dengan menyamar sebagai entitas yang tepercaya (Graham & Triplett, 2017)

Berdasarkan laporan kuartal pertama tahun 2023, Indonesia Anti-Phising Data Exchange (IDADX) menerima 26.675 laporan phishing, meningkat drastis dari 6.106 laporan pada kuartal keempat tahun 2022. Hal ini menunjukkan peningkatan sebesar 20.569 laporan dalam satu kuartal saja. Selain itu, industri media sosial menjadi target utama dengan 45% dari seluruh serangan phishing yang dilaporkan, diikuti oleh lembaga keuangan dengan 31%. Indonesia menempati posisi teratas sebagai negara penghosting situs phishing dengan domain.id, diikuti oleh Amerika Serikat (IDADX, 2023). Para pelaku phishing menggunakan berbagai teknik untuk menipu korban, seperti email palsu, situs web tiruan, dan pesan instan yang tampak sah (Yaseen, 2022). Meskipun teknologi keamanan terus berkembang, serangan phishing tetap berhasil karena memanfaatkan kelemahan manusia, seperti kurangnya kewaspadaan dan literasi digital (Chaudhary et al., 2015)

Phishing dapat menargetkan siapa saja, dari individu hingga organisasi besar, dan dampaknya bisa sangat merugikan (Yuliana, 2022) Oleh karena itu, meningkatkan kesadaran dan pemahaman tentang ancaman ini melalui literasi digital menjadi sangat penting. Literasi digital tidak hanya mencakup kemampuan menggunakan teknologi, tetapi juga memahami risiko dan cara melindungi diri dari ancaman siber seperti phishing (Iser & Brandtweiner, 2021a).

Literasi digital memainkan peran penting dalam melindungi individu dan organisasi dari ancaman digital (Tamrin et al., 2024). Literasi digital mencakup pemahaman tentang cara kerja teknologi, kemampuan untuk mengidentifikasi ancaman, dan pengetahuan tentang langkah-langkah perlindungan. Sayangnya, banyak individu masih memiliki tingkat literasi digital yang rendah, sehingga rentan terhadap serangan phishing.

Literasi digital mencakup berbagai keterampilan yang diperlukan untuk menggunakan teknologi digital secara efektif dan aman (Martin, 2008). Literasi digital tidak hanya melibatkan kemampuan teknis, seperti menggunakan perangkat dan aplikasi, tetapi juga mencakup pemahaman yang lebih luas tentang konteks digital, seperti memahami etika online, privasi, keamanan, dan kemampuan untuk mengevaluasi informasi yang ditemukan di internet (Arsyad et al., 2023). Komponen utama dari literasi digital meliputi akses, pemahaman, penciptaan, komunikasi, dan keamanan (Alam et al., 2020). Selain itu, literasi digital juga dapat memberdayakan masyarakat untuk menjaga diri mereka dari ancaman dunia digital, meningkatkan kemampuan deteksi dan respon terhadap ancaman siber seperti phishing (Fakhrudin & ., 2023). Secara khusus, literasi digital bagi siswa sangat penting karena mereka sering menjadi target phishing dan serangan siber lainnya. Siswa di sekolah menengah, seperti di SMK Darussalam Makassar, memerlukan keterampilan literasi digital yang kuat untuk melindungi diri dari ancaman siber yang semakin canggih.

Teori Motivasi Perlindungan (Protection Motivation Theory, PMT), yang dikembangkan oleh R. W. Rogers pada tahun 1975, digunakan untuk memahami bagaimana individu merespons ancaman dan

bagaimana mereka termotivasi untuk mengambil tindakan perlindungan. PMT terdiri dari empat komponen utama yang mempengaruhi keputusan individu untuk melindungi diri dari ancaman: kemungkinan terjadi ancaman, tingkat ancaman, dan respon terhadap ancaman (Maddux & Rogers, 1983). Dalam konteks serangan phishing, PMT dapat digunakan untuk memahami bagaimana individu menilai ancaman phishing dan apa yang memotivasi mereka untuk mengambil tindakan perlindungan, seperti meningkatkan literasi digital atau menggunakan alat keamanan siber.

