Cyber attack

by Ery Jullev

Submission date: 21-Mar-2023 05:09AM (UTC+0700)
Submission ID: 2042071078
File name: 272-Article_Text-1362-1-10-20220806.pdf (223.77K)
Word count: 3086
Character count: 19646

Model Perilaku Keamanan Siber Pada Pengguna Sosial Media Pada Masa Pandemi Covid-19

Ameilia Nur Aini
Sekolah Tinggi Keamanan Negara
Jakarta, Indonesia
ameilianur@gmail.com

Edy Wahyudi
School of Social and Political Sciences, Jember University, Indonesia
Jember, Indonesia
edydata75@gmail.com

Imannurdin Abdillah
School of Social and Political Sciences, Jember University, Indonesia
Jember, Indonesia
imannurdin.2014@gmail.com

Ery Setiyawan Jullev A
Information Technology Department, Politeknik Negeri Jember, Indonesia
ery@polije.ac.id

***Abstract*— The use of social media is very developed during the COVID-19 pandemic, this increases the risk of data leakage, most of which are caused by internal parties from social media users themselves. For that we need an instrument that can measure the behavior of users who are at risk of social media that is used to minimize the potential for such leaks. This research consists of three stages including a literature review on aspects that affect the security of the social media system. The second stage is the preparation of a questionnaire design regarding the risk of cyber attacks on social media. Then the third stage is testing the reliability and validity of the questionnaire. Based on the research, there are 4 aspects that affect the security of social media, namely the use of electronic devices, access to social media, internet behavior, and unusual events in health facilities. The developed questionnaire consists of 27 question items which are divided into these 4 aspects. In the overall validity test the items are valid (r count > r table). While the reliability test of the questionnaire was reliable with Cronbach's Alpha value of 0.867. The developed questionnaire design can be applied to assess the risk of cyber attacks on social media among workers. Further research is needed to implement the questionnaire design.**

Keywords*— *Cyber attack, quistioner, reliability, Social media, validity

***Abstrak*—Penggunaan social media sangat berkembang pada masa pandemic covid19, hal ini meningkatkan resiko kebocoran data, kebocoran yang terbanyak disebabkan oleh pihak internal dari pengguna social media itu sendiri. Untuk itu diperlukan sebuah instrumen yang dapat mengukur perilaku pengguna yang berisiko terhadap social media yang digunakan untuk meminimalisir potensi kebocoran tersebut. Penelitian ini terdiri dari tiga tahap meliputi kajian pustaka mengenai aspek yang berpengaruh terhadap keamanan sistem social media. Tahap kedua penyusunan desain kuesioner mengenai risiko serangan siber pada social media. Kemudian tahap ketiga pengujian reliabilitas dan validitas kuesioner. Berdasarkan penelitian terdapat 4 aspek yang berpengaruh terhadap keaman social media yaitu penggunaan perangkat elektronik, akses terhadap social media, perilaku ber-internet, dan kejadian tidak wajar di fasilitas kesehatan. Kuesioner yang dikembangkan terdiri dari 27 item pertanyaan yang terbagi dalam 4 aspek tersebut. Pada uji validitas keseluruhan item valid (r hitung > r tabel). Sedangkan pada uji reliabilitas kuesioner reliabel dengan nilai *Cronbach's Alpha* sebesar 0,867. Desain kuesioner yang dikembangkan dapat diterapkan untuk menilai risiko serangan siber pada social media di kalangan pekerja. Penelitian lanjutan diperlukan untuk mengimplementasikan desain kuesioner tersebut**

Keywords*— *Cyber attack, kuisioner, reliabilitas, Social media, Validitas

PENDAHULUAN

Selama masa *social distancing* dan kontak terbatas dengan orang lain, media sosial menjadi tempat penting untuk berinteraksi. Platform media sosial dimaksudkan untuk menghubungkan orang-orang dan membantu dunia tetap terhubung, sebagian besar meningkatkan penggunaan selama pandemi. Karena banyak orang diminta untuk tetap di rumah, mereka beralih ke media sosial untuk teteap berkomunikasi serta mengakses hiburan untuk mengisi waktu.[1]

