

SOSIALISASI TIPS MENJAGA DATA DI SMARTPHONE, MEDIA SOSIAL, DAN APLIKASI BERBASIS CLOUD AGAR TIDAK BOCOR DI SMKN 9 MUARO JAMBI

Fadhilah Febriyani, Hasan Hafidzudin, Mhd Malzi Riyandityo
Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi
Email: fadhilahfebriyani@gmail.com

Abstrak

Teknologi informasi dan komunikasi saat ini berkembang sangat pesat, hal itu memberikan dampak besar terhadap perilaku anak remaja tentunya dalam penggunaan perangkat digital. Perkembangan teknologi membuat pengguna smartphone, media sosial, dan aplikasi berbasis cloud menjadi meningkat, oleh karena itu perlu diimbangi dengan kesadaran keamanan data pribadi. Dan untuk itu dilakukanlah sosialisasi yang bertujuan untuk meningkatkan pengetahuan dan kesadaran kepada siswa kelas 11 DKV 2 SMK Negeri 9 Muaro Jambi terkait pentingnya menjaga keamanan data agar tidak terjadi kebocoran yang dapat merugikan. Metode pelaksanaan yang digunakan yaitu sosialisasi dengan memberikan materi melalui presentasi dan mengajak siswa untuk menerapkan materi yang telah diberikan. Hasil dari kegiatan memperlihatkan peningkatan pemahaman kepada siswa untuk menerapkan apa yang sudah dipaparkan yaitu menjalankan tips untuk menjaga keamanan data pribadi.

Kata kunci: Keamanan Data, Smartphone, Media Sosial, Cloud Storage, Sosialisasi.

Abstrack

Information and communication technology is currently developing very rapidly, which has a significant impact on the behavior of adolescent children, particularly in their use of digital devices. Technological advancements have led to an increase in the number of users of smartphones, social media, and cloud-based applications, which is why it needs to be balanced with awareness of personal data security. And for that, socialization was carried out with the aim of increasing knowledge and awareness among 11th-grade DKV 2 students at SMK Negeri 9 Muaro Jambi regarding the importance of maintaining data security to prevent leaks that could be detrimental. The implementation method used is socialization by providing material thru presentations and encouraging students to apply the material that has been given. The results of the activity show an increase in students' understanding of how to apply what has been presented, namely implementing tips for protecting personal data security.

Article History

Received: November 2025
Reviewed: November 2025
Published: November 2025

Plagiarism Checker No 583
Prefix DOI: Prefix DOI:
10.8734/sindoro.v1i2.360
Copyright: Author
Publish by: SINDORO



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

PENDAHULUAN

Perkembangan dunia digital saat ini menimbulkan dua sisi yang berlawanan dalam kaitannya dengan pengembangan literasi digital. Di satu sisi, kemajuan peralatan digital dan akses mudah terhadap informasi membuka peluang besar untuk pembelajaran dan inovasi. Namun, disisi lain hal ini juga menimbulkan tantangan serius, terutama terkait keamanan data pribadi. Data pribadi adalah informasi yang berhubungan langsung atau tidak langsung dengan individu yang dapat diidentifikasi, seperti nama, Alamat, tanggal lahir, informasi keuangan, Alamat IP, riwayat pembelian, catatan medis, dan data biometrik. Di era digital yang semakin canggih, data ini

telah menjadi asset berharga yang sering dikumpulkan dan diproses oleh bisnis, pemerintah, dan berbagai organisasi untuk tujuan administrative. Namun, risiko kebocoran data semakin tinggi, terutama di kalangan generasi muda yang aktif menggunakan smartphone, media sosial, dan aplikasi berbasis cloud.

Media sosial berbagai platform digital yang memungkinkan pengguna berinteraksi, berbagi konten, dan terhubung dengan orang lain melalui jaringan online, memfasilitasi pertukaran informasi, pendapat, dan pengalaman dalam komunitas virtual. Meskipun memberikan manfaat besar, media sosial juga rentan terhadap perilaku berinternet yang tidak sehat, seperti penyebaran berita hoaks, ujaran kebencian, dan intoleransi. Di Indonesia sekitar 70 juta generasi muda menghabiskan waktu hampir 5 jam per hari berinternet melalui telepon genggam, komputer, atau laptop, yang menjadikan literasi digital sebagai kebutuhan mendesak. Literasi digital bukan hanya kemampuan teknis menggunakan perangkat dan aplikasi, tetapi juga pemahaman komprehensif untuk berinteraksi secara aman, etis, dan produktif di dunia digital.

Di konteks ini, sosialisasi bertema “Tips Menjaga Data di Smartphone, Media Sosial, dan Aplikasi Berbasis Cloud Agar Tidak Bocor di SMKN 9 Muaro Jambi”, khususna untuk siswa kelas 11 DKV 2 menjadi langkah penting untuk meningkatkan kesadaran dan keterampilan generasi muda. Sosialisasi ini bertujuan untuk memberikan panduan praktis tentang cara melindungi data pribadi dari risiko kebocoran, seperti melalui pengaturan privasi, penggunaan kata sandi yang kuat, dan etika berbagai informasi di platform digital. Dengan pendekatan holistic dan berkelanjutan diharapkan siswa tidak hanya menjadi konsumen pasif teknologi, tetapi warga juga harus cerdas, kritis, dan bertanggung jawab. Peran orang tua dan pemangku kepentingan lainnya sangat krusial dalam mendukung upaya ini, memastikan generasi abad ke-21 siap menghadapi tantangan revolusi digital dengan memaksimalkan peluang dan meminimalkan risiko.