Berbagai upaya telah dilakukan untuk meningkatkan literasi digital, seperti kampanye kesadaran, pelatihan, dan edukasi formal. Misalnya, program peningkatan literasi digital yang melibatkan pelatihan interaktif dan penggunaan permainan edukatif telah terbukti efektif dalam meningkatkan pemahaman tentang keamanan siber dan deteksi phishing (Yang et al., 2012). Namun, efektivitas dari strategi-strategi ini bervariasi dan masih diperlukan penelitian lebih lanjut untuk mengidentifikasi pendekatan yang paling efektif.

Penelitian ini bertujuan untuk mengisi kekosongan tersebut dengan mengevaluasi strategi-strategi yang ada dan mengusulkan langkah-langkah yang dapat meningkatkan kesadaran terhadap phishing melalui literasi digital. Dengan menggabungkan teori literasi digital dan teori motivasi perlindungan, penelitian ini akan menganalisis bagaimana literasi digital dapat meningkatkan persepsi ancaman dan efikasi coping dalam menghadapi serangan phishing. Penelitian ini akan mengevaluasi bagaimana strategi peningkatan literasi digital dapat mempengaruhi persepsi individu terhadap ancaman phishing dan memotivasi mereka untuk mengambil tindakan perlindungan yang efektif (Milne et al., 2000). Kombinasi kedua teori ini akan memberikan kerangka kerja yang komprehensif untuk memahami dan mengembangkan strategi yang efektif dalam meningkatkan kesadaran terhadap phishing melalui literasi digital, khususnya bagi siswa di SMK Darussalam Makassar.

II. METODE

Penelitian ini menggunakan metode kuantitatif deskriptif untuk mengidentifikasi dan menjelaskan tingkat literasi digital serta kesadaran terhadap serangan phishing di kalangan siswa SMK Darussalam Makassar. Metode kuantitatif deskriptif adalah metode penelitian yang bertujuan untuk menggambarkan kondisi atau fenomena yang ada berdasarkan data kuantitatif yang dikumpulkan dari populasi tertentu (Debout, 2012). Metode ini digunakan untuk menganalisis data dengan cara mendeskripsikan atau menggambarkan data yang telah terkumpul tanpa mencari hubungan atau membuat kesimpulan umum (Blasius & Thiessen, 2014).

Populasi dalam penelitian ini adalah seluruh siswa yang ada di SMK Darussalam Makassar. Sampel penelitian dipilih menggunakan metode random sampling, dengan total 227 siswa yang berpartisipasi. Penarikan sampel dilakukan secara langsung di sekolah, di mana kuesioner disebarkan kepada siswa yang ditemui. Data dikumpulkan melalui kuesioner yang dirancang khusus untuk mengukur tingkat literasi digital dan kesadaran terhadap serangan phishing. Kuesioner tersebut disebarkan dalam bentuk Google Form, yang mencakup berbagai aspek literasi digital seperti akses, pemahaman, penciptaan, komunikasi, dan keamanan (Sharma et al., 2016)

Penelitian ini juga melaksanakan wawancara pada beberapa siswa untuk menggali lebih dalam tentang pemahaman dan pengalaman mereka terkait literasi digital dan ancaman phishing. Pendekatan ini sejalan dengan praktik yang dijelaskan oleh (Bryman, 2006), di mana penelitian kuantitatif sering didukung oleh data kualitatif untuk memberikan konteks dan penjelasan lebih lanjut terhadap temuan kuantitatif. Dalam konteks ini, wawancara kualitatif digunakan untuk memperkaya data kuantitatif dengan memberikan wawasan mendalam mengenai persepsi dan pengalaman individu terkait literasi digital dan ancaman phishing. Kegiatan ini dilaksanakan dalam kerangka Literasi Digital segmen pendidikan yang diselenggarakan oleh Kementerian Komunikasi dan Informatika serta Akademi Relawan TIK Indonesia.