Pandemi COVID-19 telah memengaruhi penggunaan media sosial oleh populasi umum dunia, selebriti, pemimpin dunia, dan profesional. Layanan jejaring sosial telah digunakan untuk menyebarkan informasi, dan untuk menemukan humor dan gangguan dari pandemi melalui meme internet.[2][3] Namun, jarak sosial telah memaksa perubahan gaya hidup bagi banyak orang, yang membebani kesehatan mental.[1] Banyak layanan konseling online yang menggunakan media sosial diciptakan dan mulai meningkat popularitasnya, karena mereka dapat dengan aman menghubungkan petugas kesehatan mental dengan mereka yang membutuhkannya.[4]

Selain menjadi ancaman global, COVID-19 disebut sebagai infodemik. Akses langsung ke konten melalui platform seperti Twitter dan YouTube membuat pengguna rentan terhadap rumor dan informasi yang meragukan.[5] Informasi ini dapat sangat mempengaruhi perilaku individu, membatasi kohesi kelompok dan akan menjadi penghambat bagi pemerintah dalam menangani pandemic itu sendiri.[5] Selain itu platform social media juga digunakan oleh politisi, gerakan politik, dan organisasi kesehatan tingkat nasional untuk berbagi informasi dengan cepat dan menjangkau banyak orang.

Sebagai dampaknya terjadi perubahan yang belum pernah terjadi sebelumnya pada perilaku masyarakat dan difusi teknologi yang sedang berkembang menghasilkan peluang baru bagi komunitas bidang penelitian dengan mempelajari perilaku masayarakat terkait teknologi dalam krisis global. Sehingga menimbulkan satu pertanyaan mendasar yang perlu dijawab adalah seberapa banyak yang diketahui tentang pemanfaatan penggunaan teknologi digital selama pandemi Covid-19. Pada penelitian sebelumnya yang dilakukan oleh

DOI: https://doi.org/10/25047/jtit.v9i1.272

Zheng Yan dalam bukunya Mobile Phone Behavior terdapat empat elemen dasar perilaku teknologi, yaitu teknologi, pengguna, aktivitas, dan efek (Yan, 2017). Tinjauan literatur dilakukan dengan mencari dari database seperti web of science, scopus dan google scholar serta literatur tentang perilaku manusia, kemudian mensintesis literatur, menyimpulkan dari hasil temuan dan harapan untuk penelitian di masa yang akan datang.

KEAMANAN SISTEM INFORMASI

Keamanan sistem informasi penting dijaga agar sistem tersebut terhindar dari segala ancaman yang membahayakan keamanan data informasi dan keamanan pelaku sistem (ISO 27799:2008, 2008). Ancaman ini dapat berupa ancaman internal dan eksternal, yaitu berbagai jenis perilaku karyawan seperti ketidaktahuan karyawan, kecerobohan, mengambil sandi karyawan lain dan memberikan password untuk karyawan lain atau virus dan serangan spyware, hacker dan penyusup di tempat.

Hasil penelitian yang menghasilkan Policy Brief (Wijayanto, 2020) mengatakan bahwa keamanan siber dari sisi pengguna dapat dipengaruhi oleh perilaku penggunaan password, bersosial media, akses perangkat internet dan jaringan, perilaku akses data informasi serta perilaku penggunaan smartphone. Hal ini didasari kegiatan-kegiatan inilah yang sering dilakukan oleh pengguna internet.

Hasil Indeks KAMI juga menunjukkan bahwa sebagian besar pengelola keamanan siber tidak memiliki kompetensi yang cukup. Rendahnya kesadaran keamanan dan kompetensi sumber daya manusia kesehatan di bidang teknologi keamanan siber menjadikan penggunaan perangkat elektronik yang tidak aman (BSSN, 2020c). Dikutip dari CNN Money, Rabu (17/5/2017), komputer dengan software kadaluwarsa yang kebanyakan banyak sektor, menjadi alasan kuat mengapa banyak fasilitas public penting yang menjadi sasaran malware (Damar, 2017).

