Jurnal Ilmiah Informatika Komputer, 28(3): 230-240.
Doi: https://doi.org/10.35760/ik.2023.v28i3.9514

ANALISIS BIBLIOMETRIK MENGENAI SERANGAN *PHISHING* DAN MEDIA SOSIAL MENGGUNAKAN *VOSVIEWER*

[1]Riyandini Devi Intan Permatasari, [2]Anisa Rahmah, [3]Fithrotuz Zuhroh, [4]Tsabita Rizqiina Putri Hidayat, [5]Nur Aini Rakhmawati
[1,2,3,4,5]Program Studi Sistem Informasi
[1,2,3,4,5]Institut Teknologi Sepuluh Nopember, Surabaya
[1]5026211026@mhs.its.ac.id, [2]5026211040@mhs.its.ac.id, [3]5026211045@mhs.its.ac.id,
[4]5026211124@mhs.its.ac.id, [5]nur.aini@is.its.ac.id
**) Penulis Korespondensi*

Abstrak

Kegiatan kriminal di dunia maya, seperti phishing, mengeksplotasi individu dengan trik menipu untuk mencuri data pribadi. Pada 2023, publikasi terkait phishing dan media sosial mencapai puncaknya dengan 57 publikasi (36.31%). Analisis peta perkembangan publikasi menunjukkan 3 kluster: Kluster 1 (biru) menyoroti kata kunci seperti phishing, cyber attack, dan jaringan komputer, menggambarkan keterkaitan dengan kejahatan siber dan kriminologi. Kluster 2 (hijau) mencakup kata kunci keamanan, internet, dan social engineering, menunjukkan potensi ancaman terhadap keamanan informasi yang membutuhkan perhatian khusus dalam menerapkan technology thread avoid. Kluster 3 (merah) menyoroti kata kunci media sosial, data pribadi, dan aplikasi, menekankan kerentanan privasi dan data pribadi, dengan penekanan pada edukasi dan sosialisasi sebagai langkah krusial dalam mengatasi kejahatan phishing di platform-media. Metodologi pemetaan kata kunci membantu mendeteksi pola hubungan dan memungkinkan pemantauan yang efektif terhadap potensi risiko phishing.

***Kata Kunci**: Analisis Bibliometrik, Media Sosial, Phishing*

Abstract

Criminal activities in the cyber realm, such as phishing, exploit individuals through deceptive tricks to steal personal data. In 2023, publications related to phishing and social media reached their peak with 57 publications (36.31%). The analysis reveals three clusters: Cluster 1 (blue) highlights keywords such as phishing, cyber attack, and computer networks, depicting associations with cybercrime and criminology. Cluster 2 (green) encompasses keywords like security, internet, and social engineering, indicating potential threats to information security requiring special attention. Cluster 3 (red) emphasizes social media, personal data, and applications, underscoring vulnerabilities in privacy and data. Education and socialization are crucial steps in addressing phishing on media platforms. Keyword mapping aids in detecting relationships, allowing more effective monitoring of potential phishing risks.

***Keywords**: Bibliometrics Analysis, Social Media, Phishing*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi menjadi pembawa perubahan besar bagi manusia dalam proses pertukaran informasi sehingga semua orang dapat mengakses internet dan berseluncur di Media sosial dengan mudah. Media sosial menjadi salah satu cara baru masyarakat dalam berkomunikasi [1]. Dengan hadirnya teknologi dan beberapa platform media sosial, manusia dapat melakukan komunikasi antar individu meskipun terpisah jarak dan waktu. Disamping berbagai macam manfaat dari perkembangan teknologi, terdapat kekurangan berupa ancaman yang dapat menganggu kenyamanan pengguna sebagai akibat dari penyalahgunaan pemanfaatan media sosial [2]. Penyalahgunaan pemanfaatan sosial media menimbulkan tantangan baru dengan munculnya berbagai tindak pidana berbasis siber oleh pihak-pihak yang tidak bertanggung jawab untuk menyebar pesan atau dokumen palsu yang memungkinkan terjadinya ancaman privasi [3]. Salah satu *cybercrime* yang sering terjadi di media sosial yakni serangan *phishing*. Serangan *phishing* memanfaatkan kondisi ketidakpedulian pengguna media sosial terhadap potensi risiko pencurian data dan kebocoran informasi serta kerugian finansial lainnya yang dapat merusak kepercayaan dan stabilitas di dunia maya. [4]. Oleh karena itu, penting bagi masyarakat untuk tetap waspada dan bijak selama menggunakan suatu aplikasi media sosial. Salah satunya dengan mewaspadai pesan tidak dikenal yang menyertakan link maupun dokumen palsu dapat mengakibatkan terjadinya pengambilan data secara ilegal [5].

