JURNAL ABDI INSANI
Volume 11, Nomor 4, Desember 2024
http://abdiinsani.unram.ac.id. e-ISSN : 2828-3155. p-ISSN : 2828-4321

PENINGKATAN WAWASAN CYBER SECURITY AWARENESS DAN TEKNIK MELINDUNGI SMARTPHONE PADA TREN DIGITAL EKONOMI

Improvement Cyber Security Awareness Insight And Techniques To Protect Smartphone In The Digital Economy Trend

Subektiningsih[1*], Irma Rofni Wulandari[2], Anggun Anindya Sekarningrum[3], Muhammad Alfi Hidayat[1], Muhamad Baharudin[1]

[1]Informatika Universitas Amikom Yogyakarta, [2]Sistem Informasi Universitas Amikom Yogyakarta, [3]Ilmu Komunikasi Universitas Amikom Yogyakarta

Jalan Padjajaran, Ring Road Utara, Condongcatur, Depok, Sleman, Yogyakarta, 55283

[*]Alamat Korespondensi: subektiningsih@amikom.ac.id

(Tanggal Submission: 22 September 2024, Tanggal Accepted : 24 November 2024)

Kata Kunci :

Cyber security, security awareness, smartphone security, phishing, scam

Abstrak :

Mitra adalah anggota kelompok usaha HNI Sleman yang menggunakan *smartphone* dan media sosial dalam pemasaran produk. Dalam proses tersebut menggunakan koneksi internet dan berinteraksi dengan berbagai pengguna. Dalam penggunaan teknologi terdapat banyak manfaat, namun memiliki berbagai celah ancaman kejahatan siber. Oleh sebab itu, Mitra perlu memahami tentang dasar-dasar keamanan siber dan teknik-teknik melindungi *smartphone*. Tujuan dari pendampingan ini adalah untuk meningkatkan wawasan atau pengetahuan Mitra tentang keamanan siber yang berkaitan dengan aspek data, informasi dan perangkat yang digunakan. Metode kegiatan adalah dengan pendampingan dan penyajian materi. Dalam pelaksanaannya sebelum pendampingan dilakukan *pre-test* dan sesudah pendampingan dilakukan *post-test.* Hasil *pre-test* dan *post-test* akan dihitung nilai indeks dalam % untuk menginterpretasikan hasil pendampingan. Hasil yang diperoleh adalah tingkat kesadaran Mitra HNI Sleman tentang keamanan siber sesudah pendampingan sebesar 98,75%. Dalam hal ini serupa dengan peningkatan sebesar 70% dalam pengetahuan peserta tentang cara-cara menanggulangi ancaman kejahatan siber, Sebelum pendampingan sebesar 28,75% dan sesudah pendampingan tingkat wawasan peserta menjadi sebesar 98,75%. Sedangkan, tingkat pengetahuan peserta dalam melindungi *smartphone* berada pada 95% sesudah pendampingan. Dalam hal ini terjadi peningkatan sebesar 37,5% dengan kondisi awal sebelum pendampingan adalah 57,5%. Peserta pendampingan menjadi mengetahui tentang modus rekayasa sosial, model-model kejahatan siber dan cara menanggulanginya. Memanfaatkan fitur-fitur keamanan yang ada di dalam *smartphone* dan melengkapi dengan menerapkan 2FA, pembatasan akses perizinan aplikasi, dan manajemen *password* yang baik.

Key word :

Cyber security, security awareness, smartphone security, phishing, scam

Abstract :

Partners are HNI Sleman business group members who use smartphones and social media in product marketing. In the process, they use internet connections and interact with various users. The use of technology has many benefits, but there are various gaps in cybercrime threats. Therefore, Partners need to understand the basics of cybersecurity and techniques to protect smartphones. This assistance aims to increase the Partners' insight or knowledge about cybersecurity related to data, information, and devices. The activity is conducted through training and the presentation of materials. In its implementation, a pre-test is carried out before training, and a post-test is carried out after training. To interpret the training results, the pre-test and post-test results will be calculated as an index value in %. The results show that HNI Sleman Partners' awareness level about cybersecurity after training was 98.75%. In this case, it is similar to a 70% increase in participants' knowledge about how to deal with cybercrime threats; before training, it was 28.75%, and after training, the level of participant insight became 98.75%. Meanwhile, participants' knowledge of protecting smartphones was 95% after training. In this case, there was an increase of 37.5%, with the initial condition before the training being 57.5%. The training participants became aware of social engineering modes and cybercrime models and how to overcome them. Utilizing the security features available in smartphones and completing them by implementing 2FA, restricting application permission access, and good password management.

Panduan sitasi / citation guidance (APPA 7th edition) :

Subektiningsih., Wulandari, I. R., Sekarningrum, A. A., Hidayat, M. A., & Baharudin, M. (2024). Peningkatan Wawasan Cyber Security Awareness dan Teknik Melindungi Smartphone Pada Tren Digital Ekonomi. *Jurnal Abdi Insani, 11(4), 2386-2400*. https://doi.org/10.29303/abdiinsani.v11i4.2018

PENDAHULUAN

Pengembangan pada ekonomi digital menjadi katalisator utama untuk mendorong pertumbuhan perekonomian nasional (Yusuf, 2023). Keberadaan teknologi menjadi pendukung dalam berbisnis, bekerja dan belajar, proses tersebut menggunakan media yang berbasis digital (Azizi *et al.,* 2020). Para anggota kelompok usaha HNI Sleman menggunakan *smartphone* dan media sosial Instagram dalam proses pemasarannya. Menurut (Dewi & Avicenna, 2020) media sosial merupakan sebuah platform komunikasi yang menjadikan anggota kelompok dapat bersosialisasi dan berbagi informasi. Berdasarkan survei per Januari 2024 menyatakan jumlah *pengguna* media sosial di Indonesia 139 juta dengan pengguna Instagram sebesar 85,3% (We Are Social & Meltwater, 2024). Dalam (Hadi & Zakiah, 2021) menyatakan bahwa digital marketing adalah kegiatan pencarian pasar atau promosi melalui media digital yang dilakukan secara *online* menggunakan fasilitas internet dengan memanfaatkan berbagai sarana, sebagai contoh jejaring sosial.

