

## Pemberdayaan Literasi Digital: Edukasi Siswa Tentang Proses Data di Platform Media Sosial

<sup>1</sup>Rifka Annisa Swasthi, <sup>2</sup>Afifah Faiqotuzzahra, <sup>3</sup>Muhammad Randy Prasetya, <sup>4</sup>Ardianto Hafidz Prabowo, <sup>5</sup>Dian Kartika Sari

Sains Data, Fakultas Informatika, Universitas Telkom Purwokerto – Indonesia<sup>1,2,3,4,5</sup>

e-mail: [wannnr23@gmail.com](mailto:wannnr23@gmail.com)<sup>1</sup>, [faigatuzzahra@student.telkomuniversity.ac.id](mailto:faigatuzzahra@student.telkomuniversity.ac.id)<sup>2</sup>, [randyprs07@gmail.com](mailto:randyprs07@gmail.com)<sup>3</sup>, [ardiantohafidzprabowo205@gmail.com](mailto:ardiantohafidzprabowo205@gmail.com)<sup>4</sup>, [dian.kartika@ittelkom-pwt.ac.id](mailto:dian.kartika@ittelkom-pwt.ac.id)<sup>5\*</sup>

\*Penulis Korespondensi

Dikirim: 23/01/2025; Direvisi: 21/02/2025; Diterima: 24/02/2025; Diterbitkan: 24/02/2025

### ABSTRACT

*Advances in digital technology have made social media such as Instagram, TikTok, and Twitter an important part of the lives of the younger generation. However, data literacy and privacy awareness are still low, especially among high school students who often only understand the basic functions of social media. This training aims to improve students' understanding of the importance of personal data protection and digital security through data literacy education, introduction to Google Authenticator, and hands-on practice to secure social media accounts. The activity was carried out offline with socialization and mentoring methods. The results showed that the training increased students' awareness and ability to maintain the security of their personal data.*

**Keywords:** Social Media, Data Literacy, Digital Security, Google Authenticator, Personal Data Protection

### ABSTRAK

*Kemajuan teknologi digital menjadikan media sosial seperti Instagram, TikTok, dan Twitter bagian penting dalam kehidupan generasi muda. Tetapi, literasi data dan kesadaran privasi masih rendah, terutama di kalangan siswa SMA yang sering kali hanya memahami fungsi dasar media sosial. Pelatihan ini bertujuan meningkatkan pemahaman siswa tentang pentingnya perlindungan data pribadi dan keamanan digital melalui edukasi literasi data, pengenalan Google Authenticator, serta praktik langsung untuk mengamankan akun media sosial. Kegiatan dilaksanakan offline dengan metode sosialisasi dan pendampingan, hasil pelatihan menunjukkan peningkatan kesadaran dan kemampuan siswa dalam menjaga keamanan data pribadi mereka.*

**Kata kunci:** Media Sosial, Literasi Data, Keamanan Digital, Google Authenticator, Perlindungan Data Pribadi



Copyright © 2025 The Author(s)  
This is an open access article under the CC BY-SA license.

## PENDAHULUAN

Di era digital ini, teknologi mengubah sebagian besar interaksi dan komunikasi antar manusia. Dengan media sosial, seseorang bisa mengekspresikan diri dan bertukar informasi dengan orang lain secara cepat. Namun, perkembangan yang pesat ini seringkali tidak diikuti oleh kesadaran serta pemahaman masyarakat pengguna. Masyarakat hanya melihat media sosial dari segi fungsinya saja tanpa menyadari bahwa data pribadi mereka dapat dikumpulkan, dianalisis, dan dimanfaatkan oleh pihak ketiga, sehingga sering menimbulkan kerentanan terhadap keamanan data yang belum terpikirkan sebelumnya.

Salah satu risiko terbesar adalah kejahatan digital yang mencakup penyalahgunaan data pribadi, yang dapat berujung pada pencurian identitas, penyebaran informasi tanpa izin, hingga manipulasi perilaku pengguna melalui algoritma yang dikendalikan oleh perusahaan teknologi. Selain itu, kurangnya literasi digital juga membuat banyak orang rentan terhadap serangan siber, seperti phishing atau peretasan akun, yang dapat membahayakan privasi dan keamanan mereka.

Oleh karena itu, diperlukan kesadaran dan edukasi yang lebih luas agar masyarakat tidak hanya menjadi konsumen pasif teknologi, tetapi juga memiliki pemahaman kritis dalam menjaga data pribadi serta mengambil langkah-langkah untuk melindungi diri mereka di dunia digital.

