https://jurnal.astinamandiri.com/index.php/JIPM
Volume 3 | Nomor 1 | Januari |2025
e-ISSN: 2985-7473

SOSIALIASI PENGENALAN PENTINGNYA CYBER SECURITY GUNA MENJAGA KEAMANAN DATA DI ERA DIGITAL PADA SISWA/I PKBM WONG SING GESIT

[1*] **Fingki Marwati,** [2]**Akrom,** [3]**Aniq Astofa**
Program Studi Sistem Informasi, Universitas Pamulang, Banten, Indonesia
dosen02817@unpam.ac.id

Keywords:
Data Security;
Education;
PKBM Wong Sing Gesit

Abstract

In summary, this proposal aims to overcome problems that increasingly arise in the digital era related to the security of personal data. With the increasing use of digital technology, awareness of the importance of protecting personal data also needs to be increased. Problems faced include a lack of understanding of personal data security principles, a lack of awareness about the risks of data leaks, and a lack of resources to provide effective education. The proposed solution is the development of a comprehensive public education program on the principles of personal data security. This program will involve various parties, including government, educational institutions, civil society organizations and the private sector. Educational materials will be tailored to various levels of understanding, from basic to advanced, and will use a variety of media, including social media campaigns, online seminars, and formal educational materials. The target outcomes to be achieved through this program include increasing public awareness about the importance of protecting their personal data, increasing understanding of data security principles, and reducing incidents of personal data breaches. In addition, an increase in the adoption of good personal data security practices by individuals, organizations and companies is expected. By implementing this public education program, it is hoped that the public will be more empowered in protecting their own personal data and can also contribute to increasing overall data security in this digital era.

Keywords:
Data Security;
Education;
PKBM Wong Sing Gesit

Abstrak

Kegiatan ini bertujuan untuk mengatasi masalah yang semakin banyak muncul di era digital terkait keamanan data pribadi. Dengan meningkatnya penggunaan teknologi digital, kesadaran akan pentingnya melindungi data pribadi juga perlu ditingkatkan. Masalah yang dihadapi mencakup kurangnya pemahaman tentang prinsip keamanan data pribadi, minimnya kesadaran akan risiko kebocoran data, serta kurangnya sumber daya untuk menyediakan edukasi yang efektif. Solusi yang diusulkan adalah pengembangan program edukasi publik yang komprehensif mengenai prinsip-prinsip keamanan data pribadi. Program ini akan melibatkan berbagai pihak, termasuk pemerintah, institusi pendidikan, organisasi masyarakat sipil, dan sektor swasta. Materi edukasi akan disesuaikan dengan berbagai tingkat pemahaman, mulai dari dasar hingga tingkat lanjutan, dan akan menggunakan berbagai media, termasuk kampanye media sosial, seminar daring, serta bahan edukasi formal. Hasil yang ditargetkan melalui program ini meliputi peningkatan kesadaran masyarakat

tentang pentingnya melindungi data pribadi mereka, peningkatan pemahaman tentang prinsip keamanan data, serta pengurangan insiden kebocoran data pribadi. Selain itu, diharapkan terjadi peningkatan dalam adopsi praktik keamanan data pribadi yang baik oleh individu, organisasi, dan perusahaan. Dengan pelaksanaan program edukasi publik ini, diharapkan masyarakat dapat lebih berdaya dalam melindungi data pribadi mereka sendiri dan juga berkontribusi dalam meningkatkan keamanan data secara keseluruhan di era digital ini.

This work is licensed under a Creative Commons Attribution 4.0 International License

PENDAHULUAN

Saat ini merupakan masa digital, dimana pertumbuhan teknologi data serta komunikasi sudah membawa pergantian besar dalam kehidupan manusia. Dalam prosesnya, informasi individu menjadi sangat penting serta sensitif sebab banyak kegiatan yang dilakukan secara online. Informasi individu mencakup data semacam nama, alamat, no bukti diri data finansial, riwayat kesehatan, serta data sensitif yang lain yang berkaitan dengan individu.