Pemasaran secara *online* memberikan banyak keuntungan; antara lain meningkatkan jangkauan pasar, meningkatkan brand awareness, meningkatkan loyalitas pelanggan, dan menghemat biaya pemasaran (Afiffah *et al.,* 2022). Internet menjadi bagian utama dalam menunjang aktivitas tersebut. Berdasarkan survei APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) menyatakan pengguna internet di Indonesia tahun 2023 mencapai 215,63 juta. Jumlah tersebut meningkat 2,67% dibanding tahun sebelumnya dengan jumlah 210,03 juta pengguna (APJII, 2023). Internet dapat dimanfaatkan dalam proses bisnis, namun internet juga mempunyai celah. Oleh sebab itu, para

anggota kelompok usaha HNI Sleman sebaiknya mengetahui tentang dasar-dasar keamanan siber *(cyber security).*

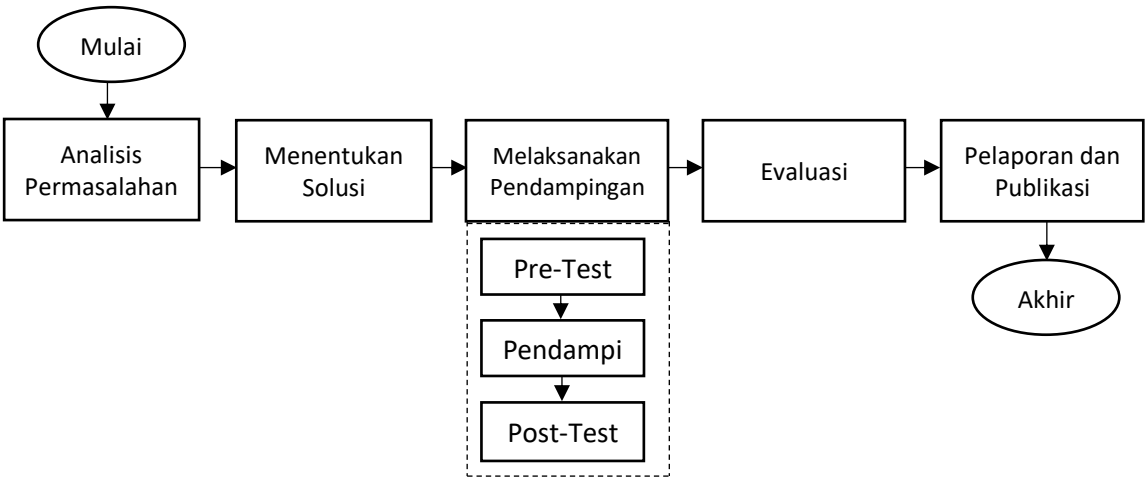
Anggota kelompok usaha HNI Sleman menggunakan media digital dan memanfaatkan internet untuk mempublikasikan berbagai informasi dan kegiatan yang dilakukan dalam pemasaran produknya. Pemanfaatan internet ini juga seiring dengan pengguna internet di Indonesia telah mencapai 202,35 juta orang yang berarti 76,8 persen dari penduduk Indonesia telah memanfaatkan internet (Darmawan, 2022). Hampir 94,9 persen pengguna internet di Indonesia mengakses internet melalui smartphone (Maulida, 2022). Indonesia juga menjadi negara kedua yang paling lama berselancar menggunakan smartphone yaitu dengan total penggunaan durasi internet harian sebanyak 59,4% (Maulida, 2022) (We Are Social, 2022). Pengguna internet juga dihimbau untuk dapat berhati – hati saat klik situs atau link dari sumber yang tidak terpercaya (Pole, 2021). Data untuk *login* media sosial yang digunakan perlu dijaga kerahasiaannya. Mengaktifkan *Two-Factor Authentication* (2FA) menjadi salah satu cara yang dapat dilakukan untuk menjaga keamanan akses. 2FA adalah verifikasi dua langkah untuk mengkonfirmasi identitas pengguna dan hak akses terhadap sistem atau akun.

Keamanan menjadi hal penting dikarenakan dalam media digital terdapat berbagai informasi yang perlu dijaga. Terdapat 3 aspek keamanan informasi yang perlu dipertimbangkan *Confidentiality (C), Integrity (I),* dan *Availability (A)* dikenal sebagai *triad CIA* (Winarianto & Daud, 2022). Kerahasiaan, integritas, dan ketersediaan dapat menghadapi ancaman yang bersifat teknis maupun non-teknis. Pengguna terkadang tidak mempunyai pengetahuan tentang ancaman kejahatan siber yang dapat dihadapi, sehingga tidak menerapkan perlindungan terhadap *smartphone*. Selain itu, pengguna tidak mengenali semua fungsi dan fitur yang ada pada *smartphone*. Permasalahan keamanan tidak hanya permasalahan teknis, namun terkait juga dengan pemahaman dan kesadaran pengguna. Meningkatkan pemahaman dan kesadaran pengguna menjadi upaya untuk mencegah kejahatan siber.

Berdasarkan uraian tersebut diperlukan peningkatan pemahaman tentang pentingnya dasar-dasar keamanan siber dan aspek keamanan informasi yang juga berkaitan dengan data dan informasi. Peningkatan kesadaran akan keamanan siber ini bukan hanya melalui media *online* yang digunakan, namun juga dalam perangkat yang digunakan untuk mengakses, yaitu smartphone. Oleh sebab itu, anggota kelompok usaha HNI Sleman sebagai Mitra dalam pengabdian ini perlu memahami tentang teknik-teknik melindungi *smartphone* yang perlu diterapkan. Peningkatan kesadaran keamanan siber ini akan dilakukan melalui pendampingan. Harapannya melalui kegiatan ini terjadi peningkatan dari para anggota kelompok usaha HNI Sleman tentang keamanan siber yang berkaitan dengan aspek informasi, media *online*, dan perangkat yang digunakan. Karena kejahatan siber bukan hanya berkaitan dengan teknis mengamankan perangkat, namun juga berkaitan dengan kesadaran keamanan dari pengguna.

METODE KEGIATAN

Model pelaksanaan pengabdian ini berupa seminar dan pendampingan dengan Mitra anggota kelompok usaha HNI Sleman yang berjumlah 10 orang yang terdiri dari Distributor Center HNI, Stock Center HNI, dan para agen HNI Sleman. Pelaksanaan program pada tanggal 20 dan 21 Agustus 2024 yang berlangsung di Hotel Ramada by Wyndham yang berada di Jl. Magelang No.KM 14, Jetis, Caturharjo, Kec. Sleman, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55515. Alur metode pelaksanaan di sajikan pada Bagan di Gambar 1.