Minimnya pengetahuan masyarakat mengenai algoritma media sosial dapat menjadi masalah yang beragam. Masyarakat menghabiskan sebagian waktunya di media sosial, tanpa menyadari bahwa pola perilaku, ketertarikan, dan kesukaan mereka telah dianalisis dan menjadi tolak ukur pemilihan konten yang akan mereka konsumsi untuk seterusnya. Alhasil masyarakat akan terjebak dalam sebuah pola konsumsi yang sempit dan atau bahkan terpapar informasi yang menyesatkan. Disamping itu, minimnya kesadaran masyarakat soal pengelolaan data pribadi membuat mereka lebih rentan terhadap manipulasi konten, eksploitasi data, dan penyalahgunaan informasi pribadi. Penggunaan media sosial merupakan sesuatu yang umum terjadi di kalangan remaja dan anak sekolah. Posisi mereka yang masih berada pada fase peralihan menuju kedewasaan sering menimbulkan gejala dalam diri mereka yang sayangnya belum diikuti oleh pengendalian diri yang maksimal. Belum lagi kesadaran diri dalam penggunaan media sosial yang cenderung sering terlewatkan, ditambah dengan ketidaksadaran mereka akan masalah yang dapat diterima.

Media sosial sendiri menurut Rahmandika merupakan media online yang memudahkan penggunaannya untuk berpartisipasi, berbagi dan menciptakan isi seperti sebuah blog dan jejaring sosial (Akbar, 2019). Ada pendapat lain dari Van Dijk sebagaimana dikutip Nasrullah yang menyatakan bahwa media sosial adalah platform media yang fokus pada eksistensi pengguna dan memfasilitasi mereka dalam beraktivitas maupun berkolaborasi. Oleh karena itu, media sosial dapat dilihat sebagai medium online yang menguatkan ikatan sosial antar pengguna (Nasrullah, 2015).

Data merupakan suatu elemen penting dari informasi karena ia dapat memberikan deskripsi dari suatu kejadian di waktu tertentu (D'Ignazio & Bhargava, 2015). Data sendiri dapat diartikan sebagai kumpulan informasi yang dapat dianalisis untuk kemudian digunakan sebagai bahan pengambilan keputusan. Kemampuan untuk menganalisis dan menginterpretasi data ini disebut sebagai literasi data. Menurut Fazil, Literasi data diartikan sebagai kemampuan untuk mengeksplorasi, memahami, dan berkomunikasi dengan data secara efektif (Putra, 2024). Literasi data dapat membantu dalam pengambilan keputusan berbasis data dan meningkatkan kualitas pemecahan masalah.

Seiring berkembangnya teknologi informasi, sarana dan prasarana keamanan digital mendorong untuk memperkuat proteksinya. Keamanan data pribadi merupakan hak asasi manusia yang harus dijamin dan dihormati (Suari & Sarjana, 2023). Data pribadi yang mencakup informasi diri semakin rentan terhadap potensi cyber crime. Maraknya kejahatan cyber menciptakan suatu urgensi dalam masyarakat untuk melakukan pengamanan data pribadi. Namun banyak orang yang tidak menyadari bahwa informasi pribadi dapat disalahgunakan oleh pihak yang tidak

---

bertanggung jawab. Perlindungan data yang buruk telah menyebabkan peretasan dan kebocoran data yang meluas (Siahaan, 2022).

Kemajuan teknologi informasi memacu berkembangnya sarana proteksi informasi itu sendiri. Saat ini, metode keamanan autentikasi dua faktor (*two-factor authentication*) telah berhasil di implementasikan. Autentikasi dua faktor merupakan metode keamanan yang mengharuskan pengguna untuk memverifikasi identitas mereka melalui dua langkah berbeda sebelum mendapatkan akses ke akun mereka (Widodo, 2019). Google sendiri sebagai salah satu perusahaan penyedia internet terbesar di dunia memiliki tanggung jawab untuk melindungi data penggunanya. Google telah menerapkan berbagai metode keamanan untuk pengguna, yang salah satunya adalah Google Authenticator yang menggunakan metode keamanan *two-factor authentication* atau biasa disingkat 2FA. (Muttaqin, 2024).

Disamping kemudahan dan keamanan yang diberikan media sosial, terdapat beberapa hal yang menjadi permasalahan bagi penggunanya. Penelitian dari Wulandari et. al (2021) mengungkapkan bahwa algoritma media sosial menciptakan "*filter bubble*" yang membatasi akses pengguna terhadap informasi yang lebih luas, sehingga hanya terpapar pada konten yang sesuai dengan preferensi mereka dan berpotensi mengurangi wawasan siswa terhadap berbagai perspektif. Siswa-siswa yang tidak memahami cara kerja algoritma media sosial ini cenderung terjebak dalam pola konsumsi informasi yang sempit. Sehingga peningkatan pemahaman tentang algoritma sangat penting untuk membantu siswa menjadi lebih kritis dalam menilai konten yang mereka lihat di media sosial (Miranti et al, 2024).

