

HUBUNGAN LITERASI DIGITAL DENGAN PERILAKU KEAMANAN SIBER PADA MAHASISWA PERPUSTAKAAN DAN SAINS INFORMASI UNIVERSITAS PADJADJARAN

Wandi Oktapiyadi

Universitas Padjadjaran

Email: wandi17001@mail.unpad.ac.id

Encang Saepudin

Universitas Padjadjaran

Email: encang@unpad.ac.id

Andri Yanto

Universitas Padjadjaran

Email: andri.yanto@unpad.ac.id

Received: 02-02-2024

Revised: 15-04-2024

Accepted: 28-05-2024

DOI: 10.24036/ib.v5i2.464

Abstract

This research aims to find the relationship between digital literacy and cybersecurity behavior among Library and Information Science students in Universitas Padjadjaran. The concept of digital literacy used in this research is based on three dimensions, including technical, cognitive and social-emotional dimensions. This study used a quantitative method with correlational approach, that attempts to analyze the relationship between two or more variables and the strength of the relationship. 75 students from classes of 2020, 2021 and 2022 in the department have been selected as the target of this study with simple random sampling technique. The results of the research show that the three dimensions, namely technical, cognitive and socio-emotional dimensions, all are having a significant relationship with cybersecurity behavior. The three are also having a low level of relationship when it comes to cybersecurity behavior. Based on the results, it can be concluded that digital literacy has a significant relationship with cybersecurity behavior, despite the level of the relationship between the two are low. Which also means that a high level of digital literacy doesn't guarantee good cybersecurity behavior either.

Keywords: *Digital Literacy; Cybersecurity Behavior; Digital Safety; Digital Competency.*

Abstrak

Penelitian ini membahas mengenai hubungan literasi digital dengan perilaku keamanan siber. Konsep literasi digital yang digunakan pada penelitian ini didasarkan pada tiga dimensi, yaitu dimensi kemampuan teknis (*technical*), kognitif (*cognitive*) dan sosio-emosional (*social-emotional*). Adapun tujuan dari penelitian ini adalah mengetahui hubungan antara literasi digital dengan perilaku keamanan siber pada mahasiswa Perpustakaan dan Sains Informasi Universitas Padjadjaran. Metode yang digunakan pada penelitian ini adalah metode kuantitatif dengan pendekatan korelasional, yang mencoba untuk melihat hubungan antara dua atau lebih variabel dan kekuatan hubungannya. Penelitian ini dilakukan kepada 75 orang mahasiswa Perpustakaan dan Sains Informasi angkatan 2020, 2021 dan 2022 di Universitas Padjadjaran, yang dipilih berdasarkan teknik *simple random sampling*. Hasil penelitian menunjukkan bahwa ketiga dimensi, yakni dimensi kemampuan teknis (*technical*), kognitif (*cognitive*) dan sosio-emosional (*social-emotional*), seluruhnya memiliki hubungan yang signifikan dengan perilaku keamanan siber. Ketiganya juga sama-sama memiliki tingkat hubungan yang rendah

saat dikaitkan dengan perilaku keamanan siber. Dari hasil tersebut, literasi digital memiliki hubungan yang signifikan dengan perilaku keamanan siber, meskipun tingkat hubungan keduanya rendah. Artinya, literasi digital yang baik tidak sepenuhnya dapat menjamin perilaku keamanan siber yang baik pula.

Kata kunci: Literasi digital; Perilaku keamanan siber; Keamanan digital; Kompetensi digital.

PENDAHULUAN

Internet saat ini telah menjadi bagian yang tak terpisahkan dari kehidupan manusia. Dengan semakin masifnya perkembangan teknologi, kebiasaan masyarakat berubah dan menjadikan kita semakin bergantung pada internet untuk beragam aktivitas. Berdasarkan penelusuran DataReportal (2023), sudah ada lebih dari 5,18 miliar orang di seluruh dunia yang telah menggunakan internet dengan angka penetrasi mencapai 64,6 persen dari total populasi dunia. APJII di sisi lain juga mencatat bahwa ada sekitar 215 juta orang di Indonesia yang telah menggunakan internet per Maret 2023, menjadikan Indonesia memiliki nilai persentase mencapai 78,19 persen dari total 275,7 juta penduduk (APJII, 2023).

