KOMMAS: Jurnal Pengabdian Kepada Masyarakat
Universitas Pamulang
Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

SOSIALISASI KEAMANAN CYBER DALAM BERMEDIA SOSIAL PADA SMK PANTI KARYA-3

Nardiono[1*], Achmad Lutfi Fuadi [2*].
[1,2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pamulang
*E-mail: dosen00834@unpam.ac.id, dosen02524@unpam.ac.id

ABSTRAK
Perkembangan teknologi dan internet yang pesat telah mengubah cara manusia berkomunikasi dan mengakses informasi, salah satunya melalui penggunaan media sosial. Meskipun media sosial menawarkan berbagai manfaat, seperti sarana interaksi dan berbagi informasi, ia juga menghadirkan risiko terkait dengan keamanan siber, seperti pencurian data pribadi, malware, serangan phishing, penyalahgunaan identitas, dan cyberbullying. Kurangnya pemahaman tentang keamanan siber dapat meningkatkan potensi pengguna menjadi korban kejahatan digital. Oleh karena itu, sosialisasi mengenai keamanan siber dalam penggunaan media sosial menjadi sangat penting untuk meningkatkan kesadaran masyarakat dalam melindungi data pribadi dan menghindari ancaman siber.
Penelitian ini bertujuan untuk menganalisis pentingnya sosialisasi keamanan siber dan mengidentifikasi strategi efektif untuk meningkatkan kesadaran masyarakat mengenai ancaman di dunia maya. Metode yang digunakan meliputi studi literatur dan survei terhadap pengguna media sosial untuk mengukur tingkat pemahaman mereka terkait dengan keamanan akun dan data pribadi. Hasil penelitian menunjukkan bahwa banyak pengguna masih kurang memahami cara penggunaan kata sandi yang kuat, penerapan verifikasi dua langkah, serta cara mengenali ancaman seperti phishing dan peretasan akun. Selain itu, pengguna juga cenderung mengabaikan langkah-langkah keamanan dasar, seperti menghindari penggunaan jaringan Wi-Fi publik yang tidak aman dan membagikan informasi pribadi secara berlebihan. Untuk mengatasi permasalahan ini, dibutuhkan sosialisasi yang lebih intensif dan masif melalui berbagai platform, seperti seminar, lokakarya, dan kampanye digital. Pemerintah, lembaga pendidikan, dan penyedia platform media sosial memiliki peran penting dalam meningkatkan literasi digital masyarakat. Dengan sosialisasi yang efektif, diharapkan masyarakat dapat lebih waspada dan bijak dalam bermedia sosial, mengurangi risiko menjadi korban kejahatan siber, serta memanfaatkan media sosial dengan lebih aman dan bertanggung jawab.

Kata kunci: Keamanan Siber, Media Sosial, Sosialisasi Keamanan Cyber, Kejahatan Digital, Kesadaran Pengguna, Literasi Digital.

ABSTRACT
The rapid development of technology and the internet has transformed the way humans communicate and access information, one of which is through the use of social media. Although social media offers various benefits, such as a means of interaction and information sharing, it also presents risks related to cybersecurity, such as personal data theft, malware, phishing attacks, identity misuse, and cyberbullying. A lack of understanding of cybersecurity can increase the potential for users to become victims of digital crime. Therefore, socialization regarding cybersecurity in the use of social media is very important to raise public awareness in protecting personal data and avoiding cyber threats. This study aims to analyze the importance of cybersecurity socialization and identify effective strategies to increase public awareness of online threats. The methods used include literature studies and surveys of social media users to measure their level of understanding regarding account security and personal data protection. The research results show that many users still lack understanding about using strong passwords, implementing two-step verification, and recognizing threats such as phishing and account hacking. Furthermore, users tend to overlook basic security measures, such as avoiding the use of insecure public Wi-Fi networks and oversharing personal information. To overcome this problem, more intensive and massive socialization is needed through various platforms, such as seminars, workshops, and digital campaigns. The government, educational institutions, and social media platform providers have important roles in enhancing the digital literacy of the public. With effective socialization, it is expected that people can be more vigilant and wise in using social media, reduce the risk of becoming victims of cybercrime, and utilize social media more safely and responsibly.

Keywords: *cybersecurity, social media, cybersecurity socialization, digital crime, user awareness, and digital literacy.*

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

PENDAHULUAN

Media sosial telah menjadi bagian tak terpisahkan dari kehidupan sehari- hari pelajar di SMK Panti Karya 3, berfungsi sebagai sarana utama untuk berkomunikasi, berbagi informasi, mencari hiburan, dan memperluas jejaring. Platform populer seperti Facebook, Instagram, WhatsApp, dan TikTok menjadi saluran interaksi utama mereka. Namun, di balik berbagai manfaatnya, sebagian besar pelajar masih cenderung tidak menyadari sepenuhnya risiko keamanan siber yang menyertainya.