Disamping itu, penelitian dari Livingstone et al (2018) menunjukkan bahwa banyak siswa tidak menyadari risiko yang terkait dengan penggunaan internet, yang dapat menyebabkan manipulasi informasi dan penyalahgunaan data pribadi. Rendahnya kesadaran siswa mengenai privasi digital dapat meningkatkan risiko penyalahgunaan data dan manipulasi informasi. Literasi data berperan penting dalam membantu siswa memahami risiko yang terkait dengan aktivitas online dan mengembangkan sikap kritis terhadap konten media sosial (Saputra, 2023).

Segala aktivitas dan perilaku yang dilakukan masyarakat dalam media sosial sepenuhnya dibentuk oleh persepsi mereka sebagai pengguna. Menurut Shoshana dalam bukunya "*The Age of Surveillance Capitalism*" (Zuboff, 2018) perusahaan teknologi menggunakan data pribadi pengguna untuk keuntungan mereka, hal ini mempengaruhi perilaku dan persepsi masyarakat terhadap media sosial. Persepsi ini merupakan representasi yang dikonstruksi dan dibangun oleh masyarakat itu sendiri. Tanpa pemahaman yang pasti mengenai algoritma dan perlindungan data media sosial, menciptakan kemungkinan dimana wawasan akan beragam perspektif mereka akan berkurang dan timbul pula risiko penyalahgunaan data pribadi mereka oleh pihak yang tidak bertanggung jawab.

Termasuk diantaranya siswa SMA Ma'arif NU Ajibarang. Siswa SMA Ma'arif NU Ajibarang tidak memahami algoritma yang membentuk media sosial dan bahaya yang ditimbulkan dari penggunaannya. Sehingga mereka cenderung menerima konten yang itu-itu saja dan

penyebaran data pribadi masih sering terjadi. Disamping kemudahan yang diberikan seringkali media sosial dijadikan sebagai alat penyebaran miss informasi oleh pihak yang tidak bertanggung jawab. Algoritma media sosial yang memprioritaskan konten berdasarkan popularitas dan reaksi emosional, berkontribusi pada penyebaran hoaks atau misinformasi (Wirasti & Wahyono, 2024). Hal ini membuat pengguna lebih rentan terhadap informasi yang menyesatkan, sehingga meningkatkan risiko terjebak dalam teori konspirasi dan hoax. Selain itu, banyak aplikasi media sosial yang mengumpulkan data pribadi seperti lokasi dan kebiasaan online tanpa pemahaman yang memadai dari pengguna. Hal ini membuat pengguna memberikan izin tanpa sadar, sehingga data mereka berisiko bocor atau disalahgunakan (Lubis & Nasution, 2023).

Tujuan dari kegiatan pengabdian ini adalah mendorong pemahaman dan kesadaran siswa SMA Ma'arif NU tentang bagaimana data dikumpulkan, dianalisis, dan dimanfaatkan di media sosial. Selain itu, siswa juga diberikan pelatihan menjaga privasi data pribadi pada media sosial. Dengan memberikan pemahaman dan pelatihan yang efektif, diharapkan siswa SMA Ma'arif NU menjadi pengguna media sosial yang kritis dan sadar akan keamanan mereka. Kegiatan ini melibatkan 28 perwakilan sekolah dari kelas X. Diharapkan dengan pemaparan materi dan pelatihan kepada 28 siswa ini dapat memberikan wawasan baru tentang cara kerja media sosial dan keamanan data pribadi secara maksimal.

## **METODE**

Kegiatan pengabdian kepada masyarakat ini akan dilakukan melalui pendekatan partisipatif edukatif, di mana siswa SMA kelas 10 akan dilibatkan secara aktif dalam setiap tahapan pembelajaran. Metode ini bertujuan untuk meningkatkan pemahaman praktis siswa tentang bagaimana data bekerja melalui pembelajaran interaktif, diskusi kelompok, dan praktik langsung. Adapun tahapan-tahapan yang akan dilalui dalam pelaksanaan kegiatan ini adalah sebagai berikut:

### **1. Tahap Persiapan**

- **Survey Kebutuhan:** Mengidentifikasi kebutuhan siswa terkait pemahaman tentang data dan teknologi melalui diskusi awal dengan guru dan siswa untuk mengetahui tingkat pemahaman mereka saat ini.
- **Pengembangan Modul dan Materi:** Menyusun modul pembelajaran yang interaktif dan sesuai dengan level pemahaman siswa. Materi akan mencakup dasar-dasar tentang data di media sosial, privasi dan keamanan data, serta contoh penggunaan data dalam kehidupan sehari-hari.

### **2. Tahap Pelaksanaan**

- **Pengenalan Konsep Dasar (Sesi Teori):** Dalam sesi ini, siswa akan diperkenalkan dengan konsep-konsep dasar tentang bagaimana data

---

dikumpulkan, diproses, dan digunakan di media sosial. Materi ini disampaikan melalui presentasi dan diskusi interaktif.

