GERVASI: Jurnal Pengabdian kepada Masyarakat
Vol. 6, No. 3, Desember 2022
ISSN 2598-6147 (Cetak)
ISSN 2598-6155 (Online)

PENINGKATAN KESADARAN KEAMANAN INFORMASI MELALUI KEGIATAN *ONLINE WORKSHOP* MENGGUNAKAN *PLATFORM QUIZIZZ*

Amiruddin[1], Ira Rosianal Hikmah[2], Tiyas Yulita[3], Dimas Febriyan Priambodo[4], Jeckson Sidabutar[5]
[1, 2, 3, 4, 5]Program Studi Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, Jalan Raya H. Usa, Putat Nutug, Kabupaten Bogor, Jawa Barat, 16120
[1]e-mail: amiruddin@bssn.go.id

Abstrak

Kesadaran keamanan informasi merupakan salah satu faktor penting dalam pengukuran *Global Cybersecurity Index* (GCI). Peningkatan jenis dan jumlah ancaman serangan siber mengakibatkan pengguna sulit mengetahui dan memahaminya. Pencurian data pelanggan *marketplace* adalah contoh nyata dari ancaman tersebut, yang apabila tidak segera ditangani, dapat menimbulkan kerugian yang lebih besar. Kegiatan pengabdian kepada masyarakat dalam bentuk *online workshop* merupakan salah satu upaya yang dilakukan di masa pandemi *Covid-19* untuk meningkatkan pemahaman dan kesadaran mengenai keamanan informasi. Kegiatan ini dilakukan di STMIK Sinar Nusantara Surakarta dengan jumlah peserta 105 orang, meliputi penyampaian materi dan evaluasi pemahaman peserta. Materi yang diberikan terkait keamanan informasi, teknologi pengambil informasi, rekayasa sosial, dan *live demo* serangan siber. Adapun evaluasi terhadap peserta *workshop* dilakukan dengan mengerjakan soal-soal terkait materi yang dibahas sebelumnya melalui *platform Quizizz.* Jawaban dari peserta dianalisis dengan metode statistik yaitu pengujian beda rataan dan diperoleh kesimpulan bahwa kegiatan ini dapat meningkatkan pemahaman keamanan informasi peserta *workshop* secara signifikan dengan rata-rata peningkatan sebesar 13%.

Kata Kunci: keamanan informasi, rekayasa sosial, kesadaran keamanan

Abstract

Information security awareness is one of the important factors in measuring the Global Cybersecurity Index (GCI). The increase in the types and numbers of cyber-attack threats makes it difficult for users to identify and understand them. The theft of marketplace customer data is a clear example of this threat, which if not addressed immediately, can cause even greater losses. Community service activities in the form of online workshops are one of the efforts made during the COVID-19 pandemic to increase understanding and awareness of information security. This activity was carried out at STMIK Sinar Nusantara Surakarta with 105 participants, including the delivery of material and evaluation of participants' understanding. The material provided is related to information security, information retrieval technology, social engineering, and live demo cyber attacks. The evaluation of the workshop participants is carried out by working on questions related to the previously discussed material through the Quizizz platform. The answers from the participants were analyzed using statistical methods, namely the average difference test and it was concluded that this activity could significantly improve the understanding of information security of workshop participants with an average increase of 13%.

Keywords: *information security, social engineering, security awareness*

PENDAHULUAN

Perkembangan teknologi informasi menyebabkan perubahan pola pikir masyarakat mengenai batas wilayah, waktu, nilai-nilai serta batas perilaku sosial yang awalnya bersifat manual menjadi digital (Ekawati, 2018). Pada tahun 2021, pengguna internet di Indonesia berjumlah 202,6 juta atau 73,7% dari total populasi, dan mengalami peningkatan sebesar 15,5% atau sekitar 27 juta dari tahun 2020 (Datereportal, 2021). Internet memberikan banyak manfaat apabila seseorang dapat menggunakannnya secara bijaksana, seperti mengakses informasi maupun berita terkini, menambah wawasan keilmuan, serta memudahkan komunikasi dengan orang lain sehingga secara perlahan menyebabkan perubahan sosial dalam masyarakat. Namun, kadangkala kemudahan mengakses informasi menjadikan seseorang lalai atau tidak waspada dengan informasi yang diperoleh maupun yang dibagikan kepada orang lain.

