

Sosialisasi Peningkatan Literasi Digital dan Keamanan Siber Pelajar di Desa Tabongo Timur

Roviana H. Dai^a, Muhammad Rifai Katili^b, Lanto Ningrayati Amali^c, Mohammad Syafri Tuloli^d, Sri Nilawaty Lahay^e, Jihan Fahira Gubali^f, Indah Belastri Sibran^g, Moh. Ardiansyah Nento^h

^{a, b, c, d, e, f, g, h} Program Studi Sistem Informasi, Universitas Negeri Gorontalo
roviana.ung@gmail.com^a, mrifaikatili@ung.ac.id^b, ningrayati_amali@ung.ac.id^c,
syafri.tuloli@ung.ac.id^d, nilawatylahay@ung.ac.id^e, jihan_s1sisfo@mahasiswa.ung.ac.id^f,
indah_s1sisfo@mahasiswa.ung.ac.id^g, diasnnto@gmail.com^h

Abstract

The low level of digital security literacy among students is an urgent issue that needs to be addressed, given that the national digital security pillar scored only 3.12 on the index, making it the lowest score among all measured digital literacy pillars. This situation is exacerbated by the high intensity of internet use among students, which has not been balanced by an adequate understanding of various cyber threats. This community service activity aims to increase middle school students' understanding and awareness of digital risks and the importance of personal data protection. The activity was held on May 18, 2026, in the Tabongo Timur Village Office Hall as part of the 2026 Impactful Community Service Program (KKN Berdampak), involving 34 participants from SMP Negeri 3 Satap Tabongo, MTs Negeri 2 Gorontalo Regency, and MAN 2 Gorontalo Regency. The method used was an interactive lecture combined with discussion and Q&A sessions, featuring a speaker from the Department of Computer Science at Gorontalo State University who specializes in digital forensics. The results of the activity demonstrated the participants' enthusiasm and active engagement throughout the session. Based on the discussion sessions, five key issues of concern to the participants were identified: the ethics of using Artificial Intelligence (AI) in education, information verification and the prevention of misinformation, password security, malware threats, and early detection of digital account hacking. This activity underscored that students already possess an initial awareness of digital risks; however, they still require ongoing guidance and education to be able to utilize technology safely, wisely, and responsibly.

Keywords : Digital Literacy; Cybersecurity; Community Service; Impactful Community Service Program; Students; Digital Risks.

Abstrak

Rendahnya literasi keamanan digital di kalangan pelajar menjadi permasalahan mendesak yang perlu ditangani, mengingat pilar keamanan digital secara nasional hanya memperoleh skor indeks 3,12, menjadikannya nilai terendah di antara seluruh pilar literasi digital yang diukur. Kondisi ini diperparah oleh tingginya intensitas penggunaan internet di kalangan pelajar yang belum diimbangi dengan pemahaman memadai terhadap berbagai ancaman siber. Kegiatan pengabdian masyarakat ini bertujuan untuk meningkatkan pemahaman dan kesadaran pelajar tingkat menengah terhadap risiko digital serta pentingnya perlindungan data pribadi. Kegiatan dilaksanakan pada tanggal 18 Mei 2026 di Aula Kantor Desa Tabongo Timur sebagai bagian dari program KKN Berdampak 2026, dengan melibatkan 34 peserta dari SMP Negeri 3 Satap Tabongo, MTs Negeri 2 Kabupaten Gorontalo, dan MAN 2 Kabupaten Gorontalo. Metode yang digunakan adalah ceramah interaktif yang dipadukan dengan sesi diskusi dan tanya jawab, dengan narasumber dari Jurusan Teknik Informatika Universitas Negeri Gorontalo yang memiliki kompetensi di bidang forensika digital. Hasil kegiatan menunjukkan antusiasme dan keterlibatan aktif peserta selama sosialisasi berlangsung. Berdasarkan sesi diskusi, teridentifikasi lima isu utama yang menjadi perhatian peserta, yaitu etika penggunaan Artificial Intelligence (AI) dalam pendidikan, verifikasi informasi dan pencegahan hoaks, keamanan kata sandi, ancaman malware, serta deteksi dini peretasan akun digital. Kegiatan ini menegaskan bahwa pelajar telah memiliki kesadaran awal terhadap risiko digital, namun masih memerlukan pendampingan dan edukasi berkelanjutan agar mampu memanfaatkan teknologi secara aman, bijak, dan bertanggung jawab.

