SWADIMAS
JURNAL PENGABDIAN KEPADA MASYARAKAT
VOL 03 NO 01 JANUARI 2025
ISSN 2964-8297 (p-issn) | 2964-8289 (e-issn)

# EDUKASI KEAMANAN SIBER DI KOMUNITAS YOUNG OZER INDONESIA SEBAGAI UPAYA MENGURANGI RISIKO TINDAK KEJAHATAN SIBER

**Ike Kurniati[1)], Andy Dharmalau[2)], Hari Suryantoro[3)], Jamah Sari[4)], Septiana Ningtyas[5)], Khusnul Khoriyah[6)], Heru Winarno[7)], Harun Ar-Rasyid[8)]**

[1,8]Prodi Sains Data, Fakultas Teknologi, ITB Swadharma Jakarta
[2,3,5,6,7]Prodi Teknik Informatika, Fakultas Teknologi, ITB Swadharma Jakarta
[4]Prodi Sistem Informasi, Fakultas Teknologi, ITB Swadharma Jakarta

Correspondence author: A. Dharmalau, andy.d@swadharma.ac.id, Jakarta, Indonesia

**Abstract**

The large number of cases of cyber attacks encourages the need for more substantial efforts to understand and overcome them. For this reason, education is needed to increase awareness of cybersecurity threats and reduce the risk of cybercrime. This community service activity is carried out in the Young Ozzer Indonesia community through education and discussions regarding Cyber Crime and cyber security, including email, smartphones and social media. The results of the community service activities are increased knowledge, understanding and awareness of participants regarding cyber security. The increasing knowledge is measured from the post-test results, which show an increase in the scores obtained by participants after the education was carried out; namely, 10 out of 11 (91%) of the participants got a score of 60 or more, and only 1 participant got a score of 50.

***Keywords:*** *education, cyber security, risk of cybercrime, awareness, community*

**Abstrak**

Banyaknya kasus serangan siber, mendorong perlunya upaya yang lebih kuat dalam memahami dan mengatasinya. Untuk itu diperlukan edukasi untuk dapat meningkatkan kesadaran dan kewaspadaan terhadap ancaman keamanan siber untuk mengurang risiko kejahatan siber. Kegiatan pengabdian masyarakat ini dilakukan di komunitas Young Ozzer Indonesia dalam bentuk Edukasi dan diskusi mengenai *Cyber Crime* dan keamanan siber yang meliputi *email*, *smartphone* dan media sosial. Hasil kegiatan pengabdian masyarakat yang dilakukan adalah meningkatnya pengetahuan, pemahaman dan kesadaran peserta dalam hal keamanan siber. Hal ini diukur dari hasil *Post Test* yang menunjukan peningkatan nilai yang diperoleh peserta setelah dilaksanakan edukasi yaitu 10 dari 11 (91%) dari peserta memperoleh nilai 60 atau lebih dan hanya 1 peserta yang memperoleh nilai 50.

**Kata Kunci:** edukasi, keamanan siber, risiko keamanan, *cyber crime*, komunitas

## A. PENDAHULUAN

Kemunculan *Internet* yang kemudian banyak merubah tatanan dalam masyarakat (Rosihan et al., 2023). Melalui Internet dapat menyatukan seluruh dunia dan dengan sifat keterbukaan, dan menjadi sebuah daya tarik yang sangat kuat. Siapapun dapat bebas membaca apa yang ada di internet dan dapat memberi sumbangsih ide dan pemikiran, memberikan komentar-komentar terhadap sajian informasi yang diberitakan. Internet menjadi media atau wadah terbesar dan terpesat bagi kegiatan komunitas komersial di dunia dengan jaringan yang sangat luas (Wahib et al., 2022).

Kemajuan teknologi Internet di satu sisi mampu membantu manusia untuk menyelesaikan banyak permasalahan, namun disisi lain kemajuan teknologi *Internet* ini juga banyak disalah gunakan untuk berbuat kejahatan. Isu keamanan siber telah menjadi isu yang penting dan semakin mendesak dalam era digital saat ini (Arifin et al., 2024). Keamanan adalah hal yang fundamental dalam dunia teknologi informasi (Sapriadi et al., 2023).

