# Edukasi Keamanan Siber sebagai Upaya Peningkatan Literasi Digital Guru dan Siswa di SMAN 3 Polewali

Anugrayani Bustamin*, Ady Wahyudi Paundu, Ingrid Nurtanio, Adnan, Amil Ahmad Ilham, Muhammad Niswar , Muhammad Alief Fahdal Imran Oemar, Muhammad Aryandi, Randy Kamal Husein, Yusri Simang, Ahmad Ali Husein, Reyhan Fahreza, A. Tyas Nur Atda, Mutiara, Ahmad Nur Alim
Departemen Teknik Informatika, Fakultas Teknik, Universitas Hasanuddin
anugrayani@unhas.ac.id*

**Abstrak**
Perkembangan teknologi digital yang semakin pesat turut meningkatkan risiko ancaman keamanan siber, khususnya di kalangan pelajar dan tenaga pendidik. Rendahnya pemahaman terkait perlindungan data pribadi, keamanan akun digital, serta ancaman *phishing* dan *malware* menjadi tantangan yang perlu diatasi melalui kegiatan edukasi yang terstruktur. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan literasi digital dan *awareness cyber security* bagi guru dan siswa di SMAN 3 Polewali melalui pelatihan interaktif berbasis gamifikasi menggunakan *platform Interland by Google*. Metode pelaksanaan dilakukan melalui tiga tahapan, yaitu persiapan dan identifikasi kebutuhan, pelaksanaan pelatihan, serta evaluasi kegiatan menggunakan *pre-test* dan *post-test* berbasis *Google Form*. Materi yang diberikan mencakup perlindungan data pribadi, keamanan *password*, keamanan OTP, kewaspadaan terhadap phishing dan malware, serta risiko penggunaan *WiFi* publik. Hasil evaluasi menunjukkan peningkatan pemahaman peserta pada sebagian besar indikator terkait keamanan digital. Berdasarkan hasil *pre-test* dan *post-test* terhadap 41 peserta, terjadi peningkatan pada sebagian besar indikator literasi keamanan digital. Peningkatan tertinggi terdapat pada keamanan *WiFi* publik (63% menjadi 73%), diikuti perlindungan data pribadi (65% menjadi 73%), penanganan *cyberbullying* (53% menjadi 58%), dan keamanan *password* (85% menjadi 87%). Sementara itu, keamanan OTP tetap mencapai 100% pada kedua tahap, menunjukkan tingkat kesadaran peserta yang sudah sangat baik sejak awal kegiatan.

Kata Kunci: Gamifikasi; Internet; Kesadaran Keamanan Siber; Literasi Digital; Pelatihan Interaktif.

***Abstract***
*The rapid development of digital technology has increased the risk of cybersecurity threats, especially among students and educators. The lack of understanding regarding personal data protection, digital account security, and the threat of phishing and malware is a challenge that needs to be addressed through structured educational activities. This community service activity aims to improve digital literacy and cybersecurity awareness for teachers and students at SMAN 3 Polewali through interactive, gamification-based training using the Interland by Google platform. The implementation method is carried out in three stages: preparation and identification of needs, training implementation, and activity evaluation using pre-tests and post-tests based on Google Forms. The material provided includes personal data protection, password security, OTP security, awareness of phishing and malware, and the risks of using public Wi-Fi. The evaluation results showed an increase in participants' understanding of most indicators related to digital security. Based on the results of the pre-test and post-test on 41 participants, there was an increase in most indicators of digital security literacy. The highest improvement was in public Wi-Fi security (63% to 73%), followed by personal data protection (65% to 73%), handling cyberbullying (53% to 58%), and password security (85% to 87%). Meanwhile, OTP security remained at 100% in both phases, indicating excellent participant awareness from the start of the program.*

*Keywords: Gamification; Internet; Cybersecurity Awareness; Digital Literacy; Interactive Training .*

## 1. Pendahuluan

Di era transformasi digital yang berkembang pesat, kemampuan literasi digital bukan lagi sekadar keunggulan kompetitif, melainkan telah menjadi kebutuhan fundamental bagi setiap individu,

termasuk para pendidik dan peserta didik. Pada tahun 2024, jumlah pengguna internet di Indonesia telah mencapai lebih dari 221 juta jiwa dengan tingkat penetrasi sebesar 79,5%, di mana mayoritas penggunanya berasal dari kalangan Gen Z dan milenial yang sebagian besar merupakan pelajar Sekolah Menengah Atas (APJII, 2024). Kondisi ini membawa peluang sekaligus ancaman yang nyata, terutama di lingkungan pendidikan tingkat menengah atas.