Aspek lain yang mempengaruhi keamanan sistem informasi kesehatan adalah akses terhadap sistem informasi kesehatan. Peraturan Pemerintah Nomor 46 Tahun 2014 Pasal 24 (1) menyatakan bahwa untuk menjaga keamanan dan kerahasiaan Informasi Kesehatan, harus ada kriteria dan batasan hak akses pengguna Informasi Kesehatan (Kementerian Kesehatan Republik Indonesia, 2014). Selain itu keamanan juga berhubungan dengan orang (personel), termasuk identifikasi, dan profil resiko dari orang yang mempunyai akses (pekerja). Kelemahan dari keamanan pada social media adalah kerawanan terhadap akjses serta share informasi hal seperti ini yaitu menyebabkan adanya teknik "social engineering" yang digunakan oleh kriminal untuk berpura-pura sebagai orang yang berhak mengakses informasi dan berpura-pura lupa passwordnya dan minta agar diganti menjadi kata lain sehingga data kesehatan dapat terakses dengan bebas (Wijayanto, Muhammad, & Hariyadi, 2020). Dalam penjaminan keamanan informasi kesehatan di fasilitas kesehatan diperlukan kesadaran seluruh tenaga kesehatan dalam berperilaku ber-internet. Perilaku ber-internet yang beresiko yang dilakukan tenaga difaskes mampu memengaruhi keamanan sistem informasi kesehatan yang ada. Dalam (Jogiyanto, 2007) menyebutkan bahwa kesalahan penerimaan informasi pada SIMRS bukan disebabkan kualitas teknik melainkan aspek keperilakuan (behavioral) sumber daya manusia. Perilaku pengabaian tata cara pengoperasian sistem informasi kesehatan juga masih sering terjadi. Survei yang dilakukan (Hadlington, 2017a) hasilnya juga menunjukkan bahwa perilaku keamanan siber yang berisiko berkorelasi negatif dengan impulsif non-perencanaan. Hal ini juga menguatkan bahwa aspek perilaku cybersecurity berisiko (RScB) dapat memperbesar peluang masalah keamanan sistem informasi. Kejadian atau kerusakan tidak wajar pada perangkat elektronik di fasilitas kesehatan juga menjadi salah satu aspek yang dapat mempengaruhi keamanan sistem informasi kesehatan. Pasalnya perangkat elektronik yang digunakan tidak selalu aman, karena tidak semua dilengkapi perangkat lunak antivirus yang mampu mencegah, mendeteksi, dan menghapus malware, termasuk virus komputer, worm komputer, Trojan horse, spyware, dan adware dll. Kurang amannya browser yang digunakan untuk mengakses website menyebabkan masuknya botnet dan malware dan mengakibatkan kebocoran data (Sendari, 2019).

METODE PENELITIAN

Dalam penelitian ini secara garis besar pengembangan kuesioner perilaku online berisiko dilakukan dalam tiga tahap. yaitu:

A. Tahap Studi Pustaka Studi pustaka dilakukan untuk mengetahui aspek yang berperan dalam risiko terjadinya serangan siber pada sistem informasi. Prosiding, jurnal, artikel ilmiah dan hasil riset Tahun 2010 - 2020 dengan kata kunci: "Cybersecurity", "Social Media Impact", dan "Cyber Risk Assessment.

B. Tahap Penyusunan Kuesioner Kuesioner disusun berdasarkan beberapa referensi antara lain Human Aspect of Information Security Questionaire (HAIS-Q), Risky Security Behavior Scale (RScB) (Hadlington, 2017 b) dan penambahan item kuesioner sesuai kondisi dan kebutuhan di Indonesia.

C. Tahap Pengujian Kuesioner Kuesioner yang telah disusun kemudian diuji reliabilitas dan validitasnya kepada 35 responden yang bekerja di beberapa fasilitas kesehatan di Indonesia. Pengujian dilakukan pada masa pandemi Covid-19 antara bulan Agustus-September 2019. Uji validitas dan reliabilitas dilakukan dengan menggunakan product moment Pearson Corelation dengan item kuesioner dikatakan valid jika r hitung lebih besar daripada r tabel. Sedangkan uji reliabilitas menggunakan uji Alpha Chroncbach instrumen dikatakan reliabel jika Alfa Chronbach lebih dari 0,6

HASIL DAN PEMBAHASAN

Kuesioner disusun berdasarkan referensi dua alat ukur mengenai perilaku beresiko terhadap sistem informasi yaitu:

1. Human Aspect of Information Security Questionaire (HAIS-Q)
2. Risky Security Behavior Scale (RScB)

Dari dua alat tersebut kemudian disusun kuesioner dan disesuaikan dengan kondisi social media di Indonesia pada umumnya. Dimana pada penelitian ini keempat aspek yaitu penggunaan perangkat elektronik, akses terhadap social media, perilaku ber-internet dan kejadian tidak wajar dikembangkan menjadi kuesioner yang terdiri dari 27 item

DOI: https://doi.org/10/25047/jtit.v9i1.272

pertanyaan yang terbagi dalam 4 aspek tersebut, ditunjukkan pada Tebel 1.

Table 1 Kuesioner Perilaku Beresiko dalam Penggunaan Sosial media

	A. Penggunaan Perangkat
1.	Saya bekerja menggunakan perangkat elektronik (laptop/ komputer/ tablet/ dsb) yang terhubung dengan jaringan di faskes.
2.	Selain perangkat elektronik dari kantor, kadang saya juga menggunakan perangkat elektronik pribadi (hp/ tablet/ laptop) di faskes.
3.	Saya pernah menggunakan perangkat elektronik kantor untuk mengakses internet diluar urusan faskes.
4.	Saya pernah mengkases internet lewat hp/ tablet/ laptop pribadi menggunakan WiFi/ akses internet faskes.
5.	Saya pernah menyimpan data dari laptop/ komputer Kerja ke USB flasdisk/hard disk eksternal milik saya.
6.	Saya pernah menyimpan data dari laptop/ komputer kerja ke penyimpanan cloud gratis. (dropbox, googledrive, dsb)
7.	Perangkat elektronik dari kantor (laptop/ komputer/ tablet, dsb) digunakan oleh lebih dari 1 pengguna.
8.	Perangkat elektronik dari kantor (laptop/ tablet/ komputer) belum terinstall antivirus.
	B. Akses Sosial Media
9.	Saya aktif menggunakan sosial media, serta aktif memberikan tanggapan terhadap postingan pelaku lain
10.	Saya bekerja menggunakan lebih dari satu sosial media ,
11.	Saya memakai password yang sederhana (nama, tanggal lahir, nomer hp, dsb) untuk mengakses sosial media tersebut.
12.	Saya pernah berbagi password tersebut dengan rekan kerja.
13.	Saya menggunakan password yang sama untuk beberapa Sosial media.
	C. Perilaku ber-internet
14.	Saya pernah membuka email lewat laptop/komputer kerja.
15.	Saya pernah meng-klik link/tautan tak dikenal dari email ketika mengakses lewat laptop/komputer kerja.
16.	Saya pernah membuka lampiran (attachment) tak dikenal dari email ketika mengakses lewat laptop/ komputer kantor.
17.	Saya pernah mengirimkan informasi penting dari kantor ke pihak yang tidak saya kenal.
18.	Saya pernah mengunduh/men-download film, lagu, software gratisan lewat komputer/ laptop kantor.
19.	Saya memiliki lebih dari 2 akun media sosial (Facebook, Youtube, dsb).
20.	Saya pernah mengakses media sosial (Facebook, Youtube, dsb) pribadi menggunakan komputer/ laptop kantor.
21.	Saya pernah mem-posting informasi penting kantor di media sosial pribadi.
22.	Saya pernah berkomunikasi lewat instant messaging (WhatsApp, Telegram, dsb) menggunakan komputer/ laptop kantor.
23.	Saya pernah berbagi informasi penting mengenai kantor melalui instant messaging (WhatsApp, Telegram, dsb) menggunakan komputer/laptop faskes.
24.	Saya pernah berbelanja online menggunakan laptop/komputer kantor.
	D. Kejadian tidak wajar
25.	Komputer/laptop kantor sering menjadi lambat /hang setelah mengakses website tertentu.
26.	Sering muncul peringatan dari antivirus di komputer/laptop kantor.
27.	Pernah muncul tampilan tertentu di layar komputer/laptop kantor sehingga tidak dapat diakses.