Penggunaan analisis bibliometrik telah menjadi sangat populer dalam penelitian selama beberapa tahun terakhir [6]. Analisis bibliometrik merupakan suatu metode yang digunakan untuk menganalisis data bibliografi yang diperoleh dari berbagai sumber literatur, termasuk artikel, jurnal, dan sebagainya. Bidang studi bibliometrik dapat memberikan pemahaman tentang signifikansi dan keunggulan suatu disiplin ilmu, terkait dengan lembaga pendidikan, serta menerapkan berbagai teori. Sebagai contoh, analisis penulisan, analisis kutipan, webometrik (bibliometri berbasis web), kolaborasi penulisan (penulis bersama), obsolesensi (kondisi usang) pada dokumen, faktor dampak, dan sebagainya [7]. Kajian bibliometrik memiliki kemampuan untuk mengilustrasikan kerjasama antara penulis yang meneliti suatu topik tertentu. Dengan menggunakan pemetaan bibliometrik, akan terlihat kata kunci yang menjadi kesamaan pada setiap artikel yang ditemukan . Perangkat lunak VOSviewer merupakan salah satu alat yang digunakan dalam pengolahan data untuk menciptakan representasi visual berdasarkan fokus pemetaan dengan membangun dan menampilkan visualisasi jaringan bibliometrik [8].

Topik penelitian *phishing* pada media sosial menjadi salah satu publikasi ilmiah yang

cukup banyak ditemui. Serangan *phishing* menjadi salah satu kasus kejahatan siber yang marak terjadi di kalangan masyarakat dengan jumlah kasus di Indonesia pada kuartal dua 2023 mencapai 20.330 kasus. Laporan tersebut menunjukkan terjadinya peningkatan kasus sebesar empat kali lipat dari tahun-tahun sebelumnya [9]. Analisis tren studi kasus korban kejahatan siber dalam rentang tahun 2010-2020 menghasilkan tren naik dari tahun ke tahun yang menunjukkan bahwa bidang tersebut menarik perhatian komunitas ilmiah terhadap bidang cybercrime [10]. Namun, kajian bibliomterik terkait *phishing* dan media sosial masih belum ditemukan. Penelitian sebelumnya dengan kajian analisis bibliometrik *phishing* dan big data dilakukan oleh Mirjana, Ivan dan Tanja (2022) dengan hasil analisis *co-occurance* menghasilkan 6 kluster kata kunci yang di dalamnya menunjukkan bahwa besar paper penelitian yang dikumpulkan berfokus pada algoritma pembelajaran mesin dan deep learning serta efisiensinya [11]. Kajian bibliometrik juga dilakukan oleh Huong dan Hai (2022) dengan topik tren penelitian korban kejahatan cybercrime selama 2010-2020 yang menghasilkan kajian berupa jaringan kolaborasi internasional antara penulis, institusi, dan negara yang dinilai berdasarkan co-authors, serta jaringan kata kunci penulis dibuat melalui analisis co-occurrence [10]. Penelitian dengan analisis bibliometrik juga dilakukan oleh Nur, Mohamed, dan Mazni (2023) pada area penelitian ancaman kejahatan siber di media sosial. Penelitian tersebut berfokus dalam memberikan wawasan tentang makalah yang paling banyak dikutip dan tren publikasi secara keseluruhan dari tahun 2011 hingga 2023 dan menemukan kesenjangan penelitian yang perlu perhatian dari para peneliti [12]