Ancaman keamanan siber di Indonesia terus meningkat secara signifikan dari tahun ke tahun. Badan Siber dan Sandi Negara (BSSN) mencatat bahwa sepanjang tahun 2024 terdapat 2.487.041 aktivitas *Advanced Persistent Threat (*APT), 514.508 serangan *ransomware*, dan 26.771.610 serangan phishing yang menyasar berbagai kalangan, termasuk pelajar (BSSN, 2024a). Ancaman siber tersebut tidak hanya bersifat teknis, tetapi juga mencakup manipulasi sosial seperti penipuan daring (*scam*), penyebaran hoaks, pencurian data pribadi, hingga konten berbahaya seperti radikalisme yang semakin marak menyasar kalangan remaja usia sekolah menengah atas (Kominfo Jatim, 2025).

Siswa SMA yang berada pada rentang usia 15–18 tahun merupakan kelompok yang sangat aktif menggunakan teknologi digital, namun sekaligus rentan terhadap ancaman siber yang lebih kompleks dibandingkan jenjang sebelumnya. Survei Kesadaran Keamanan Siber (SKKS) 2024 oleh BSSN mengungkapkan bahwa meskipun pelajar Indonesia memiliki kesadaran siber sosial yang cukup baik dengan indeks 3,00, mereka masih lemah dalam aspek teknis seperti penggunaan autentikasi dua faktor (2FA), pengelolaan kata sandi yang kuat, serta pemahaman terhadap modus *social engineering* dan *phishing* yang semakin canggih (BSSN, 2024b). Kondisi ini sangat relevan bagi siswa SMA yang mulai aktif bertransaksi digital, menggunakan *e-commerce*, dan membangun identitas daring secara mandiri.

Berbagai upaya edukasi keamanan siber khusus di jenjang SMA telah terbukti memberikan dampak positif. Penelitian Gading (2023) tentang bahaya *phishing* di kalangan siswa SMA Pattimura Jakarta Selatan menunjukkan bahwa pelajar SMA yang melek internet pun masih rentan terhadap serangan *phishing* akibat minimnya literasi keamanan digital yang spesifik. Lebih lanjut, edukasi *cyber security awareness* yang dilaksanakan di SMA Widya Darma Surabaya berhasil meningkatkan pemahaman siswa tentang jenis-jenis ancaman siber yang lazim dialami pelajar, serta langkah-langkah praktis untuk menjaga keamanan akun digital mereka (Wijayanti, 2026). Hal ini mempertegas bahwa intervensi edukatif yang kontekstual dan sesuai jenjang sangat dibutuhkan di tingkat SMA.

SMAN 3 Polewali sebagai salah satu institusi pendidikan menengah atas di Kabupaten Polewali Mandar, Sulawesi Barat dengan jumlah siswa 372 yang tentunya tidak terlepas dari tantangan tersebut (Kementerian Pendidikan Dasar dan Menengah, 2026). Minimnya pemahaman tentang perlindungan data pribadi, keamanan akun media sosial, ancaman penipuan daring, serta perilaku digital yang bertanggung jawab di kalangan guru maupun siswa SMA menjadi permasalahan yang perlu segera diatasi melalui program edukasi yang sistematis dan berkelanjutan. Penelitian ini bertujuan untuk mendeskripsikan upaya peningkatan literasi digital guru dan siswa melalui kegiatan edukasi keamanan siber di SMAN 3 Polewali, sehingga tercipta ekosistem pembelajaran digital yang kondusif dan terlindungi dari berbagai ancaman siber.

## 2. Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat telah mengubah lanskap pendidikan menengah atas secara fundamental. Siswa SMA kini tidak hanya menggunakan

teknologi untuk keperluan belajar, tetapi juga untuk transaksi digital, komunikasi intensif melalui media sosial, dan membangun identitas daring secara mandiri. Korelasi positif yang signifikan antara literasi digital dan kualitas pembelajaran menggarisbawahi pentingnya literasi digital sebagai keterampilan dasar keberhasilan pendidikan di era digital, di mana peserta didik dengan tingkat literasi digital lebih tinggi menunjukkan prestasi akademik, keterlibatan, dan kepuasan belajar yang lebih besar (Judijanto, 2024). Namun, tingginya aktivitas digital siswa SMA tanpa diimbangi pemahaman keamanan siber yang memadai justru meningkatkan kerentanan mereka terhadap berbagai ancaman di dunia maya.