Media sosial menjadi salah satu bentuk sarana interaksi yang paling mudah untuk diakses oleh masyarakat usia muda maupun tua. Terdapat berbagai jenis aplikasi media sosial yang menyajikan bermacam cara interaksi dari seseorang kepada orang lain seperti dalam bentuk tulisan, gambar, suara, dan/atau video. Kewaspadaan yang rendah menyebabkan seseorang dengan mudahnya membagikan informasi pribadi melalui media sosial seperti nomor telepon, alamat rumah, tanggal lahir, menandai ibu kandung dalam sebuah foto yang dibagikan melalui akun media sosialnya serta informasi pribadi lainnya.

Keamanan data pribadi menjadi aspek penting yang tidak dapat diabaikan, mengingat saat ini marak terjadi kejahatan yang disebabkan oleh ketidakwaspadaan seseorang terhadap data pribadinya. *Social engineering* atau rekayasa sosial menjadi salah satu bentuk kejahatan yang dilakukan dengan memanipulasi psikologis seseorang untuk mendapatkan data pribadi, sehingga dengan informasi tersebut, pelaku dapat meretas akun bank maupun *e-commerce* yang dimiliki korban untuk dimanfaatkan secara tidak wajar sehingga sangat merugikan. Selain *social engineering*, banyak bentuk kejahatan lain yang muncul akibat dari kemajuan teknologi informasi diantaranya *carding*, *hacking*, dan *phising*. Beberapa peraturan di Indonesia yang terkait dengan perlindungan data

pribadi antara lain Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Rumlus & Hartadi, 2020).

Global Cybersecurity Index (GCI) yang menjadi alat ukur tingkat keamanan siber suatu negara menjadikan kesadaran keamanan informasi sebagai salah satu faktor penting yang dinilai (International Telecommunication Union, 2021). Oleh karena itu, perlu terus dilakukan upaya-upaya untuk meningkatkan kesadaran keamanan informasi masyarakat sehingga dapat terhindar dari risiko ancaman siber termasuk pencurian data pribadi. Kegiatan yang dapat dilakukan dapat berupa *workshop* atau diskusi mengenai pentingnya memiliki kesadaran keamanan pada setiap diri masing-masing individu agar risiko tercurinya data pribadi dapat diminimalisir.

Pelaksanaan Tridharma Perguruan Tinggi adalah sebuah kewajiban bagi setiap perguruan tinggi di Indonesia untuk menjaga keberlangsungan pendidikan pada perguruan tinggi serta memberikan manfaat bagi masyarakat baik melalui riset maupun kegiatan lain yang manfaatnya bisa dirasakan oleh masyarakat. Salah satu kegiatan Tridharma Perguruan Tinggi adalah kegiatan Pengabdian kepada Masyarakat. Bentuk kegiatan Pengabdian kepada Masyarakat beragam, seperti penyuluhan, ceramah, diskusi, pelatihan, dan *workshop*. Hasil kegiatan Pengabdian kepada Masyarakat yang dilakukan oleh Universitas Sriwijaya berupa kegiatan *workshop* teknik keamanan dalam menggunakan internet pada Siswa SMK dengan hasil bahwa siswa memahami ancaman dari internet, melek terhadap penggunaan internet, dan mampu mencegah pencurian data pribadi di internet (Heryanto et al., 2018). Selain itu, kegiatan Pengabdian kepada Masyarakat dilakukan Universitas Esa Unggul berupa penyuluhan terkait keamanan dan kebenaran informasi digital melalui Zoom dengan hasil bahwa para peserta mampu mendapatkan kesimpulan atas *transfer knowledge* yang telah dilaksanakan (Adikara et al., 2020). Bentuk lainnya adalah dalam bentuk ceramah, diskusi, dan pelatihan yang dilakukan oleh Universitas Pamulang dengan hasil bahwa remaja

pondok pesantren semakin mawas diri dan memproteksi diri dalam menggunakan internet (Hutagalung et al., 2022).