Penelitian dalam bentuk analisis bibliometrik mengenai serangan *phishing* masih terbatas, mayoritas menitikberatkan pada industri khusus atau ancaman keamanan siber secara umum. Sejauh pengetahuan kami, belum ada penelitian mengenai keterkaitan antara media sosial dan *phishing* dengan menggunakan representasi visual seperti yang dilakukan oleh VOSviewer. Oleh karena itu, penelitian analisis bibliometrik mengenai serangan phising di media sosial dilakukan dengan tujuan untuk memperoleh hubungan antara *phishing* dan media sosial dengan mendeteksi titik-titik koneksi yang dihasilkan dalam jaringan pemetaan kata kunci.

METODE PENELITIAN

Penelitian ini menerapkan metode penelitian analisis bibliometrik untuk menggali informasi tentang sebaran jumlah publikasi dan kutipan dari berbagai literatur. Data yang digunakan berasal dari publikasi yang terindeks dalam Google Scholar. Proses pengumpulan sumber artikel ilmiah melibatkan pencarian dalam Google Scholar yang kemudian dianalisis melalui serangkaian langkah dalam analisis bibliometrik. Langkah-

langkah dalam penelitian mencakup tahap pencarian, tahap filterisasi, dan analisis bibliometrik. Dalam penelitian ini digunakan VOSviewer sebagai perangkat lunak pendukung dalam metode analisis bibliometrik.

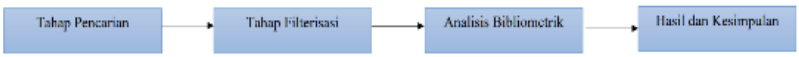
Tahap Pencarian

Pada tahap pencarian dilakukan pengumpulan artikel ilmiah yang sudah ada yang membahas terkait topik penelitan ini. Google schoolar digunakan sebagai sumber pencarian artikel ilmiah. Digunakannya Google Scholar sebagai sumber pencarian artikel ilmiah dikarenakan Google Scholar dapat diakses secara gratis dan memiliki referensi sumber artikel ilmiah yang beragam. Perangkat lunak yang digunakan dalam mendukung tahap pencarian artikel ilmiah yaitu menggunakan aplikasi Harzing's Publish or Perish. Kata kunci *"phishing,* media sosial" digunakan untuk mencari berbagai artikel ilmiah yang telah dipublikasikan sesuai dengan topik penelitian ini. Artikel ilmiah yang digunakan adalah artikel yang dipublikasikan pada tahun 2018 sampai 2023. Hasil dari pencarian dibatasi sebanyak 200. Artikel ilmiah yang sudah terkumpul dalam tahap pencarian kemudian disimpan dalam format *.ris* yang selanjutnya akan difilter kembali menggunakan aplikasi mendeley untuk melanjutkan pada tahap metode analisis bibliometrik.

Tahap Filterisasi

Tahap filterisasi merupakan proses krusial dalam memilih artikel ilmiah yang relevan untuk analisis lebih lanjut [13]. Pada tahap filterisasi digunakan aplikasi Mendeley untuk membantu melakukan seleksi artikel. Dalam tahap pencarian awal ditemukan sejumlah artikel yang memenuhi kriteria pencarian berdasarkan kata kunci "*phishing, media sosial*" yaitu sejumlah 157 artikel. Proses berikutnya melibatkan evaluasi mendalam terhadap judul dan abstrak dari setiap artikel untuk menentukan tingkat relevansinya dengan topik penelitian.

Artikel-artikel yang kurang relevan dieliminasi. Selain itu, penelusuran keyword yang mungkin tidak terbaca oleh aplikasi Mendeley juga dilakukan untuk memastikan informasi yang komprehensif dari setiap artikel terakses.Pada tahap akhir didapatkan 95 data bibliografi yang dianggap paling relevan yang siap digunakan untuk tahap analisis bibliometrik. Proses filterisasi ini merupakan langkah penting untuk memastikan bahwa data yang digunakan dalam analisis adalah data yang sangat relevan dan mewakili fokus penelitian yang sedang dilakukan.