Berdasarkan pengamatan awal, ditemukan bahwa pelajar di SMK Panti Karya 3 memiliki pemahaman yang kurang mendalam tentang pentingnya menjaga data pribadi dan mengenali ancaman siber seperti peretasan akun, phishing, dan cyberbullying. Mereka seringkali menggunakan kata sandi yang lemah atau serupa di berbagai platform, membagikan informasi pribadi secara berlebihan (seperti nomor telepon, alamat, atau lokasi), dan tidak mengoptimalkan pengaturan privasi pada akun media sosial mereka. Kebiasaan ini secara signifikan meningkatkan kerentanan mereka terhadap pencurian identitas dan peretasan akun.

Selain itu, ada kecenderungan kuat untuk mengabaikan ancaman dari pertemanan atau pesan mencurigakan di media sosial. Banyak pelajar tidak menyadari bahwa perilaku ini dapat menempatkan mereka pada risiko serius. Penggunaan media sosial juga meningkatkan risiko perundungan digital (cyberbullying), di mana pelajar dapat menjadi korban atau bahkan pelaku, seringkali tanpa memahami dampak jangka panjangnya. Penyebaran informasi palsu (hoax) dan malware melalui tautan yang dikirimkan di media sosial juga menjadi ancaman yang dapat merusak reputasi atau perangkat digital.

Permasalahan ini diperparah oleh keterbatasan program edukasi keamanan siber yang sistematis dan intensif di sekolah. Sosialisasi yang ada saat ini belum cukup menjangkau seluruh pelajar, mengakibatkan tingkat kesadaran yang masih rendah. Pihak sekolah juga mungkin menghadapi keterbatasan sumber daya untuk melaksanakan pelatihan atau seminar rutin yang komprehensif bagi seluruh siswa. Untuk mengatasi risiko-risiko ini, sosialisasi keamanan siber secara menyeluruh di SMK Panti Karya 3 menjadi sangat krusial. Sosialisasi ini harus tidak hanya membekali pelajar dengan pengetahuan teknis tentang cara melindungi data pribadi, tetapi juga meningkatkan kesadaran akan dampak luas dari berbagai ancaman digital. Metode sosialisasi dapat bervariasi, meliputi seminar, lokakarya, kelas khusus, serta integrasi pembelajaran keamanan siber ke dalam kurikulum sekolah. Melibatkan pihak terkait seperti guru, orang tua, dan komunitas digital juga dapat memperkuat efektivitas program. Dengan meningkatnya kesadaran dan pemahaman pelajar, mereka diharapkan dapat lebih bijak dalam menggunakan media sosial, melindungi diri dari ancaman digital, serta menciptakan lingkungan daring yang lebih aman, produktif, positif, dan bertanggung jawab

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

METODE

Metode kegiatan ini berupa penyuluhan dan praktik mengenai penggunaan Microsoft Office yang ditujukan bagi siswa dan siswi di pondok pesantren nafidatunnajah. Tujuannya adalah untuk memberikan pembekalan dalam menghadapi persaingan di dunia kerja. Pelatihan ini mencakup:

- Membuat surat menggunakan Microsoft Word.
- Membuat jurnal sederhana menggunakan Microsoft Excel.
- Membuat presentasi menggunakan Microsoft PowerPoint.
- Sesi tanya jawab.

Program ini dilaksanakan pada hari Sabtu, 22 Maret 2025, di SMK Panti Karya 3, Kabupaten Bogor. Metodologi kegiatan ini dibagi ke dalam tiga tahapan utama:

1. Tahap Persiapan
    - Kunjungan Awal: Tim pelaksana melakukan kunjungan dan survei ke SMK Panti Karya 3 untuk berdiskusi dengan Kepala Sekolah mengenai detail kegiatan seperti tempat, waktu, jumlah peserta, dan sarana yang dibutuhkan.
    - Penentuan Tempat dan Waktu: Menetapkan lokasi kegiatan untuk penyampaian materi dan menentukan waktu pelaksanaan selama satu hari.
    - Penyusunan Materi: Mengembangkan materi penyuluhan dengan topik utama ancaman siber, etika digital, dan tips aman bermedia sosial. Materi disusun dalam bentuk slide presentasi, infografis, dan buklet sederhana berdasarkan sumber-sumber terpercaya.
2. Tahap Pelaksanaan