Dosen Politeknik Siber dan Sandi Negara berupaya meningkatkan kesadaran keamanan informasi masyarakat khususnya mahasiswa serta tenaga kependidikan pada STMIK Sinar Nusantara, Surakarta melalui kegiatan pengabdian masyarakat *workshop* teknik dan taktik keamanan informasi. Hal ini mengingat bahwa melindungi keamanan data bukan kewajiban pemerintah saja, namun juga calon lulusan pada bidang Teknologi Informasi (TI) yang harus mengerti mengenai keamanan informasi dan teknis pengamanannya. Peserta pada kegiatan pengabdian masyarakat ini diberikan materi mengenai keamanan informasi, *social engineering*, dan teknologi pengambil informasi, serta demo serangan siber yang melibatkan mahasiswa Politeknik Siber dan Sandi Negara, yang semuanya saling berkaitan. Tujuan dari kegiatan ini adalah untuk menambah pemahaman peserta akan pentingnya kesadaran keamanan informasi sehingga dapat lebih waspada dalam menjaga kerahasiaan informasi data pribadi demi menghindari penggunaan data secara ilegal oleh pihak yang tidak berwenang.

METODE

Pra Kegiatan

Persiapan yang dilakukan dalam kegiatan pengabdian kepada masyarakat ini yaitu menentukan waktu pelaksanaan kegiatan bersama pihak STMIK Sinar Nusantara. Kegiatan dilakukan secara daring melalui aplikasi *video conference Zoom Meeting* dalam bentuk *workshop* dengan target jumlah peserta yang hadir adalah 100 orang. Selain itu, untuk mengukur pemahaman peserta, panitia mempersiapkan pertanyaan yang kemudian *diuplad* ke dalam *platform* Quizizz. Pertanyaan tersebut digunakan dalam proses *pre-test* dan *posttest* kepada peserta.

Kegiatan

Rangkaian kegiatan dituliskan secara rinci pada Tabel 1. Dokumen materi atau bahan paparan pemateri tidak diberikan kepada peserta sebelum kegiatan berlangsung, hal ini bertujuan agar peserta dapat fokus mendengarkan paparan dari pemateri dan dapat meninjau kembali setelah bahan materi diberikan. Bahan

materi tersebut diberikan kepada peserta setelah setiap pemateri selesai memaparkan materinya.

Tabel 1 Rincian Kegiatan *Workshop*

Waktu	Kegiatan Inti	Keterangan
09.00 – 09.05	Pembukaan	
09.05 – 09.25	Sambutan	Perwakilan oleh Poltek SSN dan STMIK Sinar Nusantara, Surakarta
09.25 – 09.40	*Pre-test*	
09.40 – 10.00	*Keynote speech*	Keamanan Informasi
10.00 – 10.30	Panel 1	Teknologi Pengambil Informasi
10.30 – 11.00	Panel 2	Rekayasa Sosial
11.00 – 12.00	Diskusi Panel	Sesi Tanya Jawab
12.00 – 13.00	Istirahat	
13.00 – 14.40	*Live Demonstration*	Topik: *SQL Injection,* *Sensitive Data Exposure,* *Cross Site Scripting* (XSS), *Open Source Intelligent* (OSINT)
14.40 – 14.55	*Posttest*	
14.55 – 15.00	Penutupan	

Evaluasi

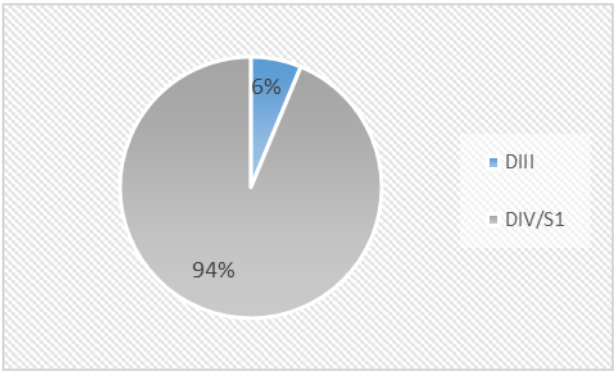
Proses evaluasi dalam kegiatan ini dengan memberikan *pre-test* dan *posttest* kepada peserta. *Pre-test* dilakukan sebelum memasuki *keynote speech*, dengan jumlah 15 soal. Soat tersebut merupakan soal pilihan ganda yang telah disesuaikan dengan materi yang disajikan kepada peserta. Saat *pre-test*, peserta tidak menerima jawaban yang benar dan peserta tidak mengetahui apakah jawabannya benar atau salah. Peserta hanya menerima nilai akhir *pre-test*. Sedangkan *posttest* dilakukan setelah *live demonstration* selesai, soal *posttest* dibuat sama dengan soal *pre-test*. Jika dalam *pre-test* peserta tidak dpat melihat jawaban yang benar dari setiap soal, namun saat *posttest*, peserta dapat melihat jawaban benar setelah mereka memilih jawaban di setiap soal. Baik *pre-test* maupun *posttest*, peserta diberikan waktu 30 detik setiap soal dan peserta tidak dapat kembali ke nomor sebelumnya atau mengubah jawaban ketika peserta salah memilih baik secara sengaja atau tidak sengaja.