- **Workshop dan Simulasi Pengolahan Data:** Sesi ini mencakup simulasi sederhana tentang pengolahan data, seperti bagaimana algoritma bekerja di media sosial untuk merekomendasikan konten berdasarkan data pengguna. Siswa akan diajak untuk langsung berpartisipasi dalam simulasi ini untuk memperkuat pemahaman mereka.
- **Diskusi dan Tanya Jawab:** Setelah setiap sesi, akan ada waktu untuk diskusi dan tanya jawab agar siswa dapat mengklarifikasi konsep-konsep yang telah dipelajari dan berdiskusi tentang dampaknya dalam kehidupan mereka.

### 3. Tahap Evaluasi dan Refleksi

- **Evaluasi Pemahaman Siswa:** melakukan post-test untuk mengukur peningkatan pemahaman siswa setelah kegiatan. Siswa juga akan diminta untuk memberikan umpan balik mengenai materi dan metode yang digunakan.
- **Refleksi dan Diskusi Kelompok:** Siswa akan diminta untuk berdiskusi dalam kelompok kecil untuk membahas hal-hal yang telah mereka pelajari dan bagaimana mereka bisa menerapkannya dalam penggunaan media sosial sehari-hari.
- **Laporan Hasil Kegiatan:** Tim pengabdian akan menyusun laporan mengenai hasil kegiatan, yang mencakup evaluasi pemahaman siswa, umpan balik, serta rekomendasi untuk kegiatan lanjutan.

### 4. Tahap Tindak Lanjut

- **Penyediaan Materi Lanjutan:** Materi pembelajaran yang telah disusun akan disediakan secara digital agar siswa dapat terus mempelajarinya secara mandiri setelah kegiatan selesai.

## HASIL DAN PEMBAHASAN

Kegiatan ini juga mencakup diskusi interaktif dan simulasi kasus nyata untuk membantu siswa memahami risiko keamanan digital serta strategi perlindungan data yang dapat diterapkan dalam kehidupan sehari-hari. Melalui pendekatan praktis, siswa diajak untuk mengenali berbagai ancaman yang dapat timbul akibat kebocoran data pribadi, seperti pencurian identitas dan penyalahgunaan informasi di dunia maya. Selain itu, peserta diberikan wawasan mengenai pentingnya pengelolaan kata sandi yang kuat, verifikasi dua langkah, serta kebijakan privasi yang diterapkan oleh berbagai platform digital. Dengan adanya kegiatan ini, diharapkan siswa tidak hanya mampu menggunakan teknologi secara lebih bijak, tetapi juga dapat menjadi agen

perubahan dalam menyebarluaskan pentingnya literasi data dan perlindungan privasi di lingkungan sekolah maupun masyarakat.

Menindaklanjuti hasil pre-tes, sesi berikutnya difokuskan pada pengenalan konsep dasar literasi data, termasuk bagaimana data pribadi dikumpulkan, diproses, dan digunakan oleh berbagai platform digital. Pemateri menjelaskan secara interaktif tentang pentingnya kesadaran akan jejak digital serta risiko yang dapat timbul akibat kurangnya perlindungan data. Setelah pemaparan teori, peserta diberikan demonstrasi langsung mengenai cara mengaktifkan dan menggunakan Google Authenticator sebagai langkah perlindungan tambahan untuk akun mereka. Dalam sesi ini, peserta juga diajak untuk mencoba mengamankan akun mereka secara mandiri dengan bimbingan tim pengabdian, sehingga mereka dapat memahami langkah-langkah yang perlu dilakukan dalam praktik sehari-hari.

Selanjutnya, tim pengabdian menyampaikan materi secara bergantian. Salah satu materi utama yang disampaikan adalah "Bagaimana Data Bekerja pada Platform Media Sosial." Dalam sesi ini, pemateri menjelaskan konsep dasar tentang bagaimana algoritma media sosial mengolah data pengguna serta risiko keamanan yang dapat timbul akibat penyalahgunaan data. Selain itu, peserta juga diberikan pelatihan praktik penggunaan Google Authenticator, yang mencakup proses instalasi, pengaktifan autentikasi dua faktor, dan cara menggunakannya untuk mengamankan akun media sosial mereka Gambar 1. Dalam sesi ini, pemateri menjelaskan konsep dasar data, termasuk bagaimana algoritma bekerja di media sosial serta pentingnya keamanan data.