Adapun Tahapan Penelitian yang kami lakukan adalah sebagai berikut:

1. **Persiapan**
    - Menyusun kuesioner berdasarkan literatur yang relevan tentang literasi digital dan phishing.
    - Memastikan validitas dan reliabilitas kuesioner melalui uji coba awal.
2. **Pelaksanaan Kegiatan Literasi Digital**
    - Mengadakan kegiatan literasi digital di SMK Darussalam Makassar yang mencakup sosialisasi dan pelatihan tentang penggunaan teknologi digital secara aman.
    - Memberikan penjelasan mengenai ancaman phishing dan cara menghindarinya.
3. **Penyebaran Kuesioner**
    - Menyebarkan kuesioner dalam bentuk Google Form kepada siswa yang berpartisipasi dalam kegiatan literasi digital.
    - Mengumpulkan kuesioner yang telah diisi untuk analisis data lebih lanjut.
4. **Pengendalian Kualitas Data**
    - Memeriksa kelengkapan pengisian kuesioner oleh responden.
    - Mengisi ulang kuesioner yang tidak lengkap untuk memastikan data yang akurat dan reliabel (Hyman et al., 2019).
5. **Analisis Data**
    - Data dianalisis menggunakan statistik deskriptif untuk menggambarkan distribusi data serta mengidentifikasi pola umum terkait literasi digital dan kesadaran terhadap phishing.
    - Tipe skala pengukuran yang digunakan adalah tipe skala Likert. Jawaban responden dihubungkan dengan bentuk pernyataan atau dukungan sikap yang diungkapkan dengan kata-kata sebagai pernyataan positif .
    - Untuk mengetahui tanggapan responden berdasarkan kelompok responden, data yang diperoleh diolah dalam bentuk persentase pada tabel frekuensi distribusi dengan rumus:

$$P = f/N \times 100\ \%$$

Dimana :

P = Persentase
f = Frekuensi

N = Jumlah Responden

Untuk mengetahui skor jawaban responden terhadap masing-masing indikator dihitung dengan rumus:

$$\mathbf{S = \sum (n_i \times Sl_i)}$$

Dimana:

S = *skor*
$\boldsymbol{n_i}$ = *jumlah responden yang memberikan jawaban dengan nilai skala i*
$\boldsymbol{Sl_i}$ = *Nilai skala Likert*

Nilai skor tertinggi diperoleh dari perkalian antara nilai skala likert tertinggi dengan jumlah responden, yaitu 5 x N

Nilai skor terendah diperoleh dari perkalian antara nilai skala likert terendah dengan jumlah responden, yaitu 1 x N

Interprestasi skore dilakukan dengan rumus:

$$\mathbf{IS = S/ST \times 100\ \%}$$

Dimana :
IS = *Interprestasi Skor*
S = *Skor*
ST = *Skor tertinggi*

1135 skor terendah			5675 Skor tertinggi

Sedangkan Kriteria interprestasi nilai ptesentase jawaban yang digunakan adalah sebagai berikut:

0 % - 20 % = Tidak penting
21 % - 40 % = Kurang penting
41 % - 60 % = Cukup penting
61 % - 80 % = Penting
81 % - 100 % = Sangat Penting

Jurnal Pengabdian Literasi Digital Indonesia
E-ISSN. 2961-9440
Volume: 3, Nomor 2, Desember, **2024**, *Hal*: 60-71

III. HASIL DAN PEMBAHASAN

Hasil penelitian mengenai pentingnya literasi digital dalam menghindari phishing di kalangan siswa SMK Darussalam Makassar dapat tergambar dari data berikut:

Tabel 1. Tanggapan Responden Terkait penggunaan Internet dan Media Sosial

Pilihan Jawaban	F	%
Sangat Sering	168	74.01
Sering	41	18.06
Cukup Sering	17	7.49
Kurang Sering	1	0.44
Tidak Sering	0	0.00
	227	**100**

Sumber : Data primer, 2024

Dari data yang kami peroleh menunjukkan jika siswa SMK Darussalam dalam menggunakan internet dan media sosial dalam keseharian tergolong tinggi dengan nilai 74.01% atau 168 orang dari 227 total sampel yang kami teliti. Kemudian untuk melihat durasi penggunaan internet dan akses sosial media dalam sehari dapat kita melihat dari tabel berikut ini.

Tabel 2. Tanggapan Responden Terkait (Durasi Total)

Pilihan Jawaban	F	%
0-4 jam	8	3.52
4-8 jam	23	10.13
8-12 jam	120	52.86
12-16 jam	34	14.98
16-20 jam	27	11.89
20-24 jam	15	6.61
	227	**100**

Sumber : Data Primer, 2024

Dari tabel di atas menunjukkan bahwa siswa SMK Darussalam menggunakan internet dan media sosial dengan durasi yang cukup tinggi. 120 siswa dengan penggunaan durasi 8-12 jam sehari mencapai 52.86%, kemudian 34 orang siswa dengan penggunaan internet 12-16 jam sehari sebesar 14.96%, 27 orang siswa mengakses internet dengan durasi 16-20 jam atau 11.89%, 23 orang siswa dengan penggunaan durasi 4-8 jam atau 10.13%, kemudian 15 orang siswa atau 6.61% mengakses 20-24 jam. Dan 8 diantaranya mengakses hanya kurang lebih 4 jam dalam sehari.