Gambar 1. Alur Metode Kegiatan

Tahap-tahap yang dilakukan dalam metode kegiatan pada Gambar 1 antara lain:

1. Analisis Permasalahan
   Tahap pertama adalah berkoordinasi dengan Mitra HNI Sleman dan menganalisis permasalahan yang ada. Analisis permasalahan menggunakan *diagram fishbone* untuk menentukan korelasi sebab-akibat.
2. Menentukan Solusi
   Berdasarkan diagram *fishbone* akan ditentukan solusi yang sesuai untuk permasalahan yang teridentifikasi. Solusi berupa pendampingan tentang aspek keamanan informasi dan pendampingan dalam mengamankan *smartphone* yang disajikan pada Tabel 1.
3. Melaksanakan Pendampingan
   Pendampingan akan dilaksanakan selama 2 hari dengan materi yang berbeda. Pendampingan pertama materi berfokus pada *cyber security* secara umum yang dilanjutkan dengan pendampingan Mitra untuk penerapan teknik dalam melindungi *smartphone* dari ancaman-ancaman kejahatan digital. Sebelum pendampingan akan dilakukan *Pre-Test* untuk mengetahui tingkat wawasan mitra dan setelah pendampingan akan dilaksanakan *Post-Test* untuk mengetahui dampak dari materi yang disajikan.
4. Evaluasi
   Melakukan evaluasi kegiatan yang sudah dilaksanakan untuk mengukur keberhasilan dari pendampingan yang sudah dilaksanakan berdasarkan hasil *pre-Test* dan *post-Test.* Pelaksanaan *pre-test* dan *post-test* dilakukan menggunakan google form yang berbentuk skala 1-8 dipadukan dengan pertanyaan dengan pilihan jawaban.
5. Pelaporan dan Publikasi
   Tahap terakhir adalah menyajikan dokumentasi pendampingan dalam bentuk laporan dan publikasi hasil pendampingan ke dalam jurnal.

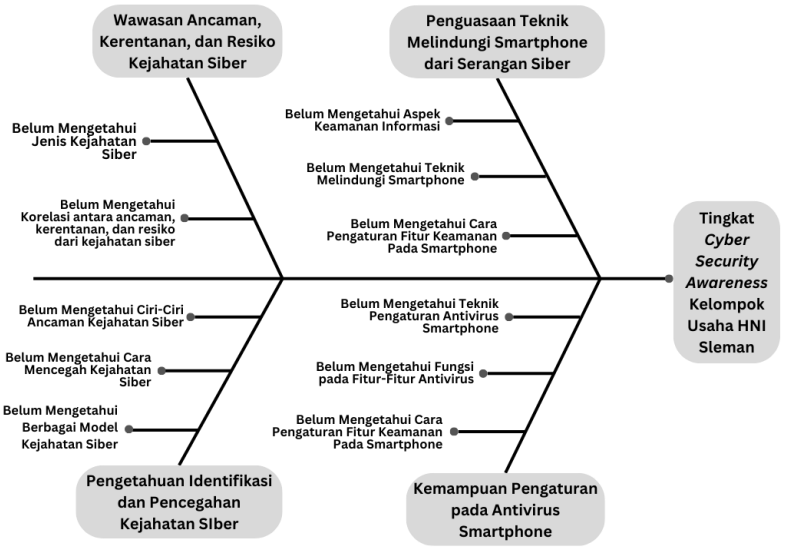
HASIL DAN PEMBAHASAN

Dalam pelaksanaan pengabdian dilakukan sesuai metode yang telah dijabarkan, yaitu:

1. Analisis Permasalahan

Pelaksanaan pengabdian dimulai dengan melakukan analisis terhadap permasalahan-permasalahan yang dialami oleh mitra. Dalam proses analisis menggunakan diagram *fishbone* yang digunakan untuk melihat keterkaitan antara sebab dan akibat dari suatu permasalahan (Subektiningsih & Yudaninggar, 2022). Penggunaan diagram *fishbone* karena dapat memvisualisasikan penyebab-penyebab dari permasalahan secara struktur dan sistematis. Sehingga, memudahkan dalam melihat korelasi antara penyebab yang mendasar dengan akibat yang ditimbulkan. Pengelompokan penyebab-

penyebab secara logis memudahkan dalam penentuan solusi. Hasil dari analisis permasalahan Mitra HNI Sleman menggunakan diagram *fishbone* ditunjukkan pada Gambar 2.



Gambar 2. Diagram *Fishbone* Permasalahan Mitra HNI Sleman

2. Menentukan Solusi

Berdasarkan diagram *fishbone* tersebut dirumuskan solusi kepada mitra untuk direalisasikan dalam bentuk pendampingan. Daftar solusi disajikan pada Tabel 1.

Tabel 1. Solusi untuk Permasalahan Mitra

Bidang/Aspek Kegiatan	Permasalahan	Solusi	Dampak
Aspek Sosial Kemasyarakatan (Kesadaran Keamanan Siber)	Kesadaran terhadap keamanan digital *(cyber security)* anggota kelompok usaha HNI Sleman yang masih rendah.	Pendampingan dasar yang berfokus pada *cyber security awareness* tentang ancaman, kerentanan, risiko dan jenis-jenis kejahatan siber	Pengetahuan tentang dasar-dasar keamanan siber
	Mitra belum mengetahui tentang model kejahatan siber dan cara menanggulanginya.	Pendampingan tentang cara identifikasi kejahatan siber berdasarkan perkembangan model-model kejahatan	Pengetahuan dan kemampuan teknis untuk mengidentifikasi model kejahatan siber
	Mitra belum mengetahui teknik untuk melindungi *smartphone* yang digunakan sebagai media pemasaran	Pendampingan tentang aspek keamanan informasi *(confidientality, integrity, availability)* dan penerapan teknik-teknik melindungi *smartphone* dengan mengaktifkan fitur keamanan pada smartphone	Pengetahuan dan kemampuan teknis untuk melindungi keamanan data, informasi, dan perangkat *smartphone*

		Pendampingan tentang instalasi antivirus smartphone dan pengaturan fitur-fitur pada antivirus.	Kemampuan teknis tentang pengaturan antivirus smartphone

3. Melaksanakan Pendampingan

Pelaksanaan program pengabdian untuk meningkatkan kesadaran keamanan siber dan penerapan teknik melindungi *smartphone* terdapat tiga pendampingan yang disajikan pada Tabel 2.

Tabel 2. Materi Pendampingan Keamanan Siber

Pendampingan Ke-	Waktu Pelaksanaan	Aspek Kegiatan	Materi Pendampingan
Pendampingan 1	20 Juli 2024 *(HalfDay)*	Sosial Kemasyarakatan	- Dasar keamanan siber - Keterkaitan tentang ancaman, kerentanan, dan risiko dalam keamanan siber - Jenis-jenis kejahatan siber - Model kejahatan siber - Cara mengantisipasi kejahatan siber
Pendampingan 2	21 Juli 2024 *(HalfDay)*	Sosial Kemasyarakatan	- Pengantar Smartphone - Aspek keamanan informasi *(confidentiality, integrity, availability)* - Ancaman keamanan smartphone - Vektor serangan smartphone - Cara melindungi smartphone - Mengaktifkan fitur keamanan smartp[hone - Instal dan pengaturan antivirus ESET Smartphone Security