Pemerintah Indonesia telah merespons kebutuhan tersebut melalui berbagai kebijakan strategis. Kementerian Komunikasi dan Informatika bersama Japelidi dan SIBERKREASI merancang kerangka literasi digital yang terdiri dari empat pilar utama, yakni Cakap Digital (*Digital Skills*), Aman Digital (*Digital Safety*), Budaya Digital (*Digital Culture*), dan Etika Digital (*Digital Ethics*) (Kominfo & SIBERKREASI, 2021). Indeks literasi digital Indonesia pada tahun 2023 berada di angka 3,65 dari skala 5, menunjukkan bahwa kemampuan literasi digital masyarakat masih berada pada tingkat sedang dan memerlukan peningkatan yang signifikan, khususnya pada pilar Aman Digital (Kemenkominfo, 2023). Dalam konteks pendidikan SMA, implementasi Kurikulum Merdeka menuntut guru tidak hanya menguasai materi ajar, tetapi juga kompeten dalam aspek pedagogi digital dan keamanan siber agar mampu membimbing siswa yang kian aktif secara digital (Sofiana dkk., 2025).

Ancaman siber yang spesifik menyasar remaja usia SMA semakin beragam dan kompleks. Penelitian tentang literasi digital keamanan siber pada remaja mengungkapkan bahwa meskipun remaja sudah memiliki pengetahuan dasar tentang keberadaan kejahatan siber, literasi mereka dalam menghadapi serangan nyata seperti *social engineering* dan *phishing* masih belum memadai. Pengetahuan tentang autentikasi dua faktor, pembuatan kata sandi yang kuat, serta langkah-langkah konkret menghadapi serangan siber masih perlu ditingkatkan secara signifikan (Effendy & Oktiana, 2024). Selain itu, laporan Kominfo dan BSSN (2024a) mencatat bahwa ancaman siber sosial seperti penipuan daring, penyebaran konten negatif, dan manipulasi psikologis daring justru lebih banyak menyasar kalangan remaja aktif media sosial yang belum memiliki kecakapan digital yang memadai.

Permasalahan literasi digital tidak hanya dialami oleh siswa, tetapi juga oleh guru SMA sebagai ujung tombak pendidikan. Hasil penelitian menunjukkan bahwa kompetensi digital guru di Indonesia, meskipun berada pada kategori cukup baik di tingkat dasar, masih memerlukan peningkatan signifikan dalam aspek keamanan siber dan pedagogi digital (Jurnal Ilmu Wawasan Pendidikan, 2024). Padahal, di era di mana siswa SMA sudah sangat mandiri secara digital, guru justru dituntut menjadi fasilitator yang lebih kompeten, bukan hanya dalam pemanfaatan teknologi, tetapi juga dalam membimbing siswa menghadapi risiko siber yang semakin kompleks. Guru yang tidak memiliki literasi keamanan siber yang memadai tidak akan mampu mengidentifikasi, apalagi mencegah, paparan ancaman siber di lingkungan belajar digital (Silvester dkk., 2024).

Urgensi edukasi keamanan siber di jenjang SMA semakin diperkuat oleh hasil-hasil penelitian terkini. Program edukasi intensif kepada siswa SMA mengenai literasi digital, keamanan siber, dan etika digital melalui pendekatan pelatihan interaktif, studi kasus, dan simulasi serangan siber sederhana, terbukti mampu memperkuat kompetensi digital siswa dan mendorong mereka menjadi warga digital yang cerdas, kritis, dan bertanggung jawab (Sofiana dkk., 2024). Demikian pula, kegiatan sosialisasi keamanan siber di lingkungan SMA yang menekankan perlindungan data

pribadi, etika bermedia sosial, dan pengenalan modus-modus kejahatan siber terkini terbukti efektif meningkatkan kesadaran dan kecakapan digital siswa secara terukur (Wijayanti, 2026).

SMAN 3 Polewali sebagai salah satu sekolah menengah atas di wilayah Kabupaten Polewali Mandar menghadapi tantangan yang serupa. Keterbatasan akses terhadap program literasi digital yang terstruktur, minimnya pelatihan keamanan siber bagi tenaga pendidik, serta meningkatnya paparan ancaman digital di kalangan siswa SMA yang sangat aktif bermedia sosial menjadi permasalahan mendasar yang perlu diatasi. BSSN merekomendasikan peningkatan edukasi keamanan digital di sekolah-sekolah dengan memasukkan materi keamanan siber dalam kurikulum, serta sosialisasi penggunaan internet yang aman melalui seminar dan kampanye digital yang relevan dengan karakteristik dan kebutuhan siswa SMA (BSSN, 2024a).