Kemudian kami ingin melihat seberapa banyak mereka menemukan tautan yang mencurigakan di media sosial dari tabel berikut ini :

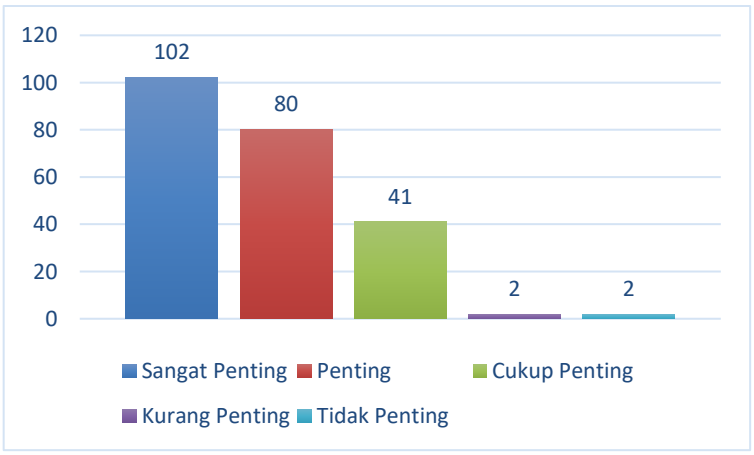
Tabel 3. Tanggapan Responden Terkait Seberapa sering Menemukan Tautan yang Mencurigakan di Media Sosial

Pilihan Jawaban	F	%
Sangat Sering	39	17.18
Sering	68	29.96
Kadang-kadang	78	34.36
Jarang	40	17.62
Tidak Pernah	2	0.88
	227	**100**

Sumber : Data Primer, 2024

Dari tabel diatas, kita bisa melihat bahwa siswa SMK Darussalam dalam mengakses internet dan media sosial sering mendapati adanya tautan-tautan yang mencurigakan hanya 40 orang atau 17.62% jarang menemukan tautan mencurigakan dan hanya 2 orang atau sekitar 0.88% tidak pernah menumukan aplikasi maupun tautan yang tergolong phishing.

Salah satu upaya untuk mencegah adanya serangan phishing yaitu dengan Literasi Digital. literasi digital juga dapat memberdayakan masyarakat untuk menjaga diri mereka dari ancaman dunia digital, meningkatkan kemampuan deteksi dan respon terhadap ancaman siber seperti phishing. Secara khusus, literasi digital bagi siswa sangat penting karena mereka sering menjadi target phishing dan serangan siber lainnya. Siswa di sekolah menengah, seperti di SMK Darussalam Makassar, memerlukan keterampilan literasi digital yang kuat untuk melindungi diri dari ancaman siber yang semakin canggih.



Gambar 1. Diagram Tanggapan responden terkait Literasi Digital dalam menghindari Phishing

Diagram di atas menunjukkan bahwa mayoritas responden, yang merupakan siswa SMK Darussalam Makassar, merasa bahwa literasi digital sangat penting dalam menghindari tindakan phishing. Dari total 227 sampel, 102 orang (44.93%) memilih sangat penting, 80 orang (35.24%) memilih penting, 41 orang (18.06%) memilih cukup penting, dan hanya 2 orang (0.88%) memilih kurang penting.