Tak bisa dipungkiri, keberadaan internet memberikan kemudahan bagi beragam aktivitas manusia baik itu mencari informasi, melakukan beragam transaksi, bertemu orang baru, maupun

menghubungkan kita dengan dunia melalui cara yang tidak pernah terbayangkan sebelumnya. Meski begitu, ada harga yang harus dibayar dari beragam kemudahan yang ditawarkan internet. Sebagaimana menurut The Guardian, Google sebagai salah satu situs penelusuran informasi yang paling sering digunakan, setidaknya menyimpan data para penggunaannya setiap saat, yang meliputi lokasi, riwayat hasil pencarian, email, file yang diupload, jadwal acara, bahkan hingga foto dan aplikasi serta transaksi yang pernah dilakukan saat menggunakan layanan mereka (Okezone, 2018).

Hal ini tentunya beresiko apabila sampai tersebar ke publik, terlebih dengan merebaknya beragam kasus kebocoran data yang belakangan ini semakin merebak. Tercatat pada tahun 2023, isu kebocoran data sempat menghebohkan publik karena terjadi pada beberapa lembaga pemerintahan

sekaligus. Dimulai dari kebocoran data pengguna BPJS Ketenagakerjaan pada Maret 2023 yang melibatkan Bjorka dan membocorkan sekitar 19,56 juta data pelanggan di *darkweb*, yang kemudian disusul oleh data nasabah BSI oleh kelompok Lockbit pada Mei 2023 yang membocorkan sekitar 15 juta data pribadi nasabah dengan total data mencapai 1,5TB. Tak berselang lama, Bjorka kembali menghebohkan publik karena membocorkan 34,8 juta data paspor WNI pada Juli 2023. Belum lagi data yang diklaim bocor dari situs milik KPU sebanyak 105 juta data penduduk yang sempat tersebar di bulan September 2022, ternyata kembali bocor pada November 2023, di mana Jimbo selaku peretas data tersebut mengklaim telah mendapatkan 252 juta data pemilih DPT untuk Pemilu 2024 (BeritaSatu, 2023). Pada 2022, Bjorka bahkan pernah membocorkan beberapa data personal dari para pejabat pemerintah, yang sayangnya malah mendapat dukungan dari netizen (Kompas, 2022).

Kasus kebocoran data ini tentunya memiliki dampak yang

berbahaya bagi kita para pengguna internet, terlebih dengan penggabungan data yang tersebar dari serangkaian kasus di atas, memungkinkan para penjahat untuk melakukan *phishing* dan *social engineering* yang sangat meyakinkan dengan mengaku sebagai kerabat, pihak perbankan atau instansi tertentu. Pengambilan akun sosial media, email maupun platform, atau bahkan rekening milik korban bisa saja terjadi apabila keamanan akun korban sangat lemah.

Di sinilah literasi digital memiliki peranan penting, di mana literasi digital dapat memberikan seseorang kecakapan dalam menguasai teknologi dan melakukan proses mediasi media digital yang dilakukan secara produktif. Literasi digital sendiri menurut Febliza dan Oktariani dalam Saputra & Salim (2020) adalah kecakapan hidup (*life skills*), yang tidak hanya melibatkan kemampuan dalam menggunakan perangkat teknologi, informasi dan komunikasi, namun juga kemampuan bersosialisasi, kemampuan dalam pembelajaran, dan memiliki sikap, berpikir kritis, kreatif, serta inspiratif

sebagai kompetensi digital. Konsep akan literasi digital sendiri berhubungan dengan “*new literacies*”, hanya saja literasi digital lebih berfokus pada pengembangan (*developmental*), yang mana secara progresif dibangun oleh fondasi kemampuan dan pengetahuan yang diperoleh. Sehingga secara teoritis, orang yang literat secara digital dinilai mampu untuk beradaptasi pada perubahan teknologi secara cepat dan mampu untuk memilih bahasa semiotik baru dalam berkomunikasi (Ng, 2012).

Literasi digital belakangan semakin digaungkan dan bahkan mendapat perhatian dari Kominfo, yang membuat rancangan program bernama “*Roadmap Literasi Digital 2021-2024*” yang merupakan kurikulum literasi digital dengan empat dimensi kompetensi, terdiri atas keterampilan digital (*digital skills*), budaya digital (*digital culture*), etika digital (*digital ethics*) dan keamanan digital (*digital safety*). Komponen kemampuan literasi ini sejalan dengan penelitian Tomczyk dan Eger yang menemukan bahwa area pada literasi digital akan semakin berkembang, terlebih dengan

meningkatnya serangan elektronik (*e-threats*) yang semakin kompleks, menyebabkan pengembangan konsep literasi digital akan semakin dinamis berkembang pada kemampuan dalam melindungi privasi, data serta menghindari *cyberbullying* dan adiksi terhadap internet (Tomczyk & Eger, 2020).