    Pelaksanaan program menggunakan beberapa metode interaktif untuk memastikan materi tersampaikan secara efektif:

    - Metode Ceramah: Pemaparan dasar mengenai ancaman siber seperti phishing, scam, dan cyberbullying. Ceramah dibuat interaktif dengan pertanyaan dan studi kasus untuk menjaga perhatian siswa.
    - Metode Penayangan Media Edukasi: Menggunakan video edukasi dan infografis animasi untuk memvisualisasikan bahaya siber dan tips keamanan.
    - Metode Diskusi dan Berbagi Pengalaman: Sesi tanya jawab dan mendorong siswa untuk berbagi pengalaman pribadi terkait isu siber.
    - Metode Simulasi: Memberikan studi kasus untuk melatih pemikiran kritis siswa dalam menghadapi skenario ancaman siber.
    - Metode Penerapan: Workshop mini di mana siswa secara langsung mempraktikkan cara membuat kata sandi yang kuat , mengaktifkan autentikasi dua faktor (2FA) , mengoptimalkan pengaturan privasi media sosial , serta mengenali dan melaporkan konten tidak pantas.

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

3. Tahap Evaluasi

Evaluasi dilakukan untuk mengukur efektivitas dan dampak program melalui beberapa cara:

- Kuis atau Kuesioner: Siswa diberikan kuis (pre-test dan post-test) untuk mengukur pemahaman mereka tentang materi yang disampaikan.
- Observasi Partisipasi Siswa: Tim pelaksana mengamati secara langsung tingkat keaktifan dan antusiasme siswa selama sesi berlangsung.
- Refleksi Tim Pelaksana: Sesi diskusi internal tim pelaksana untuk mengevaluasi hal-hal yang berjalan baik, tantangan yang dihadapi, dan ide perbaikan untuk kegiatan selanjutnya.

HASIL

c. Karakteristik Subjek PKM

subjek Pengabdian Kepada Masyarakat (PKM) ini adalah siswa SMK Panti Karya 3 yang berlokasi di Desa Pabuaran, Kecamatan Gunung Sindur, Kabupaten Bogor. Para siswa ini merupakan pengguna aktif media sosial seperti Facebook, Instagram, WhatsApp, dan TikTok. Namun, di balik aktivitas digital mereka, terdapat permasalahan mendasar yaitu kurangnya pemahaman mendalam tentang keamanan siber. Hal ini tercermin dari perilaku mereka yang sering menggunakan kata sandi lemah , membagikan informasi pribadi secara berlebihan , dan tidak mengoptimalkan pengaturan privasi akun. Akibatnya, mereka sangat rentan terhadap berbagai ancaman digital, termasuk peretasan akun, phishing, pencurian identitas, cyberbullying, serta penyebaran hoax dan malware. Kurangnya program edukasi keamanan siber yang sistematis di sekolah memperparah kondisi ini , menjadikan para siswa target yang mudah bagi kejahatan digital..

d. Hasil Pelatihan

Program sosialisasi dilaksanakan dengan sukses melalui beberapa tahapan. Kegiatan diawali dengan pembukaan oleh perwakilan sekolah dan tim pelaksana. Materi disampaikan secara interaktif menggunakan ceramah, video studi kasus nyata (seperti phishing, cyberbullying, dan hoaks), serta ilustrasi jejak digital untuk memudahkan pemahaman siswa. Sesi diskusi dan tanya jawab menunjukkan partisipasi aktif dari para siswa, yang banyak berbagi pengalaman pribadi terkait ancaman siber. Puncak acara adalah sesi workshop praktis di mana siswa langsung mempraktikkan cara membuat kata sandi yang kuat, mengaktifkan autentikasi dua faktor (2FA), dan mengoptimalkan pengaturan privasi di media sosial.

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

Gambar 1. Kegiatan Pemaparan Materi

Gambar 2. Kegiatan Pemaparan Materi

Gambar 3. Kegiatan Praktek

Evaluasi program menunjukkan hasil yang positif di berbagai aspek:

- Peningkatan Pemahaman Siswa: Hasil kuis *post-test* menunjukkan peningkatan signifikan dalam pemahaman siswa mengenai ancaman siber seperti *phishing*, *scamming*, dan *malware*. Siswa juga lebih memahami konsep etika digital, termasuk pentingnya tidak menyebarkan hoaks dan dampak perundungan siber. Mayoritas siswa mampu mengidentifikasi langkah-langkah praktis untuk mengamankan akun.

