Wacana Publik
Volume 18, No. 01, Juni 2024, pp. 35–42

ISSN 1858-2400 (p)
ISSN 2656-9558 (e)

LITERASI DIGITAL KEAMANAN SIBER PADA REMAJA MENGHADAPI *SOCIAL ENGINEERING*

M. Yusuf Effendy [1] & Hestin Oktiani[2*]
[1]Program Studi Teknik Informatika, Universitas Raharja;
[2] Program Studi Ilmu Komunikasi, Universitas Lampung
*Jalan Soemantri Brodjonegoro No. 1, Gedung Meneng, Bandarlampung, Indonesia
*Korespondensi: hestin.oktiani@fisip.unila.ac.id

Recieved: 5/6/2024|Revised: 15/6/2024|Accepted: 16/6/2024

Abstract

Personal data protection and security in information transactions in the digital era are very important. The development of digital technology has given birth to various cybercrimes. Awareness of cyber security is the key to protecting yourself from social engineering related to several key security elements, namely passwords and Two-Factor Authentication (2FA). Teenagers (Gen Z) are the age group with the highest penetration on internet/cyber media, meaning that teenagers are also at greatest risk of experiencing cybercrime. Based on the results of the study, out of 100 respondents selected with the criteria of having email, social media, internet banking, and e-commerce accounts, teenagers as the largest users of internet media in general (70%) are aware of the existence of social engineering as a cybercrime, but most (54%) do not yet have knowledge about 2-factor authentication (2FA) as a way to protect personal data. Knowledge about cybercrime has not been accompanied by a high awareness to carry out good protection procedures against cybercrime, only 38%-42% of teenagers do it. In addition, the digital literacy they have is also not adequate to deal with cybercrime attacks, especially social engineering. Teenagers' digital literacy in dealing with cybercrime is still inadequate and needs to be improved. Teenagers' knowledge of 2-factor authentication (2FA) and the use of strong passwords and their awareness of the importance of taking cyber security measures are ways to deal with cybercrime attacks. More intensive training is needed on digital literacy, especially on cyber security in dealing with social engineering cybercrime.

***Kata kunci**: digital literacy, cyber security awareness, social engineering*

Abstrak

Perlindungan data pribadi dan keamanan dalam bertransaksi informasi di era digital merupakan hal sangat penting. Perkembangan teknologi digital melahir berbagai kejahatan siber. Kesadaran akan keamanan siber menjadi kunci untuk melakukan perlindungan diri menghadapi *social engineering* terkait beberapa elemen kunci keamanan, yaitu password, dan Two-Factor Authentication (2FA). Remaja (Gen Z) adalah kelompok usia yang memiliki penetrasi tertinggi pada media internet/siber, artinya remaja juga paling beresiko mengalami kejahatan siber. Berdasarkan hasil penelitian bahwa dari 100 responden yang dipilih dengan kriteria memiliki akun email, media sosial, internet banking, dan e-comerce, remaja sebagai user terbesar dari media internet secara umum (70%) mengetahui adanya keberadaan *social engineering* sebagai kejahatan siber, namun sebagian besar (54%) belum memilki pengetahuan tentang autentikasi 2 faktor (2FA) sebagai cara perlindungan data pribadi. Pengetahuan tentang kejahatan siber belum diiringi dengan kesadaran yang tinggi untuk melakukan prosedur-prosedur perlindungan yang baik menghadapi kejahatan siber, baru 38%-42% remaja yang melakukannya. Selain itu, literasi digital yang dimiliki juga belum memadai untuk menghadapi serangan kejahatan siber, terutama *social engineering.* Literasi digital remaja dalam menghadapi kejahatan siber belum memadai dan perlu ditingkatkan. Pengetahuan remaja tentang autentikasi 2 faktor (2FA) dan penggunaan kata sandi yang kuat dan kesadaran remaja akan pentingnya melakukan langkah-langkah keamanan siber adalah cara menghadapi serangan kejahatan siber. Perlu dilakukan pelatihan yang lebih intens tentang literasi digital khususnya mengenai keamanan siber menghadapi kejahatan siber *social engineering.*