Mahasiswa sebagai salah satu kelompok yang kini hampir menghabiskan sebagian besar waktunya di internet, tentunya harus dapat memahami dasar-dasar dalam menjaga privasi dan keamanan dirinya saat berselancar di dunia digital. Sejalan dengan temuan survei APJII, pengguna berusia 19-34 tahun (termasuk di dalamnya kalangan mahasiswa) adalah salah satu kelompok yang paling banyak menghabiskan waktunya di internet dengan persentase mencapai 97.1% dan kontribusi 32.09% dari keseluruhan responden. Adapun salah satu penyebab lemahnya tingkat keamanan digital mahasiswa Indonesia adalah karena kebiasaan malas mengganti kata sandi secara rutin, yang dapat menyebabkan serangan *brute force* atau *dictionary*

attack mampu membobol kombinasi pola kata sandi yang mudah. Tercatat, 66.82% netizen Indonesia belum pernah mengganti kata sandi mereka (APJII, 2023). Hal ini juga diperkuat survei nasional dari Katadata Insight Center pada 2021, yang menemukan bahwa 85% generasi Z berusia 13-22 tahun, cenderung lebih pasrah terhadap pemberian izin akses aplikasi pada banyak data dan informasi pribadi (Katadata Insight Center, 2021). Hal ini menunjukkan bahwa tingkat kerentanan data pribadi pada generasi muda cukup tinggi, terlebih bagi data yang diambil saat mengakses sebuah aplikasi.

Penelitian terkait literasi digital dengan perilaku keamanan siber di kalangan mahasiswa di Indonesia sendiri masih terbilang belum banyak. Umumnya, kedua tema ini dibahas secara terpisah dan dihubungkan dengan bidang yang berbeda. Salah satu penelitian mengenai literasi digital adalah penelitian dari Pratama dkk. (2022) yang menghubungkan kemampuan literasi digital dengan pencegahan berita hoaks di kalangan

mahasiswa Fakultas Ilmu Komunikasi Universitas Padjadjaran. Penelitian lain mengenai literasi digital adalah dari Mundarsih (2022), yang hanya mengevaluasi kemampuan literasi digital dengan mengikuti framework literasi digital dari Kominfo di kalangan mahasiswa Ilmu Perpustakaan UIN Sunan Kalijaga Yogyakarta. Sementara itu, penelitian mengenai perilaku keamanan siber dilakukan oleh Wijayanto & Prabowo (2020), yang mengukur perilaku kerentanan keamanan siber di kalangan manajer dan administrator kampus, dengan temuan responden pada penelitian tersebut masih berada pada kategori rentan. Penelitian lain seputar keamanan siber dilakukan oleh Chasanah dan Candiwan (2020) yang menganalisis kesadaran keamanan siber di kalangan mahasiswa Indonesia dan menemukan bahwa mahasiswa masih memiliki kesadaran yang rendah terutama dalam manajemen *password*.

Berdasarkan temuan tersebut, maka penelitian ini bertujuan untuk mengetahui hubungan antara kemampuan literasi digital dengan

perilaku keamanan siber di kalangan mahasiswa, utamanya di kalangan mahasiswa Perpustakaan dan Sains Informasi Universitas Padjadjaran. Adapun pemilihan populasi ini sendiri dikarenakan adanya beragam fenomena kasus kebocoran data yang telah dipaparkan di atas, menjadikan literasi digital sebagai salah satu kemampuan yang wajib dimiliki oleh mahasiswa yang juga merupakan salah satu bagian dari pengguna internet. Terlebih, mahasiswa pada jurusan ini telah terpapar oleh materi maupun kegiatan mengenai literasi secara khusus. Pengukuran akan keamanan siber pada mahasiswa di jurusan ini juga penting, utamanya mengenai keamanan pribadi yang merupakan tanggung jawab setiap individu di dunia maya.

METODE

Penelitian ini menggunakan metode penelitian kuantitatif, yaitu penelitian yang digunakan untuk meneliti sebuah populasi atau sampel tertentu. Adapun teknik pengambilan sampling yang digunakan pada penelitian ini adalah teknik *simple random sampling*, di mana pengambilan

anggota sampel diambil secara acak tanpa memperhatikan strata yang ada (Sugiyono, 2015). Populasi pada penelitian ini adalah mahasiswa Perpustakaan dan Sains Informasi Universitas Padjadjaran angkatan 2020, 2021 dan 2022 dengan jumlah sebanyak 299 orang. Dengan menggunakan rumus Slovin dan peluang kesalahan 10%, maka diperoleh sampel sebanyak 75 orang untuk penelitian ini.