Pada pelaksanaan pendampingan *cyber security* (keamanan siber) dalam rentang *halfday* yang berlangsung dari pukul 08.00 hingga 13.00 WIB. Dalam pelaksanaan pendampingan menggunakan model *pre-test* dan *post-test* untuk mengevaluasi ketercapaian dari peningkatan wawasan dan keahlian peserta. Setiap pendampingan akan disajikan hasilnya pada poin sebagai berikut:

a. Pendampingan 1 – Cyber Security Awareness

Pelaksanaan pendampingan *cyber security awareness* dibagi menjadi 2 sesi. Dalam sesi pertama diawali dengan *pre-test* yang dilanjutkan dengan materi berisi dasar keamanan siber dan berbagai jenis kejahatan siber. Sesi kedua dilanjutkan dengan diskusi tentang berbagai *case* nyata dari model kejahatan yang sering dilakukan untuk mengelabui korban. Pembahasan case kejahatan ini spesifik terhadap jenis kejahatan siber berupa *scam* dan *phishing*. Materi berikutnya adalah diberikan tentang cara-cara yang dapat dilakukan oleh peserta untuk mengantisipasi kejahatan siber. Anggota mitra harus menyadari bahwa kejahatan siber itu ada dan mempunyai berbagai pola untuk mendapatkan korbannya. Oleh sebab itu, para peserta harus mengetahui cara-cara yang dapat diterapkan untuk menanggulangi kejahatan tersebut secara mandiri. Dalam pelaksanaan pendampingan pada awal sesi diberikan *pre-test* dan di akhir sesi ditutup dengan *post-test* untuk mengevaluasi hasil pendampingan terhadap. Instrumen yang digunakan dalam evaluasi disajikan pada Tabel 3.

Tabel 3. Instrumen Evaluasi Pengetahuan Keamanan Siber

No.	Pertanyaan Evaluasi	Bentuk Respon
1.	Bagaimana tingkat pengetahuan dasar anda tentang keamanan siber?	Skala dengan nilai 1 - 8
2.	Bagaimana pengetahuan Anda tentang jenis ancaman kejahatan siber?	
3.	Bagaimana pengetahuan Anda dalam menanggulangi ancaman kejahatan siber?	
4.	Seberapa besar tingkat kewaspadaan saat menggunakan WiFi publik?	
5.	Seberapa besar tingkat kewaspadaan Anda saat mendapatkan pesan hadiah/uang dari sumber yang tidak diketahui/dikenal?	
6.	Apakah Anda menerapkan teknik keamanan 2FA *(Two Factor Authentication)* pada aplikasi email, media sosial, atau messanger?	Ya/Tidak
7.	Bagaimana manajemen Anda dalam pembuatan password?	Pilihan

Pada akhir pelaksanaan pendampingan 1 dilakukan sesi foto bersama untuk dokumentasi yang ditunjukkan pada Gambar 3.

Gambar 3. Dokumentasi Pendampingan 1 – *Cyber Security Awareness*

b. Pendampingan 2 – Teknik Melindungi Smartphone

Pelaksanaan pendampingan teknik melindungi *smartphone* dibagi menjadi 2 sesi. Dalam sesi pertama diawali dengan *pre-test* yang dilanjutkan dengan materi berisi pengantar tentang smartphone dan berbagai jenis sistem operasi yang digunakan. Materi juga bersinggungan dengan aspek keamanan informasi dan berbagai jenis ancaman keamanan smartphone. Mengenali vektor serangan *smartphone* dan resiko yang dapat dialami oleh korban. Sesi kedua dilanjutkan dengan penerapan teknik melindungi *smartphone* berdasarkan *security guideline* dari EC-Council (EC-Council, 2011.)

Dalam sesi ini peserta melakukan praktik secara langsung menggunakan *smartphone* masing-masing. Peserta mengikuti setiap sesi dengan penuh antusias. Banyak pertanyaan dan diskusi selama pendampingan berlangsung. Selanjutnya, setiap peserta akan diberikan arahan untuk melindungi *smartphone* masing-masing dengan menginstal antivirus ESET Mobile Security (ESET, 2024). Pemilihan Smartphone ESET Smart security ini dikarenakan anti-virus dilengkapi dengan fitur *anti-phising.* Masing-masing peserta diberikan layanan ESET Mobile Security versi premium. Sesi diakhiri dengan *post-test* kepada peserta pendampingan. Dalam pelaksanaan pendampingan pada awal sesi diberikan *pre-test* dan diakhir sesi ditutup dengan *post-test* untuk mengevaluasi hasil pendampingan terhadap. Instrumen yang digunakan dalam evaluasi disajikan pada Tabel 4.

Tabel 4. Instrumen Evaluasi Pengetahuan Teknik Melindungi *Smartphone*

No.	Pertanyaan Evaluasi	Bentuk Respon
1.	Seberapa penting untuk selalu memperbaharui aplikasi dan sistem operasi android?	Skala dengan nilai 1 - 8
2.	seberapa sering anda memeriksa dan melakukan update/pembaharuan **Aplikasi** yang diinstal pada *smartphone*?	
3.	seberapa sering anda memeriksa dan melakukan update/pembaharuan **Sistem Operasi (android)** yang diinstal pada *smartphone*?	
4.	Seberapa Penting data-data dan informasi yang ada dalam Smartphone anda?	
5.	Seberapa penting instal anti-virus pada *smartphone?*	
6.	Seberapa sering anda akan melakukan scanning/pembersihan files dan sistem pada *smartphone* anda?	
7.	Bagaimana tingkat pengetahuan Anda dalam upaya untuk mengamankan/melindungi *smartphone yang* dimiliki?	
8.	Apa alasan Anda jarang/tidak melakukan pembaharuan aplikasi dan sistem operasi?	Pilihan

Pada akhir pendampingan dilakukan dokumentasi dengan seluruh peserta ditunjukkan Gambar 4.

Gambar 4. Dokumentasi Pendampingan 2 – Teknik Melindungi *Smartphone*

4. Evaluasi

Evaluasi kegiatan yang sudah dilaksanakan untuk mengukur keberhasilan dari pendampingan yang sudah dilaksanakan berdasarkan hasil *pre-Test* dan *post-Test.* Dalam pendampingan pertama dilakukan tahap evaluasi dengan cara penyajian hasil *pre-test* dan *post-test* dengan rentang penilaian 1 – 8 jenis instrumen dengan skala. Nilai 1 berarti Tidak Mengetahui/waspada hingga Nilai 8 yang berarti Sangat Mengetahui/waspada. Hasil evaluasi disajikan berdasarkan instrumen yang telah disusun untuk diperoleh nilai total. Nilai yang diberikan oleh responden akan diinterpretasikan berdasarkan perhitungan skor yang diperoleh. Interpretasi Penyelesaian akhir dihitung berdasarkan nilai indeks dalam persen dengan formula yang digunakan adalah sebagai berikut (Fajri, 2023):

$$\text{Indeks \%} = \frac{Total\ Nilai}{Y} \times 100$$

Keterangan:
Total Nilai : Nilai skala x jumlah responden yang memilih pada nilai skala tersebut
Y : Nilai tertinggi skala X jumlah responden

Tahap berikutnya adalah menghitung Nilai Total dan Nilai Indeks berdasarkan hasil kuesioner sebelum *(pre-test)* dan sesudah *(post-test)* pendampingan. Responden yang juga menjadi peserta dalam pendampingan ini adalah 10 orang. Dalam mencari nilai indeks diperlukan Nilai Y, yang diperoleh dari nilai tertinggi skala (8) dikalikan dengan jumlah responden (10), maka Nilai Y adalah 80. Nilai indeks untuk menginterpretasikan hasil kuesioner akan disajikan pada poin berikut:

a. Pendampingan 1 – Cyber Security Awareness

Hasil instrumen evaluasi pendampingan pertama, sebelum pendampingan ditunjukkan pada Tabel 5 dan sesudah pendampingan pada Tabel 6.