Keywords: literasi digital, kesadaran keamanan siber, social engineering

PENDAHULUAN

Era digital terus berkembang, peran teknologi informasi telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari. Baik dalam transaksi perbankan, pengelolaan data pribadi, hingga akses

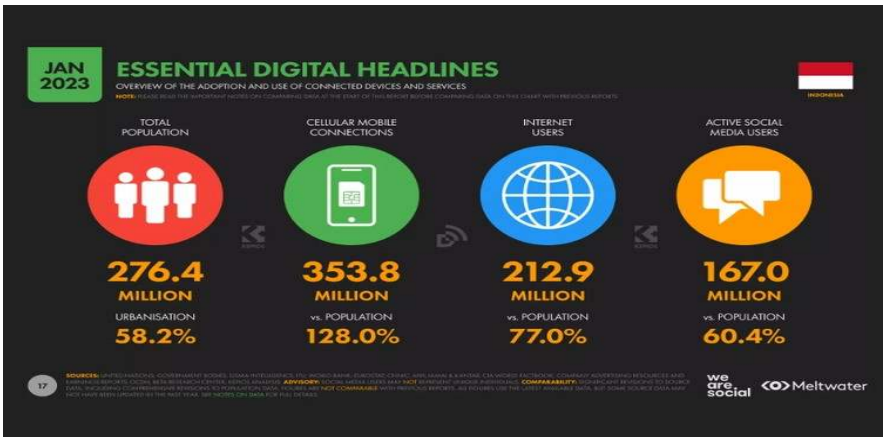
ISSN 1858-2400 (p)
ISSN 2656-9558 (e)

ke informasi sensitif lainnya, penggunaan platform digital memerlukan perlindungan yang kuat agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Keamanan informasi menjadi hal yang sangat vital dalam menyelaraskan kenyamanan pengguna dengan perlindungan terhadap risiko-risiko potensial.

Penggunaan password sebagai pertahanan pertama dalam melindungi akses ke akun dan data pribadi telah menjadi standar keamanan. Meskipun demikian, tren peretasan yang semakin canggih dan metode serangan yang terus berkembang mendorong perlunya evaluasi terhadap keamanan password. Penggunaan Two-Factor Authentication (2FA) menjadi solusi yang semakin umum untuk meningkatkan tingkat keamanan, menuntut adopsi teknologi yang lebih maju dalam melindungi identitas dan informasi sensitif. Sukariana Yasa dkk (2023) menyatakan *Information security is an asset that has value so it must be protected, along with increasing assets it is undeniable that many people wish to gain access and control it so that behind the convenience in the digital world there are many risks to information assets* (https://jutif.if.unsoed.ac.id/)

Ancaman dari *Social Engineering* dan *Phishing* di dalamnya semakin marak dalam dunia digital. Serangan yang melibatkan manipulasi psikologis dan teknik penipuan semacam ini menimbulkan risiko yang sangat besar. Literasi digital dalam keamanan siber memiliki peran strategis dalam menghadapi berbagai kejahatan dalam media siber, termasuk dalam bentuk *social engineering*. Dengan pengetahuan yang memadai dan adanya kesadaran yang tinggi akan keamanan siber, diharapkan para pengguna internet dapat melakukan upaya-upaya melindungi data pribadi dan terhindar dari berbagai bentuk kejahatan siber.

Indonesia merupakan negara yang memiliki jumlah pengguna internet yang sangat tinggi. Dikutip dari data We Are Social (2023) bahwa pengguna internet diindonesia per-Januari 2023 berjumlah212,9 juta (77,0%) dari populasi 276,4 juta jiwa.



Gambar 1. Jumlah Pengguna Internet di Indonesia
Sumber: We Are Social, 2023

Remaja adalah pengguna terbanyak media internet (34,40%), yang terus bertambah dari tahun ke tahun. Berikut data hasil riset Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2024 mengenai penetrasi internet berdasarkan usia.

ISSN 1858-2400 (p)
ISSN 2656-9558 (e)

Gambar 2. Pengguna Internet di Indonesia
Sumber: http://www.apjii.or.id, 2024

Pada UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik pada pasal 40 ayat 2 dan 3 menyatakan tentang adanya kewajiban pemerintah untuk melindungi kepentingan umum dari penyalahgunaan informasi elektronik dan mencegah penyebarluasan dan penggunaan informasi elektronik yang memiliki muatan yang dilarang oleh ketentuan undang-undang. Perlu berbagai upaya untuk membangun kesadaran keamanan siber di kalangan masyarakat, mengingat masyarakat sangat rentan terhadap berbagai kejahatan siber, mulai dari penyebaran virus, pencurian data pribadi, dan penipuan online.