Instrumen yang digunakan untuk pemrolehan data primer adalah kuesioner, sementara untuk data sekunder diperoleh melalui studi pustaka. Wawancara kepada sebagian kecil responden juga dilakukan untuk memperoleh detail tambahan pada data primer. Data yang diperoleh dari kuesioner kemudian dilakukan uji validitas dan reabilitas dengan menggunakan IBM SPSS *Statistics* versi 25, yang mana akan mengukur 14 item pernyataan pada variabel literasi digital (X) dan 16 pernyataan pada variabel perilaku keamanan siber (Y). Setiap item pernyataan dihitung menggunakan teknik korelasi *pearson product moment* dan dinyatakan valid apabila koefisien

korelasinya $> 0,227$. Sementara itu, kestabilan skor atau reliabilitas setiap item diukur menggunakan rumus *Alpha Cronbach*, di mana nilai minimal koefisiennya adalah 0.6 agar bisa dinyatakan reliabel.

Berdasarkan hasil perhitungan, nilai korelasi seluruh item pada variabel literasi digital (X) $> 0,227$, sehingga dapat dinyatakan bahwa semua item adalah valid dan dapat digunakan untuk penelitian. Sementara dari 16 item pada variabel perilaku keamanan siber (Y), 1 diantaranya memiliki nilai di bawah 0,227, sehingga item pernyataan tersebut dibuang dan tidak digunakan untuk penelitian. Seluruh item pada variabel literasi digital (X) memiliki nilai *Cronbach Alpha* sebesar 0,904, sementara item pada variabel perilaku keamanan siber (Y) memiliki nilai *Cronbach Alpha* sebesar 0,717. Hal ini menggambarkan bahwa semua butir item pada variabel X dan Y reliabel dan dapat digunakan untuk analisis lebih lanjut.

Penelitian ini menggunakan dua teknik analisis data, yaitu teknik analisis data deskriptif atau pemaparan jawaban

yang diperoleh ke dalam bentuk yang lebih mudah dipahami melalui tabel yang disertai dengan penjelasan, serta teknik analisis data inferensial yang bertujuan untuk menguji hipotesis dengan menganalisis jawaban responden melalui teknik perhitungan statistik tertentu. Adapun hipotesis nol (H_0) dalam penelitian ini adalah kemampuan literasi digital tidak memiliki hubungan dengan perilaku keamanan siber pada mahasiswa Perpustakaan dan Sains Informasi Universitas Padjadjaran, sementara hipotesis alternatif (H_1) pada penelitian ini adalah kemampuan literasi digital memiliki hubungan dengan perilaku keamanan siber pada mahasiswa Perpustakaan dan Sains Informasi Universitas Padjadjaran. Mengingat data pada penelitian ini adalah data ordinal, maka analisis korelasi yang digunakan adalah uji korelasi *rank spearman*.

HASIL DAN PEMBAHASAN

Berdasarkan hasil penelitian dengan mengikuti konseptualisasi literasi digital dari Lilian (2022) yang memodifikasi model dari Ng (2012),

maka variabel literasi digital terdiri atas tiga dimensi atau sub variabel, yang terdiri atas dimensi kemampuan teknis (*technical*), dimensi kemampuan kognitif (*cognitive*) dan dimensi kemampuan sosio-emosional (*social-emotional*). Sementara itu, variabel perilaku keamanan siber mengikuti instrumen yang dibentuk oleh Egelman dan Peer (2015) bernama *Security Behaviour Intentions Scale (SeBIS)*.

Analisis korelasi dilaksanakan untuk melihat hubungan antara kemampuan literasi digital dengan perilaku keamanan siber pada mahasiswa Perpustakaan dan Sains Informasi Universitas Padjadjaran. Adapun hasil dari perhitungan setiap sub-variabel dan setiap variabel dalam penelitian ini adalah sebagai berikut:

- 1) Hubungan dimensi *technical* dengan perilaku keamanan siber

Tabel 1. Hubungan dimensi *technical* dengan perilaku keamanan siber

Hubungan	Koefisien Korelasi	α	Nilai Signifikansi	Tingkat Hubungan	Kesimpulan
Hubungan dimensi <i>technical</i> dengan perilaku keamanan siber	0,271	0,05	0,019	Rendah	Terdapat hubungan

Sumber: Data primer penelitian, 2024

Dapat diketahui bahwa dengan nilai koefisien korelasi *rank spearman* (r_s) sebesar 0,271 serta nilai signifikansi (*sig*) hubungan sebesar 0,019 yang berarti $< \alpha = 0,05$, maka dapat dikatakan bahwa terdapat hubungan yang signifikan dengan tingkat hubungan yang rendah antara dimensi kemampuan teknis (*technical*) dengan perilaku keamanan siber pada

mahasiswa Perpustakaan dan Sains Informasi Universitas Padjadjaran. Artinya, mahasiswa yang memiliki kemampuan teknis yang tinggi, tidak menjamin memiliki perilaku keamanan siber yang tinggi pula, terlebih karena tingkat hubungan keduanya termasuk rendah.