Keywords : Literasi Digital; Keamanan Siber; Pengabdian Masyarakat; KKN Berdampak; Pelajar; Risiko Digital.

1. Pendahuluan

Perkembangan teknologi digital telah berjalan sangat cepat, termasuk di Indonesia yang telah menjadikan internet sebagai penunjang utama berbagai aktivitas sehari-hari. Lebih dari 212 juta penduduk Indonesia tercatat aktif menggunakan internet, dengan pelajar sebagai salah satu kelompok pengguna terbesar untuk keperluan akademik, komunikasi, penelusuran informasi, hingga interaksi sosial di berbagai platform digital (Najma, 2026). Meski pemanfaatan teknologi terus meningkat, kondisi ini belum diimbangi dengan pemahaman dan kesadaran yang memadai tentang keamanan digital. Peningkatan penggunaan internet juga seiring dengan meningkatnya risiko digital yang mengancam pengguna, seperti phishing yang memanfaatkan manipulasi psikologis untuk mencuri data secara ilegal, penyebaran berita bohong yang menggiring opini publik ke arah yang salah, serangan malware yang merusak perangkat, pencurian data pribadi, serta cyberbullying yang berdampak serius pada kesehatan mental korbannya (Arsyad et al., 2024). Kondisi ini semakin mengkhawatirkan mengingat sektor pendidikan menempati posisi teratas yang paling sering menjadi target serangan digital akibat rendahnya kesadaran pengguna terhadap risiko digital (Nuranisa et al., 2026). Kesadaran keamanan digital kini bukan sekadar wacana akademis, melainkan kebutuhan strategis yang mendesak untuk ditangani secara terstruktur.

Kondisi tersebut diperparah oleh rendahnya pemahaman pelajar terhadap ancaman digital itu sendiri. Data nasional menunjukkan bahwa pilar keamanan digital hanya memperoleh skor indeks 3,12 yang merupakan nilai terendah di antara seluruh pilar literasi digital yang diuji mencerminkan rendahnya kemampuan pengguna dalam memahami dan menerapkan prinsip-prinsip dasar keamanan digital dalam kehidupan sehari-hari (Saraswati and Gani, 2024). Bahkan pelajar dari bidang teknologi informasi pun masih kerap ditemukan menyebarkan informasi yang tidak terverifikasi di platform digital, sehingga rentan menjadi korban sekaligus pelaku penyebaran informasi menyesatkan (Malahayati and Nabilah, 2024). Perilaku berisiko yang umum dijumpai di kalangan pelajar antara lain penggunaan kata sandi yang lemah dan mudah diretas serta mengeklik tautan sembarangan tanpa memverifikasi keamanannya. Seluruh perilaku ini membuka celah bagi pihak tidak bertanggung jawab untuk melakukan tindakan ilegal terhadap pengguna digital yang kurang waspada (Tamu, 2026). Penelitian menunjukkan bahwa hanya sekitar 40% pelajar yang memahami dengan baik tentang phishing dan malware, sementara sebagian besar lainnya masih sulit mengenali pentingnya kewaspadaan terhadap risiko digital sehingga lebih mudah menjadi korban berbagai modus penipuan yang semakin canggih (Nuranisa et al., 2026). Kesenjangan antara intensitas penggunaan teknologi dan lemahnya pemahaman terhadap ancaman siber menjadikan pelajar sebagai kelompok yang sangat rentan terhadap serangan siber yang kian modern dan kompleks.