Gambar 3. Kasus Kerentanan Keamanan Data
Sumber : Sumber: http://www.apjii.or.id, 2024

Dalam rangka melakukan berbagai upaya meningkatkan kesadaran keamanan siber di kalangan masyarakat, terutama remaja sebagai user terbesar internet di Indonesia, penting untuk diketahui terlebih dahulu bagaimana kondisi literasi digital remaja khususnya tentang keamanan siber. Kejahatan siber dengan menggunakan *social engineering* menyasar pengguna internet, termasuk remaja dengan berbagai jenis cara seperti *phishing* (manipulasi emosi), *baitling* (daya tarik), *pretexting* (alasan palsu), dan *scaraware (intimidasi)*. Metode social engineering bisa melibatkan komunikasi secara langsung, juga komunikasi digital seperti email, pesan teks, dan media sosial. (bakrie.ac.id, akses 2024)

METODE

Penelitian ini menggunakan pendekatan kuantitatif. Populasi dalam penelitian ini adalah remaja pengguna internet dengan kriteria memiliki akun email, akun media sosial, dan akun *e-*

ISSN 1858-2400 (p)
ISSN 2656-9558 (e)

comerce. Sampel diambil dengan memadukan teknik *puposive-random sampling* . Jumlah sampel adalah 100 orang responden remaja usia 17-26 tahun yang mengirimkan jawaban . Pengumpulan data dilakukan dengan menyebarkan kuesioner dalam bentuk *google form.*

Analisa data dilakukan dengan menggunakan analisa data kuantitatif, menggunakan tabel tunggal dan rumus presentase . Berdasarkan teknik tersebut, diketahui kecenderungan data dan keterkaitan antardata.

HASIL DAN PEMBAHASAN

Pengetahuan Remaja tentang Social Engineering dan Kunci Keamanan Akun Media

Pemahaman tentang keamanan informasi sangat penting demi menjaga data privasi dan meminimalisasi tindak kejahatan siber atau kejahatan dunia maya dan masalahkeamanan informasi lainnya (Batmetan, 2018). Keamanan password merupakan pertahanan pertama dalam melindungi data. Pendekatan terhadap password telah berkembang dari sekadar kombinasi huruf dan angka menjadi metode yang lebih kompleks dengan penggunaan karakter khusus dan panjang yang dianjurkan. Kedua, 2FA menjadi langkah lanjutan untuk memperkuat sistem keamanan. Konsep ini melibatkan penggunaan dua faktor identifikasi, seperti password dan kode yang dikirim melalui perangkat lain.

Tabel 1. Distribusi jawaban tentang aspek pengetahuan

No	Pertanyaan	Jawaban						Jumlah	
		T	%	KT	%	TT	%	Res	%
1	Apakah Anda mengetahui tentang Autentikasi Dua Faktor (2FA)?	46	46%	6	6%	48	48%	100	100%
2	Apakah Anda mengetahui tentang *phising*?	70	70%	6	6%	24	24%	100	100%
3	Apakah Anda mengenali tanda-tanda umum dari upaya *phising* atau serangan *social engineering*?	72	72%	12	12%	16	16%	100	100%
4	Apakah Anda mengetahui tentang *social engineering*?	59	59%	14	14%	27	27%	100	100%