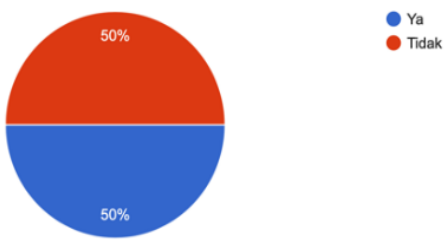
Tabel 5. Tabel Pre-Test Pendampingan 1 – Cyber Security Awareness

No.	Pertanyaan Evaluasi	1	2	3	4	5	6	7	8	Total Nilai	Indeks %
1.	Bagaimana tingkat pengetahuan dasar anda tentang keamanan siber?	2	1	0	1	3	2	1	0	42	52,5
2.	Bagaimana pengetahuan Anda tentang jenis ancaman kejahatan siber?	3	1	2	2	1	1	0	0	30	37,5
3.	Bagaimana pengetahuan Anda dalam menanggulangi ancaman kejahatan siber?	3	3	2	2	0	0	0	0	23	28,75
4	Seberapa besar tingkat kewaspadaan saat menggunakan WiFi publik?	0	0	2	4	3	0	1	0	44	55
5	Seberapa besar tingkat kewaspadaan Anda saat mendapatkan pesan hadiah/uang dari sumber yang tidak diketahui/dikenal?	0	0	2	2	1	2	3	0	52	65

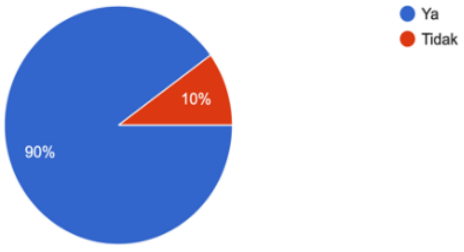
Tabel 6. Tabel Post-Test Pendampingan 1 – Cyber Security Awareness

No.	Pertanyaan Evaluasi	1	2	3	4	5	6	7	8	Total Nilai	Indeks %
1.	Bagaimana tingkat pengetahuan dasar anda tentang keamanan siber?	0	0	0	0	0	1	6	3	72	90
2.	Bagaimana pengetahuan Anda tentang jenis ancaman kejahatan siber?	0	0	0	0	0	0	4	6	76	95
3.	Bagaimana pengetahuan Anda dalam menanggulangi ancaman kejahatan siber?	0	0	0	0	0	0	1	9	79	98,75
4	Seberapa besar tingkat kewaspadaan saat menggunakan WiFi publik?	0	1	0	0	1	0	1	7	70	87,5
5	Seberapa besar tingkat kewaspadaan Anda saat mendapatkan pesan hadiah/uang dari sumber yang tidak diketahui/dikenal?	0	0	0	0	0	0	1	9	79	98,75

Pada instrumen berikutnya adalah tentang Penerapan Teknik Keamanan 2FA *(Two Factor Authentication)"*. Hasil sebelum pendampingan menyatakan 50% peserta sudah menerapkan 2FA dan 50% belum menerapkan teknik keamanan ini. Setalah pendampingan mengalami peningkatan sebesar 40%, yaitu 90 peserta mengaktifkan teknik keamanan dua arah atau *Two Factor Authentication.* Hasil penerapan 2FA sebelum pendampingan ditunjukkan pada Gambar 5 dan sesudah pendampingan pada Gambar 6.

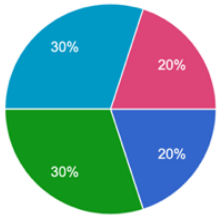


Gambar 5. 2FA Sebelum Pendampingan

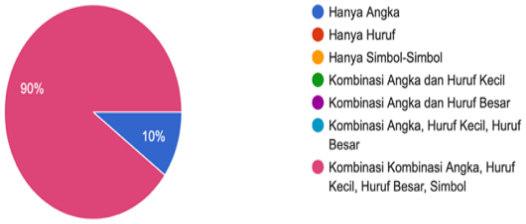


Gambar 6. 2FA Sesudah Pendampingan

Evaluasi terakhir adalah tentang “Manajemen Dalam Pembuatan password”. Kriteria password yang baik (password ideal) adalah disusun menggunakan kombinasi huruf besar, huruf kecil, angka, dan simbol. Sebelum pendampingan yang menyatakan menggunakan password ideal hanya 20%, namun setelah pendampingan mengalami peningkatan sebesar 70%, yaitu 90% peserta menyatakan penggunaan password kombinasi dan 10% atau 1 peserta memilih untuk tetap menggunakan password angka saja. Hasil manajemen *password* sebelum pendampingan ditunjukkan pada Gambar 7 dan Sesudah pendampingan pada Gambar 8.