HASIL DAN PEMBAHASAN

Gambaran Peserta Kegiatan

Peserta *workshop* yang terdaftar dapat dilihat pada Gambar 1 hingga Gambar 3. Gambar 1 dan Gambar 2 memperlihatkan bahwa terdapat 130 orang yang mendaftarkan diri sebagai peserta *workshop* dengan sebaran mayoritas adalah mahasiswa sejumlah 112 orang dan sisanya yaitu 18 orang berstatus sebagai pendidik dan tenaga kependidikan. Dari 112 mahasiswa, hanya 6% (7 peserta) yang terdaftar dan berstatus sebagai mahasiswa dengan jenjang pendidikan DIII sedangkan sisanya yaitu 94% (105 peserta) dengan jenjang pendidikan yang sedang ditempuh DIV/S1.

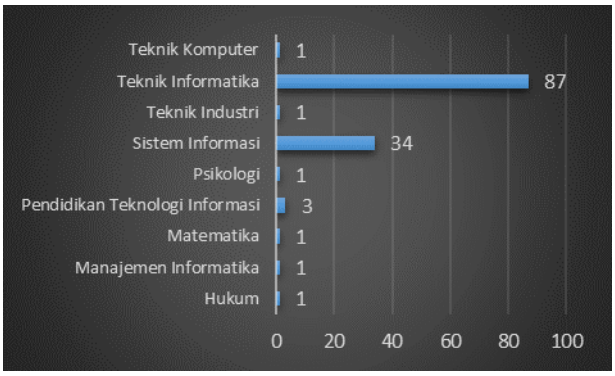
Gambar 1 Sebaran Status Pekerjaan Peserta *Workshop* yang Terdaftar



Gambar 2 Sebaran Jenjang Pendidikan Peserta *Workshop* yang Terdaftar dengan Status Mahasiswa

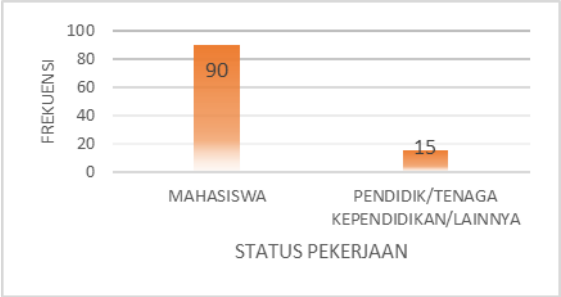
Gambar 3 menunjukkan sebaran bidang Pendidikan atau keahlian peserta *workshop* yaitu dengan mayoritas menempuh Program Studi Teknologi Informatika, disusul dengan Program Studi Sistem Informasi. Bidang Pendidikan lainnya adalah Teknik Komputer, Teknik Industri, Psikologi, Pendidikan

Teknologi Informasi, Matematika, Manajemen Informatika, dan Hukum. Kegiatan ini ditargetkan untuk program studi di bidang teknologi informasi dan komunikasi. Namun, terdapat minat dari program studi lain di luar bidang yang ditargetkan. Hal ini menunjukkan bahwa kebutuhan akan kesadaran dan pemahaman terkait keamanan informasi tidak hanya diperlukan bagi mahasiswa di bidang teknologi informasi dan komunikasi, tetapi bagi mahasiswa lain yang memanfaatkan teknologi khususnya internet.