Tabel 4. Tanggapan Responden tekait Seberapa penting literasi digital untuk menghindari phishing

Pernyataan	Pilihan Jawaban	Bobot	F	f (%)	Skor (Bobot x F)
Seberapa penting Anda merasa literasi digital untuk menghindari phishing?	Sangat Penting	5	102	44.93	510
	Penting	4	80	35.24	320
	Cukup Penting	3	41	18.06	123
	Kurang Penting	2	2	0.88	4
	Tidak Penting	1	2	0.88	2
	Jumlah		227	100,00	959

Sumber: Hasil Pengolahan Data Sekunder, 2024

Dari tabel tersebut jumlah skor total jawaban responden sebesar 959, untuk nilai tertinggi diberi skor 5, dan untuk nilai terendah diberi skor 1, maka:

Nilai indeks minimum = 1 x 5 x 227 = 1135
Nilai indeks maksimum = 5 x 5 x 227 = 5675
Range = 5675 - 1135 = 4540
Jenjang range = 4540 : 5 = 908

Tabel 5. Deskripsi Interval Kategori Skor Jawaban Responden

No.	FaktorLiterasi Digital	Interval Skor	Posisi (√)
1	Sangat penting	4768 - 5675	
2	Penting	3860 - 4767	√
3	Cukup penting	2952 - 3859	
4	Kurang penting	2043 - 2951	
5	Tidak penting	1135 - 2043	

Sumber : Hasil Pengolahan Data, 2024

Dari keterangan data tersebut dapat diketahui bahwa penilaian responden terkait pentingnya literasi digital terhadap ancaman phishing itu penting. Jika di persentasikan akan mencapai angka (4540/5675) x100% = 80% , hal ini berarti bahwa menurut responden Literasi Digital memiliki peranan penting dalam mengatasi atau menghindari bahaya Phishing.

Mengacu pada hasil penelitian tersebut, teori Motivasi Perlindungan (Protection Motivation Theory, PMT) yang dikembangkan oleh R. W. Rogers pada tahun 1975 memberikan kerangka untuk memahami bagaimana individu merespons ancaman seperti phishing. PMT menyatakan bahwa keputusan individu untuk mengambil tindakan perlindungan dipengaruhi oleh persepsi mengenai kemungkinan ancaman,

tingkat ancaman, efektivitas respons, dan keyakinan pada kemampuan pribadi untuk menghadapi ancaman (Maddux & Rogers, 1983).

Dalam wawancara, siswa atas nama Irhamnah Dirmiati mengungkapkan bahwa phishing dapat menginfeksi perangkat dengan malware, ransomware, dan virus lainnya serta merusak reputasi dan kredibilitas. Pernyataan ini mencerminkan pemahaman tentang tingkat ancaman yang tinggi. Dalam kerangka PMT, semakin tinggi persepsi tentang tingkat ancaman, semakin besar motivasi individu untuk melindungi diri mereka.

Siswa atas nama Nur Salwa Mulya menambahkan, "Karena phishing dapat mengakibatkan pencurian identitas dan informasi pribadi," yang menunjukkan pemahaman tentang kemungkinan ancaman. Dalam PMT, kesadaran akan kemungkinan ancaman dapat meningkatkan motivasi untuk mengambil tindakan perlindungan.

Data survei menunjukkan bahwa siswa percaya pada efektivitas literasi digital dalam mencegah phishing. Ini mencerminkan pemahaman tentang efektivitas tindakan perlindungan, yang sejalan dengan prinsip PMT bahwa efektivitas respon yang dianggap tinggi akan meningkatkan motivasi untuk melaksanakan tindakan perlindungan.

Pernyataan dari Abdurrahman Fadhil Al Bahy selaku siswa SMK Darussalam Makassar, bahwa pelatihan literasi digital membantu melindungi akun online, serta keyakinan pada kemampuan untuk melindungi diri, menunjukkan peningkatan self-efficacy. PMT menekankan bahwa keyakinan dalam kemampuan pribadi untuk mengatasi ancaman (self-efficacy) adalah faktor penting dalam memotivasi tindakan perlindungan.

Sejalan dengan temuan dari Yaseen (2022) dan Chaudhary et al. (2015), yang menyebutkan bahwa serangan phishing terus meningkat dan memanfaatkan kelemahan manusia, serta hasil dari Iser & Brandtweiner (2021) dan Alam et al. (2020) tentang pentingnya literasi digital dalam memahami dan melindungi diri dari ancaman siber, data ini menunjukkan bahwa peningkatan literasi digital dapat meningkatkan kemampuan individu untuk mengidentifikasi dan menghindari serangan phishing, serta melindungi integritas dan keamanan pribadi mereka di dunia digital.