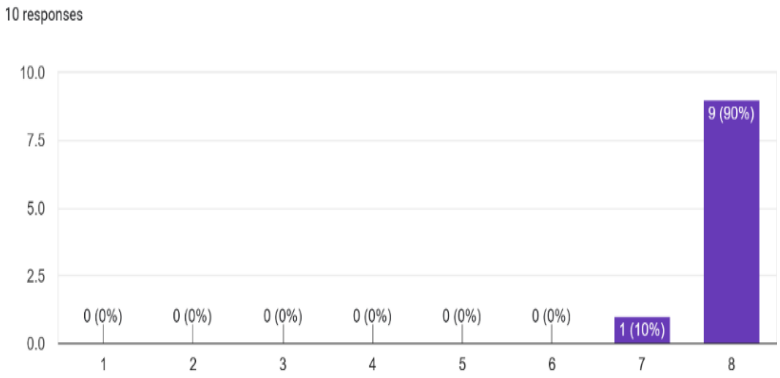


Gambar 7. Sebelum Pendampingan



Gambar 8. Sesudah Pendampingan

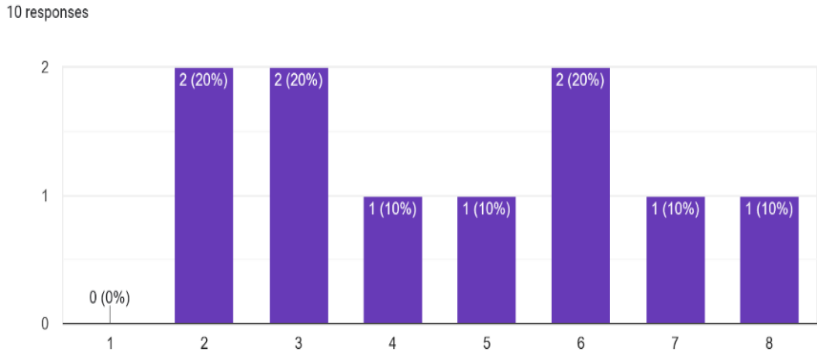
Berdasarkan pendampingan pertama yang telah dilakukan menyatakan bahwa 98,75% peserta menjadi sadar atau *aware* tentang keamanan siber. Hal ini dibuktikan pada Gambar 9 tentang tingkat wawasan atau pengetahuan peserta tentang keamanan siber sesudah pendampingan. Skala 7 dan 8 menyatakan sangat pentingnya pengetahuan tentang keamanan siber. Mitra menjadi sadar dan paham dalam mengidentifikasi berbagai model kejahatan dan cara menanggulanginya. Terjadi peningkatan karena sebelum dilaksanakan pendampingan tingkat *awareness* mitra adalah 52,5%.



Gambar 9. Tingkat Kesadaran Peserta Tentang Wawasan Keamanan Siber

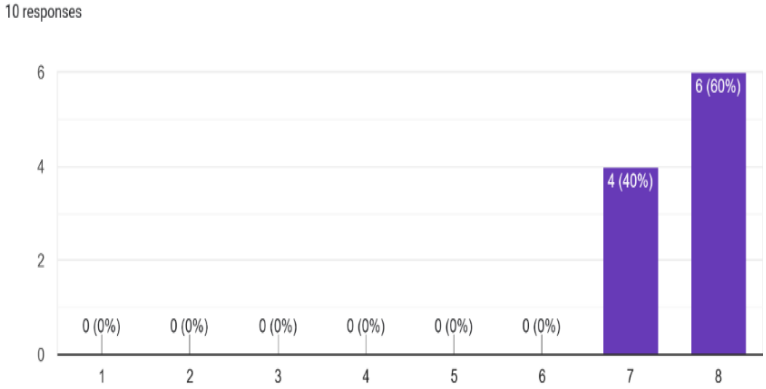
b. Pendampingan 2 – Teknik Melindungi Smartphone

Hasil *pre-test* yang menggunakan basis skala 1 – 8 dinyatakan dengan sumbu X dan Y, di mana X menyatakan skala dari tingkat pengetahuan/keterampilan dan Y adalah jumlah peserta (10 orang). sebelum pendampingan menyatakan bahwa pengetahuan peserta dalam penguasaan teknik mengamankan smartphone beragam. Sebesar 20% peserta menyatakan tidak mengetahui dalam upaya mengamankan smartphoe, 30% menyatakan cukup mengetahui, dan 30% menyatakan mengetahui tentang cara mengamankan smartphone. Sedangkan, 20% menyatakan sudah sangat mengetahui cara-cara dalam mengamankan smartphone. Hasil *pre-test ini* disajikan pada Gambar 10.



Gambar 10. Tingkat Penguasaan Teknik Melindungi Smartphone Sebelum Pendampingan

Pada akhir pendampingan dilakukan *post-test* untuk mengetahui hasil dari peningkatan pengetahuan peserta. Hasil evaluasi menyatakan bahwa 95% peserta menjadi sangat menguasai teknik-teknik dalam melindungi smartphone dari kejahatan siber yang dimungkinkan menyerang. Sajian hasil evaluasi ada pada Gambar 11.



Gambar 11. Tingkat Penguasaan Teknik Melindungi Smartphone Sesudah Pendampingan

Pada Pendampingan 2 nilai skala adalah 1 yang berarti Tidak Penting/Tidak Sering (Tidak Pernah) hingga Sangat Penting/Sangat Sering (Selalu) adalah 8. Hasil instrumen evaluasi pendampingan 2 tentang teknik melindungi *smartphone* sebelum pendampingan ditunjukkan pada Tabel 7 dan Sesudah pendampingan pada Tabel 8.

Tabel 7. Tabel Pre-Test Pendampingan 2 – Teknik Melindungi Smartphone

No.	Pertanyaan Evaluasi	1	2	3	4	5	6	7	8	Total Nilai	Indeks %
1.	Seberapa penting untuk selalu memperbaharui aplikasi dan sistem operasi android?	1	1	3	0	0	2	1	2	47	58,75
2.	Seberapa sering anda memeriksa dan melakukan update/pembaharuan **Aplikasi** yang diinstal pada *smartphone*?	1	1	2	1	1	3	1	0	43	53,75
3.	Seberapa sering anda memeriksa dan melakukan update/pembaharuan **Sistem Operasi (android)** yang diinstal pada *smartphone*?	3	1	1	1	2	1	1	0	35	43,75
4	Seberapa Penting data-data dan informasi yang ada dalam *smartphone* anda?	0	1	0	0	1	0	1	7	70	87,5

5	Seberapa penting instal anti-virus pada *smartphone*?	0	0	1	1	1	2	1	4	63	78,75
6	Seberapa sering anda akan melakukan scanning/pembersihan files dan sistem pada *smartphone* anda?	0	2	0	2	2	1	1	2	51	63,75
7	Bagaimana tingkat pengetahuan Anda dalam upaya untuk mengamankan/melindungi *smartphone* yang dimiliki?	0	2	2	1	1	2	1	1	46	57,5

Tabel 8. Tabel Post-Test Pendampingan 2 – Teknik Melindungi Smartphone

No.	Pertanyaan Evaluasi	1	2	3	4	5	6	7	8	Total Nilai	Indeks %
1.	Seberapa penting untuk selalu memperbaharui aplikasi dan sistem operasi android?	0	0	0	0	0	0	2	8	78	97,5
2.	seberapa sering anda memeriksa dan melakukan update/pembaharuan **Aplikasi** yang diinstal pada *smartphone*?	0	0	0	0	1	0	2	7	75	93,75
3.	seberapa sering anda memeriksa dan melakukan update/pembaharuan **Sistem Operasi (android)** yang diinstal pada *smartphone*?	0	0	0	0	0	0	3	7	77	96,25
4	Seberapa Penting data-data dan informasi yang ada dalam *smartphone* anda?	0	0	0	0	0	0	2	8	78	97,5
5	Seberapa penting instal anti-virus pada *smartphone*?	0	0	0	0	0	0	1	9	79	98,75
6	Seberapa sering anda akan melakukan scanning/pembersihan files dan sistem pada *smartphone* anda?	0	0	0	0	0	0	3	7	77	96,25
7	Bagaimana tingkat pengetahuan Anda dalam upaya untuk mengamankan/melindungi *smartphone* yang dimiliki?	0	0	0	0	0	0	4	6	76	95

Nilai indeks % *pre-test* dan *post-test* akan dibandingkan untuk memperoleh peningkatan (dalam %) yang terjadi. Perhitungan peningkatan ini dilakukan untuk hasil pada Pendampingan 1 dan Pendampingan 2. Hasil perbandingan *pre-test* dan *post-test* Pendampingan 1 ditunjukkan pada Tabel 9. Sedangkan, untuk Pendampingan 2 di tunjukkan pada Gambar 10.