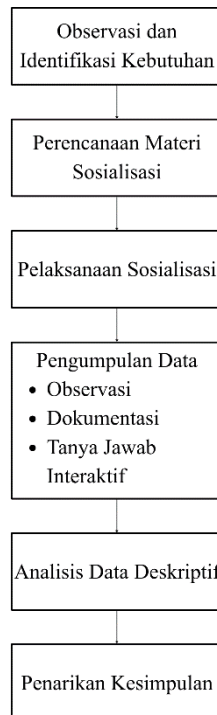
Meskipun risiko ini telah terdokumentasi, upaya intervensi langsung berupa sosialisasi tentang keamanan digital masih sangat terbatas dilakukan, khususnya di lingkungan sekolah menengah pertama. Program edukasi digital yang ada umumnya bersifat umum dan tidak secara spesifik menyentuh pemahaman pelajar terhadap berbagai jenis ancaman siber seperti cyberbullying, berita hoaks, phishing, malware, maupun perlindungan data pribadi (Handayani et al., 2026). Di sisi lain, kegiatan pengabdian masyarakat yang berbasis kampus pun belum banyak menjadikan literasi keamanan digital sebagai fokus program, padahal pelajar tingkat menengah merupakan kelompok yang aktif menggunakan internet namun minim pembekalan tentang keamanan digital di lingkungan formal mereka (Ridwan et al., 2022). Selain itu, pelajar masih memerlukan

pemahaman yang lebih komprehensif mengenai berbagai risiko digital, sehingga diperlukan kegiatan edukasi yang mampu membahas seluruh aspek tersebut secara terpadu (Nuranisa et al., 2026). Pelajar jenjang pendidikan menengah di Desa Tabongo Timur dipilih sebagai sasaran kegiatan karena aktif menggunakan internet dan media sosial, tetapi masih minim memperoleh edukasi tentang keamanan digital. Oleh karena itu, diperlukan sosialisasi yang terstruktur untuk meningkatkan literasi dan kesadaran keamanan digital sesuai kebutuhan mereka.

Berdasarkan permasalahan yang ditemukan terkait rendahnya kesadaran keamanan digital di kalangan pelajar, kegiatan pengabdian masyarakat ini dilaksanakan sebagai bagian dari program KKN Berdampak 2026. Kegiatan ini bertujuan meningkatkan pemahaman dan kesadaran pelajar tingkat menengah mengenai berbagai risiko digital, ancaman siber, dan pentingnya perlindungan data pribadi melalui sosialisasi. Kegiatan ini penting dilaksanakan mengingat pelajar merupakan pengguna aktif teknologi digital yang rentan terhadap berbagai ancaman di dunia maya akibat keterbatasan pemahaman mengenai keamanan digital. Diharapkan kegiatan ini dapat memberikan kontribusi nyata dalam meningkatkan kewaspadaan pelajar terhadap ancaman siber, membentuk perilaku digital yang bijak dan bertanggung jawab, serta mendorong kolaborasi antara institusi pendidikan dan pemangku kebijakan untuk mengembangkan program edukasi keamanan digital yang lebih terstruktur dan berkelanjutan.

2. Metode Pelaksanaan

Kegiatan pengabdian kepada masyarakat ini dilaksanakan melalui program Kuliah Kerja Nyata (KKN) di Desa Tabongo Timur, Kabupaten Gorontalo. Salah satu kegiatan yang dilaksanakan dalam program tersebut adalah sosialisasi literasi digital dan keamanan siber dengan tema “Kenali Risiko Digital: Agar Teknologi Jadi Manfaat, Bukan Bahaya.” Kegiatan ini bertujuan untuk meningkatkan pemahaman pelajar mengenai berbagai risiko penggunaan teknologi digital serta mendorong pemanfaatan teknologi secara aman, bijak, dan bertanggung jawab. Sosialisasi dilaksanakan pada tanggal 18 Mei 2026 di Aula Kantor Desa Tabongo Timur dengan melibatkan 34 peserta yang berasal dari SMP Negeri 3 Satap Tabongo, MTs Negeri 2 Kabupaten Gorontalo, dan MAN 2 Kabupaten Gorontalo. Sasaran kegiatan dipilih karena pelajar merupakan kelompok pengguna aktif internet dan media sosial yang memiliki peluang besar untuk memperoleh manfaat teknologi, namun juga rentan terhadap berbagai ancaman dan risiko di ruang digital (Bansal et al., 2024). Penggunaan metode pelaksanaan kegiatan terdiri atas beberapa tahapan, yaitu observasi dan identifikasi kebutuhan, perencanaan materi sosialisasi, pelaksanaan sosialisasi, pengumpulan data, analisis data deskriptif, serta penarikan kesimpulan. Alur metode pelaksanaan kegiatan disajikan pada Gambar berikut.