Di tengah masa digital yang pesat, informasi individu orang terus menjadi rentan terhadap kemampuan penyalahgunaan serta pelanggaran pribadi Keamanan informasi individu ialah hak asasi manusia yang wajib dipastikan serta dihormati. Indonesia, selaku negeri tumbuh dengan adopsi teknologi yang pesat, mempunyai tanggung jawab buat melindungi informasi individu selaku hak pribadi Dalam konteks ini, hak pribadi jadi isu yang menekan buat diatasi. Hak pribadi merupakan hak asasi tiap orang buat melindungi kerahasiaan serta keamanan informasi individu mereka. Dengan meningkatnya permasalahan pelanggaran pribadi serta penyalahgunaan informasi individu berarti untuk tiap negeri buat mempunyai peraturan perundang-undangan yang efisien buat melindungi hak pribadi warganya.

Bukan hanya itu saja, dikarenakan pesatnya perkembangan era digital, maka data pribadi individu menjadi sangat rentan terhadap potensi pelanggaran dan penyalahgunaan privasi. Keamanan data pribadi dimaksudkan sebagai hak asasi manusia yang harus dijamin serta dihormati. Indonesia, sebagai negara berkembang dimana proses adopsi teknologi yang pesat, memiliki tanggung jawab dalam melindungi data pribadi sebagai hak privasi. Dalam konteks ini, hak privasi selalu menjadi isu yang mendesak untuk diatasi. Hak privasi diartikan sebagai hak asasi setiap individu untuk menjaga kerahasiaan serta keamanan data pribadi mereka. Dengan semakin meningkatnya kasus pelanggaran privasi serta penyalahgunaan data pribadi, maka penting bagi setiap negara untuk memiliki dan membuat peraturan perundang-undangan yang efektif agar hak privasi warganya selalu terlindungi.

Di Indonesia, pemahaman tentang perlunya perlindungan data pribadi telah semakin bertambah, terutama seiring dengan pesatnya penggunaan internet dan aplikasi berbasis teknologi. Hak membela diri adalah salah satu hak hukum yang digariskan di dalam UUD 1945. Menurut Pasal 28G Ayat (1), warga negara berhak atas perlindungan diri pribadi , kehormatan, keluarga , martabat, dan harta miliknya. Dengan demikian, adanya kemajuan teknologi komunikasi dan informasi, hak pribadi seharusnya tidak hanya diarahkan sebagai hak milik saja seperti yang diatur dalam pasal tersebut. Hak privasi harus menjadi hal yang paling mendasar. Karena berurusan dengan identitas seseorang atau informasi pribadi, hak privasi menjadi lebih sensitif dan dapat dilihat sebagai hak pribadi. Sebagai contoh kebocoran data pribadi yang saat ini telah menjadi masalah yang parah. Beberapa di antaranya terdiri dari:

1. Kasus Tokopedia (2020): Pada awal tahun 2020, platform e-commerce besar di Indonesia yaitu Tokopedia, dilaporkan telah mengalami pelanggaran keamanan yang mengakibatkan pencurian jutaan data informasi pribadi dari pengguna. Data yang diambil meliputi nama, alamat, nomor telepon, alamat email, dan kata sandi terenkripsi.

2. Kasus Bukalapak (2021): Platform e-commerce lainnya di Indonesia yaitu Bukalapak, juga dilaporkan mengalami pelanggaran data di tahun 2021. Lebih dari 13 juta akun pengguna dilaporkan terjadi kebocoran data, dengan data seperti nama pengguna, alamat email, nomor telepon, dan kata sandi.
3. Kasus TokoTalk (2021): Selanjutnya pada tahun 2021, aplikasi pesan instan asal Indonesia, TokoTalk, juga dilaporkan mengalami pembobolan data lebih dari 91 juta akun

