PENDAMPINGAN MASYARAKAT UNTUK MENINGKATKAN KESADARAN DAN PENGETAHUAN SIBER PEKERJA MIGRAN INDONESIA DI HONG KONG

Imam Riadi[1], Iman Sumarlan[2], Ika Maryani[3]
[1]Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan, Jalan Ring Road Selatan Tamanan, Yogyakarta
[2]Ilmu Komunikasi, Fakultas Sastra, Budaya, dan Komunikasi, Universitas Ahmad Dahlan, Jalan Ring Road Selatan Tamanan, Yogyakarta
, [1]Pendidikan Guru Sekolah Dasar, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Ahmad Dahlan, Jalan Ring Road Selatan Tamanan, Yogyakarta
[1]Alamat e-mail: imam.riadi@is.uad.ac.id

Abstrak

Program ini bertujuan untuk meningkatkan kesadaran dan pengetahuan keamanan siber anggota PCIA Hong Kong dan pekerja migran Indonesia. Program dilaksanakan secara daring melalui zoom meeting dan luring melalui pendampingan langsung. Sebanyak 20 peserta terlibat dalam pendampingan. Pretes-postes dilakukan untuk mengukur kesadaran dan pengetahuan keamanan digital sebelum dan setelah pendampingan. Sebelum program dimulai, data awal menunjukkan bahwa hanya sekitar 21,34% dari PMI yang memiliki pemahaman tentang konsep keamanan siber, sementara hanya 35,71% yang menyadari risiko cybercrime. Selain itu, adanya fakta bahwa sebagian besar dari mereka (lebih dari 78%) belum menggunakan autentikasi 2 faktor pada akun media sosial mereka menunjukkan kelemahan dalam perlindungan data pribadi. Setelah pelaksanaan program, terdapat perubahan yang signifikan dalam pemahaman dan praktik keamanan siber di antara peserta. 96,43% PMI memiliki pemahaman yang lebih baik tentang risiko cybercrime, 53,57% mengadopsi autentikasi 2 faktor pada akun media sosial. Lebih dari 32,14% telah mengatur pengaturan privasi pada akun media sosial.

Kata Kunci: keamanan siber, pendampingan, kesadaran, pengetahuan.

Abstract

This program aims to increase the cyber security awareness and knowledge of PCIA Hong Kong members and Indonesian migrant workers. The program was implemented boldly through Zoom meetings and offline through direct assistance. A total of 20 participants were involved in mentoring. A pre- and post-test was conducted to measure digital security awareness and knowledge before and after mentoring. Before the program started, preliminary data showed that only around 21.34% of PMI had an understanding of cyber security concepts, while only 35.71% were aware of the risks of cybercrime. In addition, the fact that the majority of them (more than 78%) have not used 2-factor authentication on their social media accounts indicates weaknesses in personal data protection. After the implementation of the program, there was a significant change in cybersecurity understanding and practice among participants. 96.43% of PMIs have a better understanding of cybercrime risks, and 53.57% adopt 2-factor authentication on social media accounts. More than 32.14% have set privacy settings on social media accounts.

Keywords: *cyber security, support, awareness, knowledge.*

PENDAHULUAN

Gerakan Literasi Nasional yang dicanangkan oleh pemerintah dalam hal ini adalah Kemendikbud di tahun 2017 perlu mendapat dukungan dari berbagai pihak. Pemerintah menetapkan enam literasi dasar yang perlu dimiliki oleh setiap warga yaitu literasi baca-tulis-hitung, literasi sains, literasi budaya dan literasi kewargaan, literasi keuangan, dan literasi teknologi dan

komunikasi (Sinar, 2022). Enam literasi ini merupakan kemampuan literasi minimum yang perlu dimiliki oleh setiap warga negara Indonesia dalam menyongsong abad ke- 21. Literasi dan teknologi memiliki hubungan yang erat dalam masyarakat modern.