Pada beberapa tahun terakhir ini telah terjadi peningkatan jumlah dan kompleksitas dalam kasus serangan Siber. *Cyber Security* merupakan sebuah upaya yang dilakukan untuk melindungi sebuah data, jaringan, system, program, aplikasi dari serangan digital yang dilakukan oleh pihak yang tidak bertanggung jawab dikenal dengan *cybercrime* (Arifin et al., 2024; Hidayat et al., 2023). *Cyber security* sangat penting untuk menjaga keamanan dunia digital, terutama bagi perusahaan yang mengandalkan teknologi untuk operasional sehari-hari (Susanti et al., 2023). Sebuah program keamanan siber yang efektif dapat mengurangi risiko gangguan operasional bisnis, kerugian keuangan, mengurangi kerusakan reputasi.

*Cyber Crime* merupakan suatu kejahatan virtual dengan memanfaatkan media komputer yang terhubung pada internet dan mengeksploitasi komputer lain yang terhubung internet juga (Karim et al., 2023; Pratama et al., 2023).

Serangan siber yang terjadi mengancam sistem komputer dan data di seluruh dunia. Jenis serangan yang banyak dilakukan seperti pencurian data, *malware*, peretasan, dan serangan *DDoS* telah menyebabkan kerugian finansial yang signifikan, kerusakan reputasi, dan gangguan pada operasi bisnis dan juga pada peserta pribadi (Pribady, 2024). Serangan siber dunia mengalami peningkatan 75% dibandingkan periode yang sama pada tahun lalu. Banyaknya kasus pada kuartal ketiga tahun 2024 ini sebanyak 1.876 serangan setiap minggunya pada organisasi (Fa'izi, 2024).

*Kaspersky* sebuah perusahaan yang bergerak dalam bisnis keamanan siber mengungkapkan bahwa wilayah Asia Pasifik masih diintai sejumlah ancaman keamanan siber di tahun 2024 (Prasasti, 2024). Di kawasan Asia-Pasifik, negara Singapura dengan intensitas serangan tertinggi di kawasan ini dengan rata-rata 2.229 serangan per minggu. Menurut data dari *Check Point Research (CPR),* mengungkapkan terjadinya peningkatan hingga 129% dibandingkan periode lalu (Fa'izi, 2024).

Banyaknya kasus dan tingkat terjadinya ancaman ini mendorong perlunya upaya yang lebih kuat dalam memahami dan mengatasi tantangan keamanan *siber*. Mengingat dunia *siber* tidak mengenal batas waktu dan wilayah, salah satu kegiatan yang dilakukan adalah memberikan edukasi (Nugroho et al., 2019). Melalui kegiatan Edukasi keamanan siber ini diharapkan dapat meningkatkan kesadaran dan kewaspadaan terhadap ancaman keamanan *Siber* (Hidayat et al., 2023; Syaddan, 2024).

Adanya edukasi keamanan *Siber* ini sebagai media pembelajaran dan pemahaman baru, menambah wawasan dan pengetahuan dalam memanfaatkan teknologi internet. Edukasi ini juga diharapkan dapat menambah kewaspadaan dari kejahatan dunia maya dan pentingnya kesadaran akan *Cyber Security.*

SWADIMAS
JURNAL PENGABDIAN KEPADA MASYARAKAT
VOL 03 NO 01 JANUARI 2025
ISSN 2964-8297 (p-issn) | 2964-8289 (e-issn)

Kegiatan Pengabdian dalam Masyarakat ini dilakukan dalam bentuk Edukasi dan diskusi mengenai keamanan *Siber,* di email, *Smartphone* dan *Social media.*Melalui kegiatan edukasi ini dapat memberikan gambaran seperti apa dan bagaimana kejahatan *Internet* dilakukan baik melalui media sosial maupun *Smartphone* dan lainnya**.** Diajarkan juga bagaimana cara menerapkan keamanan data privasi dalam bersosial media, serta dampak bahaya dari kejahatan dunia maya.

## B. PELAKSANAAN DAN METODE

Kegiatan observasi dilakukan dengan Kegiatan pengabdian masyarakat yang dilakukan di komunitas Young Ozzer Indonesia yang berlokasi di Jl. Pangeran Jayakarta, No. 66, Komplek Ruko Jayakarta Lestari, Jakarta. Young Ozzer Indonesia merupakan sebuah Organisasi Muda Mudi Tantrayana Vajrayana khususnya Aliran Nyingma.