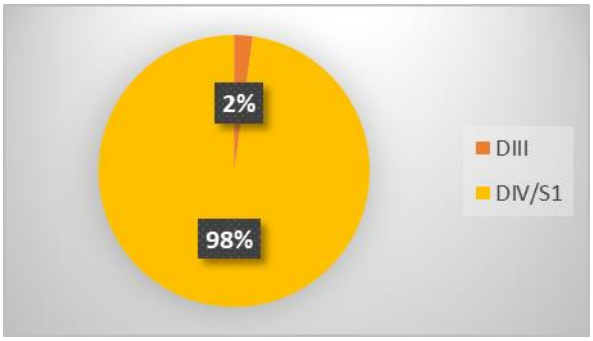


Gambar 3 Sebaran Bidang Pendidikan Peserta *Workshop* yang Terdaftar

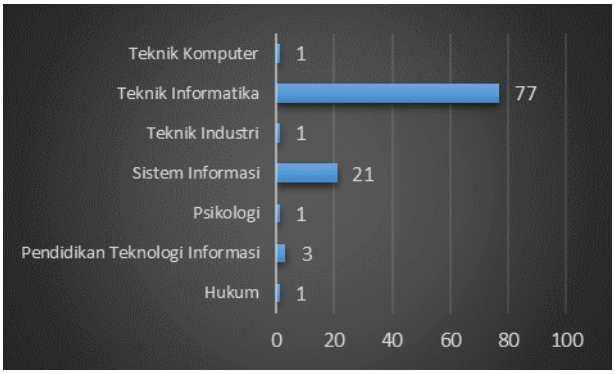
Saat pelaksanaan *workshop*, dari 130 peserta yang terdaftar, terdapat 25 peserta yang tidak hadir *workshop* sehingga jumlah peserta adalah 105 orang (81% yang hadir). Jumlah ini melebihi dari target jumlah peserta yang hadir pada kegiatan *workshop* yaitu 100 orang. Gambaran peserta *workshop* yang menghadiri kegiatan dari awal hingga akhir dapat dilihat pada Gambar 4 hingga Gambar 6.



Gambar 4 Sebaran Status Pekerjaan Peserta *Workshop* yang Hadir



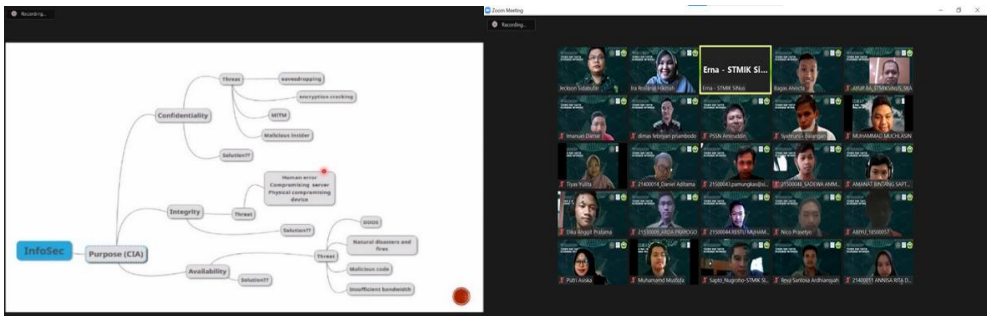
Gambar 5 Sebaran Jenjang Pendidikan Peserta *Workshop* yang Hadir dengan Status Mahasiswa



Gambar 6 Sebaran Bidang Pendidikan Peserta *Workshop* yang Hadir

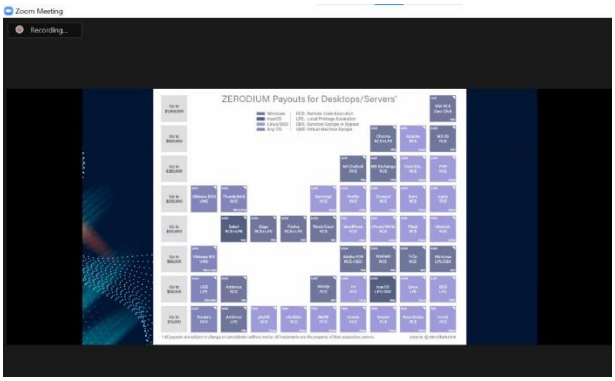
Pelaksanaan Kegiatan

Inti dari kegiatan ini adalah penyampaian materi oleh pemateri pertama sekaligius sebagai *keynote speeaker* yang menjelaskan mengenai konsep dasar keamanan informasi yang meliputi *confidentiallity*, *integrity*, *availability* (Gambar 7). Berlanjut pada materi kedua yang menjelaskan mengenai jenis-jenis teknologi yang dapat dimanfaatkan untuk mengambil informasi (Gambar 8). Materi ketiga adalah penyampaian mengenai rekayasa sosial (*social engineering*) dengan berbagai jenis praktik yang ada di dalamnya (Gambar 9).