Berdasarkan uraian di atas, kegiatan pengabdian ini hadir untuk menjawab kebutuhan tersebut dengan mendeskripsikan proses dan hasil peningkatan literasi digital guru dan siswa melalui program edukasi keamanan siber yang dilaksanakan di SMAN 3 Polewali. Dengan menyesuaikan pendekatan edukasi pada karakteristik siswa SMA yang lebih mandiri, kritis, dan aktif secara digital, diharapkan program ini dapat menjadi model yang dapat direplikasi oleh sekolah-sekolah menengah atas lain di wilayah Sulawesi Barat maupun di Indonesia pada umumnya.

## 3. Metode

Berdasarkan hasil analisis kebutuhan mitra serta upaya implementasi hasil riset yang dikembangkan di Departemen Teknik Informatika Universitas Hasanuddin, kegiatan pengabdian masyarakat ini diwujudkan dalam bentuk edukasi dan pelatihan keamanan siber. Metode pelaksanaan kegiatan dilakukan melalui tiga tahapan, yaitu:

### *3.1 Tahap persiapan dan identifikasi target capaian*

Pada tahap persiapan, tim melakukan koordinasi dengan pihak sekolah, identifikasi kebutuhan peserta, penyusunan materi pelatihan, serta penyusunan instrumen evaluasi berupa *pre-test* dan *post-test* berbasis *Google Form*. Melalui pelatihan ini, kami berharap adanya peningkatan literasi dan level *awareness* dari peserta terkait keamanan digital dan teknologi informasi secara umum.

### *3.2 Tahap Pelaksanaan*

Tahap pelaksanaan dilakukan dalam bentuk pelatihan interaktif dengan tema "Pelatihan Literasi Digital: Peningkatan *Awareness Cyber Security*". Materi yang diberikan meliputi literasi digital, pengenalan ancaman keamanan siber (*cyber security awareness*), perlindungan data pribadi, praktik penggunaan *password* yang aman, kewaspadaan terhadap *phishing* dan *malware*, serta penggunaan teknologi digital secara bijak dan bertanggung jawab. Penyampaian materi dilakukan melalui pendekatan gamifikasi menggunakan platform *Interland by Google* yang dipadukan dengan demonstrasi sederhana, studi kasus, dan sesi diskusi bersama peserta untuk meningkatkan keterlibatan dan pemahaman peserta secara lebih interaktif.

### *3.3 Tahap Evaluasi*

Untuk mengukur efektivitas kegiatan, tim menggunakan metode evaluasi berupa *pre-test* dan *post-test*. Instrumen evaluasi disusun dalam bentuk kuesioner berbasis *Google Form* yang terdiri atas pertanyaan terkait pengetahuan dasar keamanan digital serta *awareness* peserta terhadap keamanan siber. Instrumen evaluasi terdiri atas pertanyaan terkait pengetahuan dasar keamanan digital dan tingkat *awareness* peserta terhadap keamanan siber sebagai berikut:

a. Jika mendapati pesan dari orang tidak dikenal meminta data pribadi (nama, tanggal lahir, alamat,...), yang harus dilakukan.
b. Seperti apa kriteria *password* yang kuat.
c. Pengetahuan terkait *One-Time Password* (OTP)
d. Jika mengalami *cyberbullying* (hinaan/ejekan online), apa yang harus dilakukan?
e. Di tempat umum, menggunakan *WiFi* yang tidak dikenal, aplikasi apa yang bisa saya jalankan?

Selain aspek pengetahuan, instrumen juga mengukur persepsi dan perilaku peserta terkait keamanan data pribadi, penggunaan *password* yang aman, kewaspadaan terhadap tautan mencurigakan, serta kemampuan mengenali ancaman siber seperti phishing dan *malware* menggunakan skala Likert 1–5. Adapun instrumen pertanyaan yang diberikan dijabarkan sebagai berikut:

a. Saya memahami pentingnya menjaga keamanan data pribadi
b. Saya menggunakan *password* yang berbeda untuk setiap akun
c. Saya berhati-hati saat mengklik *link* dari pesan/email
d. Saya memahami risiko penggunaan *WiFi* publik
e. Saya merasa mampu mengenali ancaman siber (misalnya *phishing, malware*)

Data hasil *pre-test* dan *post-test* dianalisis menggunakan pendekatan deskriptif kuantitatif dengan membandingkan hasil sebelum dan sesudah pelatihan. Analisis dilakukan berdasarkan persentase jawaban benar dan rerata skor *awareness* peserta untuk mengidentifikasi peningkatan pemahaman serta perubahan persepsi peserta setelah mengikuti kegiatan pelatihan.