Kemampuan teknis yang tinggi memungkinkan penggunaanya untuk dapat menggunakan perangkat yang

dimiliki sebaik mungkin, terlebih dalam hal menghindari hal-hal berbahaya di dunia maya seperti terkena *scam*, *phishing* atau pun menyebarkan informasi yang salah. Di samping itu, pemahaman akan sikap keamanan pengguna dalam menggunakan perangkat dapat memprediksi kebiasaan mereka ke depannya. Kurangnya kepatuhan untuk mematuhi sebuah aturan tertentu saat menggunakan perangkat digital, akan berakibat pada praktik keamanan yang buruk. Sebagaimana temuan dari Kovačević dkk. (2020) yang

menemukan bahwa meski seseorang sering menggunakan perangkat digital dan memiliki pengetahuan yang baik mengenai perangkatnya, hal tersebut tetap dapat menyebabkan perilaku keamanan siber yang buruk. Hal ini disebabkan karena mereka merasa percaya diri dan merasa lebih *tech-savvy*, sehingga kerap kali abai akan ancaman di dunia maya. Sehingga wajar apabila kemampuan teknis memiliki hubungan yang cukup rendah dengan perilaku keamanan siber.

2) Hubungan dimensi *cognitive* dengan perilaku keamanan siber

Tabel 2. Hubungan dimensi *cognitive* dengan perilaku keamanan siber

Hubungan	Koefisien Korelasi	α	Nilai Signifikansi	Tingkat Hubungan	Kesimpulan
Hubungan dimensi <i>cognitive</i> dengan perilaku keamanan siber	0,240	0,05	0,038	Rendah	Terdapat hubungan

Sumber: Data primer penelitian, 2024

Dapat diketahui bahwa dengan nilai koefisien korelasi *rank spearman* (r_s) sebesar 0,240 serta nilai signifikansi (*sig*) hubungan sebesar 0,038 yang berarti $\alpha = 0,05$, maka dapat dikatakan bahwa terdapat hubungan yang signifikan dengan tingkat hubungan yang rendah antara dimensi

kemampuan kognitif (*cognitive*) dengan perilaku keamanan siber pada mahasiswa Perpustakaan dan Sains Informasi Universitas Padjadjaran. Artinya, mahasiswa yang memiliki kemampuan kognitif yang tinggi, tidak menjamin memiliki perilaku keamanan siber yang tinggi pula, terlebih karena

tingkat hubungan keduanya termasuk rendah.

Kemampuan kognitif yang baik dapat membantu mahasiswa untuk menghindari beberapa trik tipuan di internet yang kerap kali disebar melalui *email*, pesan singkat (*chat*) atau bahkan iklan yang muncul di sosial media. Dengan pemikiran yang kritis, mahasiswa dapat melakukan *crosscheck* terhadap informasi yang diterima dan menilai kesesuaian informasi tersebut sebelum menyalin atau membagikannya. Kemampuan ini juga dapat membantu mahasiswa untuk memilah mana informasi yang penting dan berguna baginya. Saat dikaitkan dengan perilaku keamanan siber, maka kemampuan kognitif berperan penting untuk memverifikasi kebenaran sebuah informasi dan berkaitan erat dengan kesadaran akan isyarat kontekstual, atau beberapa komponen pada *web* yang umum ditemui saat berselancar di dunia maya, seperti bagian alamat URL atau enkripsi pada sebuah *website*.

3) Hubungan dimensi *social-emotional* dengan perilaku keamanan siber

Tabel 3. Hubungan dimensi *social-emotional* dengan perilaku keamanan siber

Komponen ini dapat membantu pengguna mengenali dan menghindari potensi terkena modus penipuan *phishing*.

Berdasarkan temuan pada penelitian ini, dapat diketahui bahwa sebagian kecil dari responden masih belum dapat membedakan situs dan *link* yang mencurigakan pada beberapa pernyataan yang diberikan. Hal ini yang menyebabkan nilai uji korelasi sub-variabel ini rendah saat dihubungkan dengan perilaku keamanan siber. Hal ini sejalan dengan penelitian dari Wijayanto dan Prabowo (2020) yang juga menemukan bahwa masih terdapat indikasi kerentanan dalam kebiasaan mengunjungi situs di internet, termasuk di kalangan mahasiswa yang tercatat memiliki pemikiran yang lebih kritis dan rutin menggunakan teknologi dalam kesehariannya. Dengan demikian, wajar apabila kemampuan kognitif memiliki hubungan yang cukup rendah dengan perilaku keamanan siber.