Pelaksanaan kegiatan ini dilakukan dalam bentuk Edukasi dan diskusi mengenai keamanan Cyber, di Social media dan Smartphone yang dipimpin oleh tim pelaksana pengabdian

Materi pelatihan disampaikan oleh narasumber yang ahli dalam *Cyber Security*. Edukasi disampaikan dalam dua sesi yaitu sesi ceramah dan sesi tanya jawab untuk memperkuat pemahaman peserta.

Mekanisme pelaksanaan kegiatan Edukasi keamanan Cyber di social media dilaksanakan melalui beberapa tahapan sebagai berikut:

1. Perencanaan: untuk merencanakan kegiatan, termasuk penetapan tujuan, target peserta, materi pelatihan, jadwal pelaksanaan, dan metode evaluasi.
2. Persiapan Materi: untuk menyiapkan materi pelatihan yang mencakup konsep-konsep dasar keamanan Cyber, macam dan jenis kejahatan Cyber, metode pencegahannya,
3. Pendataan Peserta: Melakukan pendataan peserta yang akan mengikuti edukasi keamanan cyber.
4. Pelaksanaan: Edukasi dilakukan melalui sesi ceramah dan diskusi, dipimpin oleh narasumber yang kompeten dalam bidang keamanan Cyber.
5. Evaluasi awal: Sebelum pelatihan dimulai, dilakukan evaluasi awal (pre-test) untuk mengukur pengetahuan awal peserta terkait keamanan Cyber.
6. Edukasi: Materi edukasi keamanan Cyber disampaikan dalam bentuk pemaparan via projector oleh narasumber, dilanjutkan dengan sesi diskusi dan tanya jawab.
7. Evaluasi Akhir: Setelah edukasi selesai dilakukan evaluasi akhir untuk mengukur peningkatan pengetahuan peserta setelah mengikuti edukasi.
8. Ramah tamah: untuk mendapatkan masukan langsung terkait manfaat dan keberhasilan pelatihan yang telah dilakukan.

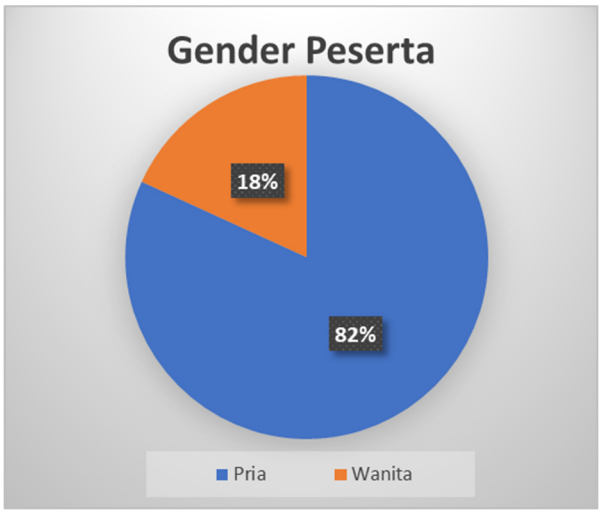
## C. HASIL DAN PEMBAHASAN

Proses Kegiatan Edukasi keamanan Cyber ini diawali dengan membuat Flyer yang dipublikasikan pada media sosial Instagram organisasi komunitas Young Ozzer Indonesia dua minggu sebelum pelaksanaan acara. Gambar 1 di bawah ini merupakan tampilan dari Flyer yang di buat.


Gambar 1. *Flyer* Edukasi Keamanan *Cyber*

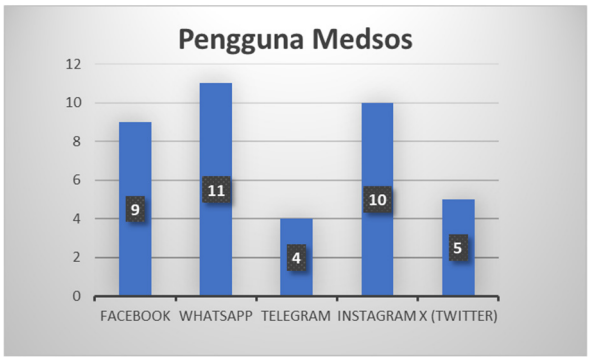
Publikasi *flyer* ini yang merupakan media komunikasi antar anggota komunitas, sehingga adanya acara edukasi ini dapat diketahui oleh seluruh anggota komunitas.