Gambar 1. Pemaparan materi mengenai data dan keamanan data

---

*Google authenticator* dipilih sebagai keamanan kedua yang digunakan, dengan menyoroti keunggulannya seperti kemudahan dalam penggunaan, dan fleksibilitas dalam penerapan aplikasi meta. Setelah memahami konsep dasar literasi data dan risiko keamanan digital, peserta diberikan pelatihan teknis mengenai perlindungan akun media sosial dengan *Google Authenticator*. Pemateri menguraikan konsep autentikasi dua faktor (2FA), yang merupakan metode keamanan tambahan untuk melindungi akun dari akses yang tidak sah. Penjelasan dimulai dengan pengenalan tentang bagaimana 2FA bekerja, di mana pengguna perlu memasukkan kode verifikasi dari aplikasi autentikator selain kata sandi utama mereka.

Pada tahap implementasi, peserta diberikan panduan langkah demi langkah untuk mengaktifkan autentikasi dua faktor di platform media sosial Instagram. Proses ini dimulai dengan pengunduhan aplikasi *Google Authenticator* dan dilanjutkan dengan konfigurasi akun. Berikut langkah-langkah yang diajarkan secara rinci kepada peserta:

1. Mengunduh dan Menginstal *Google Authenticator*  
Peserta diarahkan untuk mencari aplikasi *Google Authenticator* di Play Store atau App Store dan menginstalnya di perangkat mereka. Pemateri menekankan bahwa aplikasi ini tidak membutuhkan koneksi internet untuk menghasilkan kode verifikasi, sehingga tetap aman digunakan di berbagai kondisi.
2. Mengaktifkan Autentikasi Dua Faktor di Instagram  
Setelah aplikasi terpasang, peserta membuka aplikasi Instagram dan mengikuti langkah-langkah berikut:
  - a) Masuk ke menu pengaturan dan privasi.
  - b) Pilih opsi pusat akun untuk mengakses pengaturan keamanan akun.
  - c) Masuk ke bagian kata sandi dan keamanan, lalu pilih autentikasi dua faktor.
3. Menghubungkan Akun Instagram dengan *Google Authenticator*
  - a. Setelah memilih autentikasi dua faktor, peserta memilih opsi Aplikasi Autentikasi sebagai metode keamanan tambahan.
  - b. Instagram akan menampilkan kunci penyiapan atau kode QR.
  - c. Peserta membuka aplikasi *Google Authenticator* dan menekan ikon “+” untuk menambahkan akun baru.
  - d. Jika menggunakan kunci penyiapan, peserta menyalin kode dari Instagram dan memasukkannya secara manual di *Google Authenticator*. Jika menggunakan kode QR, peserta cukup memindainya.
4. Menggunakan Kode Verifikasi untuk Login yang Lebih Aman

- a. Setelah akun terhubung, Google Authenticator akan menghasilkan kode unik yang berubah setiap beberapa detik.
- b. Peserta kembali ke Instagram, memasukkan kode dari aplikasi autentikator, dan menekan tombol Berikutnya untuk menyelesaikan proses aktivasi.
- c. Setelah autentikasi dua faktor aktif, setiap kali peserta login ke Instagram di perangkat baru, mereka harus memasukkan kode verifikasi yang dihasilkan oleh Google Authenticator untuk memastikan keamanan akun mereka.

Pelatihan ini juga mencakup pembahasan mengenai bagaimana autentikasi dua faktor tidak hanya berguna untuk media sosial tetapi juga dapat diterapkan pada akun email, layanan perbankan digital, dan platform lainnya untuk mencegah pencurian data. Peserta didorong untuk segera mengaktifkan fitur ini di berbagai akun mereka agar lebih aman dari ancaman siber. Selain itu, diberikan pemahaman mengenai berbagai jenis metode autentikasi, seperti kode verifikasi melalui aplikasi autentikator, SMS, atau perangkat fisik, sehingga peserta dapat memilih opsi yang paling sesuai dengan kebutuhan mereka. Dengan penerapan autentikasi dua faktor, diharapkan peserta dapat meningkatkan kesadaran akan pentingnya keamanan digital dan melindungi informasi pribadi mereka dari upaya peretasan atau penyalahgunaan data.

Setelah pemaparan materi selesai, peserta langsung diarahkan untuk praktik dengan pendampingan pemateri, sehingga siswa dapat segera mengatasi kesulitan dengan bertanya langsung. Hal ini bertujuan agar pemahaman peserta terhadap materi dapat segera diterapkan dalam bentuk praktik nyata.

Pemateri memulai dengan menjelaskan langkah-langkah untuk menghubungkan aplikasi dengan pihak kedua (authenticator), mulai dari proses pemindaian kode QR hingga proses verifikasi kode yang dihasilkan. Peserta diberikan kesempatan untuk mencoba secara langsung dengan akun mereka masing-masing, sehingga mereka dapat merasakan manfaat autentikasi dua faktor secara nyata.