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

- Tingkat Partisipasi Siswa: Tingkat keterlibatan siswa tergolong tinggi, terutama selama sesi diskusi dan *workshop* praktis. Antusiasme ini mengindikasikan bahwa metode interaktif yang digunakan sangat efektif.
- Refleksi Tim Pelaksana: Tim pelaksana menyimpulkan bahwa penggunaan studi kasus nyata dan demonstrasi langsung sangat efektif. Tantangan yang dihadapi adalah keterbatasan waktu untuk sesi praktik yang lebih mendalam bagi setiap individu. Tim juga melihat adanya antusiasme dan kebutuhan yang tinggi dari para siswa untuk program sejenis ini.

Gambar 4. Foto Penyerahan Brosur Unpam

Gambar 4. Foto Bersama Kegiatan

PEMBAHASAN

Hasil pelaksanaan sosialisasi menunjukkan bahwa program ini berjalan efektif dalam meningkatkan kesadaran dan pengetahuan siswa SMK Panti Karya 3 tentang keamanan siber dan etika digital. Metode interaktif yang diadaptasi, seperti ceramah interaktif, penayangan media edukasi,

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

diskusi, serta simulasi dan penerapan, terbukti mampu memfasilitasi pemahaman kompleks mengenai Teori Kriminologi Siber, Teori Kerentanan Sistem, Teori Paparan Konten, dan berbagai prinsip Etika Digital.

Peningkatan pemahaman siswa yang terukur melalui kuis/kuesioner mengindikasikan bahwa pesan-pesan kunci mengenai risiko online dan langkah- langkah pencegahannya tersampaikan dengan baik. Partisipasi aktif siswa, seperti yang teramati, menunjukkan bahwa mereka merasa topik ini relevan dengan kehidupan sehari-hari mereka sebagai pengguna media sosial. Ini sejalan dengan konsep Tanggung Jawab Digital, di mana individu akan lebih bertanggung jawab jika mereka memahami dampak dan memiliki keterampilan untuk bertindak.

Meskipun sosialisasi berhasil, refleksi tim menggarisbawahi pentingnya tindak lanjut atau sesi lanjutan untuk praktik yang lebih mendalam, mengingat kompleksitas pengaturan keamanan digital di berbagai platform. Program ini dapat menjadi fondasi awal yang kuat bagi siswa untuk menjadi warga digital yang lebih cerdas dan aman di masa depan

SIMPULAN

c. Kesimpulan

Sosialisasi keamanan siber dan etika digital di SMK Panti Karya 3 telah berhasil meningkatkan kesadaran dan pemahaman siswa tentang ancaman di dunia maya serta pentingnya perilaku digital yang bertanggung jawab. Melalui metode interaktif seperti ceramah, penayangan media edukasi, diskusi, simulasi, dan praktik langsung, siswa menunjukkan peningkatan pengetahuan yang signifikan mengenai phishing, cyberbullying, hoax, hingga cara mengamankan akun dengan kata sandi kuat dan autentikasi dua faktor (2FA).

Keterlibatan aktif dan antusiasme siswa dalam setiap sesi menegaskan bahwa topik ini sangat relevan dan dibutuhkan oleh mereka sebagai generasi digital. Program ini tidak hanya membekali siswa dengan teori ancaman siber dan etika digital, tetapi juga memberikan keterampilan praktis yang langsung dapat diterapkan untuk melindungi diri dan berinteraksi secara positif di media sosial.

Secara keseluruhan, sosialisasi ini merupakan langkah penting dalam membentuk warga digital yang cerdas, aman, dan bertanggung jawab di tengah perkembangan teknologi yang pesat.

d. Saran

Berdasarkan hasil pelaksanaan dan evaluasi program sosialisasi keamanan siber yang telah dilakukan, berikut adalah beberapa saran untuk pengembangan dan keberlanjutan program di masa mendatang:

a) Pertimbangkan untuk mengadakan sesi tindak lanjut atau membuat modul materi yang lebih mendalam, khususnya untuk praktik keamanan akun (seperti penggunaan password manager tingkat lanjut atau manajemen privasi di platform

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

yang berbeda).

b) Ajak siswa yang memiliki minat dan pemahaman baik untuk menjadi "Duta Keamanan Siber" atau "Duta Etika Digital" di sekolah.

c) Pertimbangkan untuk mengintegrasikan materi keamanan siber dan etika digital ke dalam mata pelajaran TIK atau kegiatan ekstrakurikuler yang relevan.