Gambar 1. Tahapan Metode Pelaksanaan

Tahap pertama dilakukan melalui observasi lapangan dan koordinasi dengan pemerintah Desa Tabongo Timur untuk mengidentifikasi dan mengetahui kebutuhan dari masyarakat desa yang dapat dijadikan sebagai fokus program edukasi. Berdasarkan hasil observasi dan diskusi bersama pihak desa, diperoleh informasi bahwa pemahaman pelajar terkait penggunaan teknologi digital yang aman dan bertanggung jawab masih perlu ditingkatkan. Temuan tersebut menjadi dasar dalam penentuan tema dan materi kegiatan sosialisasi. Tahap kedua adalah penyusunan materi sosialisasi yang dilakukan oleh dosen dari Jurusan Teknik Informatika Universitas Negeri Gorontalo yang memiliki kompetensi di bidang forensika digital selaku sebagai pemateri. Materi yang disiapkan mencakup pengenalan risiko digital, ancaman siber, keamanan data pribadi, ancaman malware, pemanfaatan teknologi secara bijak, serta literasi pentingnya literasi informasi di era digital. Penyusunan materi dilakukan dengan mempertimbangkan perkembangan ancaman siber yang semakin kompleks serta tingginya keterlibatan generasi muda dalam aktivitas digital (Silalahi, 2022).

Tahap ketiga merupakan pelaksanaan sosialisasi yang diselenggarakan pada tanggal 18 Mei 2026 di Aula Kantor Desa Tabongo Timur. Kegiatan dilaksanakan melalui metode ceramah interaktif yang dipadukan dengan sesi diskusi dan tanya jawab. Metode ini dipilih untuk menciptakan komunikasi dua arah antara narasumber dan peserta sehingga materi yang disampaikan dapat dipahami dengan lebih baik oleh peserta. Selain menerima materi, peserta juga diberikan kesempatan untuk menyampaikan pengalaman dan permasalahan yang mereka hadapi dalam penggunaan teknologi digital sehari-hari. Pendekatan partisipatif tersebut dinilai mampu meningkatkan keterlibatan peserta sekaligus mendorong tumbuhnya kesadaran mengenai pentingnya keamanan digital (Putri et al., 2025). Tahap berikutnya adalah pengumpulan data kegiatan yang dilakukan melalui observasi partisipatif, dokumentasi, dan pencatatan hasil sesi tanya jawab. Observasi partisipatif digunakan untuk mengamati tingkat perhatian, antusiasme, dan keterlibatan peserta selama kegiatan berlangsung (Almadira et al., 2024). Dokumentasi

dilakukan untuk merekam seluruh rangkaian kegiatan sebagai data pendukung, sedangkan hasil tanya jawab digunakan untuk mengidentifikasi berbagai isu literasi digital dan keamanan siber yang menjadi perhatian peserta.

Tahap terakhir dilakukan melalui analisis data deskriptif terhadap data yang diperoleh dari observasi, dokumentasi, dan hasil sesi tanya jawab selama kegiatan berlangsung. Analisis dilakukan dengan mendeskripsikan berbagai pertanyaan dan respons peserta yang muncul selama sosialisasi sebagai gambaran mengenai isu-isu literasi digital dan keamanan siber yang menjadi perhatian pelajar. Hasil analisis tersebut kemudian disajikan dalam bentuk uraian untuk mendukung pembahasan mengenai pelaksanaan kegiatan sosialisasi, serta digunakan sebagai dasar dalam menarik kesimpulan mengenai isu-isu literasi digital dan keamanan siber yang menjadi perhatian pelajar selama kegiatan sosialisasi berlangsung.