Literasi tidak lagi terbatas pada kemampuan membaca dan menulis, tetapi juga mencakup pemahaman dan pemanfaatan teknologi informasi. Seiring dengan perkembangan teknologi informasi, literasi tidak hanya mengacu pada kemampuan membaca dan menulis dalam bentuk tradisional, tetapi juga melibatkan pemahaman dan pemanfaatan teknologi informasi. Salah satu pengaruh paling besar dalam masyarakat informasi adalah ditemukannya internet. Menurut survei Asosiasi Penyelenggara Jasa Internet Internet Indonesia (2017), penetrasi pengguna internet di Indonesia sekitar 143, 26 juta jiwa atau 54, 68% dari total populasi penduduk Indonesia 262 juta orang (Kurniawan & Rofiah, 2020). Kehadiran internet menyebabkan manusia tidak dapat lepas dari arus komunikasi dan informasi. Kemajuan bidang Teknologi informasi yang begitu pesat sebagaimana data yang telah disebutkan di samping memberikan berkat apabila digunakan dengan penuh tanggungjawab dan akan sebaliknya yaitu menimbulkan bencana berbagai kejahatan bila digunakan tanpa disertai tanggungjawab (Randi, 2022).

Saat ini Indonesia sedang mengalami keadaan mendesak *cyber-security* atau keamanan dunia maya. Indonesia termasuk negara yang lemah dalam hal *cyber security*. Kelemahan keamanan dunia maya suatu negara melibatkan banyak faktor dan kompleksitas. Pada kasus ini, indikasinya adalah tingkat kejahatan dunia maya atau *cyber-crime* di Indonesia sudah mencapai tahap mengkhawatirkan. Dampak dari kejahatan ini sangat luas dan banyak merugikan perekonomian (Hermawan, 2013). Hasil penelitian perusahaan keamanan *Symantec* dalam *internet security Threat Report* volume 17, Indonesia menempati peringkat 10 sebagai negara dengan aktifitas *cybercrime* terbanyak sepanjang tahun 2011 2011 (Juditha, 2015). Kerugiaan akibat *cyber-crime* di Indonesia tahun 2013 mencapai USD 895 billion yang artinya mencapai 1,20% dari total keseluruhan perkiraan kerugian akibat *cybercrime* secara global mencapai USD 71,620 billion (Danuri & Suharnawi, 2017). Maka diperlukan perhatian dan keseriusan dalam mengembangkan cyber security bagi semua *stakeholder* yang memiliki data-data penting yang harus dijaga keamanannya. Mengingat maraknya aksi hacking lebih dikarenakan lemahnya sistem keamanan internet dan komputer di Indonesia (Ardiyanti, 2014).

Cybersecurity merupakan kumpulan kebijakan keamanan yang dapat difungsikan untuk melindungi lingkungan *cyber*, organisasi, aset pengguna (Hafid et al., 2023; Soesanto et al., 2023). Organisasi maupun aset pengguna dalam *cybersecurity* termasuk perangkat yang terhubung pada

komputasi, personil, aplikasi, layanan, maupun sistem telekomunikasi yang dikirimkan dan/atau disimpan dalam lingkungan maya (Moenawar et al., 2019; Putra et al., 2018). Ini sebagai upaya untuk memastikan terpeliharanya kemanan data dan informasi organisasi dan aset pengguna dari kejahatan. Keamanan data berperan penting dalam mencegah serangan siber dan upaya kejahatan *cyber* seperti pencurian data, *ransomware*, atau serangan *phishing*. Melalui kebijakan keamanan yang efektif, organisasi dapat mengurangi risiko dan dampak dari serangan tersebut.

Salah satu organisasi dengan kebutuhan keamanan siber yang tinggi adalah Aisyiyah. Aisyiyah merupakan organisasi wanita yang terkait erat dengan Muhammadiyah. Aisyiyah didirikan bertujuan untuk mengembangkan masyarakat melalui pendidikan dan kesehatan. Aisyiyah berperan dalam mendukung program-program Muhammadiyah dan memiliki peran yang signifikan dalam pemberdayaan perempuan. Organisasi ini terlibat dalam pendidikan, kesehatan, dan kegiatan sosial lainnya yang bertujuan untuk meningkatkan kesejahteraan dan pendidikan perempuan.