Tabel 9. Peningkatan Hasil Evaluasi Sebelum *(pre-test)* dan Sesudah *(post-test)* Pendampingan 1

No.	Pertanyaan Evaluasi	Hasil Sebelum Pendampingan	Hasil Setelah Pendampingan	Peningkatan
1.	Bagaimana tingkat pengetahuan anda tentang keamanan siber?	52,5%	90%	37,5%
2.	Bagaimana pengetahuan Anda tentang jenis ancaman kejahatan siber?	37,5%	95%	57,5%
3.	Bagaimana pengetahuan Anda dalam menanggulangi ancaman kejahatan siber?	28,75%	98,75%	70%
4.	Seberapa besar tingkat kewaspadaan	55%	87,5%	32,5%

	saat menggunakan WiFi publik?			
5.	Seberapa besar tingkat kewaspadaan Anda saat mendapatkan pesan hadiah/uang dari sumber yang tidak diketahui/dikenal?	65%	98,75%	33,75%
6.	Apakah Anda menerapkan teknik keamanan 2FA *(Two Factor Authentication)* pada aplikasi email, media sosial, atau messanger?	50%	90%	40%
7.	Bagaimana manajemen Anda dalam pembuatan password *(Password ideal adalah kombinasi Huruf Besar, Huruf Kecil, Angka, dan Simbol)?*	20%	90%	70%

Tabel 10. Peningkatan Hasil Evaluasi Sebelum *(pre-test)* dan Sesudah *(post-test)* Pendampingan 1

No.	Pertanyaan Evaluasi	Hasil Sebelum Pendampingan	Hasil Setelah Pendampingan	Peningkatan
1.	Seberapa penting untuk selalu memperbaharui aplikasi dan sistem operasi android?	58,75%	97,5%	38,75%
2.	seberapa sering anda memeriksa dan melakukan update/pembaharuan **Aplikasi** yang diinstal pada smartphone?	53,75%	93,75%	40%
3.	seberapa sering anda memeriksa dan melakukan update/pembaharuan **Sistem Operasi (android)** yang diinstal pada *smartphone*?	43,75%	96,25%	52,5%
4.	Seberapa Penting data-data dan informasi yang ada dalam s*martphone anda*?	87,5%	97,5%	10%
5.	Seberapa penting instal anti-virus pada smartphone?	78,75%	98,75%	20%
6.	Seberapa sering anda akan melakukan scanning/pembersihan files dan sistem pada *smartphone* anda?	63,75%	96,25%	32,5%
7.	Bagaimana tingkat pengetahuan Anda dalam upaya untuk mengamankan/melindungi *smartphone* yang dimiliki?	57,5%	95%	37,5%

Berdasarkan hasil dari nilai indeks sebelum dan sesudah pendampingan memperoleh hasil bahwa pendampingan 1 dan pendampingan 2 semua peserta mengalami peningkatan pengetahuan atau wawasan. Pada Pendampingan 1 peningkatan paling besar terjadi pada manajemen password, yaitu 70% peserta menjadi sadar bahwa password yang ideal terdiri dari kombinasi huruf besar, huruf kecil, angka, dan simbol. Sedangkan peningkatan paling rendah berada pada kewaspadaan dalam menggunakan WiFi publik. Sesudah pendampingan hanya terjadi peningkatan sebesar 32,5%. Hal ini terjadi dikarenakan para peserta sudah berhati-hati dalam menggunakan Wi-Fi publik dan sesudah pendampingan mereka menjadi lebih waspada akan keamanan data dan informasi yang dibagikan.

Pada pendampingan 2 peningkatan paling besar terjadi pada frekuensi dalam memeriksa pembaharuan pada sistem. Memperbaharui sistem operasi pada smartphone menjadi hal yang penting

karena aktivitas ini bertujuan untuk memperbaiki apabila dalam sistem terdapat celah kerentanan. Dalam frekuensi pembaharuan sistem operasi ini mengalami peningkatan sebesar 52,5%. Selain itu, melakukan pembersihan atau *scanning files* dan *system* pada smartphone menjadi langkah yang penting karena berkaitan dengan kinerja smartphone. Sedangkan, peningkatan paling rendah pada Pendampingan 2 terjadi pada seberapa pentingnya data dan informasi dimiliki. Peningkatan terjadi sebesar 10% saja, hal ini terjadi karena dari awal pendampingan para peserta yaitu Mitra HNI Sleman sudah menyadari tentang pentingnya keamanan data dan informasi.

Tingkat kesadaran Mitra HNI Sleman tentang keamanan siber sesudah pendampingan adalah 98,75%. Hal ini menyatakan bahwa para peserta pendampingan telah mengetahui tentang berbagai ancaman dari kejahatan siber dan risiko yang dapat dialami apabila menjadi korban. Para peserta menjadi mengetahui tentang model-model kejahatan siber dan cara menanggulanginya. Peserta menjadi mengetahui tentang rekayasa sosial *(social engginering)* yang sering digunakan oleh pelaku kejahatan untuk mendekati korban. Selain itu, para peserta pendampingan lebih memanfaatkan fitur-fitur keamanan yang ada di dalam *smartphone* mereka dan melengkapinya dengan menerapkan 2FA, pembatasan akses perizinan aplikasi, dan manajemen password yang baik. Kejahatan siber bukan hanya berkaitan dengan teknis mengamankan perangkat, namun juga berkaitan dengan kesadaran keamanan dari pengguna.

5. Pelaporan dan Publikasi

Pelaporan pelaksanaan pendampingan dilakukan untuk mendokumentasikan dari setiap aktivitas yang telah dilakukan. Dalam pengabdian ini terdapat luaran berupa Jurnal dan Buku Panduan Keamanan Siber dan Teknik Melindungi *Smartphone.* Peran Mitra adalah mengkoordinasikan anggota-anggota kelompok usaha HNI Sleman untuk menjadi peserta dalam pendampingan ini. Kendala yang dialami selama pelaksanaan pengabdian adalah tantangan dalam penyampaian materi yang harus menerjemahkan bahasa teknis ke dalam bahasa sehari-hari. Penyelesaian dari kendala ini adalah menggunakan analogi-analogi sederhana untuk membuat peserta memahami konteks materi yang disampaikan. Sebagai contoh, dalam materi keamanan smartphone yang berkaitan dengan *backdoor* adalah menganalogikan dengan rumah dan akses pintu belakang. Kendala berikutnya adalah waktu kedatangan peserta yang bervariasi, sehingga perlu menyesuaikan waktu pelaksanaan supaya sesuai dengan *rundown* acara.