Sumber: Hasil Pengolahan Data, 2024

Tampak pada data hasil temuan di lapangan, masih banyak remaja (48%) yang belum memiliki pengetahuan mengenai autentikasi 2 faktor (2 FA). Hal ini dapat diartikan bahwa masih banyak remaja yang rentan terkena kejahatan siber karena minimnya pengetahuan mengenai hal ini di sebagaian remaja. Hal serupa juga terjadi pada pengetahuan remaja tentang *phishing.* Meskipun sebagain besar remaja (70%) mengetahui tentang *phising*, tetapi masih terdapat 24% yang tidak tahu dan 6% yang kurang mengetahui mengenai keberadaan kejahatan siber ini. Sebuah kondisi yang cukup mengkhawatirkan juga, mengingat masih besarnya potensi korban akibat ketidaktahuan tentang *phishing.* Pengetahuan mengenai phishing tidak cukup hanya mengetahui adanya kejahatan siber ini, tetapi remaja juga harus memiliki pengetahuan tentang tanda-tanda *phishing*, sehingga remaja dapat mengenali ketika tanda-tanda tersebut ketika muncul pada saat mereka melakukan aktivitas di dunia maya. Data penelitian menunjukkan, masih terdapat 28% remaja yang tidak tahu dan kurang tahu mengenai tanda-tanda umumnya, sebuah angka yang cukup besar bagi kondisi tidak aman dalam bertransaksi informasi di internet.

Social engineering merupakan satu dari sekian banyak kejahatan siber yang marak terjadi saat ini pada berbagai bidang dengan beragam bentuk seperti penipuan, kejahatan perbankan, kejahatan dalam jual beli online. *Phishing* merupakan salah satu bentuk *social engineering*. Remaja hendaknya juga mengetahui dengan baik apa itu *social engineering* dan berbagai jenisnya. Namum berdasar data yang ditemukan, masih banyak yang belum mengetahui dan kurang mengetahui (40,9%) mengenai *social engineering.* Angka ini cukup besar dan tentu saja menyimpan bahaya yang besar pula bagi keamanan siber terutama di kalangan *user* remaja.

ISSN 1858-2400 (p)
ISSN 2656-9558 (e)

Literasi digital dalam hal keamanan siber, yang didalamnya berawal dari adanya pengetahuan dan kesadaran akan keamanan siber merupakan syarat utama bagi perlindungan data pribadi dan perlindungan dari kejahatan siber di era saat ini. Merujuk pada apa yang dikemukakan oleh Potter (2001) dalam Hestin Oktiani dkk (2019) bahwa *media literacy* dapat juga didefinisikan sebagai kemampuan dan keinginan untuk membuat kemajuan dalam memahami isi, memperhatikan dan menyaring informasi media. Selain itu juga sebagai kemampuan untuk berpikir kritis tentang pesan media dan sebuah pengetahuan untuk memahami dampak media. Pengetahuan mengenai keamanan siber yang masih rendah akan berdampak pula pada kesadaran dan kecenderungan perilaku remaja dalam menghadapi kejahatan siber.

***Kesadaran Remaja Menghadapi* Social Engineering**

Kemampuan literasi digital yang berawal dari pengetahuan yang kemudian membangun kesadaran, dan kesadaran ini akan menjadi rujukan dalam berperilaku dalam transaksi informasi di media internet. Pengetahuan mengenai keamanan siber yang masih rendah akan berdampak pada kesadaran dan kecenderungan perilaku remaja dalam menghadapi kejahatan siber. Kesadaran remaja menghadapi kejahatan siber *social engineering* memunculkan kecenderungan-kecenderungan perilaku saat remaja berinteraksi di dunia maya.

Beberapa dari mereka mungkin memiliki pengetahuan yang memadai namun tidak selalu menerapkannya dengan baik. Dengan begitu, security awareness atau kesadaran keamanan sangat perlu dimiliki oleh setiap orang untuk menghindari pelanggaran keamanan. Security Awareness adalah kontrol/aturan yang dirancang untuk mengurangi insiden pelanggaran terhadapkeamanan informasi, akibat dari kelalaian maupun tindakan yang telah direncanakan (Whitman dan Mattord, 2011). Berikut hasil temuan mengenai kecenderungan-kecenderungan tersebut.