Aisyiyah adalah organisasi perempuan Muhammadiyah yang memiliki fokus gerakan pada Perempuan dan Anak di berbagai aspek yaitu Pendidikan, Kesehatan, Keorganisasian, Ekonomi, Sosial, Dakwah KeIslaman, dan Kaderisasi. Visi dari organisasi ini adalah terbentuknya wanita Islam yang berguna untuk keluarga, agama dan bangsa. Dalam rangka mencapai visinya tersebut, 'Aisyiyah memiliki misi yaitu (1) melaksanakan dakwah Islam amar ma'ruf nahi munkar dalam membina putri Islam yang berarti bagi agama, bangsa, dan negara menuju terwujudnya masyarakat yang sebenar-benarnya. (2) Melaksanakan pencerahan dan pemberdayaan perempuan menuju masyarakat yang menjunjung tinggi harkat, martabat dan nilai-nilai kemanusiaan yang sesuai dengan ajaran Islam. (3) Menyelenggarakan amal usaha dan meningkatkan peran 'Aisyiyah sebagai pelopor, pelangsung dan penyempurna perjuangan Muhammadiyah. Misi tersebut diimplementasikan dalam bentuk berbagai program kerja dan kegiatan yang terstruktur mulai dari tingkat pusat sampai ranting (Susanto, 2013).

Pimpinan Cabang Istimewa 'Aisyiyah (PCIA) merupakan tingkat kepemimpinan untuk menjangkau warga 'Aisyiyah di luar negeri. Negara yang sudah ada PCIA-nya adalah Hongkong. Kedua negara tersebut merupakan negara tujuan pekerja migran Indonesia (PMI) dan mahasiswa menempuh pendidikan tingkat lanjut. Tempat kerja atau studinya yang berjauhan dari keluarga membuat para PMI dan mahasiswa tersebut sulit sering bertemu fisik dengan keluarganya di Indonesia. Hal itu mengharuskan para PMI dan mahasiswa tadi berkomunikasi dengan keluarganya secara *online*. Di samping itu, sejak pandemi merebak komunikasi diantara mereka banyak

dilakukan secara online meskipun secara fisik para PMI dan mahasiswa tadi lokasinya berdekatan dan relatif mudah untuk berkumpul secara fisik.

Komunikasi *online* yang lebih intensif menimbulkan masalah baru terkait dengan *cybersecurity*, misalnya *scamming*, *phising*, *faking*, maupun pencurian data-data pribadi. Hal tersebut membuat para penggiat PCIA Hongkong rawan mendapatkan ancaman terkait *cybersecurity*. Latar belakang pendidikan para penggiat PCIA Hongkong juga beragam. Hal tersebut membuat literasi terkait *cybersecurity* juga tidak sama. Sebagian besar PMI, termasuk yang aktif di PCIA Hongkong adalah generasi milenial sudah cukup melek terhadap teknologi komunikasi dan interaksinya secara online pun cukup besar. Namun, masih banyak yang belum melek terhadap keamanan di dunia siber (*cybersecurity*) termasuk adanya UU ITE.

METODE

Pendampingan ini dilaksanakan selama 4 kali pertemuan secara daring melalui zoom meetingpada bulan Juni sampai September 2023, dilanjutkan dengan luring pada tanggal 30 September 2023 sampai 2 Oktober 2023. Peserta terdiri dari 20 anggota PCIA Hong Kong dan Pekerja Migran Indonesia. Langkah-langkah pendampingan sebagai berikut: 1) Melakukan koordinasi dengan PCIA Hongkong, 2) Melakukan koordinasi dengan Majelis Pustakan dan Informasi Muhammadiyah dan 'Aisyiyah, 3) Memberikan penyuluhan *cyber security* dan permasalahannya kepada pimpinan dan anggota PCIA Hongkong, 4) Memberikan sosialisasi mengenai Undang-Undang Informasi dan Transaksi Elektronik, dan 5) Pelatihan penggunaan aplikasi Mobile *Cyber Security*.

HASIL DAN PEMBAHASAN

PkM ini dilakukan dengan memberikan pengetahuan tentang *Cyber Security* dan Literasi Digital untuk Pekerja Migran Indonesia (PMI) dengan memberikan buku saku terkait *Cyber Security* dan Literasi Digital. Indikator yang digunakan dalam mengukur pengetahuan tentang Keamanan Siber dan Literasi Digital meliputi aspek pemahaman, pengetahuan tentang bahaya kejahatan siber (Hidayat et al., 2023), pengetahuan otentikasi (Radiansyah et al., 2016), kesadaran tentang pembaruan perangkat lunak (Susanto et al., 2023), sensitivitas cek dan validasi file dalam mengirim pesan (Rahmawati, 2017), kepekaan cadangan data dalam percakapan media sosial (Tandirerung & Mangesa, 2023), memeriksa sebelum memposting di media sosial, pengaturan

privasi di akun media sosial dan keterampilan digital yang terkait dengan penggunaan media sosial (Sabrina, 2019).