Selain itu, pemateri juga menjelaskan bagaimana cara mengelola akun yang telah dikaitkan dengan aplikasi autentikator, termasuk langkah-langkah untuk mencadangkan kode keamanan guna mengantisipasi kehilangan akses ke perangkat autentikator. Peserta juga diberikan panduan mengenai cara melepaskan keterkaitan dengan pihak kedua jika diperlukan, misalnya saat mereka mengganti perangkat atau ingin mengubah metode autentikasi yang digunakan.

Selama sesi praktik, pemateri dan tim pendamping aktif memberikan bimbingan dan memastikan setiap peserta berhasil mengaktifkan fitur keamanan ini dengan benar. Dengan pendekatan langsung ini, diharapkan peserta dapat lebih memahami pentingnya perlindungan

data pribadi dan mampu menerapkan langkah-langkah keamanan digital dalam kehidupan sehari-hari.



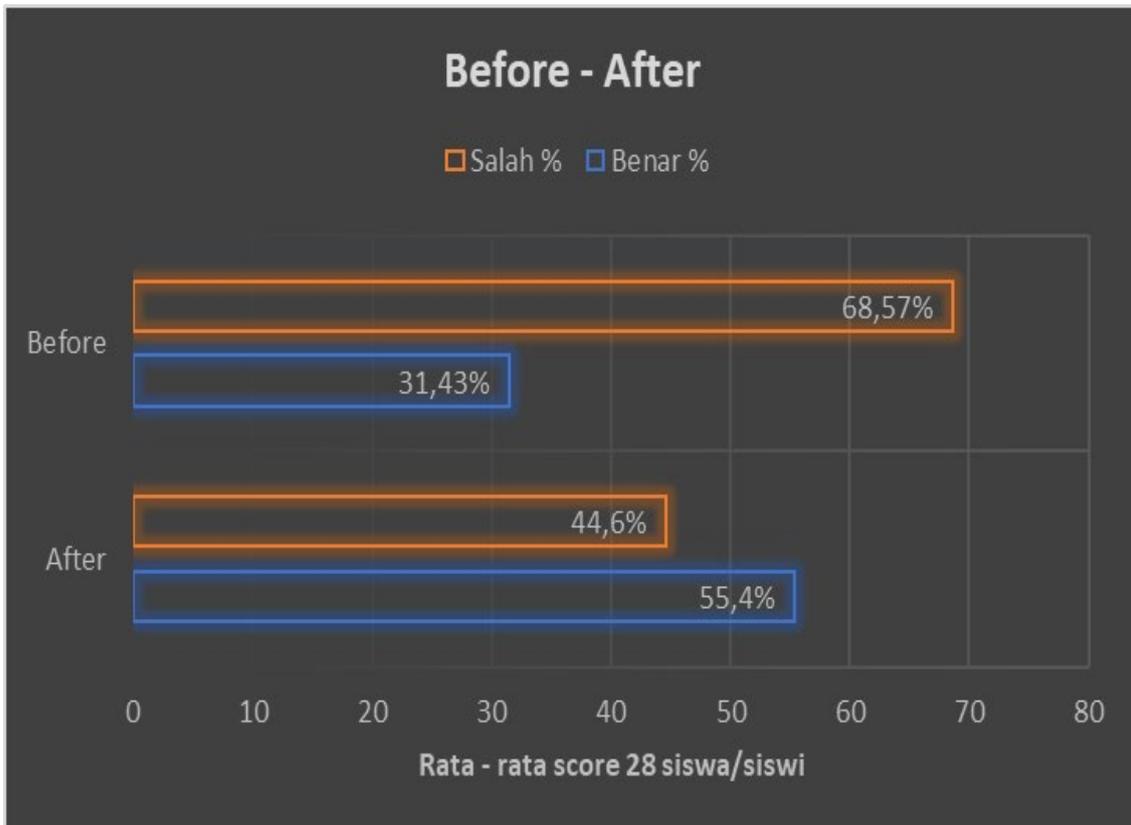
**Gambar 3.** Praktik autentikasi dua langkah di media sosia

Setelah sesi pematerian selesai, kegiatan dilanjutkan dengan pemberian post-tes kepada peserta. Post-test ini bertujuan untuk mengukur keberhasilan kegiatan serta mengetahui sejauh mana pemahaman peserta meningkat setelah mengikuti pelatihan. Soal yang diberikan dalam post-tes serupa dengan pre-tes, sehingga memungkinkan adanya perbandingan yang jelas mengenai perkembangan pemahaman peserta terkait literasi data dan keamanan digital.

Hasil post-tes menunjukkan bahwa terjadi peningkatan pemahaman yang signifikan, terutama dalam aspek pengetahuan mengenai pentingnya perlindungan data pribadi, cara kerja autentikasi dua faktor, serta langkah-langkah yang dapat dilakukan untuk meningkatkan keamanan akun digital. Peserta yang sebelumnya belum memahami konsep keamanan data kini lebih sadar akan risiko kebocoran informasi dan lebih siap untuk menerapkan praktik perlindungan data dalam kehidupan sehari-hari.