Gambar 1. Alur Metodologi Penelitian

Tahap Analisis Bibliometrik

Pada tahap ini dilakukan analisis bibliometrik dengan menggunakan aplikasi VOSviewer yang berguna untuk memvisualisasikan peta bibliometrik. VOSviewer memiliki kemampuan *text-mining* yang memungkinkan visualisasi jaringan atau hubungan antara kutipan artikel dalam bentuk grafik [14]. Analisis bibliometrik tidak hanya bergantung pada komputerisasi dalam pengolahan data, tetapi juga memerlukan pengaturan data tertentu secara berurutan untuk memastikan hasil yang dapat diandalkan secara statistik [15]. Teknik analisis bibliometrik yang digunakan dalam penelitian ini yaitu menggunakan metode *co-occurance.* Metode ini mengukur hubungan antara dua atau lebih artikel ilmiah berdasarkan jumlah kata kunci yang sama yang muncul dalam artikel-artikel tersebut [16].

Data bibliografi yang telah terkumpul pada tahap filterisasi kemudian diimport ke VOSviewer untuk dapat dihitung jumlah kutipan yang diterima oleh setiap artikel ilmiah. Hasil perhitungan jumlah kutipan kemudian digunakan untuk menghitung nilai *co-occurance* antara dua atau lebih artikel ilmiah. Nilai *co-occurance* yang tinggi menunjukan bahwa dua atau lebih artikel ilmiah tersebut memiliki hubungan erat [17]. Hubungan ini dapat berupa hubungan antara topik penelitian, metode penelitian, atau penulis artikel ilmiah. Dalam penelitian ini digunakan parameter minimum *number of occurance* sebesar 3 yang berarti bahwa tiga atau lebih artikel ilmiah memiliki hubungan erat apabila memiliki setidaknya tiga kata kunci yang sama. Hasil analisis bibliometrik ini kemudian divisualisasikan dalam bentuk peta bibliometrik. Peta bibliometrik ini digunakan untuk mengetahui tren penelitian, topik-topik penelitian yang saling terkait [18].

HASIL DAN PEMBAHASAN

Perkembangan Publikasi

Perkembangan publikasi topik *phishing* yang diambil dari data Google Scholar dalam rentang tahun 2018 hingga 2023 dengan menggunakan pencarian kata kunci *phishing* dan media sosial menunjukkan angka sejumlah 157 artikel. Berikut data jumlah publikasi dengan topik pencarian *phishing* dan media sosial dalam rentang tahun 2018-2023 berdasarkan data yang diambil dari Google Scholar.

Berdasarkan tabel 1 diperoleh data jumlah publikasi dengan kata kunci pencarian *phishing* dan media sosial menunjukkan adanya peningkatan dari tahun ke tahun. Persentase tersebut merupakan jumlah perbandingan artikel pada tahun publikasi dengan keseluruhan jumlah artikel yang ada di Google Scholar yang memuat kata kunci *phishing* dan media sosial. Tren publikasi yang dihasilkan dalam grafik pada gambar 2 menunjukkan garis tren yang terus naik dari tahun 2018 hingga 2023. Perkembangan tertinggi terjadi pada tahun 2023 dengan jumlah publikasi sebesar 57 artikel (36.31%).

Terdapat peningkatan jumlah publikasi secara signifikan terjadi pada tahun 2022 dengan jumlah publikasi sebesar 52 artikel yang mengalami peningkatan dibandingkan dengan jumlah publikasi pada tahun sebelumnya sebanyak 18 artikel.