Kegiatan edukasi ini diikuti oleh 11 peserta peserta, adapun profil dan latar belakang peserta dapat dilihat pada gambar dibawah ini.



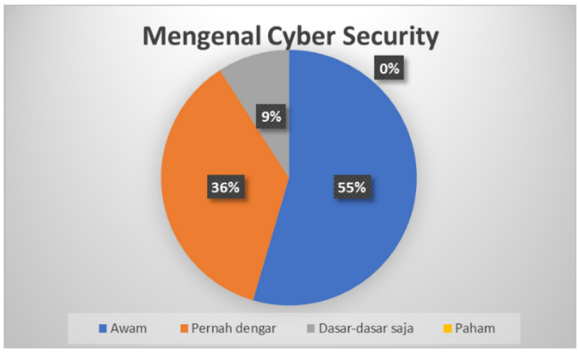

Gambar 2. Gender Peserta.

Jumlah peserta yang mengikuti acara ini ada 11 peserta terdiri dari 9 peserta pria sebanyak 82% dari peserta dan 2 peserta wanita 18 % dari peserta.



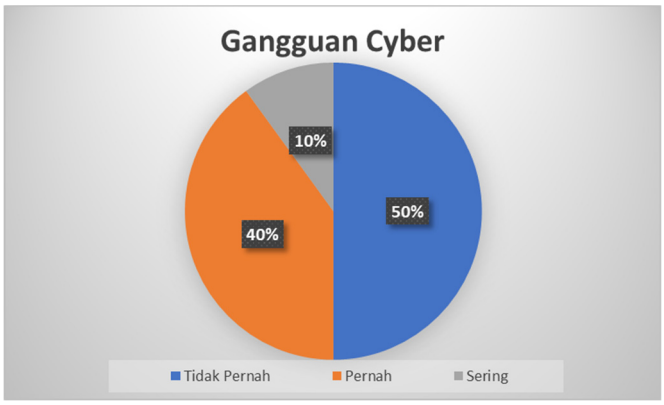

Gambar 3. Media Sosial Peserta

Dari peserta yang mengikuti edukasi ini dapat diketahui media sosial yang mereka gunakan, hasilnya sebagai berikut: Untuk pengguna media sosial Facebook 9 peserta, pengguna media sosial Whatsapp 11 peserta, pengguna media sosial Telegram 4 peserta, pengguna media sosial Instagram 10 peserta, pengguna media sosial X (Twitter) 5 peserta. Dari data dapat diketahui semua peserta menggunakan media sosial *Whatsapp* dan *Facebook* dan *Instagram* yang populer digunakan.




Gambar 4. Cyber Security

Hasil pre-test yang dilakukan mencakup pengenalan peserta terhadap *Cyber security*. Hasilnya dapat diketahui 55% (6 peserta) awam akan istilah *Cyber Security*. 36% (4 peserta) pernah mendengar istilah *Cyber security* dan 9% (1 peserta) mengenal istilah *Cyber Security* meski hanya sebatas pengetahuan umum saja.




Gambar 5. Gangguan *Cyber Security*

Hasil pre-test yang dilakukan mencakup pertanyaan apakah peserta pernah mengalami gangguan Cyber security. Hasilnya dapat diketahui satu peserta sering mengalami 10% (1 peserta). Gangguan yang didapatkan berupa banyaknya nomor yang masuk ke *Whatsapp* menawarkan undangan berupa *Link* yang memaksa untuk dibuka, panggilan tidak dikenal dengan nomor luar negeri dan banyaknya email masuk yang tidak dikenal.

SWADIMAS
JURNAL PENGABDIAN KEPADA MASYARAKAT
VOL 03 NO 01 JANUARI 2025
ISSN 2964-8297 (p-issn) | 2964-8289 (e-issn)

Selanjutnya ada 4 peserta 40 % dari peserta yang pernah mengalami meski hanya beberapa kali, dan yang terakhir 5 peserta atau 50% dari peserta yang belum pernah mengalami gangguan Cyber sama sekali.