Selain itu, melalui diskusi reflektif setelah post-tes, peserta juga mengungkapkan bahwa mereka merasa lebih percaya diri dalam menggunakan fitur keamanan digital dan memahami cara mengamankan akun mereka di berbagai platform. Dengan adanya peningkatan pemahaman ini, diharapkan peserta dapat menerapkan serta menyebarkan informasi yang mereka

peroleh kepada lingkungan sekitarnya, sehingga kesadaran akan pentingnya literasi data dan keamanan digital dapat terus berkembang.



Gambar 4. Perbandingan pemahaman siswa sebelum dan setelah melakukan pelatihan

Dari seluruh siswa yang mengikuti kegiatan mencakup materi “bagaimana data bekerja pada platform media sosial”, sebanyak 28 peserta mengisi kuesioner yang disediakan oleh tim pengabdian. Hasil analisis menunjukkan bahwa sebelum pelatihan, hanya 31,43% peserta yang menjawab dengan benar, mencerminkan rendahnya pemahaman awal mereka tentang keamanan data. Setelah pelatihan, persentase jawaban benar meningkat signifikan menjadi 55,4%, menandakan adanya peningkatan pemahaman siswa terhadap literasi digital dan perlindungan data pribadi.

Selain itu, umpan balik dari peserta menunjukkan bahwa materi yang disampaikan sangat relevan dan bermanfaat dalam meningkatkan rasa aman mereka saat menggunakan media sosial. Mereka juga lebih memahami jenis data pribadi yang harus dilindungi serta langkah-langkah pencegahan yang dapat diterapkan untuk menjaga keamanan akun mereka dari potensi ancaman digital.

Hasil ini menunjukkan bahwa pelatihan yang dilakukan efektif dalam meningkatkan pemahaman peserta, terutama dalam aspek literasi data dan keamanan digital. Peningkatan skor dari pre-test ke post-test mencerminkan keberhasilan metode pembelajaran yang diterapkan,

---

seperti penyampaian materi secara sistematis, diskusi interaktif, serta praktik langsung dalam mengamankan akun media sosial menggunakan autentikasi dua faktor.

Peserta tidak hanya memperoleh pemahaman tentang pentingnya perlindungan data pribadi, tetapi juga mampu menerapkan langkah-langkah keamanan secara mandiri. Pendekatan berbasis praktik, seperti simulasi penggunaan Google Authenticator, terbukti membantu siswa memahami cara kerja fitur keamanan ini dengan lebih baik. Selain itu, umpan balik dari peserta menunjukkan bahwa metode pelatihan yang menggabungkan teori dan praktik membuat materi lebih mudah dipahami dan diterapkan dalam kehidupan sehari-hari.

## **SIMPULAN**

Pelatihan tentang bagaimana data bekerja di media sosial sangat diperlukan oleh siswa. Berdasarkan hasil pelatihan, beberapa siswa menunjukkan kurangnya pengetahuan tentang data pribadi dan alternatif cara mengamankan data selain menggunakan sandi. Namun, setelah menerima informasi mengenai data pribadi dan kasus-kasus nyata yang dipaparkan oleh pemateri tentang bahaya serangan terhadap data pribadi, siswa menjadi lebih perhatian terhadap ancaman keamanan, termasuk upaya peretasan di akun media sosial mereka. Pengetahuan baru yang relevan ini mudah diterapkan oleh siswa dalam aktivitas sehari-hari. Selain itu, kasus nyata yang dipaparkan membantu siswa memahami dampak serius dari kebocoran data pribadi.

Pelatihan serupa sebaiknya dilakukan secara rutin dan tidak hanya terbatas pada siswa SMA. Materi yang disampaikan perlu diperluas dengan mencakup topik keamanan digital yang lebih mendalam, seperti pengelolaan kata sandi, penggunaan autentikasi dua faktor, serta pengenalan perangkat lunak keamanan. Edukasi mengenai perlindungan dan keamanan data juga perlu menjangkau masyarakat secara lebih luas, termasuk guru, orang tua, dan para pengguna aktif media sosial.

Selain itu, pengembangan modul atau panduan digital yang mudah diakses dapat menjadi sumber referensi mandiri yang bermanfaat bagi masyarakat. Namun, terdapat beberapa kekurangan dalam pelatihan ini. Cakupan pelatihan terbatas hanya pada siswa SMA, sehingga kelompok lain yang juga rentan terhadap ancaman keamanan data belum terjangkau. Selain itu, waktu pelatihan yang singkat membatasi pembahasan lebih mendalam mengenai langkah-langkah teknis untuk melindungi data.