METODE PALAKSANAAN

Dalam kegiatan ini metode yang digunakan dalam sosialisasi tema “Tips Menjaga Data Di Smartphone, Media Sosial, Dan Aplikasi Berbasis Cloud” memerlukan persiapan dan metode yang tepat agar siswa dapat memahami dengan baik materi yang diberikan. Materi perlu disampaikan dengan bahasa yang mudah dimengerti agar efektif dan efisien oleh siswa/siswi.

Metode sosialisasi ini dipilih karena dinilai lebih mudah penerapannya dengan mempersentasikan materi di depan dan membuka sesi tanya jawab kemudian berdiskusi.

Kegiatan sosialisasi ini dilakukan disela jam belajar mengajar dan dilakukan diruang kelas yang bisa membuat siswa/i lebih berkonsentrasi. Materi sosialisasi berupa tips ataupun cara menjaga data dismartphone, media sosial, dan aplikasi cloud. Sosialisasi dilakukan di SMK Negeri 9 Muaro Jambi tepatnya kelas 11 dkv dengan jumlah 21 Murid.

HASIL DAN PEMBAHASAN

Sebagai siswa DKV yang aktif di dunia digital, melindungi data pribadi dan aset kreatif adalah hal yang sangat penting. keamanan dimulai dari perangkat yang paling sering anda gunakan. Pada smartphone, pastikan anda menggunakan kata sandi layar yang rumit dan mengktufkan biometrik. selalu perbarui sistem operasi dan aplikasi untuk menutup celah keamanan. hindari *login* ke akun penting melalui wi-fi publik yang tidak aman, dan hanya *install*

aplikasi dari toko resmi (Melinda, 2020). Untuk media sosial dan akun digital, perlindungan utamanya adalah disiplin. gunakan kata sandi yang berbeda dan kuat untuk setiap akun, danwajibkan penggunaan autentikasi dua faktor (2FA). bersikaplah bijak dalam berbagi, jangan unggah dokumen identitas dan atur pengaturan privasi agar postingan anda hanya dilihat oleh orang terpercaya. (Nugroho, 2024)

Sementara untuk aplikasi berbasis cloud yang menyimpan aset desain, 2FA adalah keharusan mutlak. ketika berbagi file, berikan izin akses yang terbatas (hanya lihat) dan pertimbangkan untuk mengenkripsi file yang sangat rahasia. Waspada terhadap ancaman seperti phishing jangan pernah mengklik tautan mencurigakan yang meminta data pribadi anda. ingat, keamanan digital adalah kebiasaan harian yang harus terus diterapkan agar karya dan privasi anda terlindungi sepenuhnya. (satria, 2024)

Salah satu upaya yang harus dilakukan dalam melindungi data pribadi yaitu dengan menjaga keamanan kata sandi pribadi. Adapun beberapa cara untuk membuat kata sandi atau password yang kuat agar aman dari kebocoran data. Menurut (Dewaweb team, 2023) sebagai berikut:

1. Menggunakan kata sandi berbeda-beda di setiap akun
Menggunakan kata sandi yang berbeda-beda di setiap akun memungkinkan pengguna untuk menghindari terjadinya pembajakan secara sekaligus di setiap akun ketika kata sandi yang dimiliki oleh seseorang diketahui oleh orang lain.
2. Menghindari bentuk kata sandi yang mudah ditebak
Menggunakan bentuk kata sandi yang mudah ditebak adalah salah satu kesalahan yang sering dilakukan oleh banyak orang seperti "qwerty", "12345678", atau "admin#123", karena orang lain bisa saja mengetahui kata sandi yang digunakan oleh seseorang dari informasi yang diunggah oleh orang tersebut di media-media online.
3. Rahasiakan dan amankan kata sandi
Merahasiakan kata sandi ataupun *username* kepada siapapun meskipun orang terdekat sekalipun, ataupun tidak membeberkan *username* dan kata sandi di tempat umum.
4. Menggunakan kata sandi generator dan manajer
Kata sandi generator dan manajer adalah *tools* yang berfungsi untuk menghasilkan kata sandi secara otomatis, kata sandi yang kuat biasanya terdiri dari huruf besar dan kecil, angka, hingga karakter khusus, alat ini biasanya sudah tersedia di pengguna akun *google*.
5. Mematuhi syarat kata sandi yang kuat
Sebuah aplikasi biasanya merekomendasikan beberapa syarat pembuatan kata sandi yang harus dipatuhi agar keamanan akun terjamin, seperti menggunakan huruf besar, huruf kecil, angka, simbol atau tanda baca khusus.
6. Mengaktifkan verifikasi 2 langkah
Verifikasi 2 langkah berfungsi sebagai langkah kedua setelah memasukan kata sandi, alat ini sudah banyak diterapkan pada layanan *online* seperti media sosial, *email*, *mobile banking*, dan sebagainya.
7. Memperbaharui *software*
Sebagian besar aktivitas *hacker* menargetkan celah atau kerentanan yang terdapat pada *software*. Sehingga pengguna gawai harus sering memperbaharui *software* ke versi terbaru, guna memperbaiki *bug* dan kerentanan yang ada sebelumnya dalam *software*.
8. Menggunakan kata sandi pada semua gawai
Setiap gawai yang dimiliki oleh seseorang diusahakan menggunakan kata sandi untuk mencegah akses tanpa izin dari pihak ketiga.