Sebelum pelaksanaan PkM terlebih dahulu diberikan pretes untuk mengukur pengetahuan para pekerja migran tentang *Cyber Security* dan Literasi Digital. Dari *pretest* tersebut, pada umumnya belum mengetahui tentang *Cyber Security* (21,34%) namun terkait bahaya *cybercrime*, sekitar 35,71% pekerja migran mengetahui. Seluruh pekerja migran mempunyai akun media sosial (100,00%) akan tetapi belum ada yang melakukan autentikasi 2 faktor pada akun media sosial (0,00%). Sekitar 32,14 % sudah melakukan *update software* media sosial dan 75,00% sudah melakukan cek dan validasi file dalam mengirim pesan di media sosial. Namun sekitar 3,57% yang melakukan *backup* data hasil percakpaan media sosial dan melakukan *checking* sebelum posting di media sosial sebanyak 82,14%. Beberapa PMI sudah mengatur privasi pada akun media sosial (3,57%) ironisnya tidak dibarengi dengan pengetahuan literasi digital terkait penggunaan media sosial (0,00%).

Setelah dibagikan buku saku dan pengetahuan terkait *Cyber Security* dan Literasi Digital, terjadi peningkatan pengetahuan para pekerja migran. Seperti pada Tabel 1 dapat dilihat bahwa pengetahuan PMI secara keseluruhan meningkat dengan hasil *posttest* diatas 90%. Sekitar 96,43% telah mengetahui tentang bahaya *cybercrime* sehingga 53,57% PMI melakuka 2 faktor pada akun media sosial. Sebanyak 67,36% sudah melakukan *update software* media sosial dan telah mengecek serta memvalidasi file dalam mengirim pesan (89,29%). Dengan pengetahuan yang didapat PMI melakukan *backup* data (25,00%) dan melakukan *checking* sebelum posting di media sosial sebanyak 92,86%. Pekerja migran juga melakukan pengaturan privasi pada akun media sosial sekitar 32,14%. Sebanyak 50,00% PMI sudah mengetahui terkait literasi digital.

Hasil postes menunjukkan bahwa dengan memberikan buku saku dan pengetahuaun terkait *Cyber Security* dan Literasi Digital telah berhasil meingkatkan pengetahuan PMI tentang bagaimana cara mengamankan sosial media dan menggunakan sosial media dengan bijak.

Tabel 1. Pengetahuan PMI *Cyber Security* dan Literasi Digital

No.	Parameter pengetahuan *cyber security* dan lietrasi digital	% Jawaban sesuai	
		Pretest	***Postest***
1	Pemahaman *Cyber Security*	21,43	92, 86
2	Bahaya *Cybercrime*	35,71	96,43
3	Memiliki akun media sosial	100,00	100,00

No.	Parameter pengetahuan *cyber security* dan lietrasi digital	% Jawaban sesuai	
		Pretest	***Postest***
4	autentikasi 2 faktor	0,00	53,57
5	*Update software*	32,14	67,36
6	Cek dan validasi file dalam mengirim pesan	75,00	89,29
7	Backup data hasil percakapan media sosial	3,57	25,00
8	*Checking* sebelum posting di media sosial	82,14	92, 86
9	Pengaturan privasi pada akun media sosial	3,57	32,14
10	Pengetahuan literasi digital terkait penggunaan media sosial	0,00	50,00

Pemahaman masyarakat terhadap keamanan siber sangat penting dalam menghadapi ancaman siber yang semakin kompleks (Maulindar & Hartanti, 2023). Pemahaman ini mencakup pengetahuan tentang potensi risiko, tindakan pencegahan, dan perilaku yang aman secara digital (Manurung et al., 2023). Program-program pendidikan dan pendampingan kesadaran publik dapat meningkatkan pemahaman masyarakat terhadap risiko keamanan siber. Ini dapat mencakup kampanye informasi, seminar, pelatihan *online*, pendampingan untuk meningkatkan pengetahuan. Kejadian-kejadian penting dan kasus-kasus keamanan siber yang terkenal dapat mempengaruhi pemahaman masyarakat. Serangan siber yang mendapatkan liputan media dapat meningkatkan kesadaran dan pemahaman tentang ancaman keamanan digital (Isnaini et al., 2020). Pengalaman pribadi dengan serangan siber, seperti serangan phishing atau perangkat lunak berbahaya, dapat memperkuat pemahaman masyarakat tentang risiko dan perlunya tindakan keamanan. Cara masyarakat menggunakan teknologi, termasuk perangkat mobile, media sosial, dan internet, dapat mempengaruhi pemahaman mereka tentang keamanan siber. Semakin banyak interaksi dengan dunia digital, semakin penting pemahaman tentang keamanan.