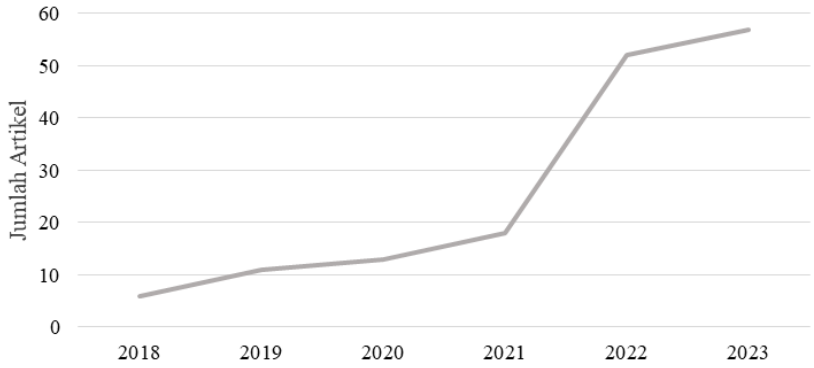
Analisis Co-Occurance

Berdasarkan analisis yang telah dilakukan mengenai kata kunci *phishing* terindeks Google Scholar tahun 2018-2023 membentuk peta sebaran dengan jumlah kluster yang dihasilkan sebanyak tiga kluster. Analisis dilakukan dengan menggunakan *co-occurance* dalam perangkat lunak VOSviewer yang menghasilkan 249 *keywords* dengan batasan jumlah minmum kemunculan kata kunci adalah 3. Dengan batasan tersebut, diperoleh 49 kata kunci yang memenuhi. Berdasarkan analisis co-occurance dari VOSviewer diperoleh hasil deteksi bahwa terdapat 35 kata kunci yang saling terkoneksi. Pemetaan dari 35 kata kunci ditampilkan dalam gambar 3 yang menunjukkan jaringan hubungan antar kata kunci dari paper yang telah dikumpulkan. Kata kunci dengan frekuensi terbesar merupakan *phishing* dan media sosial yang saling terhubung dengan satu sama lain melaui kata kunci-kata kunci lainnya.

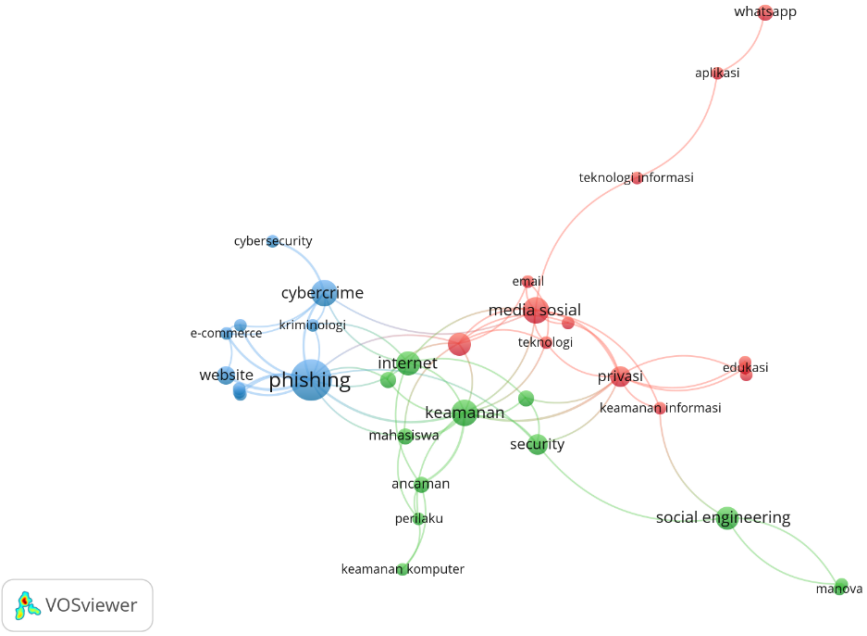
Tabel 1. Jumlah Publikasi Artikel Tahun 2018-2023

Tahun Publikasi	Jumlah Artikel	Persentase
2018	6	3.82%
2019	11	7.01%
2020	13	8.28%
2021	18	11.46%
2022	52	33.12%
2023	57	36.31%
Total	**157**	

Sumber : Hasil Perhitungan Penulis



Gambar 2. Grafik Tren Perkembangan Publikasi Artikel dalam Rentang Tahun 2018-2023