Hubungan	Koefisien Korelasi	α	Nilai Signifikansi	Tingkat Hubungan	Kesimpulan
Hubungan dimensi <i>social-emotional</i> dengan perilaku keamanan siber	0,347	0,05	0,002	Rendah	Terdapat hubungan

Sumber: Data primer penelitian, 2024

Dapat diketahui bahwa dengan nilai koefisien korelasi *rank spearman* (r_s) sebesar 0,347 serta nilai signifikansi (sig) hubungan sebesar 0,002 yang berarti $\alpha = 0,05$, maka dapat dikatakan bahwa terdapat hubungan yang signifikan dengan tingkat hubungan yang rendah antara dimensi kemampuan sosio-emosional (*social-emotional*) dengan perilaku keamanan siber pada mahasiswa Perpustakaan dan Sains Informasi Universitas Padjadjaran. Artinya, mahasiswa yang memiliki kemampuan sosio-emosional yang tinggi, tidak menjamin memiliki perilaku keamanan siber yang tinggi pula, terlebih karena tingkat hubungan kedua variabel ini termasuk rendah.

Kemampuan sosio-emosional memungkinkan seseorang untuk dapat berinteraksi di dunia digital dengan memenuhi etika dan peraturan yang berlaku. Selain itu, mereka juga

mengetahui akan resiko serta cara untuk mengamankan diri mereka di dunia maya (Eshet & Alkalai, 2004). Kemampuan ini dapat membantu mahasiswa untuk berinteraksi dengan baik di dunia maya serta menghindari beragam serangan siber yang modusnya semakin beragam di internet. Berdasarkan temuan pada penelitian ini, dapat diketahui bahwa sebagian kecil dari responden masih memiliki kebiasaan yang buruk dalam mengamankan diri mereka di dunia maya, utamanya dalam mengamankan *password* mereka. Diketahui bahwa sebagian kecil responden masih enggan untuk merubah *password* mereka secara rutin, atau bahkan menggunakan *password* yang sama untuk beragam situs. Hal ini tentunya amat beresiko karena dapat menjadikan akun yang dimiliki mahasiswa sangat rentan terhadap serangan di dunia maya.

Temuan ini sejalan dengan penelitian Chasanah dan Candiwan (2020) yang menemukan bahwa banyak dari mahasiswa yang tidak memiliki kebiasaan mengubah *password* secara rutin, meskipun mereka sadar dan mengetahui resiko akan keamanan *password* tersebut. Begitu pula survei dari APJII yang menemukan bahwa

66,82% netizen di Indonesia hampir tidak pernah mengubah *password* mereka (APJII, 2023). Atas dasar tersebut, maka wajar apabila kemampuan sosio-emosional memiliki hubungan yang cukup rendah dengan perilaku keamanan siber.

4) Hubungan literasi digital dengan perilaku keamanan siber

Tabel 4. Hubungan literasi digital dengan perilaku keamanan siber

Hubungan	Koefisien Korelasi	α	Nilai Signifikansi	Tingkat Hubungan	Keputusan	Kesimpulan
Hubungan literasi digital dengan perilaku keamanan siber	0,295	0,05	0,010	Rendah	H1 diterima	Terdapat hubungan

Sumber: Data primer penelitian, 2024

Dapat diketahui bahwa dengan nilai koefisien korelasi *rank spearman* (r_s) adalah sebesar 0,295 serta nilai signifikansi (*sig*) hubungan sebesar 0,010 yang berarti $\alpha = 0,05$, maka H_0 ditolak dan H_1 diterima. Dengan demikian, dapat dikatakan bahwa terdapat hubungan yang signifikan antara kompetensi literasi digital dengan perilaku keamanan siber pada mahasiswa Perpustakaan dan Sains Informasi Universitas Padjadjaran. Hal

ini menunjukkan bahwa mahasiswa yang memiliki tingkat literasi digital yang baik, masih memiliki kecenderungan untuk memiliki perilaku keamanan siber yang rendah, hal ini wajar karena hubungan kedua variabel ini rendah.