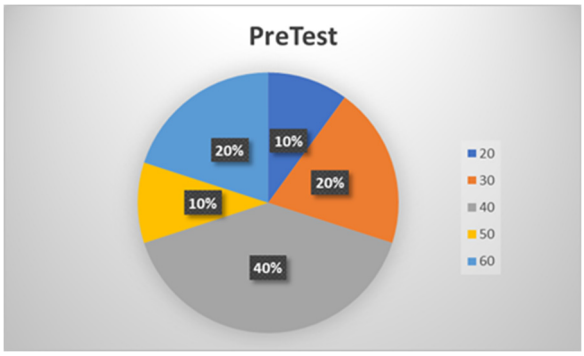
**Proses Edukasi**

Sebelum kegiatan edukasi berjalan dilakukan Pre-test terlebih dahulu untuk mengukur wawasan tentang keamanan Cyber dari para anggota. Adapun hasil dari pre-test yang dilakukan dapat dilihat pada tabel sebagai berikut:

Tabel 1. Hasil Nilai Pre Test

| Nilai Pre test | Jumlah |
|---|---|
| Nilai 20 | 1 Peserta |
| Nilai 30 | 2 Peserta |
| Nilai 40 | 5 Peserta |
| Nilai 50 | 1 Peserta |
| Nilai 60 | 2 Peserta |
| Total | 11 Peserta |

Untuk memudahkan dapat dilihat pada gambar 6 dibawah ini.




Gambar 6. Diagram hasil *pre-test*

Dari data Hasil pre-test tentang keamanan *Cyber Security*, dapat diketahui sebagian besar dari peserta belum mengetahui terkait dengan keamanan system informasi atau dikenal dengan *Cyber Security*. Meskipun semua peserta telah menggunakan internet melalui *smartphone* dan sosial media yang mereka gunakan. Para peserta hanya sebatas menggunakannya saja untuk kepentingan sehari hari, tetapi mereka belum mengetahui ancaman dan resiko yang mengintai dari penggunaan internet dan sosial media. Hal ini menjadi salah satu faktor penting untuk dilakukan edukasi terkait keamanan *Cyber security*.

Setelah kegiatan pre-test dilakukan maka dilanjutkan dengan pemaparan materi.


Gambar 7. Materi Edukasi

Adapun isi dari materi yang diberikan meliputi:

- Pengguna Internet di Indonesia, berapa banyak pengguna media sosial dan smartphone, aplikasi apa yang populer digunakan.
- Kesalahan konsep umum keamanan *Cyber* dalam penggunaan media sosial, *smartphone* dan *Internet*.
- Risiko Teknologi Informasi bagi masyarakat baik sebagai pengguna organisasi maupun pengguna pribadi.
- Risiko *Cyber Security* terhadap keamanan data baik sebagai Perusahaan maupun pengguna pribadi.
- Risiko terkait dengan privasi pengguna dan keamanan data pribadi.
- Risiko Sosial Media yang sering terjadi apa, bagaimana dan seberapa besar dampaknya.
- Aspek utama Information Security yang perlu diketahui, sebagai pedoman dalam keamanan data.

- Ancaman apa saja yang ada dan sering terjadi terkait Keamanan Cyber.
- Apa dan bagaimana serangan Malware, Phising.
- Contoh kasus yang terjadi terkait kejahatan di dunia Cyber.
- Pengamanan Password dan Backup Data, bagaimana kombinasinya, seberapa penting dan manfaatnya.
- Tips pencegahan keamanan informasi, terkait dengan penggunaan Smartphone, Ecommerce, Email dll.

Pemateri memberikan penjelasan dari masing masing poin dari isi materi secara lugas dan detail, berikut dengan contoh modus dan kasus yang sering terjadi. Berikut ini foto peserta dan kegiatan yang dilakukan.