Kuesioner ini menggunakan skala linkert untuk mengetahui skala sikap dari responden. Dalam instrumen ini skala jawaban terdiri dari (Sangat Tidak Setuju=5, Tidak Setuju=4, Netral=3, Setuju=2 dan Sangat Setuju=1). Evaluasi kuesioner dalam penelitian ini dilakukan dengan pengujian validitas dan reliabel pada kuesioner yang dikembangkan.

Table 2 Hasil Validitas instrumen

No Item	*r hitung*	*r tabel*
X1A	.495**	0.334
X1B	.715**	0.334
X1C	.727**	0.334
X1D	.733**	0.334
X1E	.690**	0.334
X1F	.707**	0.334
X1G	.444**	0.334
X1H	.499**	0.334
X2A	.425*	0.334
X2B	.730**	0.334
X2C	.850**	0.334
X2D	.682**	0.334
X2E	.789**	0.334
X3A	.688**	0.334
X3B	.497**	0.334
X3C	.527**	0.334
X3D	.628**	0.334
X3E	.804**	0.334
X3F	.674**	0.334
X3H	.814**	0.334
X3I	.735**	0.334
X3J	.780**	0.334
X3K	.708**	0.334
X3L	.693**	0.334
X4A	.865**	0.334
X4B	.841**	0.334
X4C	.933**	0.334

Tabel 2 menunjukan hasil uji validitas pada instrumen yang dikembangkan dalam penelitian. R tabel pada *p=0,05* dengan uji 2 sisi dan *n=35*, didapat *r* tabel sebesar *0,334*. Pada uji validitas ini, keseluruhan item memiliki *r* hitung > *r* tabel. Hal tersebut bermakna bahwa masing-masing item dalam kuesioner yang dikembangkan valid.

Hasil uji reliabilitas kuesioner ini ditunjukkan pada Tabel 3 yang menunjukan nilai Alfa Chronbach = 0,867. Ini bermakna bahwa butir-butir instrument yang disusun dalam penelitian ini reliabel atau konsisten

Table 3 Cronbanch Alpha

Reliability Statistics

Cronbach's Alpha	N of Items
0.867	35

Seperti halnya pada masa pandemi *Corona Virus Disease* 2019 (*COVID-19*) saat ini. Kondisi tersebut dimanfaatkan oleh *threat actor* untuk menyebarkan malware (*virus*, *ransomware*, dan lainnya) dan spam email ke berbagai pihak. Penyebaran malware ini sangat berpotensi menyebabkan kebocoran data sensitif pasien (*COVID-19*) (BSSN, 2020b). Di Tiongkok kebocoran data *Covid-19* muncul dari data *National University of Defence Technology* yang bocor kepada 100 *Reporters* dan menyebabkan data pasien *Covid-19* di Tiongkok tersebar di *Twitter* (Sinuhaji, 2020). Di Indonesia kebocoran data juga terjadi, dimana akun atas nama *Database Shopping* mengklaim > 200.000 data pribadi pasien *Covid-19*. Data tersebut berisi data sensitif pasien *Covid-19*, yang berisi indentitas lengkap

dari pasien *Covid-19* dan akan dijual ke *RaidForums* (Mukharomah, 2020).

Penelitian lain terkait keamanan penggunaan sistem informasi kesehatan, sebagian besar meneliti hubungan antara sosial media dengan keamanan pada sistem informasi kesehatan (*organization, people, process and technology*). Dimana dalam penelitiannya meneliti perilaku sumber daya manusia secara umum (kemampuan, tanggung jawab, kepatuhan prosedur dan lainnya) dan belum menilai perilaku beresiko dalam penggunaan sosial media pada sistem informasi kesehatan. Oleh karena itu kuesioner perilaku beresiko dalam penggunaan SIK pada penelitian ini sangat penting untuk dikembangkan.

Hasil dari uji validitas dan reliabel ini juga menjadi dasar bahwa kuesioner yang dikembangkan pada penelitian ini layak untuk diimplementasikan/ diterapkan untuk menilai risiko serangan siber pada sosial media pada saat krisis covid19 merebak.