Tabel 1. Distribusi Jawaban tentang Aspek Kesadaran Keamanan Siber

No	Pertanyaan	Jawaban					
		Y	%	K/R	%	T	%
1	Apakah Anda menggunakan kata sandi yang kuat?	74	74%	24	24%	2	2%
2	Apakah Anda menggunakan password yang sama untuk beberapa akun *online*?	44	44%	18	18%	38	38%
3	Apakah Anda menggunakan autentikasi dua faktor (2FA) jika tersedia di akun Anda?	42	42%	22	22%	36	36%
4	Apakah anda sering memeriksa riwayat login atau aktivitas akun Anda untuk memastikan keamanan?	42	42%	52	52%	6	6%
5	Apakah Anda pernah menerima panggilan atau pesan yang meminta informasi pribadi seperti kata sandi, nomor kartu kredit, atau informasi akun?	42	42%	16	16%	42	42%
6	Seberapa sering Anda menerima email atau pesan dari sumber yang tidak dikenal yang meminta informasi yang sensitif atau mengarrahkan anda untuk mengklik tautan yang mencurigakan?	30	30%	40	40%	30	30%
7	Seberapa sering Anda menggunakan tindakan pencegahan (seperti tidak mengklik tautan yang mencurigakan) ketika menerima pesan atau panggilan yang mencurigakan?	58	58%	25	25%	17	17%
8	Apakah Anda pernah mendapatkan pelatihan atau membaca informasi tentang cara mengidentifikasi atau melindungi diri dari serangan social engineering dan *phising*?	58	58%	14	14%	28	28%

Sumber: Hasil Pengolahan Data, 2024

ISSN 1858-2400 (p)
ISSN 2656-9558 (e)

Kata sandi yang kuat, sebaiknya memenuhi beberapa kriteria, termasuk panjang, kompleksitas karakter, dan penggunaan elemen khusus. Dalam sebuah aplikasi mengharuskan pengguna menggunakan password minimal 5 dan maksimal 8. Setiap password boleh menggunakan angka, simbol, dan huruf. Antara huruf besar dan huruf kecil dibedakan (Alghani dan Addin, 2019).

Pada tabel di atas 74% remaja menyatakan sudah menggunakan kata sandi yang kuat untuk akun media internetnya. Namun masih tersisa 26% yang belum menggunakan kombinasi sesuai kriteria untuk kemanan data pribadi maupun akun media nya. Selain itu masih terdapat 62% remaja yang menggunakan kata sandi yang sama untuk beberapa akun media online nya. Hal ini tentu tidak aman untuk dilakukan. Artinya kesadaran remaja mengenai kata sandi belum cukup baik. Sementara kata sandi (password) adalah perlindungan pertama bagi keamanan data pribadi.

Two-Factor Authentication (2FA) menjadi langkah lanjutan untuk memperkuat sistem keamanan. Konsep ini melibatkan penggunaan dua faktor identifikasi, seperti password dan kode yang dikirim melalui perangkat lain. Namun sayang sebagain besar remaja (56%) belum memakai model autentikasi ini. Hal ini dapat diartikan remaja masih belum menyadari pentingnya auntetikasi bagi perlindungan dari kejahatan siber.

Pemeriksaan secara berkala riwayat login atau aktivitas akun Anda untuk memastikan keamanan adalah bentuk kesadaran pengguna internet untuk meminimalisir terjadinya kejahatan siber. Namun sayangnya, masih terdapat 58% remaja yang belum secara konsisten melakukan pemeriksaan secara rutin. Hal ini akan membuka peluang yang besar untuk terjadinya kejahatan siber, karena peretasan tidak dapat segera diketahui dan tidak dapat segera dicarikan solusi agar dampaknya tidak semakin luas. Penelitian yang dilakukan oleh Hastuti (2021)bahwa keamanan tidak bisa hanya dikaitkan dengan teknologi saja, tetapijuga aspek psikologis. Apabila seseorang yang memiliki informasi vital membocorkannya tanpa sadar, seluruh jaringan keamanan dapat runtuh.

Ada beberapa titik lemah manusia yang bisa dimanfaatkan terkait kegiatan *social engineering* ini, diantaranya rasa takut. Jika seseorang dimintai data atau informasi dari pihak-pihak yang memiliki kekuasaan dan kewenangan, biasanya akan langsung memberikan. Titik lemah lainnya adalah rasa percaya. Jika seorang individu dimintai data atau informasi dari orang-orang terdekat, biasanya akan langsung memberikannya tanpa merasa curiga. Titik lemah berikutnya adalah rasa ingin menolong. Apabila seseorang dimintai data atau informasi dari orang yang sedang tertimpa musibah, dalam keadaan berduka dan sejenisnya, perasaan perihatin seringkali menjadikan yang bersangkutan tidak mempertanyakan peruntukkannya dan cenderung memberikan dalam rangka memberi pertolongan.