Pandemi COVID-19 telah menyebabkan peningkatan aktivitas online, termasuk bekerja dari rumah dan belajar daring. Hal ini mendorong pergeseran pemahaman masyarakat terhadap risiko dan perlunya menjaga keamanan di lingkungan digital. Pendidikan formal dan informal memainkan peran penting dalam membentuk pemahaman masyarakat tentang keamanan siber (Pambudi et al., 2023). Program-program keamanan siber di sekolah dan universitas, serta pelatihan di tempat kerja, dapat membantu meningkatkan pemahaman individu. Kerjasama antara pemerintah, sektor swasta, dan masyarakat sipil dapat membantu meningkatkan pemahaman masyarakat. Program-program

kerjasama, seperti seminar keamanan siber di tingkat komunitas, dapat memberikan informasi dan saran praktis. Ketersediaan informasi tentang keamanan siber secara mudah diakses dan dipahami dapat memainkan peran penting dalam membentuk pemahaman masyarakat. Materi edukasi yang jelas dan dapat diakses secara online dapat membantu meningkatkan kesadaran.

SIMPULAN

Dari hasil kegiatan pengabdian ini dapat diambil kesimpulan bahwa perbandingan pengetahuan *cybersecurity* dan kecerdasan digital sebelum dan sesudah mengalami perbaikan dalam aspek pemahaman, pengetahuan tentang bahaya kejahatan *cyber*, pengetahuan autentikasi, kesadaran pembaruan perangkat lunak, kesedaran pemeriksaan dan validasi file dalam mengirim pesan, kebangkitan hasil backup data dari percakapan media sosial, sensitivitas backup hasil data media sosial, memeriksa sebelum posting di media sosial, pengaturan privasi di akun media sosial dan pengetahuan literatur digital yang terkait dengan penggunaan media sosial.

UCAPAN TERIMA KASIH

Ucapan terima kasih khusus disampaikan kepada LPPM UAD sebagai pemberi dana pengabdian kepada Masyarakat melalui hibah pengabdian kepada masyarakat skema internasional dengan nomor kontrak U.12/SPK-PkM-International-4/LPPM-UAD/VI/2023.

DAFTAR PUSTAKA

Ardiyanti, H. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *5*(1), 95–110.

Danuri, M., & Suharnawi. (2017). Trend Cyber Crime Dan Teknologi Informasi Di Indonesia. *Informasi Komputer Akuntansi Dan Manajemen*, *13*(2), 55–65.

Hafid, M., Firjatullah, F. Z., Pamungkaz, B. W., Magister, S., Hukum, I., Wijaya, U., & Surabaya, K. (2023). Tantangan Menghadapi Kejahatan Cyber dalam Kehidupan Bermasyarakat dan Bernegara. *Pendidikan Tambusai*, *7*(2), 9548–9556.

Hermawan, R. (2013). Kesiapan Aparatur Pemerintah Dalam Menghadapi. *Jurnal Teknik Informatika*, *6*(1), 43–50.

Hidayat, A., Samudra, Y., & Andriyanto, L. P. (2023). Sosialisasi Pengenalan Pentingnya Cyber SecurityBagi Siswa Untuk Membangun Keamanan Informasi Dalam Era Digital. *Jurnal Pengabdian Masyarakat*, *2*(5), 450–457.

Juditha, C. (2015). Pola Komunikasi Dalam Cybercrime (Kasus Love Scams). *Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika*, *6*(2), 122582.

Khairunnisak Nur Isnaini, Dina Fajar Sulistiyani, & Manut Sutrisno. (2020). Data Security Awarenesssebagai Upaya Peningkatan Literasi Tentang Cyber AttacksdanThreats. *JPMB: Jurnal Pemberdayaan Masyarakat Berkarakter*, *3*(2), 121–132.