Gambar 3. Peta Perkembangan Bidang Topik *Phishing* Terindeks Google Scholar Tahun 2018-2023

Tabel 2. Kluster Kata Kunci

Klaster	Kata Kunci	Fokus Klaster
1	phishing, cyber attack, cybercrime, cyberscurity, e-commerce, jaringan komputer, kriminologi, network forensic, tindak pidana, dan website	Fokus pada aspek teknis seperti phishing, cyber attack, dan jaringan komputer dengan melibatkan topik seperti e-commerce, kriminologi, dan network forensic.
2	keamanan, internet, ancaman, information, mahasiswa, keamanan komputer, manova, perbankan, social engineering, security, technology thread avoid, dan perilaku	Berfokus pada keamanan secara umum dengan aspek seperti internet, ancaman, dan keamanan komputer.
3	media sosial, data pribadi, teknologi, aplikasi, email, teknologi informasi, whatsapp, privasi, edukasi, keamanan data, keamanan informasi, perlindungan, dan sosialisasi	Memusatkan perhatian pada media sosial dan aspek privasi dengan kata kunci seperti data pribadi, teknologi, dan aplikasi disertai cakupan topik lain seperti edukasi, keamanan data, dan perlindungan

Sumber : Hasil Analisis Penulis

Terdapat tiga kluster yang dihasilkan oleh VOSViewer untuk 35 kata kunci tersebut. Klaster diberi penanda berdasarkan fokus spesifik mereka. Representasi setiap klaster pada jaringan kata kunci dibedakan melalui warna. Ukuran node menunjukkan frekuensi kata kunci yang apabila semakin besar ukuran node maka semakin besar frekuensi kata kunci tersebut. Ketebalan garis atau lintasan jaringan ditentukan oleh kedekatan hubungan antara

dua istilah [19]. Berdasarkan gambar 3 kluster terbagi menjadi tiga warna yaitu klaster 1 berwarna biru, klaster 2 berwarna hijau, dan klaster 3 berwarna merah. Klaster yang berfokus pada keamanan secara umum seperti internet, keamanan komputer, dan social engineering menjadi penghubung antar kedua klaster lainnya. Penyajian ketiga kluster juga ditampilkan dalam tabel 2 beserta fokus kata kunci yang dimuat dalam setiap kluster.

Kluster 1 yang berwarna biru terdiri dari kata kunci *phishing*, *cyber attack*, *cybercrime*, *cyberscurity*, *e-commerce*, jaringan komputer, kriminologi, *network forensic*, tindak pidana, dan website. Kata kunci tersebut menujukkan keterkaitan kata kunci *phishing* sebagai salah satu jenis kejahatan siber. Aktivitas tersebut juga terindikasi sebagai kriminologi yang berkaitan erat dengan tidak pidana. Kluster 2 berwarna hijau terdiri dari kata kunci keamanan, internet, ancaman, information, mahasiswa, keamanan komputer, manova, perbankan, *social engineering*, security, *technology thread avoid*, dan perilaku. Kata kunci pada kluster 2 mengindikasikan potensi ancaman terhadap keamanan informasi dan komputer yang memerlukan perhatian terhadap keamanan atau *security* dalam intenet dengan menerapkan *technology thread avoid* sebagai upaya mengurangi resiko ancaman terhadap infrasturktur teknologi. Kluster 3 berwarna merah terdiri dari kata kunci media sosial, data pribadi, teknologi, aplikasi, email, teknologi informasi, *whatsapp*, privasi, edukasi, keamanan data, keamanan informasi, perlindungan, dan sosialisasi. Kata kunci tersebut berpusat pada media sosial yang berkaitan erat dengan privasi dan data pribadi yang cukup rentan. Kemunculan kata kunci aplikasi, *whatsapp,* dan email menunjukkan bahwa media tersebut menjadi tempat sasaran yang umum terjadi dalam kejahatan *phishing*. Kata kunci ini berkaitan dengan edukasi dan sosialasi yang mengindikasikan bahwa penting untuk memberikan edukasi dan sosialisasi terhadap masyarakat terkait kejahatan-kejahatan digital yang sering terjadi di sekitar mereka.