KESIMPULAN DAN SARAN

Hasil dari pendampingan terdapat peningkatan kesadaran keamanan siber yang signifikan sebelum pendampingan dan setelah pendampingan. Hal ini dibuktikan dengan hasil *pre-test* dan *post-test* yang dilakukan. Hasil menunjukkan 98,75% peserta pendampingan menyatakan telah mengetahui dan mengetahui cara menanggulangi ancaman kejahatan siber. Hasil ini menunjukkan peningkatan sebesar 70% yang awalnya tingkat pengetahuan peserta sebesar 28,75%. Seluruh peserta juga menjadi sadar untuk tidak sembarang klik link. Peserta memilih meningkatkan keamanan akses akun menggunakan *password* kombinasi dengan angka, huruf kapital, huruf kecil, serta simbol. Peserta juga memutuskan untuk selalu melakukan pembaharuan sistem operasi dan aplikasi walaupun pada awal pre-test menyatakan 50% mereka tidak melakukan pembaharuan karena media penyimpanan penuh. Hal ini sebanding dengan hasil tingkat pengetahuan peserta dalam upaya melindungi *smartphone* yang dimiliki sebesar 95%. Dalam hal ini mengalami peningkatan sebesar 37,5% dengan hasil sebelum pendampingan sebesar 57,5%. Keberadaan teknologi memang mempunyai berbagai manfaat, namun juga mempunyai berbagai celah kerentanan yang dapat dieksploitasi untuk menyebabkan risiko terhadap penggunanya. Oleh sebab itu, pengguna harus menyadari tentang ancaman kejahatan siber dan berbagai cara yang dapat diterapkan untuk menanggulanginya, sehingga dapat terhindar dari risiko yang berkaitan dengan data, informasi, dan hak akses. Saran untuk pendampingan berikutnya adalah tentang keamanan konten digital. Kelompok Usaha HNI Sleman selain menggunakan *smartphone* untuk pemasaran juga menggunakan berbagai bentuk media digital untuk dipublikasikan pada sosial media. Media digital yang digunakan berupa gambar dan video. Penggunaan media digital yang dipublikasikan melalui sosial media perlu dilindungi supaya terhindar dari pencurian, plagiasi,

maupun penggunaan tanpa izin. Oleh sebab itu, dalam hal ini dapat dilakukan pendampingan berikutnya tentang teknik perlindungan media digital menggunakan watermark maupun *digital signature*.

UCAPAN TERIMA KASIH

Terima kasih kepada Direktorat Riset, Teknologi, dan Pengabdian kepada Masyarakat (DRTPM) Direktorat Jenderal Pendidikan Tinggi Kementerian Pendidikan, kebudayaan, Riset dan Teknologi atas Pendanaan pada Program Pengabdian kepada Masyarakat Skema Pemberdayaan Kemitraan Masyarakat tahun 2024.

DAFTAR PUSTAKA

Afiffah, S. R., Fortuna, O. D., Kusumah, T. M., & Fauzi, A. (2022). Penerapan Strategi Digital Marketing Model AIDA Dalam Pemberdayaan Masyarakat Kelompok Usaha Bersama (KUBE) Cakrawala, Rawalumbu, Kota Bekasi. *Jurnal Abdi Masyarakat Indonesia*, *2*(2), 623–630. https://doi.org/10.54082/jamsi.286

APJII. (2023). *Internet Indonesia*. Retrieved from https://apjii.or.id

Azizi, M., Umiyati, H., Nugroho, L., Utami, A. R., Sudirman, A., Aryani, L., Irwansyah, R., Purbowo, Mardiana, S., Witi, F. L., Pratiwi, C. P., Syahputra, Hanika, I. M., & Johassan, D. M. R. Y. (2020). Effective Digital Marketing. In Suparyanto dan Rosad (Eds.), *Journal of Digital Business*, *5*(3).

Darmawan, H. (2022). Kemenkominfo Mencatat Jumlah Pengguna Internet di Indonesia Mencapai 202,35 juta orang. *Tribunnews*. Retrieved from https://www.tribunnews.com

Dewi, W. W. A., & Avicenna, F. (2020). Social Media Marketing: Consumer Behavior on The Cruelty-Free Concern of Beauty Brands. *Jurnal Ilmu Komunikasi*, *17*(1), 95–106. https://doi.org/10.31315/jik.v17i1.2379

EC-Council. (2011). *Securing mobile devices*. EC-Council Press.

ESET. (2024). *ESET Mobile Security untuk Android*. Retrieved from https://www.eset.com/id/home/mobile-security-android/

Fajri, D. L. (2023). Pengertian, Rumus, dan Cara Menghitung Skala Likert. Retrieved from https://katadata.co.id

Hadi, D. F., & Zakiah, K. (2021). Strategi Digital Marketing Bagi UMKM (Usaha Mikro Kecil dan Menengah) Untuk Bersaing di Era Pandemi. *Competitive*, *16*(1), 32–41. Retrieved from http://ejurnal.poltekpos.ac.id/index.php/competitive%7C32

Maulida, L. (2022). Lebih dari 90 Persen Warganet Indonesia Mengakses Internet Lewat Ponsel. *Kompas.com*. Retrieved from https://www.kompas.com

Pole, M. N. (2021). Pentingnya Perlindungan Data Pribadi Serta Tips Mencegah Kejahatan Cyber Crime. Retrieved from https://kominfo.kotabogor.go.id

Subektiningsih, S., & Yudaninggar, K. S. (2022). Pemanfaatan Website Sebagai Media Promosi Untuk Meningkatkan Minat Calon Peserta Didik Pada Sekolah Dasar Negeri Sumberagung Sleman. *Kacanegara: Jurnal Pengabdian Pada Masyarakat*, *5*(2), 135–142. https://doi.org/10.28989/kacanegara.v5i2.1129

We Are Social. (2022). *Digital 2022: Global Overview Report*. Retrieved from https://www.hootsuite.com/resources/digital-trends

We Are Social., & Meltwater. 2024. *Digital Indonesia 2024*. Retrieved from https://wearesocial.com

Winarianto, P., & Daud, D. E. (2022). CIA Triad. Retrieved from https://student-activity.binus.ac.id/csc/2022/08/cia-triad/

Yusuf. (2023). Pemerintah Siapkan Tiga Fase Transformasi Digital Nasional. *Kementerian Komunikasi dan Informatika Republik Indonesia*. Retrieved from https://www.kominfo.go.id/content/detail/53419/pemerintah-siapkan-tiga-fase-transformasi-digital-nasional/0/berita