Hasil penelitian ini menunjukkan bahwa literasi digital berperan penting dalam mengatasi ancaman phishing, meskipun terdapat faktor eksternal yang memengaruhi penilaian responden, seperti pengaruh teman sekolah, lingkungan keluarga, atau komunitas sebaya. Faktor-faktor ini membentuk persepsi dan sikap siswa terhadap ancaman phishing serta pentingnya literasi digital. Oleh karena itu, penting bagi pembuat kebijakan, pemerintah, dan sekolah untuk merumuskan kebijakan yang lebih spesifik dalam meningkatkan literasi digital siswa. Pengembangan program literasi digital yang berkelanjutan dapat menjadi solusi untuk memastikan siswa memiliki keterampilan yang cukup dalam mengidentifikasi dan menghindari ancaman phishing di masa mendatang. Temuan ini sejalan dengan penelitian sebelumnya yang menekankan peran literasi digital dalam melawan ancaman siber, seperti yang disampaikan oleh Yaseen (2022), Chaudhary et al. (2015), dan Iser & Brandtweiner (2021), yang menunjukkan bahwa peningkatan literasi digital dapat memperkuat kemampuan individu dalam melindungi diri dari serangan siber (Iser & Brandtweiner, 2021b)

Program yang diusulkan untuk meningkatkan literasi digital dan mencegah phishing mencakup pengurangan durasi screen time bagi pelajar dengan menggantinya dengan aktivitas membaca buku. Ini membantu menyeimbangkan penggunaan teknologi dan mengurangi risiko phishing. Penelitian juga mendukung kebijakan pemerintah yang lebih ketat, seperti memblokir akses ke situs web berbahaya melalui penyedia layanan internet (ISP). Teknologi pembelajaran mesin dapat digunakan untuk mendeteksi dan mencegah akses ke situs phishing secara real-time, meningkatkan keamanan digital (Maurya & Jain, 2020) Selain itu, hukuman berat bagi pelaku phishing penting untuk mengurangi angka kejahatan siber. Penegakan hukum yang ketat akan mengurangi motivasi untuk melancarkan serangan di masa depan. Dalam hal ini, literasi digital juga berfungsi sebagai alat pencegahan dengan meningkatkan kesadaran individu tentang ancaman phishing dan cara menghindarinya (Arachchilage & Love, 2014)

IV. KESIMPULAN

Penelitian ini menunjukkan bahwa literasi digital adalah kunci untuk meningkatkan kesadaran remaja terhadap serangan phishing di SMK Darussalam Makassar. Hasil penelitian mengindikasikan bahwa hampir setengah dari siswa merasa literasi digital sangat penting dalam mengurangi risiko terkena phishing. Dengan adanya program literasi digital, siswa dapat lebih memahami dan menghindari ancaman phishing. Strategi pendidikan yang holistik, penggunaan teknologi yang tepat terbukti efektif dalam memperkuat perlindungan terhadap serangan phishing. Peningkatan literasi digital berkontribusi signifikan dalam mempersiapkan remaja menghadapi tantangan keamanan siber di era digital.

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih kepada Kementerian Komunikasi dan Informatika (Kominfo) melalui Pandu Digital Indonesia atas dukungannya dalam kegiatan literasi digital pada sektor pendidikan untuk siswa SMK Darussalam Makassar yang berjumlah 300 orang. Terima kasih juga kepada Akademi Relawan TIK Indonesia yang telah mendampingi kami dalam membuat kegiatan literasi digital yang berkualitas dan berkelanjutan. Tidak lupa kami ucapkan terima kasih kepada Universitas Pejuang Republik Indonesia yang telah memberikan ruang di luar kampus untuk melaksanakan kegiatan penelitian ini. Kegiatan ini merupakan bagian dari program Kementerian Komunikasi dan Informatika untuk meningkatkan literasi digital pada segmen pendidikan.

DAFTAR PUSTAKA

Alam, M. N., Sarma, D., Lima, F. F., Saha, I., Ulfath, R. E., & Hossain, S. (2020). Phishing attacks detection using machine learning approach. *Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020*, 1173–1179. https://doi.org/10.1109/ICSSIT48917.2020.9214225

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Arsyad, A. A. J., Tamrin, U., & S., S. A. S. (2023). Transformasi UMKM Melalui Pendampingan Keterampilan Literasi Digital. *KAREBA: Jurnal Ilmu Komunikasi*.