3. Hasil dan Pembahasan

3.1. Hasil

3.1.1. Antusiasme dan Partisipasi Peserta

Kegiatan sosialisasi literasi digital dan keamanan siber yang dilaksanakan pada tanggal 18 Mei 2026 di Aula Kantor Desa Tabongo Timur diikuti oleh 34 peserta yang berasal dari SMP Negeri 3 Satap Tabongo, MTs Negeri 2 Kabupaten Gorontalo, dan MAN 2 Kabupaten Gorontalo. Selama kegiatan berlangsung, peserta menunjukkan antusiasme yang tinggi terhadap materi yang disampaikan. Hal ini terlihat dari perhatian peserta selama sesi pemaparan materi serta keterlibatan aktif dalam sesi diskusi dan tanya jawab. Antusiasme peserta menunjukkan bahwa isu keamanan digital merupakan topik yang dekat dengan kehidupan pelajar. Tingginya penggunaan internet dan media sosial di kalangan remaja menyebabkan mereka berhadapan langsung dengan berbagai risiko digital, sehingga kebutuhan akan edukasi literasi digital menjadi semakin penting. Kondisi ini sejalan dengan temuan (Putri et al., 2025) yang menyatakan bahwa peningkatan aktivitas digital perlu diimbangi dengan pemahaman yang memadai mengenai keamanan data dan perlindungan privasi.



Gambar 2. Dokumentasi Penyampaian Materi Sosialisasi

3.1.2. Isu Literasi Digital dan Keamanan Siber yang Menjadi Perhatian Pelajar

Berdasarkan hasil sesi diskusi dan tanya jawab, diperoleh beberapa pertanyaan yang mencerminkan isu-isu digital yang sering dihadapi peserta dalam kehidupan sehari-hari. Pertanyaan tersebut meliputi penggunaan kecerdasan buatan (*Artificial Intelligence*)

dalam pendidikan, verifikasi informasi dan hoaks, keamanan kata sandi, penanganan malware, serta keamanan akun digital.

Tabel 1. Isu Literasi Digital dan Keamanan Siber yang Menjadi Perhatian Peserta

No	Tema	Pertanyaan
1	Etika penggunaan AI	Apakah penggunaan AI untuk mengerjakan tugas masih dianggap sebagai bentuk usaha belajar?
2	Hoaks dan disinformasi	Bagaimana cara memastikan kebenaran informasi sebelum mengambil kesimpulan?
3	Keamanan kata sandi	Mengapa akun masih dapat diretas meskipun menggunakan kata sandi yang kuat?
4	Malware	Apa yang harus dilakukan jika laptop terindikasi terkena malware?
5	Keamanan akun digital	Bagaimana cara mengetahui apakah akun Google telah diretas?



Gambar 3. Sesi Diskusi dan Tanya Jawab

3.2. Pembahasan

3.2.1. Etika Penggunaan *Artificial Intelligence* dalam Pendidikan

Salah satu peserta dari MTs Negeri 2 Kabupaten Gorontalo menanyakan apakah penggunaan kecerdasan buatan (*Artificial Intelligence/AI*) untuk menyelesaikan tugas sekolah masih dapat dianggap sebagai bentuk usaha belajar. Pertanyaan ini menunjukkan bahwa teknologi AI mulai dimanfaatkan oleh pelajar dalam kegiatan akademik, namun masih terdapat keraguan mengenai batasan etis penggunaannya. Fenomena tersebut mengindikasikan bahwa perkembangan teknologi AI telah menjadi bagian dari proses pembelajaran modern. Oleh karena itu, literasi digital tidak hanya mencakup kemampuan menggunakan teknologi, tetapi juga kemampuan memahami etika, tanggung jawab, dan integritas akademik dalam pemanfaatannya. Sejalan dengan (Oktavian and Sulistyowati, 2024), kemampuan literasi digital perlu dibarengi dengan kemampuan berpikir kritis agar teknologi dapat dimanfaatkan secara positif tanpa mengurangi proses belajar peserta didik.