UCAPAN TERIMAKASIH

Kami panjatkan puji Syukur kepada Allah SWT yang telah memberikan Rahmat dan hidayah-Nya, sehingga kami bisa menyelesaikan kegiatan Pengabdian Kepada Masyarakat ini dengan baik. Kami juga mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Dr. Pranoto, SE., MM selaku Ketua Yayasan Sasmita Jaya.
2. Dr. E. Nurzaman, AM., M.M., M.Si selaku Rektor Universitas Pamulang.
3. Dr. Susanto, S.H., M.M., M.H selaku Ketua LPPM Universitas Pamulang.
4. Yan Mitha Djaksana, S.Kom.,M.Kom. selaku Dekan Fakultas Ilmu Komputer.
5. Semua pihak yang telah membantu penulis yang tidak bisa penulis sebutkan satu persatu, terima kasih atas bantuan, dorongan dan semangatnya.

Akhir kata semoga kegiatan pengabdian kepada masyarakat ini dapat bermanfaat bagi kita semua.

DAFTAR PUSTAKA

Badan Nasional Penanggulangan Terorisme (BNPT). (2022). Buku Saku Kontra Radikalisme.

Badan Siber dan Sandi Negara (BSSN). (2024). Panduan Keamanan Siber. Badan Siber dan Sandi Negara (BSSN). (2024). Tips Keamanan Akun.

Bishop, M. (2005). Computer security: Art and science. Addison-Wesley Professional.

Common Sense Education. (2023). Digital Citizenship Curriculum.

Cyber Security Agency of Singapore (CSA). (2023). Cybersecurity Tips for Individuals.

Dewan Pers Indonesia. (2023). Pedoman Pemberitaan Media Siber.

Direktorat Jenderal Aplikasi Informatika (Ditjen Aptika) Kominfo. (2024). Modul Literasi Digital.

Direktorat Jenderal Kekayaan Intelektual (DJKI). (2023). Undang-Undang Hak Cipta.

Floridi, L. (2013). The Ethics of Information. Oxford University Press.

Gerakan Nasional Literasi Digital Siberkreasi. (2024). Modul Cakap Digital.

Greenwald, R., & D'Amato, A. (2012). The Digital Citizen's Handbook. Common Sense Media.

Hadnagy, C. (2010). Social Engineering: The Art of Human Hacking. Wiley. Interpol. (2023). Cybercrime Threats and Trends Report.

Volume: 6 Nomor: 2
p - ISSN: 2721-0235 | e - ISSN: 2723-4517

Kementerian Komunikasi dan Informatika (Kominfo). (2022). Undang-Undang Perlindungan Data Pribadi (UU PDP).

Kementerian Komunikasi dan Informatika (Kominfo). (2023). Laporan Tahunan Keamanan Siber Indonesia.

Lessig, L. (2004). Free Culture. Penguin Press.

Livingstone, S. (2008). Internet literacy: A narrower focus on a wider agenda.

Media@LSE Working Paper, 15.

Livingstone, S., & Helsper, E. J. (2008). Parental mediation of children's internet

use. Journal of Broadcasting & Electronic Media, 52(4), 581-599.

National Institute of Standards and Technology (NIST). (2022). Digital Identity Guidelines.

Nurhayati, S. (2020). Analisis Faktor-Faktor yang Mempengaruhi Penipuan Online pada Mahasiswa. Jurnal Ilmiah Komputer dan Informatika, 9(1), 1-8.

Pusat Bantuan dan Kebijakan Privasi Instagram. (n.d.). (Tidak ada tahun publikasi spesifik yang disebutkan dalam teks Anda, jadi ditandai "n.d." atau "tanpa tanggal").

Pusat Bantuan Keamanan TikTok. (n.d.). (Tidak ada tahun publikasi spesifik yang disebutkan dalam teks Anda, jadi ditandai "n.d.").

Pusat Penanggulangan Kejahatan Siber Polri. (2024). Waspada Penipuan Online. Puspitasari, H., & Prasetiyo, K. (2021). Pentingnya Etika Digital dalam

Penggunaan Media Sosial di Kalangan Remaja. Jurnal Pengabdian Masyarakat Indonesia, 1(2), 127-134.

Safer Internet Centre. (2024). Cara Melapor Konten Berbahaya. Siberkreasi. (2024). Panduan Etika Berinternet.

Smith, P. K., Mahdavi, J., Carvalho, I., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry, 49(4), 376-385.

Twenge, J. M. (2017). iGen: Why Today's Super-Connected Kids Are Growing Up Less Rebellious, More Tolerant, Less Happy—and Completely Unprepared for Adulthood—and What That Means for the Rest of Us. Atria Books.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe.

Westin, A. F. (1967). Privacy and Freedom. Atheneum.