Berdasarkan ketiga dimensi yang ada pada literasi digital yang terdiri atas *technical dimension*, *cognitive dimension* dan *social-emotional dimension*, seluruhnya memiliki hubungan yang

rendah namun signifikan dengan perilaku keamanan siber. Analisis hubungan setiap sub-variabel literasi digital dengan variabel perilaku keamanan siber di atas menggambarkan bahwa setiap dimensi literasi digital memiliki peran tersendiri dalam mengetahui perilaku keamanan siber mahasiswa, meskipun hubungannya terbilang rendah. Hal ini sejalan dengan penelitian dari Dodel dan Mesch (2018) yang menemukan bahwa literasi digital atau kemampuan digital berpengaruh terhadap adopsi perilaku keamanan di dunia siber, di mana dengan peningkatan kesadaran terhadap kemampuan digital dapat mempengaruhi kesenjangan digital pada keterampilan keamanan siber. Penelitian ini juga menemukan bahwa kemampuan digital dapat menjadi prediktor dari kebiasaan dalam berperilaku di dunia siber, namun terdapat faktor lain yang mempengaruhi kebiasaan ini, utamanya dalam hal perbedaan sosio-demografis, seperti pengaruh umur, pendidikan, pendapatan atau bahkan status pekerjaan dan skema stratifikasi.

Penelitian lain yang juga mendukung temuan pada penelitian ini adalah penelitian dari Kovačević dkk. (2020) yang juga menemukan bahwa meskipun penggunaan dan pengetahuan akan teknologi (dalam hal ini kompetensi digital) merupakan prediktor yang signifikan terhadap kebiasaan berperilaku di dunia siber, namun kedua faktor tadi tetap tidak menjadi penentu dalam beberapa kebiasaan, utamanya dalam hal *password*. Meskipun para responden sadar dan mengetahui bahwa data mereka kemungkinan tidak aman, namun hal tersebut tidak membuat mereka terpacu untuk belajar mengenai keamanan siber ataupun berusaha untuk bertindak secara lebih aman di dunia siber.

Temuan ini dapat menjadi gambaran bahwa mahasiswa memang tercatat telah literat dalam hal penggunaan teknologi, terlebih karena kebiasaan mereka yang kini tak bisa dipisahkan dari beragam perangkat digital. Meski demikian, mengingat literasi digital yang juga terdiri dari beragam aspek, ditemukan pula bahwa

saat dikaitkan dengan perilaku di dunia siber, mahasiswa masih memerlukan perhatian dalam hal pengetahuan maupun kesadaran mengenai keamanan siber. Intervensi dari lembaga pendidikan seperti kampus melalui pendekatan yang lebih aktif dan terstruktur seperti *workshop* atau pelatihan dapat menjadi salah satu jawaban untuk meningkatkan pengetahuan mahasiswa mengenai bidang keamanan siber, terutama mengenai perilaku yang perlu dibarengi dengan praktik. Dengan demikian, wajar apabila kemampuan literasi digital memiliki hubungan yang cukup rendah dengan perilaku keamanan siber.

PENUTUP

Simpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa terdapat hubungan yang signifikan antara kemampuan literasi digital dengan perilaku keamanan siber di kalangan mahasiswa Perpustakaan dan Sains Informasi Universitas Padjadjaran. Namun, mengingat tingkat hubungan keduanya rendah, maka kemampuan literasi digital yang baik tidak

sepenuhnya menjamin perilaku keamanan siber yang baik. Hal ini juga berlaku kepada seluruh sub-variabel pada variabel literasi digital, yang terdiri atas dimensi kemampuan teknis (*technical*), kognitif (*cognitive*) dan sosio-emosional (*social-emotional*), di mana seluruh sub-variabel juga tercatat memiliki hubungan yang signifikan dengan variabel perilaku keamanan siber. Walau demikian, karena tingkat hubungan yang rendah, ketiganya juga tidak sepenuhnya menjamin adanya perilaku keamanan siber yang tinggi di kalangan mahasiswa. Penelitian ini membuktikan bahwa mahasiswa Perpustakaan dan Sains Informasi Universitas Padjadjaran bisa dikatakan literat secara digital dengan pemahaman kemampuan teknis, kognitif dan sosio-emosional yang baik. Namun, saat dikaitkan dengan keamanan siber, masih diperlukan perhatian khusus untuk meningkatkan kesadaran mereka utamanya dalam berperilaku secara aman di dunia siber.

Saran

- 1) Tingkat *awareness* mahasiswa saat membuka *link* ataupun situs yang

mencurigakan masih terbilang cukup rentan karena berada pada kategori sedang, maka sebaiknya mahasiswa dapat mempelajari dan menambah pemahaman mereka mengenai ciri-ciri halaman yang mencurigakan agar terhindar dari metode *phishing* dan *scam*.

- 2) Mahasiswa perlu memperhatikan kebiasaan mereka dalam mengelola *password*-nya. Penggunaan aplikasi manajemen *password* dapat dipertimbangkan karena mempermudah pengelolaan *password* yang dimiliki, terlebih untuk *password* yang beragam dengan kombinasi yang rumit dan kuat, tanpa harus mengingat keseluruhannya.
- 3) Pengetahuan mahasiswa mengenai literasi digital yang sudah baik pada penelitian ini masih dapat ditambah lagi, terutama kemampuan *digital safety* atau keamanan digital yang telah menjadi salah satu bagian dari literasi digital. Pengetahuan akan keamanan digital yang baik akan sangat membantu mereka melindungi diri mereka dari

serangan siber yang bisa sangat menjebak dan berkembang setiap harinya.