Hasil temuan dari penelitian ini adalah masih banyak ditemukan celah keamanan pada penggunaan media sosial khususnya pada saat pandemic covid-19 berlangsung, yang memperparah kondisi ini adalah masih seringnya pengguna media sosial yang kurang bijak dalam memanfaatkan media sosial tersebut, sering membuka link yang mencurigakan serta menggunakan ebanking pada jaringan public sehingga beberapa credential mereka diretas oleh pihak yang tidak bertanggung jawab.

KESIMPULAN

Desain kuesioner yang dikembangkan dapat diterapkan untuk menilai risiko serangan siber, meminimalisir kebocoran data atau pencurian yang terjadi pada sosial media khsusunya bagi pekerja kantoran saat pandemic berlangsung, desain kuesioner ini dapat digunakan untuk pengujian di tempat kerja dan menggunakan beberapa device yang diberikan kantor. Penelitian selanjutnya juga dapat memodifikasi kuesioner dari *likert scale* menjadi skoring dengan juga melakukan uji validitas dan reliabilitas. Penelitian selanjutnya perlu dilakukan studi tentang penyusunan kebijakan-kebijakan mitigasi keamanan siber serta standar operasional prosedur dalam penggunaan teknologi informasi dan komputer dilingkungan pekerjaan sehingga didapatkan model dalam menangani pencurian data pada saat pandemi.

Daftar Pustaka

[1] BSSN. (2020a). Buku Putih Keamanan Siber . Jakarta: Badan Siber dan Sandi Negara (BSSN).

[2] BSSN. (2020b). Buku Putih Mitigasi Insiden Siber Saat Pandemi Covid-19. Jakarta: Badan Siber dan Sandi Negara (BSSN).

[3] BSSN. Indeks Keamanan Informasi (KAMI). , (2020).

[4] DAMAR, A. M. (2017). Mengapa WannaCry Serang Komputer di Fasilitas Kesehatan? Retrieved September 5, 2020, from Liputan 6 website: https://www.liputan6.com/tekno/read/2955041

[5] /mengapa-wannacry-serang-komputer-di- fasilitas-kesehatan

[6] HADLINGTON, L. (2017a). Cybercognition: Brain, behaviour and the digital world. New York: SAGE.

[7] HADLINGTON, L. (2017b). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes

[8] towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

[9] HOOTSUITE, W. A. S. (2020). Digital 2020.

[10] Indonesia. Retrieved from https://datareportal.com/reports/digital-2020- indonesia

[11] INDOTELKO. (2019). Serangan siber target layanan kesehatan di Indonesia. Retrieved September 2, 2020, from IndoTelko website: https://www.indotelko.com/read/1568065603/ serangan-keseshatan

[12] ISO 27799:2008. Health informatics — Information security management in health using ISO/IEC 27002. , (2008).

[13] JOGIYANTO. (2007). Model Kesuksesan Sistem Teknologi Informasi. Yogyakarta: Andi Publisher.

[14] KAMALIAH, A. (2020). Data Pribadi Marak Dijual di Dark Web, Kalau Kena Bagaimana?

[15] KEMENTERIAN KESEHATAN REPUBLIK

[16] INDONESIA. Peraturan Pemerintah Republik Indonesia. Nomor 46 Tahun 2014. Tentang. Sistem Informasi Kesehatan. , (2014).

[17] KEMENTERIAN KESEHATAN REPUBLIK

[18] INDONESIA. Peraturan Menteri Kesehatan No 97 Tahun 2015. , (2015).

[19] MUKHAROMAH, V. F. (2020). Data Pasien Covid-

[20] 19 Diduga Bocor, Mengapa Hal Ini Bisa Terjadi? Retrieved September 5, 2020, from Kompas website:

[21] https://www.kompas.com/tren/read/2020/06/2 0/180500065/data-pasien-covid-19-diduga- bocor-mengapa-hal-ini-bisa-terjadi?page=all

[22] SAMUEL, R. (2018). Serangan Masif Cyber Attack Global. Retrieved September 2, 2020, from KOMITE.ID website:

[23] https://www.komite.id/2018/06/26/serangan- masif-cyber-attack-global/

[24] SENDARI, A. A. (2019). 12 Jenis Virus Komputer yang Perlu Diwaspadai, Bisa Rusak komputer.