3.2.2. Verifikasi Informasi dan Pencegahan Hoaks

Pertanyaan lain disampaikan oleh peserta dari MAN 2 Kabupaten Gorontalo mengenai cara menyikapi informasi yang beredar di media sosial agar tidak langsung mengambil kesimpulan sebelum memperoleh fakta yang valid. Pertanyaan tersebut muncul karena peserta melihat banyak informasi yang dapat menimbulkan kepanikan di masyarakat, termasuk isu yang berkaitan dengan kondisi ekonomi dan kebijakan pemerintah. Temuan ini menunjukkan bahwa pelajar telah menyadari keberadaan hoaks dan disinformasi di ruang digital. Namun demikian, kemampuan untuk melakukan verifikasi informasi masih perlu diperkuat. Kemampuan berpikir kritis dan memeriksa sumber informasi merupakan salah satu kompetensi penting dalam literasi digital untuk

menghindari penyebaran informasi yang tidak benar (Oktavian and Sulistyowati, 2024). Oleh karena itu, edukasi mengenai teknik verifikasi informasi perlu menjadi bagian penting dalam kegiatan literasi digital.

3.2.3. Keamanan Kata Sandi dan Perlindungan Akun Digital

Peserta juga menanyakan alasan akun digital masih dapat diretas meskipun menggunakan kata sandi yang dianggap kuat. Pertanyaan ini menunjukkan adanya kesadaran mengenai pentingnya penggunaan kata sandi sebagai bentuk perlindungan akun digital. Meskipun kata sandi yang kuat merupakan langkah awal dalam menjaga keamanan akun, ancaman siber saat ini tidak hanya bergantung pada kelemahan kata sandi, tetapi juga memanfaatkan teknik rekayasa sosial (social engineering), phishing, dan pencurian kredensial pengguna. (Safi and Singh, 2023) menjelaskan bahwa teknik phishing masih menjadi salah satu metode yang paling sering digunakan untuk memperoleh informasi pribadi pengguna secara tidak sah. Oleh karena itu, penggunaan autentikasi dua faktor (two-factor authentication) dan kewaspadaan terhadap tautan mencurigakan perlu terus disosialisasikan kepada pelajar.

3.2.4. Ancaman Malware pada Perangkat Elektronik

Pertanyaan mengenai langkah yang harus dilakukan ketika laptop terindikasi terkena malware menunjukkan bahwa peserta telah menyadari adanya ancaman perangkat lunak berbahaya terhadap perangkat digital yang digunakan sehari-hari. Malware dapat menyebabkan berbagai dampak negatif, mulai dari penurunan kinerja perangkat hingga pencurian data pribadi pengguna. Oleh karena itu, peserta diberikan pemahaman mengenai pentingnya memperbarui sistem operasi, menggunakan perangkat lunak keamanan, serta menghindari pengunduhan file dari sumber yang tidak terpercaya. Edukasi mengenai ancaman malware menjadi penting karena pelajar merupakan kelompok yang aktif mengakses berbagai platform digital dan berpotensi menjadi sasaran serangan siber (Silalahi, 2022).

3.2.5. Deteksi Dini Peretasan dan Kebocoran Akun

Pertanyaan terakhir berkaitan dengan cara mengetahui apakah akun Google telah mengalami peretasan atau kebocoran data. Pertanyaan ini menunjukkan meningkatnya kesadaran peserta terhadap pentingnya perlindungan identitas digital. Keamanan akun menjadi aspek penting dalam kehidupan digital karena sebagian besar aktivitas pengguna saat ini terhubung dengan akun daring. Menurut (Zieni et al., 2023), faktor manusia masih menjadi salah satu titik paling rentan dalam keamanan siber sehingga peningkatan kesadaran pengguna menjadi langkah penting dalam mencegah berbagai bentuk serangan digital. Dalam kegiatan ini, narasumber menjelaskan beberapa indikator yang dapat digunakan untuk mendeteksi potensi peretasan akun, seperti adanya aktivitas login yang tidak dikenal, perubahan informasi akun tanpa izin, munculnya notifikasi keamanan yang mencurigakan, serta akses dari perangkat atau lokasi yang tidak dikenali. Selain itu, narasumber juga memperkenalkan layanan “Have I Been Pwned” sebagai salah satu platform yang dapat digunakan untuk memeriksa apakah alamat email pengguna pernah terlibat dalam insiden kebocoran data. Melalui layanan tersebut, pengguna dapat mengetahui riwayat kebocoran data yang berkaitan dengan akun email yang dimiliki sehingga dapat segera melakukan langkah pengamanan, seperti mengganti kata sandi dan mengaktifkan autentikasi dua faktor. Penjelasan ini memberikan pemahaman praktis

kepada peserta mengenai pentingnya melakukan pemeriksaan keamanan akun secara berkala sebagai upaya perlindungan identitas digital.