Kesadaran remaja sebagai pengguna internet untuk tidak langsung mengklik tautan-tautan yang dikirim melalui pesan dan tidak langsung mengangkat telephone dari nomor yang tidak dikenal, juga penting dimiliki oleh remaja. Kesadaran ini dapat menghindarkan remaja dari berbagai kejahatan siber seperti pencurian data pribadi, penyebaran virus, penipuan dan sebagainya. Namun berdasarkan data yang didapat dari 100 responden, masih terdapat 42% remaja yang belum secara konsisten menerapkan hal tersebut. Mereka yang demikian memiliki potensi untuk mengalami kejahatan siber akibat kurangnya kesadaran akan pentingnya mewaspadai isi pesan dan telephone yang mencurigakan. Shaw dalam Sulaiman (2022) menjelaskan bahwa kesadaran terhadap keamanan siber mencakup sejauh mana memahami urgensi keamanan informasi, tanggung jawab mereka, dan kemampuan untuk menerapkan kontrol keamanan informasi yang memadai guna melindungi data dan jaringan.

Data yang juga tampak pada tabel adalah 30%-42% remaja secara yakin menyadari bahwa pernah mengalami *social engineering,* dan 16% -40% masih ragu apakah pernah mengalaminya/tidak. Keraguan ini dapat saja muncul karena remaja belum memahami sepenuhnya mengenai adanya kejahatan siber *social engineering* dan seperti apa tanda-tanda dari kejahatan tersebut. S*ocial engineering* bertujuan untuk membangun kepercayaan pada korban dengan maksud mencuri data, informasi, dan dana. *Social engineering* melibatkan komunikasi yang menciptakan rasa mendesak, ketakutan, atau emosi serupa pada korban, dengan tujuan mendorong mereka untuk segera mengungkapkan informasi yang bersifat sensitif Ada beberapa indikator mengenai *social engineering*, diantaranya: permintaan informasi rahasia atau kredensial, penggunaan teknik manipulasi

ISSN 1858-2400 (p)
ISSN 2656-9558 (e)

emosional untuk mendapatkan kepercayaan, pemanfaatan email phishing atau pesan palsu, pemanfaatan informasi publik untuk menciptakan serangan yang lebih meyakinkan, dan penggunaan identitas palsu atau pura-pura menjadi pihak yang berwenang. Selain itu beberapa kemungkinan kerentanan dari sisi pengguna meliputi kecerobohan ketika memvalidasi kontendalam email, pesan SMS, kunjungan ke tautan berupa URL, mengunduh lampiran, menggunakan koneksi Wi-Fi publik saat melakukan pembayaran, penggunaan access point palsu pada jaringan yang sama, penggunaan situs webpalsu, hingga ketiadaan minimal standar peraturan untuk menginstal aplikasi dan berkas yang tidak terpercaya pada perangkat (Bosamia dan Patel, 2019).

Kesadaran keamanan siber dapat dilihat dari tiga hal, yaitu kesadaran untuk patuh pada kebijakan keamanan siber, kesadaran untuk mengikuti pelatihan secara rutin dan kesadaran melakukan perlindungan secara rutin seperti penyimpanan cadangan data, pemakaian kata sandi yang kuat (strong password) dan penggantian kata sandi secara berkala. Data pada tabel menunjukkan terdapat 58% responden remaja yang secara yakin menyatakan pernah mengikuti pelatihan keamanan siber. Masih cukup banyak remaja (42%) yang belum pernah mengikuti kegiatan tersebut dan ada juga yang mungkin tidak menyadari bahwa pelatihan yang mereka ikuti adalah pelatihan keamanan media siber. Menurut Hansche dalam Alif (2020) tujuan dari program pelatihan keamanan siber adalah untuk meningkatkan kesadaran akan pentingnya keamanan sistem informasi dan potensi dampak negatif dari pelanggaran atau kegagalan dalam keamanan tersebut. Perlu upaya yang berkesinambungan untuk menumbuhkan dan meningkatkan kesadaran keamanan siber di kalangan remaja dalam rangka mencegah terjadinya kejahatan siber yang lebih luas lagi di masa mendatang.