Kata kunci *phishing* dan media sosial menghasilkan garis hubungan yang menunjukkan adanya keterkaitan antar keduanya disertai keterkaitan dengan berbagai kata kunci lainnya. Berdasarkan jaringan kata kunci yang telah dihasilkan dapat mengindikasikan bahwa topik *phishing* dan media sosial berpotensi untuk dapat dikembangkan dalam berbagai bidang seperti teknologi, hukum, dan sosial. Hal ini juga mengingat terhadap tren kasus *phishing* yang cenderung mengalami kenaikan jumlah kasus setiap tahunnya dengan perkembangan jenis dan teknik yang baru.

KESIMPULAN

Analisis bibliometrik adalah suatu metode penelitian ilmiah yang bermanfaat bagi para peneliti yang ingin menjelajahi sejarah

penelitian di dalam bidang yang luas dan penuh informasi.

Pendekatan bibliometrik ini memudahkan dalam mengakses dan mengevaluasi sejumlah besar data ilmiah. Berdasarkan hasil dan pembahasan analisis Google Scholar tahun 2018-2023 terhadap kata kunci "phishing," terbentuk tiga kluster dengan 35 kata kunci terkoneksi. Kluster pertama (biru) menunjukkan fokus pada kejahatan siber seperti *phishing*, cyber attack, dan jaringan komputer, terindikasi sebagai kriminologi. Kluster kedua (hijau) menyoroti ancaman keamanan informasi dan komputer, dengan penerapan technology thread avoid sebagai upaya mengurangi risiko.

Kluster ketiga (merah) berpusat pada media sosial, menekankan privasi dan data pribadi yang rentan, terutama melalui aplikasi, WhatsApp, dan email sebagai sasaran umum dalam kejahatan *phishing*. Berdasarkan analisis bibliometrik tersebut kata kunci "phishing" pada penelitian yang telah terpublikasi memiliki hubungan yang sangat erat dengan keamanan dan media sosial. Beberapa penelitian menyoroti banyaknya kasus serangan *phishing* yang terjadi di media sosial. Karenanya, edukasi dan sosialisasi dianggap penting dalam mengatasi ancaman kejahatan digital khususnya ancaman *phishing*. Selain itu, hal ini juga menggambarkan kompleksitas dan dinamika kata kunci "phishing" serta relevansinya dalam konteks keamanan siber dan interaksi sosial. [20]

DAFTAR PUSTAKA

[1] A. Setiadi. "Pemanfaatan Media Sosial Untuk Efektifitas Komunikasi". Karawang, 2016.

[2] M. Malahayati dan D. Fata. "Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phishing". Djtechno : Journal of Information Technology Research, vol. 2, no. 1, 2021.

[3] S. K. Mohd Shuraddin dan Z. Abd Latiff. "The Consequences of the Misuse of Social Media as a Medium for News and Information". Journal of Media and Information Warfare, vol. 15, no. 1, hlm. 1–11, 2022, [Daring]. Tersedia pada: https://www.researchgate.net/publication/361877108

[4] R. Syah. "Strategi Kepolisian Dalam Pencegahan Kejahatan Phishing Melalui Media Sosial di Ruang Siber". Jurnal Impresi Indonesia, vol. 2, no. 9, Sep 2023, doi: 10.58344/jii.v2i9.3594.

[5] R. Akraman, C. Candiwan, dan Y. Priyadi. "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia". Jurnal Sistem Informasi Bisnis, vol. 8, no. 2, Okt 2018, doi: 10.21456/vol8iss2pp1-8.

[6] N. Donthu, S. Kumar, D. Pattnaik, dan W. M. Lim. "A bibliometric retrospection of marketing from the lens

of psychology: Insights from Psychology & Marketing". Psychol Mark, vol. 38, Mei 2021, doi: 10.1002/mar.21472.