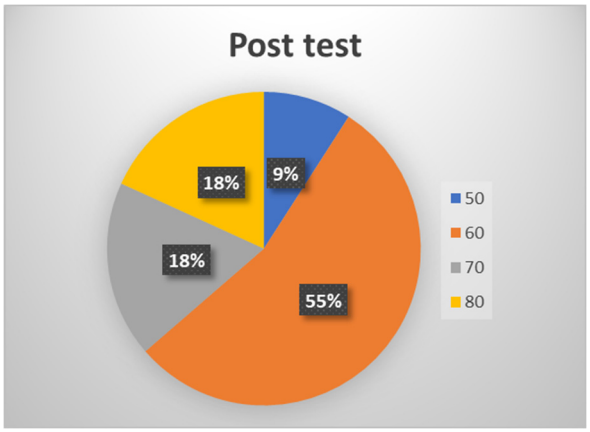
Gambar 8. Pemaparan materi

Untuk mengukur pemahaman peserta edukasi akan materi keamanan Cyber security yang telah disampaikan, maka di akhir pelatihan diberikan post-test. Adapun hasil dari post-test yang dilakukan dapat dilihat pada tabel sebagai berikut:

Tabel 2. Hasil Nilai Post Test

| Nilai Pre test | Jumlah |
|---|---|
| Nilai 50 | 1 Peserta |
| Nilai 60 | 6 Peserta |
| Nilai 70 | 2 Peserta |
| Nilai 80 | 2 Peserta |
| Total | 11 Peserta |

Untuk memudahkan dapat dilihat pada gambar 9 dibawah ini.




Gambar 9. Diagram Post-test.

Hasil Post Test menunjukan peningkatan nilai yang diperoleh, dimana pada setelah dilaksanakan edukasi nilai terkecil yang diperoleh adalah nilai 50 sebanyak 1 peserta dan nilai tertinggi dengan nilai 80 sebanyak 2 peserta. Nilai 60 merupakan nilai yang banyak dicapai oleh peserta yaitu 6 peserta dan dua peserta mendapatkan nilai 70.

Secara umum kegiatan pengabdian masyarakat yang dilakukan berupa Edukasi dan diskusi mengenai keamanan *Cyber,* berlangsung cukup sukses dalam meningkatan pengetahaun dan pemahaman peserta terkait keamanan siber

## D. PENUTUP

Kegiatan pengabdian masyarakat yang dilakukan berupa Edukasi dan diskusi mengenai keamanan siber dapat disimpulkan bahwa beberapa tahun terakhir ini telah terjadi peningkatan jumlah dan kompleksitas dalam kasus serangan siber. Sehingga pengetahuan akan Cyber Security sangat penting, untuk menjaga keamanan dunia digital, terutama bagi perusahaan yang mengandalkan teknologi untuk operasional sehari-hari.

Banyaknya kasus dan tingkat terjadinya ancaman ini mendorong perlunya upaya yang lebih kuat dalam memahami dan mengatasi tantangan keamanan cyber. Untuk itu

diperlukan memberikan edukasi, diharapkan dapat meningkatkan kesadaran dan kewaspadaan terhadap ancaman keamanan Cyber.

Kegiatan Pengabdian dalam Masyarakat ini dilakukan dalam bentuk Edukasi dan diskusi mengenai keamanan Cyber di email, *smartphone* dan media sosial.

Secara umum kegiatan pengabdian masyarakat yang dilakukan berlangsung cukup sukses. Hal ini diukur dari hasil Post Test menunjukan peningkatan nilai yang diperoleh, dimana pada persentase perolehan nilai setelah dilaksanakan edukasi sebagai berikut: 91 % memperoleh nilai diatas 60 dan hanya 1% yang memperoleh nilai 50.

Untuk lebih efektif dalam Edukasi dan diskusi mengenai keamanan Cyber ini perlu dilakukan secara berkala dan berkelanjutan, karena kejahatan dalam dunia Cyber terus berkembang dengan cepat.