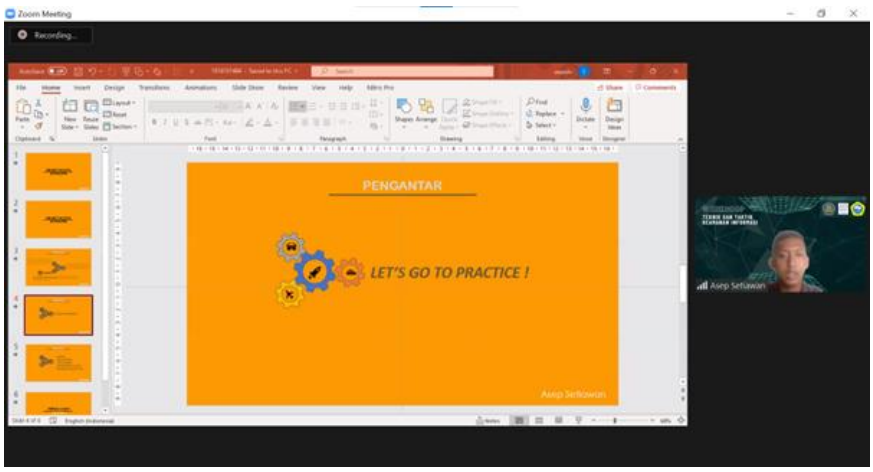
Gambar 7 Dokumentasi *Keynote Speech* Materi "Keamanan Informasi"

Antusiasme peserta dapat terlihat dari banyaknya pertanyaan yang diajukan selama kegiatan berlangsung. Rangkaian kegiatan diakhiri dengan *live demonstration* yang dibawakan oleh taruna Politeknik Siber dan Sandi Negara (Gambar 10). Dalam kegiatan tersebut para taruna mempraktikan mengenai *Sensitive Data Exposure*, *SQL Injection, Cross Site Scripting,* dan *Open Source Intelligent.*



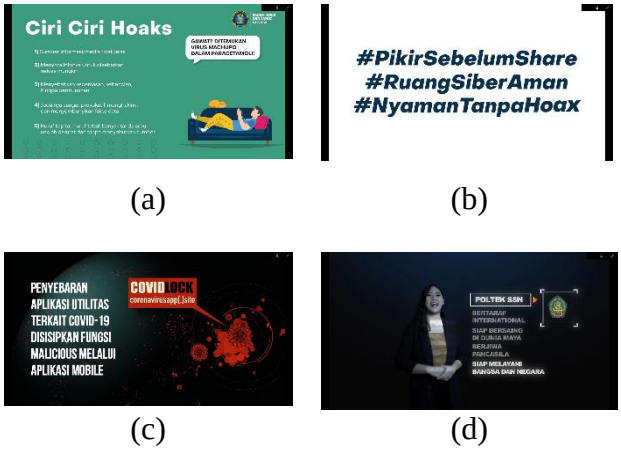
Gambar 8 Dokumentasi Materi "Teknologi Pengambil Informasi"

Gambar 9 Dokumentasi Materi "Rekayasa Sosial"



Gambar 10 Dokumentasi *Live Demonstration* oleh taruna Poltek SSN

Selama istirahat, peserta diimbau tidak meninggalkan *Zoom Meeting* dan dapat menonton video literasi mengenai keamanan informasi dan video profil Politeknik Siber dan Sandi Negara (Poltek SSN) sebagai upaya sosialisasi pengenalan Perguruan Tinggi Kedinasan. Tujuannya adalah untuk menemani peserta yang sedang istirahat dan juga menghindari berkurangnya peserta karena meninggalkan *Zoom Meeting* setelah istirahat. Beberapa dokumentasi video yang ditayangkan selama istirahat dapat dilihat pada Gambar 11.