Blasius, J., & Thiessen, V. (2014). Assessing the Quality of Survey Data. In *Assessing the Quality of Survey Data*. SAGE Publications Ltd. https://doi.org/10.4135/9781446251874

Bryman, A. (2006). Integrating quantitative and qualitative research: How is it done? *Qualitative Research*, *6*(1), 97–113. https://doi.org/10.1177/1468794106058877

Chaudhary, S., Berki, E., Li, L., & Valtanen, J. (2015). Time up for phishing with effective anti-phishing research strategies. *International Journal of Human Capital and Information Technology Professionals*, *6*(2), 49–64. https://doi.org/10.4018/IJHCITP.2015040104

Corradini, I., & Nardelli, E. (2020). Developing Digital Awareness at School: A Fundamental Step for Cybersecurity Education. *Advances in Intelligent Systems and Computing*, *1219 AISC*, 102–110. https://doi.org/10.1007/978-3-030-52581-1_14

Debout, C. (2012). Quantitative methodology and simple descriptive studies. In *Soins* (Vol. 57, Issue 768, pp. 55–60). Elsevier Masson s.r.l. https://doi.org/10.1016/j.soin.2012.07.017

Fakhrudin, A., & . H. (2023). Digital Literacy Analysis of Primary School Students. *KnE Social Sciences*, *2022*, 13-22–13–22. https://doi.org/10.18502/kss.v8i8.13280

Graham, R., & Triplett, R. (2017). Capable Guardians in the Digital Environment: The Role of Digital Literacy in Reducing Phishing Victimization. *Deviant Behavior*, *38*(12), 1371–1382. https://doi.org/10.1080/01639625.2016.1254980

Hyman, M. R., Kostyk, A., Zhou, W., & Paas, L. (2019). Novel Approaches for Improving data Quality from Self-Administered Questionnaires. *International Journal of Market Research*, *61*(5), 552–555. https://doi.org/10.1177/1470785319870622a

IDADX. (2023). *Laporan Aktifitas Phishing Domain.ID Periode Q1 2023*. Indonesia Anti-Phishing Data Exhange

Iser, B., & Brandtweiner, R. (2021a). Role Of Awareness To Prevent Personal Disasters: Reducing The Risks Of Falling For Phishing By Strengthening User Awareness. *WIT Transactions on the Built Environment*, *207*, 79–88. https://doi.org/10.2495/DMAN210061

Iser, B., & Brandtweiner, R. (2021b). Role of Awareness To Prevent Personal Disasters: Reducing the Risks of Falling for Phishing By Strengthening User Awareness. *WIT Transactions on the Built Environment*, *207*, 79–88. https://doi.org/10.2495/DMAN210061

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Martin, A. (2008). *Digital Literacy and the Digital Society*. 151–176.

Maurya, S., & Jain, A. (2020). Deep learning to combat phishing. *Journal of Statistics and Management Systems*, *23*(6), 945–957. https://doi.org/10.1080/09720510.2020.1799496

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106–143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Sharma, R., Fantin, A. R., Prabhu, N., Guan, C., & Dattakumar, A. (2016). Digital literacy and knowledge societies: A grounded theory investigation of sustainable development. *Telecommunications Policy*, *40*(7), 628–643. https://doi.org/10.1016/j.telpol.2016.05.003

Tamrin, U., RS, A. H., Arsyad, A. A. J., Umar, N., & Kurniawan, D. (2024). Analisis Peranan Pemilih Pemula dan Pentingnya Teknologi Digital Untuk Pemilihan Umum 2024 di Indonesia (Studi Kasus: Pemilih Pemula SMA Negeri 20 Makassar). *Journal of Digital Literacy and Volunteering*, *2*(2), 52–60.

Yang, C. C., Tseng, S. S., Lee, T. J., Weng, J. F., & Chen, K. (2012). Building an anti-phishing game to enhance network security literacy learning. *Proceedings of the 12th IEEE International Conference on Advanced Learning Technologies, ICALT 2012*, 121–123. https://doi.org/10.1109/ICALT.2012.174

Yaseen, K. A. Y. (2022). Importance of Cybersecurity in The Higher Education Sector 2022. *Asian Journal of Computer Science and Technology*, *11*(2), 20–24. https://doi.org/10.51983/ajcst-2022.11.2.3448

Yuliana, Y. (2022). The Importance Of Cybersecurity Awareness For Children. *Lampung Journal of International Law*, *4*(1), 41–48. https://doi.org/10.25041/lajil.v4i1.2526