## 4. Hasil dan Diskusi

### *4.1. Implementasi Pelaksanaan Pelatihan*

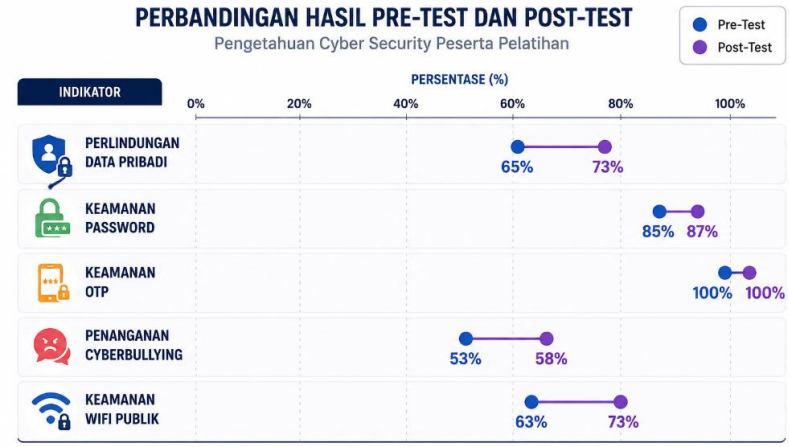
Kegiatan pelatihan dilaksanakan pada tanggal 17 April 2026 di SMAN 3 Polewali dengan tema "Pelatihan Literasi Digital: Peningkatan *Cyber Security Awareness* yang sekaligus bertujuan untuk mendukung peningkatan literasi digital di lingkungan pendidikan. Pelatihan diikuti oleh siswa dan guru sebanyak 41 orang (30 siswa dan 11 guru) dengan pendekatan pembelajaran interaktif berbasis gamifikasi menggunakan *platform Interland* by Google. Metode ini digunakan untuk meningkatkan keterlibatan peserta dalam memahami konsep keamanan siber secara lebih aplikatif dan kontekstual.


Gambar 1. Dokumentasi Kegiatan Pelatihan

Dalam pelaksanaannya, kegiatan dibagi ke dalam beberapa sesi yang terdiri atas penyampaian materi, demonstrasi penggunaan *platform* edukasi digital, simulasi sederhana, serta diskusi interaktif bersama peserta seperti yang dapat dilihat pada Gambar 1. Selain melibatkan dosen sebagai pemateri, kegiatan ini juga melibatkan mahasiswa Departemen Teknik Informatika dari jenjang sarjana (S1), magister (S2), hingga doktor (S3) sebagai bagian dari implementasi pembelajaran kolaboratif dan penguatan kompetensi mahasiswa melalui pengalaman belajar di luar kampus.

### *4.2. Hasil Evaluasi Pelatihan*

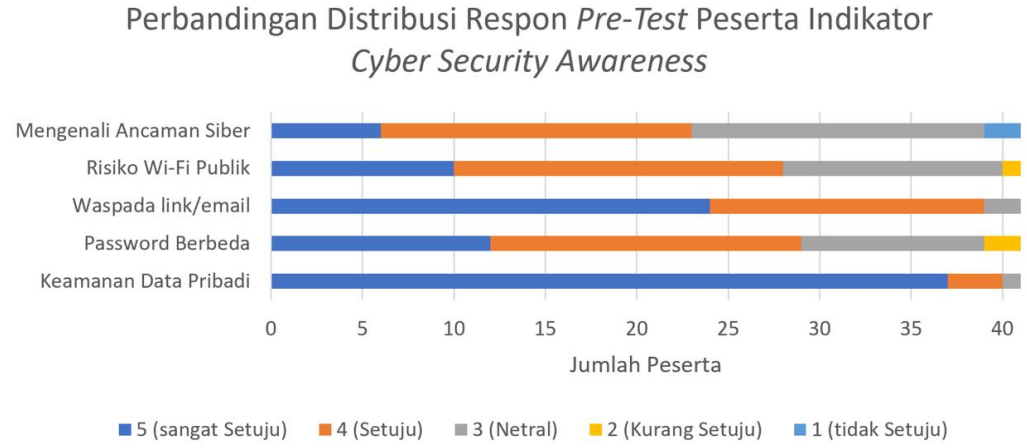
Evaluasi kegiatan dilakukan menggunakan metode kuantitatif melalui pengukuran hasil *pre-test* dan *post-test* untuk 41 peserta guru dan siswa. Pengambilan data dilakukan menggunakan instrumen berbasis *Google Form* yang terdiri atas lima indikator pengetahuan keamanan siber, yaitu perlindungan data pribadi, keamanan *password*, keamanan OTP, penanganan *cyberbullying*, dan keamanan *WiFi* publik. Hasil evaluasi menunjukkan adanya peningkatan pemahaman peserta pada sebagian besar indikator setelah pelaksanaan pelatihan. Perbandingan hasil *pre-test* dan *post-test* ditunjukkan pada Gambar 2.