KESIMPULAN

Menjaga privasi dan keamanan data pribadi merupakan tanggung jawab bersama yang harus disadari oleh semua pengguna teknologi, termasuk siswa SMKN 9 Muaro Jambi yang aktif memanfaatkan perangkat digital untuk belajar, berkomunikasi, dan berinteraksi secara daring. Upaya perlindungan ini dapat dimulai dari langkah sederhana, seperti membuat kata sandi yang kuat, mengaktifkan fitur keamanan biometrik, serta rutin memperbarui sistem operasi dan aplikasi pada smartphone guna mencegah potensi celah keamanan.

Dalam konteks penggunaan media sosial, siswa diharapkan lebih selektif dan berhati-hati saat membagikan informasi pribadi. Pengaturan privasi akun perlu dioptimalkan agar data tidak mudah diakses oleh pihak yang tidak bertanggung jawab. Begitu pula dalam penggunaan layanan berbasis cloud, siswa sebaiknya hanya mengunggah dokumen atau data ke platform yang memiliki reputasi baik, serta selalu keluar dari akun setelah menggunakan perangkat bersama atau publik.

Dengan menerapkan kebiasaan digital yang aman dan bertanggung jawab, siswa SMKN 9 Muaro Jambi tidak hanya melindungi diri dari risiko kebocoran data, tetapi juga menjaga nama baik pribadi dan institusi sekolah. Lebih jauh, penerapan kebiasaan ini menjadi langkah penting dalam membangun budaya literasi digital yang etis, cerdas, dan berkelanjutan di lingkungan pendidikan.

DAFTAR PUSTAKA

- Meilinda, N., Malinda, F., & Aisyah, S. M. (2020). Literasi digital pada remaja digital (Sosialisasi pemanfaatan media sosial bagi pelajar Sekolah Menengah Atas). *Jurnal Abdimas Mandiri*, 4(1).
- Nugroho, F. N. P., Listanto, M. F., Amelia, N., & Annisa, S. (2024). Analisis Kebocoran Data Pribadi Dalam Media Sosial. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, 1(2), 58-65.
- Setyaningsih, R., Abdullah, A., Prihantoro, E., & Hustinawaty. (2019). Model Penguatan Literasi Digital Melalui Pemanfaatan E-Learning. *Jurnal ASPIKOM*, 3(6), 1200-1214.
- Wahyuni, S. (2019). *Menumbuhkan Literasi Digital Generasi Millenial di Era Revolusi Industri 4.0*. Prosiding Seminar Nasional Pendidikan Program Pascasarjana Universitas PGRI Palembang.
- Wiratama, B. A., & Darma, G. S. (2021). Media Sosial dan Dampaknya terhadap Perilaku Konsumen di Indonesia. *Jurnal Manajemen dan Bisnis*, 18(1), 1-15.
- Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data
- Konsumen Financial Technology di Indonesia: Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, 3(2), 145-160.
- Dewaweb team. (2023). *10 Cara Membuat Password yang Kuat Agar Aman dari Hacker*. Dewaweb. Diakses dari: <https://www.dewaweb.com/blog/cara-membuat-password-yang-kuat/>

- Djafar, W. (2019). Hukum perlindungan data pribadi di indonesia: lanskap, urgensi dan kebutuhan pembaruan. In Seminar Hukum dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM (Vol. 26). 1-14.
- EIKON Technology. (2019). 6 Langkah Meningkatkan Keamanan Email Dari Serangan Cyber. EIKON Technology. Diakses dari: <https://blog.eikontechnology.com/keamanan-email/>.*
- Fajri, D. L. (2022). 4 cara mencegah kebocoran data pribadi. Katadata. Diakses dari: <https://katadata.co.id/berita/nasional/6316e77ce470b/4-cara-mencegah-kebocoran-data-pribadi>.*
- Febriansyah, F., & Muksin, N. N. (2020). Fenomena Media Sosial: Antara Hoax, Destruksi Demo
- Melinda, N. (2020). literasi digital pada remaja digital(sosialisasi pemanfaatan media sosial bagi sekolah menengah atas). *jurnal abdimas mandiri*.
- satria. (2024). analisa keamana dan privasi data pada sistem penyimpanan icloud. *prosiding seminar nasional teknologi informasi dan bisnis*.