[7] T. Tupan dan R. Rachmawati. "ANALISIS BIBLIOMETRIK ILMU DAN TEKNOLOGI PANGAN: PUBLIKASI ILMIAH DI NEGARA-NEGARA ASEAN". Khizanah al-Hikmah : Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan, vol. 6, no. 1, hlm. 26–40, 2018, doi: 10.24252/kah.v6a1a4.

[8] V. B. P. Perkasa, W. Erwina, dan K. Kusnandar. "Studi Bibliometrik dengan VOSviewer terhadap Publikasi Ilmiah mengenai Situs Astana Gede Kawali". Nautical: Jurnal Ilmiah Multidisiplin, vol. 1, no. 8, 2022.

[9] idadx.id. "Laporan Aktivitas Phishing Domain .ID Q2 2023". Diakses: 1 Oktober 2023. [Daring]. Tersedia pada: https://idadx.id/

[10] H. T. N. Ho dan H. T. Luong. "Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis". SN Social Sciences, vol. 2, no. 4, Jan 2022, doi: 10.1007/s43545-021-00305-4.

[11] M. Pejic-Bach, I. Jajic, dan T. Kamenjarska. "A bibliometric analysis of phishing in the big data era: High focus on algorithms and low focus on people" dalam Procedia Computer Science. Elsevier B.V., 2023, hlm. 91–98. doi: 10.1016/j.procs.2023.01.268.

[12] N. A. Zaimy, M. A. Saip, dan M. Fikri. "Cybersecurity Threat in Social Media: A Bibliometric Analysis". 2023. [Daring]. Tersedia pada: www.majmuah.com

[13] R. Riswano dan A. Rahmat. "Analisis Bibliometrik terhadap Tren Kompetensi untuk Green jobs pada Bidang Keahlian Pariwisata". Jurnal Manajemen Perhotelan dan Pariwisata, vol. 6, no. 2, 2023.

[14] U. A. Bukar, M. S. Sayeed, S. F. Abdul Razak, S. Yogarayan, O. A. Amodu, dan R. A. Raja Mahmood. "A method for analyzing text using VOSviewer". MethodsX, Des 2023, doi: 10.1016/j.mex.2023.102339.

[15] K. Khaeriyah, G. Wibisono, dan G. Pradini. "ANALISIS BIBLIOMETRIK PADA ACARA KONSER". Turn Journal, vol. 2, no. 2, hlm. 51–70, 2022.

[16] U. Sahudi, Y. M. Saputra, A. Ma'mun, N. Nuryadi, dan D. Sofyan. "Co-Authorship and Co-Occurrence Bibliometric Analysis of the Scientific Literature on Social Capital and Sports". Journal of Physical Education, Sport, Health, and Recreations, vol. 11, no. 3, hlm. 133–140, 2022, [Daring]. Tersedia pada: http://journal.unnes.ac.id/sju/index.php/peshr

[17] T. W. Widyaningsih, M. A. Dewi, dan A. Andrianingsih. "Analisis Bibliometrik untuk Memetakan Tren Penelitian Covid-19 dalam Topik Ilmu Komputer". Techno.COM, vol. 20, no. 3, hlm. 440–454, 2021, [Daring]. Tersedia pada: www.vosviewer.com.

[18] R. Andrian. "ANALISIS BIBLIOMETRIK : TREN TOPIK PENELITIAN PRODI PENDIDIKAN FISIKA DI BANDAR LAMPUNG". Maret 2022.

[19] F. N. Zakiyyah, Y. Winoto, dan R. Rohanda. "Pemetaan bibliometrik terhadap perkembangan penelitian arsitektur informasi pada Google Scholar menggunakan VOSviewer". Informatio: Journal of Library and Information Science, vol. 2, no. 1, hlm. 43, Jun 2022, doi: 10.24198/inf.v2i1.37766.

[20] R. I. P. Sari. "Analisis Bibliometrik Mengenai Serangan Phishing Pada Media Sosial Menggunakan VosViewer". Zenodo. Diakses: 1 Oktober 2023. [Daring]. Tersedia pada: https://doi.org/10.5281/zenodo.8403216