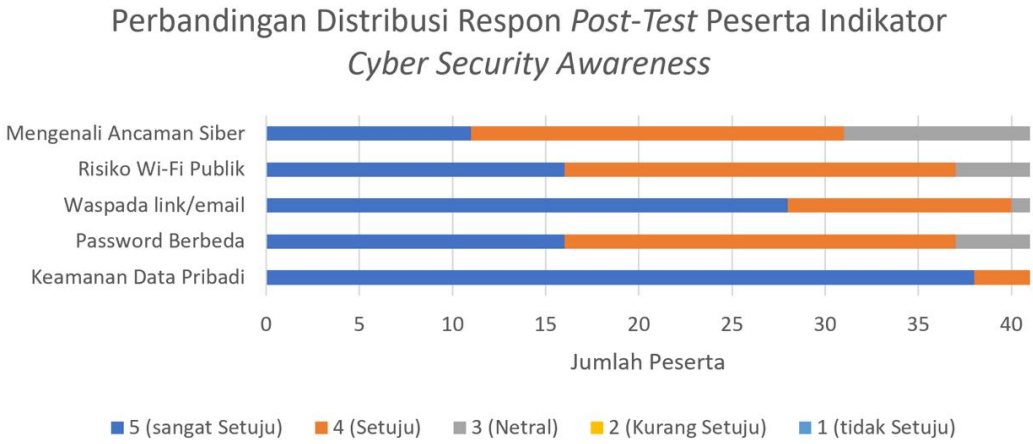

Gambar 2. Perbandingan Hasil *Pre-test* dan *Post-test* untuk Tingkat *Pengetahuan Cyber Security* dari peserta

Berdasarkan hasil pengukuran, terjadi peningkatan pemahaman peserta pada sebagian besar indikator setelah pelatihan dilaksanakan. Indikator *Perlindungan Data Pribadi* meningkat dari 65% menjadi 73%, sedangkan *Keamanan WiFi Publik* mengalami peningkatan tertinggi dari 63% menjadi 73%. Pada indikator *Penanganan Cyberbullying*, nilai meningkat dari 53%

menjadi 58%, meskipun masih memerlukan penguatan lebih lanjut. Sementara itu, indikator *Keamanan Password* meningkat dari 85% menjadi 87%, yang menunjukkan peserta telah memiliki pemahaman awal yang cukup baik. Indikator *Keamanan OTP* memperoleh nilai 100% pada *pre-test* maupun *post-test*, menunjukkan tingkat *awareness* peserta yang sudah sangat baik terkait keamanan OTP.




(a)




(b)

Gambar 3. Perbandingan Hasil *Pre-test* (a) dan *Post-test* (b) untuk *Survey* Indikator *Awareness Cyber Security*

Berdasarkan Gambar 3, distribusi respon peserta pada skala *Likert* menunjukkan adanya peningkatan *awareness* terhadap keamanan siber setelah pelaksanaan pelatihan. Secara umum, terjadi peningkatan jumlah peserta yang memilih kategori *Setuju* dan *Sangat Setuju* pada seluruh indikator yang diukur pada tahap *post-test* dibandingkan *pre-test*. Pada indikator *Keamanan Data Pribadi*, mayoritas peserta sejak awal telah menunjukkan tingkat pemahaman yang tinggi, yang terlihat dari dominasi jawaban *Sangat Setuju* pada tahap *pre-test* (37 orang) maupun *post-test* (38 orang). Setelah pelatihan, jumlah peserta yang memilih kategori *Netral* menurun dari 1 menjadi 0, sehingga menunjukkan peningkatan keyakinan peserta terhadap pentingnya menjaga keamanan data pribadi.