3.2.6. Implikasi Kegiatan terhadap Kesadaran Digital Pelajar

Berbagai pertanyaan yang muncul selama sesi diskusi menunjukkan bahwa pelajar telah memiliki kesadaran awal terhadap berbagai risiko penggunaan teknologi digital. Namun demikian, masih terdapat kebutuhan untuk memperkuat pemahaman mengenai keamanan akun, verifikasi informasi, etika penggunaan teknologi, dan perlindungan data pribadi. Temuan ini menunjukkan bahwa kebutuhan literasi digital pelajar tidak hanya berkaitan dengan aspek teknis penggunaan teknologi, tetapi juga mencakup kemampuan berpikir kritis, etika digital, perlindungan data pribadi, dan kesadaran terhadap ancaman siber. Munculnya berbagai pertanyaan selama sesi diskusi mengindikasikan bahwa pelajar telah menyadari keberadaan risiko digital, namun masih memerlukan pendampingan dan edukasi yang berkelanjutan agar mampu memanfaatkan teknologi secara aman, bijak, dan bertanggung jawab. Oleh karena itu, kegiatan sosialisasi literasi digital dan keamanan siber perlu terus dilakukan sebagai upaya memperkuat budaya keamanan digital di kalangan generasi muda.



Gambar 4. Foto Bersama Peserta dan Narasumber

4. Kesimpulan

Kegiatan sosialisasi literasi digital dan keamanan siber yang dilaksanakan melalui program Kuliah Kerja Nyata (KKN) di Desa Tabongo Timur berlangsung dengan baik dan mendapat respons positif dari peserta. Antusiasme peserta terlihat dari keterlibatan aktif selama kegiatan serta berbagai pertanyaan yang diajukan pada sesi diskusi dan tanya jawab. Hasil kegiatan menunjukkan bahwa pelajar telah memiliki kesadaran awal terhadap berbagai risiko digital yang mereka hadapi dalam kehidupan sehari-hari, seperti penggunaan kecerdasan buatan (*Artificial Intelligence*) dalam pembelajaran, penyebaran hoaks, keamanan kata sandi, ancaman malware, serta perlindungan akun digital dari peretasan dan kebocoran data.

Temuan tersebut menunjukkan bahwa kebutuhan literasi digital pelajar tidak hanya terbatas pada kemampuan menggunakan teknologi, tetapi juga mencakup pemahaman mengenai etika digital, kemampuan berpikir kritis dalam memverifikasi informasi, serta kesadaran untuk melindungi data dan identitas digital. Oleh karena itu, kegiatan edukasi mengenai literasi digital dan keamanan siber perlu terus dilakukan secara berkelanjutan sebagai upaya membangun budaya digital yang aman, bijak, dan

bertanggung jawab di kalangan generasi muda. Melalui peningkatan literasi digital, pelajar diharapkan mampu memanfaatkan teknologi secara optimal sekaligus meminimalkan berbagai risiko yang dapat muncul dalam aktivitas digital sehari-hari.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Pemerintah Desa Tabongo Timur atas dukungan dan fasilitasi selama pelaksanaan kegiatan. Terima kasih juga disampaikan kepada SMP Negeri 3 Satap Tabongo, MTs Negeri 2 Kabupaten Gorontalo, dan MAN 2 Kabupaten Gorontalo atas partisipasi dan kerja sama yang diberikan. Apresiasi turut disampaikan kepada Dosen Pembimbing Lapangan (DPL) serta seluruh anggota KKN Desa Tabongo Timur yang telah berkontribusi dalam menyelesaikan kegiatan ini.