[25] SINUHAJI, J. (2020). Data Bocor, Kasus COVID-19

[26] di Tiongkok Disebut 8 Kali Lebih Banyak dari yang Dilaporkan. Retrieved September 5, 2020, from Pikiran Rakyat website: https://www.pikiran- rakyat.com/internasional/pr-01383375/data-bocor-kasus-covid-19-di-tiongkok-disebut-8- kali-lebih-banyak-dari-yang-dilaporkan

[27] WIDUP, S. (2019). 2019 Verizon Data Breach Investigations Report. United State.

[28] WIJAYANTO, H. (2020). Policy Brief : Kesiapan Perguruan Tinggi Wilayah Jawa Tengah Dalam Menghadapi Serangan Siber. Indonesia: Lembaga Penelitian dan Pengabdian pada Masyarakat Universitas Dian Nuswantoro.

[29] WIJAYANTO, H., MUHAMMAD, A. H., & HARIYADI, D. (2020). Analisis

[30] Penyalahgunaan Data Pribadi Dalam Aplikasi Fintech Ilegal Dengan Metode Hibrid. Jurnal Ilmiah SINUS, 18(1), 1–10.

[31] https://doi.org/10.30646/sinus.v18i1.433

DOI: https://doi.org/10/25047/jtit.v9i1.272

Cyber attack

ORIGINALITY REPORT

19%	16%	6%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Muria Kudus Student Paper	3%
2	Submitted to Universitas Islam Indonesia Student Paper	3%
3	media.neliti.com Internet Source	2%
4	johanzoe.wordpress.com Internet Source	1%
5	www.slideshare.net Internet Source	1%
6	Patriadi, Himawan Bayu, Mohd. Zaini Abu Bakar, and Zahri Hamat. "Human Security in Local Wisdom Perspective: Pesantren and its Responsibility to Protect People", Procedia Environmental Sciences, 2015. Publication	1%
7	id.m.wikipedia.org Internet Source	1%
8	slideplayer.info Internet Source	

		1 %
9	Celintara Anindya Ayu Wardhani, Sarah Kristina, Priyo Hari Adi. "Pengaruh Penerapan E-filing terhadap Kepatuhan Pelaporan Wajib Pajak dengan Media Sosial sebagai Variabel Moderasi", Permana : Jurnal Perpajakan, Manajemen, dan Akuntansi, 2020 Publication	1 %
10	Rizal M. R. Sompotan, Silvya L. Mandey, Ivonne S. Saerang. "Pengaruh Kualitas Informasi, Kualitas Sistem Dan Regulasi Pemerintah Terhadap Implementasi E-Procurement Pada Kantor Dinas Pekerjaan Umum Kota Bitung", Aksara: Jurnal Ilmu Pendidikan Nonformal, 2021 Publication	1 %
11	Submitted to Binus University International Student Paper	1 %
12	eprints.stta.ac.id Internet Source	1 %
13	core.ac.uk Internet Source	<1 %
14	D P S Setyohadi, H Y Riskiawan, S Kautsar, P Destarianto. "Development of Low Cost Toxic Gas Explosive Modeling System using Wireless Array Sensor Netwok", IOP	<1 %

	Conference Series: Earth and Environmental Science, 2018 Publication	
15	eprints.ums.ac.id Internet Source	<1 %
16	id.scribd.com Internet Source	<1 %
17	www.jogloabang.com Internet Source	<1 %
18	www.kompas.com Internet Source	<1 %
19	Jeyhun Hajiyev, Basil John Thomas. "The Direct and Indirect Effects of Personality on Data Breach in Education Through the Task-Related Compulsive Technology use: M-Learning Perspective", International Journal of Computing and Digital Systems, 2020 Publication	<1 %
20	docplayer.org Internet Source	<1 %
21	ejournal.unsrat.ac.id Internet Source	<1 %
22	es.scribd.com Internet Source	<1 %
23	jurnal.untad.ac.id Internet Source	<1 %

24	repository.unmuhjember.ac.id Internet Source	<1%
25	daten-quadrat.de Internet Source	<1%
26	oa.upm.es Internet Source	<1%
27	doku.pub Internet Source	<1%

Exclude quotes	On	Exclude matches	< 3 words
Exclude bibliography	On		

Cyber attack

GRADEMARK REPORT

FINAL GRADE

/30

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4