Edukasi perlindungan data pribadi perlu dilakukan secara berkelanjutan, baik di sekolah maupun di komunitas masyarakat. Pemerintah dan lembaga pendidikan diharapkan dapat mendukung kegiatan pelatihan ini dengan menyediakan sumber daya seperti pemateri ahli dan perangkat pelatihan. Kolaborasi antara berbagai pihak, termasuk sektor teknologi, diperlukan untuk meningkatkan kesadaran dan menyediakan solusi keamanan data yang mudah diakses. Monitoring terhadap efektivitas pelatihan juga penting dilakukan untuk memastikan keberlanjutan program edukasi ini. Dengan langkah-langkah di atas, diharapkan kesadaran akan pentingnya perlindungan data pribadi dapat menyebar luas, menciptakan lingkungan digital yang lebih aman.

## UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah mendukung pelaksanaan kegiatan pengabdian kepada masyarakat ini. Terima kasih juga kami sampaikan kepada Ibu Dian Kartika Sari selaku dosen pembimbing, yang telah memberikan bimbingan, arahan, dan dukungan dalam penyusunan dan pelaksanaan kegiatan ini. Tak lupa, penulis berterima kasih kepada SMA MAARIF NU 1 AJIBARANG atas kesempatan yang diberikan, fasilitas yang disediakan, serta dukungan penuh yang telah membantu kelancaran

## DAFTAR REFERENSI

- D'Ignazio, C., & Bhargava, R. (2015). *Approaches to Building Big Data Literacy*. Bloomberg Data for Good Exchange Conference.
- Livingstone, S., et al (2018). "European Research on Children's Internet Use: Assessing the Past and Anticipating the Future", *New Media and Society*, 20(3), 1103-1122. DOI: 10.1177/1461444816685930.
- Lubis, S.N. & Nasution, M.I.P. (2023). "Analisis Penyalahgunaan Data Pribadi Dalam Menggunakan Media Sosial", *Journal of Sharia Economics Scholar*, 2(2), pp. 75-78. DOI: <https://doi.org/10.5281/zenodo.12527836>.
- Miranti, M., Purboyo, M.G., & Junaidi. (2024). "Backlash di Era Digital: Memahami Respons Negatif Terhadap Konten Sensitif di Platform Media Sosial", *Jurnal Pendidikan Kreativitas Pembelajaran*, 6(4), pp. 219-230.
- Muttaqin, F.F (2024). Implementasi Two-Factor Authentication sebagai Lapisan Keamanan Tambahan pada Google. DOI: 10.13140/RG.2.2.34499.21284.
- Saputra, D.F. (2023). "Literasi Digital untuk Perlindungan Data Pribadi", *Jurnal Ilmu Kepolisian*, 17(3), pp. 1-8.
- Siahaan, A.L.S (2022). "Urgensi Perlindungan Data Pribadi di Platform Marketplace Terhadap Kemajuan Teknologi", *Majalah Hukum Nasional*, 52(2), 209-223. DOI: 10.33331/mhn.v52i2.169.
- Suari, K.R.A. & Sarjana, I.M. (2023). "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia", *Jurnal Analisis Hukum*, 6(1), 132-146. DOI: 10.38043/jah.v6i1.4484.
- Widodo, S. (2019). "Implementasi dan Evaluasi Two-Factor Authentication untuk Meningkatkan Keamanan Sistem Informasi", *Jurnal Sistem Informasi*, 15(2), pp. 1-10.
- Wirasti, M.K. & Wahyono, S.B. (2024). "Studi Resepsi Khalayak terhadap Disinformasi Pandemi Covid-19 pada Media Sosial di Yogyakarta", *Jurnal Komunikasi*, 19(1), pp. 23-46.
- Wulandari, V., Rullyana, G., & Ardiansah. (2021). "Pengaruh Algoritma Filter Bubble dan Echo Chamber Terhadap Perilaku Penggunaan Internet", *Berkala Ilmu Perpustakaan dan Informasi*, 17(1), pp. 98-111.

## Buku:

- Akbar, R.S. (2019). *Peran Media Sosial dalam Perubahan Gaya Hidup Remaja*. Skripsi. Fakultas Ilmu Sosial dan Ilmu Politik. Universitas Airlangga: Surabaya.
- Nasrullah, Ri. (2015). *Media Sosial: Perspektif Komunikasi, Budaya, dan Sosioteknologi*. Bandung: Simbiosis Rekatama Media.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.

## Sumber Internet:

- Putra, M.F.I. (2024). *Pentingnya Literasi Data untuk Kesuksesan di Era Digital*. Fakultas Teknologi Maju dan Multidisiplin (Online). Tersedia di: dari <https://ftmm.unair.ac.id/pentingnya-literasi-data-untuk-kesuksesan-di-era-digital/>  
Diakses: 22 Desember 2024.