Indikator *Password Berbeda untuk Setiap Akun* juga mengalami perubahan distribusi jawaban yang cukup baik. Pada tahap *post-test,* jumlah respon *Sangat Setuju* dan *Setuju* meningkat (total 37 orang), sementara kategori *Netral* dan *Kurang Setuju* mengalami penurunan dari 2 orang menjadi 0. Hal ini menunjukkan meningkatnya kesadaran peserta mengenai pentingnya penggunaan *password* yang unik untuk setiap akun digital. Pada indikator *Waspada terhadap Link atau Email*, terjadi peningkatan jumlah peserta pada kategori *Sangat Setuju* (24 orang), yang menunjukkan bahwa peserta menjadi lebih berhati-hati terhadap potensi ancaman *phishing* maupun tautan mencurigakan setelah mengikuti pelatihan (28 orang).

Sementara itu, indikator *Risiko WiFi Publik* menunjukkan perubahan distribusi yang cukup signifikan. Jumlah responden pada kategori *Netral* menurun pada tahap *post-test* (dari 12 orang menjadi 4 orang) dan diikuti peningkatan pada kategori *Sangat Setuju* serta *Setuju* (dari 28 orang menjadi 37 orang). Hasil ini menunjukkan bahwa peserta memperoleh pemahaman baru terkait risiko keamanan saat menggunakan jaringan *WiFi* publik. Pada indikator *Kemampuan Mengenali Ancaman Siber*, terjadi peningkatan jumlah peserta yang memilih kategori *Sangat Setuju* dan *Setuju* (dari 23 menjadi 31 orang), serta penurunan pada kategori *Netral* dan *Tidak Setuju*. Hal ini menunjukkan bahwa pelatihan membantu peserta dalam meningkatkan kemampuan mengenali ancaman siber seperti *phishing* dan *malware*.

Secara umum, hasil *post-test* menunjukkan adanya peningkatan pengetahuan dan *awareness* peserta terhadap praktik keamanan digital. Berdasarkan analisis kuantitatif, pendekatan pembelajaran berbasis gamifikasi yang dipadukan dengan diskusi interaktif mampu membantu peserta memahami materi keamanan siber secara lebih menarik dan mudah dipahami.

Selain hasil kuantitatif, hasil observasi selama kegiatan juga menunjukkan adanya peningkatan partisipasi aktif peserta dalam sesi diskusi dan simulasi. Peserta terlihat lebih mampu mengidentifikasi risiko keamanan digital serta memberikan respons yang lebih tepat terhadap skenario ancaman siber yang diberikan selama pelatihan. Temuan ini menunjukkan bahwa kegiatan pelatihan tidak hanya meningkatkan aspek pengetahuan, tetapi juga memperkuat awareness dan perilaku digital yang lebih aman dan bertanggung jawab.

## 5. Kesimpulan

Kegiatan pelatihan literasi digital dan *awareness cyber security* yang dilaksanakan di SMAN 3 Polewali berhasil meningkatkan pemahaman dan kesadaran peserta terhadap praktik keamanan digital. Hasil evaluasi *pre-test* dan *post-test* terhadap 41 peserta menunjukkan adanya peningkatan pada sebagian besar indikator pengetahuan keamanan siber. Indikator perlindungan data pribadi meningkat dari 65% menjadi 73%, sedangkan indikator keamanan *WiFi* publik mengalami peningkatan tertinggi dari 63% menjadi 73%. Selain itu, indikator penanganan *cyberbullying* meningkat dari 53% menjadi 58%, sementara keamanan *password* meningkat dari 85% menjadi 87%. Indikator keamanan OTP memperoleh nilai 100% pada tahap *pre-test* maupun *post-test*, yang menunjukkan tingkat *awareness* peserta yang sudah sangat baik sejak awal kegiatan.

Pendekatan pembelajaran berbasis gamifikasi menggunakan *platform Interland* by Google yang dipadukan dengan demonstrasi dan diskusi interaktif dinilai efektif dalam meningkatkan keterlibatan peserta selama pelatihan. Kegiatan ini tidak hanya meningkatkan aspek pengetahuan, tetapi juga mendorong terbentuknya perilaku digital yang lebih aman dan bertanggung jawab di lingkungan sekolah. Dengan demikian, program edukasi keamanan siber berbasis interaktif dapat

menjadi salah satu model pembelajaran literasi digital yang relevan untuk diterapkan pada jenjang pendidikan menengah atas.

## Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Fakultas Teknik Universitas Hasanuddin melalui hibah Pengabdian Masyarakat Departemen Teknik Informatika yang telah memberikan dukungan atas terlaksananya kegiatan pengabdian masyarakat tahun anggaran 2026. Selain itu, kami juga mengapresiasi dan berterima kasih kepada pihak SMAN 3 Polewali selaku mitra pada kegiatan ini yang telah memberikan dukungan sehingga kegiatan ini dapat terlaksana dengan baik.

## Daftar Pustaka

APJII (2024). Laporan Survei Internet Indonesia 2024. Asosiasi Penyelenggara Jasa Internet Indonesia. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

BSSN (2024a). Laporan Lanskap Keamanan Siber Indonesia 2024. Badan Siber dan Sandi Negara. https://www.bssn.go.id/wp-content/uploads/2025/02/Laporan-SKKS-2024.pdf

BSSN (2024b). Survei Kesadaran Keamanan Siber (SKKS) 2024. Badan Siber dan Sandi Negara.. https://andi.link/hasil-survei-bssn-2024/

Dinas Komunikasi dan Informatika Jawa Timur (2025). Ancaman Siber Sosial Meningkat: Kesadaran Keamanan Digital Harus Ditingkatkan. Kominfo Jatim.. https://kominfo.jatimprov.go.id/berita/ancaman-siber-sosial-meningkat-kadis-kominfo-harap-kesadaran-keamanan-digital-ditingkatkan.

Effendy, M. Y., dan Oktiani, H. (2024). *Literasi digital keamanan siber pada remaja menghadapi social engineering*. Wacana Publik, 18(1).

Gading, M. (2023). Bahaya Phising di Kalangan Remaja Melek Internet kepada Siswa/I SMA Pattimura Jakarta Selatan. *Jurnal Pengabdian Masyarakat Mandira Cendikia*, 2(11), 88–99.. https://www.jurnalahsana.org/index.php/home/article/view/367

Judijanto, L. (2024). Analisis Pengaruh Tingkat Literasi Digital Guru dan Siswa terhadap Kualitas Pembelajaran di Era Digital di Indonesia. Sanskara Pendidikan dan Pengajaran, 2(02), 50–60.. https://www.researchgate.net/publication/382069874

Kemendikbud (2024). Pemahaman Literasi Digital adalah Salah Satu Kunci Melanjutkan Gerakan Merdeka Belajar. Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi.. https://www.kemdikbud.go.id/main/blog/2024/03/pemahaman-literasi-digital-adalah-salah-satu-kunci-melanjutkan-gerakan-merdeka-belajar

Kemenkominfo (2023). Indeks Literasi Digital Indonesia 2023. Kementerian Komunikasi dan Informatika. https://gnld.siberkreasi.id/modul/

Kominfo dan SIBERKREASI (2021). Modul 4 Pilar Literasi Digital CABE (Cakap, Aman, Budaya, Etika). Kementerian Komunikasi dan Informatika.. https://gnld.siberkreasi.id/modul/

Kementerian Pendidikan Dasar dan Menengah, *Profil SMAN 3 Polewali*.", Diakses 18 Juni 2026, https://referensi.data.kemendikdasmen.go.id/snpmb/site/sekolah?npsn=40600654

Silvester, S., Saputro, T. V. D., dan Manggu, B. (2024). Pendampingan Literasi Digital bagi Guru dalam Mengimplementasikan Kurikulum Merdeka. Lumbung Inovasi: Jurnal Pengabdian kepada Masyarakat, 9(4).. https://doi.org/10.36312/linov.v9i4.2276

Sofiana, A., Lubis, E. R., Agustina, K., dan Fajriyah, R. Z. (2025). Kurikulum merdeka dan literasi digital: Evaluasi infrastruktur dan sumber daya sekolah. Jurnal Ilmiah Wahana Pendidikan, 11(11.D), 181–186. https://jurnal.peneliti.net/index.php/JIWP/article/view/11984JERKIN.

Wijayanti, B.E. (2026). Edukasi Cyber Security Awareness sebagai Upaya Peningkatan Literasi Keamanan Digital Siswa SMA Widya Darma Surabaya. Bina Informatika Surabaya, Telkom University. https://bif-sby.telkomuniversity.ac.id/edukasi-cyber-security-awareness-sebagai-upaya-peningkatan-literasi-keamanan-digital-siswa-sma-widya-darma-surabaya/