## E. DAFTAR PUSTAKA

Arifin, N. Y., Veza, O., Setyabudhi, A. L., & Fernandes, A. L. (2024). Sosialisasi Pentingnya Cyber Security untuk Menjaga Keamanan Online Studi Fakultas Teknik Informatika Universitas Ibnu Sina. *Karya Nyata: Jurnal Pengabdian Kepada Masyarakat*, *1*(3), 46–51. https://doi.org/10.62951/karyanyata.v1i3.451

Fa'izi, M. B. N. (2024). *Serangan Siber Global Melonjak 75% di Q3 2024*. Www.Cloudcomputing.Id. https://www.cloudcomputing.id/berita/serangan-siber-global-melonjak-di-2024

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. https://journal.mediapublikasi.id/index.php/amma/article/view/2905

Karim, A., Biharudin, A., Hidayat, A. R., & Arifin, M. S. (2023). Edukasi dan Sosialisasi Cybercrime terhadap Keamanan Data bagi Kelompok Pembina Kesejahteraan Keluarga. *JILPI: Jurnal Imiah Pengabdian Dan Inovasi*, *2*(2), 373–380. https://doi.org/10.57248/jilpi.v2i2.298

Nugroho, E. P., Nugraha, E., & Zulfikar, M. N. (2019). Sistem Reporting Keamanan pada Jaringan Cloud Computing Melalui bot Telegram dengan Menggunakan Teknik Intrussion Detection and Prevention System. *Jurnal Teknologi Terpadu*, *5*(2), 49–57. https://doi.org/10.54914/jtt.v5i2.233

Prasasti, G. D. (2024). *Deretan Ancaman Siber Ini Masih Intai Wilayah Asia Pasifik di 2024*. Www.Liputan6.Com. https://www.liputan6.com/tekno/read/5507299/deretan-ancaman-siber-ini-masih-intai-wilayah-asia-pasifik-di-2024

Pratama, T. G., Rosita, D., Anwari, A., & Purbowati, P. (2023). Peningkatan Kesadaran Keamanan Data Pribadi dan Hukum Cyber. *Jurnal Abdimas Indonesia*, *5*(2), 96–100. https://doi.org/10.26751/jai.v5i2.2204

Pribady, M. L. (2024). *Tren Kejahatan Siber 2024, Ransomware Masih Jadi Ancaman*. Https://Inet.Detik.Com. https://inet.detik.com/security/d-7214869/tren-kejahatan-siber-2024-ransomware-masih-jadi-ancaman

Rosihan, R. I., Spalanzani, W., Hamdani, H., Febryanto, A., & Manalu, F. N. (2023). Sosialisasi Cyber Security Dan Perkembangan Teknologi Masa Kini Untuk Anak Usia Dini. *Jurnal Pengabdian Masyarakat Bumi Raflesia*, *6*(2023), 289–296. https://doi.org/10.36085/jpmbr.v6i2.5405

Sapriadi, S., Eko Syaputra, A., Septi Eirlangga, Y., Hariani Manurung, K., & Hayati, N. (2023). Sosialisasi dan Pelatihan Secure Computer dalam

Meningkatan Kesadaran Siswa terhadap Keamanan Data. *Majalah Ilmiah UPI YPTK*, *30*(2), 38–43. https://doi.org/10.35134/jmi.v30i2.149

Susanti, L., Akrom, Baskhara, D. R., Khairudin, & Astofa, A. (2023). Sosialisasi Pentingnya Cyber Security Guna Mengurangi Resiko Tingkat Pencurian Data Yang Berimbas Pada Tindak Penipuan Kepada Para Karang Taruna Benda Baru Pamulang. *JAMAIKA: Jurnal Abdi Masyarakat Universitas Pamulang*, *3*(2), 207–214. https://openjournal.unpam.ac.id/index.php/JAMAIKA/article/view/20840

Syaddan, S. (2024). Sosialisasi Keamanan Data di Dunia Siber untuk Meningkatkan Kewaspadaan SMK 1 Negeri Tarakan Terhadap Ancaman Cybercrime. *Archive: Jurnal Pengabdian Kepada Masyarakat*, *3*(2), 289–299. https://doi.org/10.55506/arch.v3i2.103

Wahib, P., Narotama, A. T., Rijki, N. M., Sahrudin, Permana, F., Sagara, D., Azkhal, D. I., Anwar, M., & Juniawan, M. R. (2022). Sosialisasi Cyber Security Untuk Meningkatkan Literasi Digital. *Abdi Jurnal Publikasi*, *1*(2), 64–68. https://jurnal.portalpublikasi.id/index.php/AJP/article/view/21