Kurniawan, M. R., & Rofiah, N. H. (2020). Pola Penggunaan Internet di Lingkungan Sekolah Dasar Se-Kota Yogyakarta. *Southeast Asian Journal of Islamic Education*, *2*(2), 93–105. https://doi.org/10.21093/sajie.v2i2.1930

Manurung, J., Putra Emas Sihombing, A., & Pandiangan, B. (2023). Sosialisasi Dan Edukasi Tentang Keamanan Data Dan Privasi Di Era Digital Untuk Meningkatkan Kesadaran Dan Perlindungan Masyarakat. *Jurnal Pengabdian Masyarakat Nauli*, *2*(1), 1–7. https://ejournal.marqchainstitute.or.id/index.php/Nauli/article/view/103

Maulindar, J., & Hartanti, D. (2023). Pelatihan Perlindungan Data Pribadi dan Keamanan Siber Untuk Siswa SMK Negeri 2 Surakarta. *Madaniya*, *4*(4), 1851–1856.

Moenawar, M. G., Mandjusri, A., & Septayuda, T. (2019). Transforming Cybersecurity through Sustainability in Living Harmony: Facing the Dissemination of Hoax Information based on Digital Media. *International Journal of Multicultural and Multireligious Understanding*, *6*, 119–125. https://www.semanticscholar.org/paper/eccd4e707dc5bf38fe787c105d8ba1da382050f3

Pambudi, R., Budiman, A., Rahayu, A. W., Sukanto, A. N. R., & Hendrayani, Y. (2023). Dampak Etika Siber Jejaring Sosial Pada Pembentukan Karakter Pada Generasi Z. *JURNAL SYNTAX IMPERATIF : Jurnal Ilmu Sosial Dan Pendidikan*, *4*(3), 289–300. https://doi.org/10.36418/syntax-imperatif.v4i3.262

Putra, R. D., Supartono, & Deni, D. A. R. (2018). Ancaman Siber dalam Persfektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta). *Jurnal Prodi Perang Asimetris*, *4*(2), 99–120.

Radiansyah, I., Rusdjan, C., & Priyadi, Y. (2016). Analisis Ancaman Phishing Dalam Layanan Online Banking. *Journal of Innovation in Business and Economics*, *7*(1), 1. https://doi.org/10.22219/jibe.vol7.no1.1-14

Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara*, *7*(2), 72–78. https://doi.org/10.33172/jpbh.v7i2.179

Randi, Y. (2022). Perlindungan Hukum Konsumen Terhadap Penjualan Produk Kesehatan Palsu Pada Situs Online di Masa Covid-19. *MORALITY: Jurnal Ilmu Hukum*, *8*(1), 1. https://doi.org/10.52947/morality.v8i1.223

Sabrina, A. R. (2019). Literasi Digital Sebagai Upaya Preventif Menanggulangi Hoax.

Communicare : Journal of Communication Studies, *5*(2), 31. https://doi.org/10.37535/101005220183

Sinar, T. S. (2022). Meninjau Program Literasi Budaya Dalam Membangun Kemajuan Masyarakat Melayu Di Sumatera Utara. *TALENTA Conference Series: Local Wisdom, Social, and Arts R*, *5*(2). https://doi.org/10.32734/lwsa.v5i2.1372

Soesanto, E., Aprillia, D. P., Anjani, N. D., & Halimatusa'diah. (2023). Pengaruh sistem pengamanan objek vital, file dan cyber terhadap manajemen sekuriti pada pt pln (persero) TBK. *Cross-Border*, *6*(1), 705–714.

Susanto, D. (2013). Gerakan Dakwah Aktivis Perempuan 'Aisyiyah Jawa Tengah. *Sawwa: Jurnal Studi Gender*, *8*(2), 323. https://doi.org/10.21580/sa.v8i2.660

Susanto, E., Dairo Lende, A., Firjatullah, A. R., & Pratama, R. A. (2023). Analisis Keamanan Informasi PT. Indofood Sukses Makmur, Tbk : Studi Kasus tentang Peran Objek Vital, Pengamanan File, dan Pengamanan Cyber. *Jurnal Manajemen Dan Ekonomi Kreatif*, *1*(3), 79–87. https://doi.org/10.59024/jumek.v1i3.116

Tandirerung, V. A., & Mangesa, R. T. (2023). Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas. *Jurnal Pengabdian Masyarakat*, *1*(2), 89–94. https://journal.unm.ac.id/index.php/TEKNOVOKASI/article/view/131