DAFTAR PUSTAKA

- APJII. (2023). *Survei Penetrasi & Perilaku Internet 2023* (p. <https://survei.apjii.or.id/survei/2023>). APJII.
- BeritaSatu. (2023, November 30). *Deretan Kasus Kebocoran Data yang Pernah Terjadi di Indonesia Selama 2023*. BeritaSatu. <https://www.beritasatu.com/totekno/2784168/deretan-kasus-kebocoran-data-yang-pernah-terjadi-di-indonesia-selama-2023/>
- Chasanah, B. R., & Candiwan. (2020). Analysis of College Students' Cybersecurity Awareness In Indonesia. *SISFORMA*, 7(2), 49–57. <https://doi.org/10.24167/sisforma.v7i2.2706>
- DataReportal. (2023, April). *Digital Around the World*. DataReportal. <https://datareportal.com/global-digital-overview>
- Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society*, 21(5), 1–17. <https://doi.org/10.1080/1369118X.2018.1428652>

- Egelman, S., & Peer, E. (2015). *Scaling the Security Wall: Developing a Security Behavior Intentions Scale*. CHI 2015, Seoul. <http://dx.doi.org/10.1145/2702123.2702249>
- Eshet, Y., & Alkalai. (2004). Digital Literacy: A Conceptual Framework for Survival Skills in the Digital Era. *Journal of Educational Multimedia and Hypermedia*, 13(1), 93–106.
- Katadata Insight Center. (2021). *Persepsi Masyarakat Atas Perlindungan Data Pribadi: Survei Nasional Tahun 2021*. Ditjen Aptika Kominfo.
- Kompas. (2022, September 20). *Kilas Balik Isu Kebocoran Data: Munculnya Bjorka hingga RUU PDP Disahkan*. Kompas. <https://www.kompas.com/tren/read/2022/09/20/121000865/kilas-balik-isu-kebocoran-data--munculnya-bjorka-hingga-ruu-pdp-disahkan?page=all>
- Kovačević, A., Putnik, N., & Toskovic, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access*, 8, 125140–125148. <https://doi.org/10.1109/ACCESS.2020.3007867>
- Lilian, A. (2022). Motivational beliefs, an important contrivance in elevating digital literacy among university students. *Heliyon*, 8(12), 1–10. <https://doi.org/10.1016/j.heliyon.2022.e11913>
- Mundarsih, Y. M. (2022). *Evaluasi Kemampuan Literasi Digital di Kalangan Mahasiswa Ilmu Perpustakaan UIN Sunan Kalijaga Yogyakarta* [UIN Sunan Kalijaga]. <http://digilib.uin-suka.ac.id/id/eprint/53106>
- Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education*, 59, 1065–1078. <https://doi.org/10.1016/j.compedu.2012.04.016>
- Okezone. (2018, April 2). *Sadarkah Anda, Ini 10 Data yang "Diambil" Google dari Kita Setiap Saat*. Oketechno. <https://techno.okezone.com/read/2018/03/31/207/1880445/sadarkah-anda-ini-10-data-yang-diambil-google-dari-kita-setiap-saat>
- Pratama, F. R., Komariah, N., & Rodiah, S. (2022). Hubungan antara kemampuan literasi digital dengan pencegahan berita hoaks di kalangan mahasiswa. *Informatio*, 2(3), 165–184. <https://doi.org/10.24198/inf.v2i3.43792>
- Saputra, H. N., & Salim. (2020). Potret Sikap Mahasiswa dalam Penggunaan Literasi Digital. *Jurnal Komunikasi Pendidikan*, 4(2), 94–101. <https://doi.org/10.32585/jkp.v4i2.667>
- Sugiyono. (2015). *Metode Penelitian Pendidikan (Pendekatan*

Kuantitatif, Kualitatif, dan R&D). Alfabeta.

Tomczyk, Ł., & Eger, L. (2020). Online Safety as a New Component of Digital Literacy for Young People. *Integration of Education*, 24(2), 172–184. <https://doi.org/10.15507/1991-9468.099.024.202002.172-184>

Wijayanto, H., & Prabowo, I. A. (2020). Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal SISFOKOM (Sistem Informasi Dan Komputer)*, 9(3), 395–399. <https://doi.org/10.32736/sisfokom.v9i3.1021>