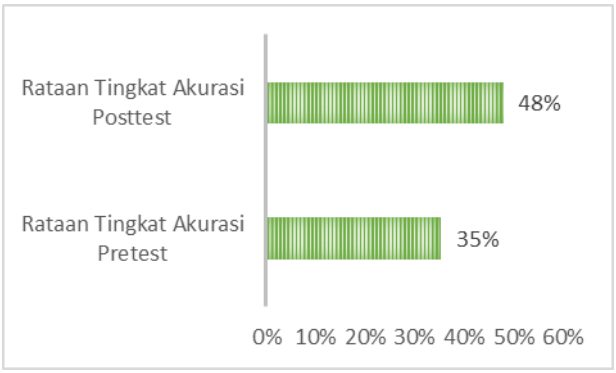
(a) (b)

(c) (d)

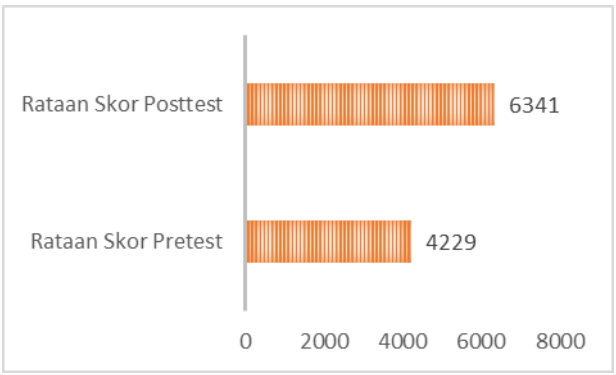
Gambar 11 Dokumentasi Video Saat Istirahat (Video Literasi dan Video Profil Poltek SSN)

Hasil Evaluasi dan Analisis Data

Sebagai upaya evaluasi dari kegiatan ini, dilakukan tes sebanyak dua kali yang dilaksanakan sebelum kegiatan inti (*pre-test*) dan setelah kegiatan inti (*posttest*). Selanjutnya, dilakukan pengujian beda dua rataan (*mean*) untuk mengetahui apakah terdapat peningkatan yang signifikan terhadap tingkat akurasi jawaban dan skor peserta *workshop* sebelum dan setelah kegiatan. Rata-rata tingkat akurasi dan skor peserta saat *pre-test* dan *posttest* dapat dilihat pada Gambar 12 dan Gambar 13.



Gambar 12 Rataan Tingkat Akurasi *Pretest* dan *Posttest*



Gambar 13 Rataan Skor *Pretest* dan *Posttest*

Secara deskriptif, jika dibandingkan antara rataan *pre-test* dan *posttest*, diperoleh kenaikan pada tingkat akurasi maupun skornya, sehingga dapat dikatakan bahwa kecepatan peserta menjawab dengan benar juga semakin meningkat. Artinya, kegiatan *workshop* ini mampu meningkatkan rataan tingkat akurasi dan skor peserta *workshop* masing-masing sebesar 13% dan 2112 poin. Selanjutnya, dilakukan pengujian beda *mean* untuk melihat secara umum, apakah terdapat perbedaan signifikan antara rata-rata skor *pre-test* dan *posttest* dengan menggunakan tingkat signifikansi 5%. Metode pengujian yang dilakukan tergantung pada sebaran data. Oleh karena itu, dilakukan uji kenormalan dengan Shapiro-Wilk (Razali, 2011; Keskin, 2006; Royston, 1995). Hasil pengujian dapat dilihat pada Tabel 2.

Tabel 2 Hasil Uji Kenormalan Data dengan Uji *Shapiro-Wilk*

Data Uji	Statistik Uji	*P-Value*
Tingkat Akurasi	0,8739	0.0008448
Skor	0,88238	0.001373

Berdasarkan Tabel 2, diperoleh *p-value* < 0,05 artinya data tidak menyebar normal. Oleh karena itu, untuk mengukur keefektifan kegiatan *workshop*, dilakukan uji beda rataan Wilcoxon. Hasil uji beda rataan Wilcoxon dapat dilihat pada Tabel 3.

Tabel 3 Hasil Uji Beda Rataan dengan Uji Wilcoxon

Data Uji	Statistik Uji	*P-Value*
Tingkat Akurasi	35,5	0,000648
Skor	51	1,588e-05

Berdasarkan Tabel 3, diperoleh nilai p < 0,05 dan karena rataan *posttest* lebih besar dibandingkan rataan *pre-test*, maka rangkaian kegiatan *workshop* ini dapat meningkatkan pemahaman peserta *workshop* mengenai keamanan informasi secara signifikan. Hal tersebut menjadi bukti secara ilmiah bahwa rangkaian kegiatan tersebut bermanfaat bagi peserta.