PENUTUP

Berdasarkan hasil temuan dan analisis terhadap data tersebut maka dapat disimpulkan bahwa remaja sebagai user terbesar dari media internet belum banyak yang memiliki literasi digital tentang keamanan siber. Selain itu, literasi digital yang dimiliki juga belum memadai untuk menghadapi serangan kejahatan siber, terutama *social engineering.* Pengetahuan remaja tentang autentikasi 2 faktor (2FA) dan pengguanaan kata sandi yang kuat, masih perlu ditingkatkan. Remaja sudah memiliki pengetahuan yang baik tentang keberadaan kejahatan siber, namun mereka belum memiliki kesadaran yang tinggi akan pentingnya melakukan prosedur-prosedur perlindungan dari kejahatan siber. Perlu dilakukan pelatihan yang lebih intens tentang literasi digital khususnya mengenai kejahatan siber *social engineering.*

DAFTAR PUSTAKA

Algani, I. Y. & Rizky,A. S. M. (2019). Penggunaan Teknik Bruteforce untuk menentukan keamanan Setiap Kata Sandi Menggunakan Metode Kombinatorial. http://journal.unnes.ac.id/sju/index.php/ujm

Alif, M. S. (2020). Analisis Kesadaran Keamanan Dalam Penggunaan E-Wallet Di Indonesia. https://journal.uii.ac.id/AUTOMATA/article/view/17279

Batmetan, J.R. (2018). Tingkat Kesadaran Privasi Atas Masalah Keamanan Informasi (Lack Of Security Awareness). DOI: 10.31219/osf.io/cahzr. https://osf.io/preprints/osf/cahzr

Bosamia, M. & D. Patel. (2019). Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures. *Int. J. Comput. Sci. Eng*, 7(1). pp. 810–817.

Annur, C. M.(2020). Kenali Maraknya Penipuan Onlien saaat Pandemi. *Katadata.co.id.* https://katadata.co.id/muhammadridhoi/analisisdata/5f7c5da0cc927/kenali-maraknya-penipuan-online-saat-pandemi#google_vignette. Diakses pada Tanggal 24 Januari 2024 Pukul 16.38 WIB

Hastuti, T., Djuyandi, Y., & Darmawan, W. B. (2021). Deteksi Dini Ancaman Social Engineering Hacker Terhadap Mata Pelajaran Rahasia Di Sekolah Staf Dan Komando Angkatan Udara. *Paradigma Polistaat: Jurnal Ilmu Sosial Dan Ilmu Politik.* https://journal.unpas.ac.id/index.php/paradigmapolistaat/article/view/4503/2145

http://www.apjii.or.id, 2024

ISSN 1858-2400 (p)
ISSN 2656-9558 (e)

https://bakrie.ac.id/articles/587-waspada-ini-4-social-engineering-attacks-yang-bisa-menyerangmu.html
https://wearesocial.com
Oktiani, H. dkk. (2019). Pelatihan Digital Parenting melalui Pemanfaatan Aplikasi Parenting Tools sebagai Upaya Pencegahan Media Addiction (Kecanduan Media) pada Anak dan Remaja (Pelatihan dan Penyuluhan pada Guru dan Orang Tua Murid di Kecamatan Rajabasa, Kota Bandar Lampung). *Prosiding Seminar Nasional Penelitian dan Pengabdian Masyarakat Universitas Muhammadiyah Metro*.
Potter, J. (2001). *Media Literacy*. USA: Sage Publications.
Sukariana Y. & Agus, I. G. dkk. (2023). Measurement of Information Security and Privacy Awareness Using the Multiple Criteria Decision Analysis (MCDA) Method. *Jurnal Teknik Informatika*. https://jutif.if.unsoed.ac.id/index.php/jurnal/article/view/692
Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information*, *13*(9), 413. https://www.mdpi.com/2078-2489/13/9/413
Whitman, M.E., and H. J. Mattord. (2011). *Principles of Information Security (Fourth Edition)*, Learning, Canada: Nelson Education pp. 269, 289.
Undang-Undang No.19 Tahun 2016 tentang Informasi dan Transaksi Elektronik.