Daftar Pustaka

- Almadira, A., Pratama, Y., Purwani, F., 2024. Protecting data in the Digital World: the Strategic Role of Encryption in Data Security. *J. Sci. Res. Dev.* 6 (2), 540–549.
- Arsyad, A.A.J., Tamrin, U., Lande, J.P., Umar, N., 2024. Meningkatkan Kesadaran Remaja Terhadap Phishing Melalui Literasi Digital: Studi Kasus di SMK Darussalam Makassar. *J. Pengabd. Literasi Digit. Indones.* 3(2), 60–71. <https://doi.org/10.57119/abdimas.v3i2.122>
- Bansal, S., Garg, N., Singh, J., Van Der Walt, F., 2024. Cyberbullying and mental health: past, present and future. *Suhans. Front. Psychol.* 14, 01–19. <https://doi.org/10.3389/fpsyg.2023.1279234>
- Handayani, N.S., Prajawinanti, A., Wasi'ah, D.A., 2026. Literasi Digital Sebagai Strategi Preventif Cyber Crime Di Kalangan Mahasiswa. *J. Ilmu Perpust.* 8(1), 69–82. <https://doi.org/10.31764/jiper.v7i1.37994>
- Malahayati, Nabilah, N., 2024. Analisis Tingkat Kesadaran Mahasiswa Terhadap Serangan Rekayasa Sosial (Studi Kasus: Mahasiswa Teknologi Informasi Universitas Islam Negeri Ar-Raniry). *JINTECH J. Inf. Technol.* 5(1), 1–12. <https://doi.org/10.22373/jintech.v5i1.4262>
- Najma, S., 2026. Literasi Digital dan Implikasinya terhadap Pemahaman Fikih Ibadah Mahasiswa PAI di Perguruan Tinggi Keagamaan Islam Negeri (PTKIN). *Al-Tarbiyah J. Ilmu Pendidik. Islam* 4(2), 62–72. <https://doi.org/https://doi.org/10.59059/al-tarbiyah.v4i2.2993>
- Nuranisa, P., Hidayasari, N., Ristra, P., 2026. Analisis tingkat kesadaran mahasiswa terhadap keamanan informasi melalui simulasi serangan email phishing menggunakan gophish. *JATI (Jurnal Mhs. Tek. Inform.* 10(2), 2297–2303. <https://doi.org/10.36040/jati.v10i2.17410>
- Oktavian, E.R., Sulistyowati, F., 2024. PERAN LITERASI DIGITAL REMAJA DALAM MENGHADAPI PENYEBARAN BERITA HOAKS. *J. Komun. Pemberdaya.* 3(1), 38–46. <https://doi.org/10.47431/jkp.v3i1.401>
- Putri, A., Sari, N., Fajrina, P., Aisyah, S., 2025. Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). *J. Pengabd. Nas. Indones.* 6(1), 38–52. <https://doi.org/10.35870/jpni.v6i1.1097>
- Ridwan, Yusran, Maulidia, C.A., 2022. Analisis Pemahaman Literasi Digital Pada Mahasiswa Uin Arraniry Terhadap Digital Skill Dan Digital Safety. *Cybersp. J. Pendidik. Teknol. Inf.* 6(2), 142–148. <https://doi.org/10.22373/cj.v6i2.15433>
- Safi, A., Singh, S., 2023. A systematic literature review on phishing website detection techniques. *J. King Saud Univ. - Comput. Inf. Sci.* 35, 590–611. <https://doi.org/10.1016/j.jksuci.2023.01.004>
- Saraswati, S.S., Gani, R., 2024. Efektivitas Penerapan Konsep Keamanan Digital oleh Mahasiswa. *J. Ris. Jurnalistik dan Media Digit.* 4(2), 55–60. <https://doi.org/10.29313/jrjmd.v4i1.3840>
- Silalahi, F.D., 2022. Keamanan Cyber, Yayasan Prima Agus Teknik & Universitas STEKOM. Semarang.
- Tamu, Z.J.D., 2026. Kenali Risiko Digital Agar Teknologi Jadi Manfaat, Bukan Bahaya. Gorontalo.