Kendala dalam Pelaksanaan Kegiatan

Kegiatan ini dilaksanakan secara daring melalui *Zoom Meeting*, kendala yang dialami adalah lambatnya jaringan internet hingga beberapa kali terputusnya koneksi internet peserta selama kegiatan berlangsung. Solusinya adalah tim menyarankan peserta untuk memilih tempat dengan fasilitas internet yang lebih stabil.

SIMPULAN

Kegiatan pengabdian kepada masyarakat (*online workshop*) ini diikuti oleh 105 (81%) dari 130 orang yang mendaftar. Rangkaian kegiatan *workshop* ini meliputi *pre-test, keynote speech* terkait Keamanan Informasi, penyampaian informasi oleh panelis terkait teknologi pengambil informasi dan rekayasa sosial, diskusi panel, *live demonstration*, dan *posttest*. Seluruh peserta dapat mengikuti kegiatan dengan lancar terutama saat diskusi panel, banyak peserta yang mengajukan pertanyaan terkait dengan keamanan informasi. Hal ini menunjukkan antusias peserta yang sangat baik. Hasil *pre-test* dan *posttest* dianalisis dan dilakukan pengujian. Hasil menunjukkan bahwa dengan tingkat signifikansi 5%,

kegiatan ini mampu meningkatkan pemahaman peserta kegiatan karena nilai *posttest* lebih besar dibandingkan nilai *pre-test*. Selanjutnya, rangkaian kegiatan pengabdian kepada masyarakat ini dapat dilakukan kembali di lokus yang berbeda untuk meningkatkan kesadaran dan pemahaman keamanan informasi di masyarakat. Saran kegiatan selanjutnya adalah untuk dapat melaksanakan kegiatan serupa dengan para pelajar sebagai pesertanya, dikarenakan pelajar masih rentan terhadap ancaman terhadap keamanan informasi terutama saat berselancar di media sosial.

DAFTAR PUSTAKA

Adikara, F., Sandfreni, & Alam, P. F. (2020). Penyuluhan mengenai keamanan dan kebenaran informasi digital saat pandemik covid-19. *Abdimas*, 6(4), 216–221.

Datereportal. (2021). *Digital: 2021 Indonesia*. (Online), (https://datareportal.com/reports/digital-2019-indonesia)

Ekawati, D. (2018). Perlindungan hukum terhadap nasabah bank yang dirugikan akibat kejahatan skimming ditinjau dari perspektif teknologi informasi dan perbankan. *Jurnal Unes Law Review*, 1(2), 157–171.

Heryanto, A., Stiawan, D., Arsalan, O., & Kurniati, R. (2018). Workshop teknik keamanan dalam menggunakan internet pada siswa smk di indralaya tahun 2018. *Prosiding Annual Research Seminar 2019 Computer Science and ICT*, 4(1), 31–33.

Hutagalung, D. D., Saprudin, & Megasari, D. (2022). Keamanan data dan informasi pada era digital pada remaja pondok pesantren daar el hikam ciputat. *AMMA: Jurnal Pengabdian Masyarakat*, 1(5), 444–452.

International Telecommunication Union. (2021). *Global Cybersecurity Index 2021*. (Online), (https://www.itu.int/pub/D-STR-GCI.01)

Keskin, S. (2006). Comparison of Several Univariate Normality Tests Regarding Type I Error Rate and Power of The Test in Simulation Based Small Samples. *Journal of Applied Science Research*, *2*(5), 296–300.

Razali, N. M. (2011). Power Comparisons of Shapiro-Wilk, Kolmogorov-Smirnov, Lilliefors and Anderson-Darling Tests. *Journal of Statistical Modeling and Analytics*, *2*(1), 21–33.

RDocumentation. (1970). *The R Stats Package*. (Online), (https://rdocumentation.org/packages/stats/versions/3.6.2)

Royston, P. (1995). Remark AS R94: A Remark on Algorithm AS180: The W-test for Normality. *Journal of the Royal Statistical Society*, *44*(4), 547–551.

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan penanggulangan pencurian data pribadi dalam media elektronik. *Jurnal HAM*, 11(2), 285–299.