Menurut analisis oleh Australian Cyber Security center (ACSC), ada 59.806 laporan kejahatan dunia maya yaitu diantara bulan juli 2019 sampai juni 2020, atau rata- rata 164 kejahatan dunia maya setiap tahun. Cyber Security menjadi masalah yang serius untuk ditangani di Indonesia dengan kebocoran data yang sering terjadi di Indonesia selama 2020-2021. Menurut riset Trend Micro, Indeks Risiko Siber (CRI) Indonesia pada tahun 2020 adalah 0,26 %, yang menunjukan tingkat bahaya yang moderat. Sebaliknya, berangsur turun menjadi -0,12 % pada tahun 2021, menunjukan bahwa bahaya meningkat walau belum tercatat adanya resiko kerugian yang tinggi. (Wahyu Tisno Atmojo, 2021)

Perhatian terhadap pemberian proteksi kepada informasi individu (*privacy informasi protection*) yang dicuri terus menjadi menemukan atensi dari warga kala salah satu industri (*company*) media sosial terbanyak di dunia hadapi pencurian informasi individu oleh sebagian pihak. Suatu kabar pencurian informasi individu tersebut telah tersebar dengan sangat cepat di bermacam media elektronik yang setelah itu dengan menemukan pengakuan dari industri tersebut kalau sudah terjalin pencurian informasi individu ataupun pengambilan informasi individu milik orang lain tanpa izin yang setelah itu diketahui dengan istilah infromatik "pencurian informasi ataupun pembobolan informasi Kondisi ini terjalin diakibatkan sebab terdapatnya kelemahan pada sistem yang digunakan buat menyimpanan informasi yang dipunyai oleh industri sehingga informasi individu kepunyaan orang lain bisa dicuri oleh pihak yang tidak bertanggung jawab. (Rudi Natamiharja, 2018).

Berkaitan dengan pencurian data pribadi yang dilakukan oleh perusahan besar seperti facebook dimana hal ini pernah ditulis dalam artikel Rudi Natamiharja dalam jurnal Fiat Justisia yang berjudul "A Case Study on Facebook Data Theft in Indonesia" tentang pencurian data yang dialami perusahaan media sosial Facebook (Rudi Natamiharja, 2018). Mekanisme pengumpulan data pribadi dapat dilakukan dengan sederhana. Sebagai contoh, konsumen memberikan data tanpa ada paksaan. Ia memberikan data pribadi kepada Facebook dengan cara mengisi formulir pendaftaran. Hal ini dilakukan dengan penuh kesadaran memberikan persetujuan secara terang-terangan atau tersembunyi.

Namun, dengan meningkatnya ketergantungan pada teknologi digital, juga muncul risiko terkait keamanan data pribadi. Terlebih lagi, para siswa dan siswi di PKBM Wong Sing Gesit, yang mungkin memiliki keterbatasan akses dan pengetahuan terhadap teknologi, perlu diberi pemahaman yang kuat tentang prinsip-prinsip keamanan data pribadi.

Peneliti Badan Litbang SDM Kemkominfo menyatakan bahwa diperlukan upaya-upaya untuk meningkatkan kesadaran, pengetahuan dan keterampilan anak dan remaja Indonesia dalam kaitannya dengan keamanan berinternet. Mengingat Internet telah menjadi bagian yang tidak dapat dipisahkan dari kehidupan seharihari anak dan remaja di Indonesia. "Hal ini dapat dicapai melalui sosialisasi, pendidikan Iiterasi maupun pelatihan. Pemahaman penggunaan dan keamanan media digital sangat penting utamanya dari perspektif anak-anak dan remaja, sebelum merancang program-program informasi tentang keamanan digital. Termasuk memahami tentang cara mereka mengartikan dan menggunakan teknologi digital, komunikasi secara online dan perilaku berisiko atau tidak aman (Banyumurti, Indroyatno, 2018).

Seringkali para pengguna internet tidak menyadari bahwa pencurian data sangatlah membahayakan diri sendiri maupun orang lain. Pencurian data ini dapat disalahgunakan sebagai bentuk kejahatan, semakin banyak data yang bocor maka akan semakin tinggi pula bahaya yang mengintai. Penyalahgunaannya bisa berbentuk phising, penipuan berkedok pinjaman online (pinjol), atau juga peretasan akun media sosial untuk menipu keluarga dan kerabat dekat yang dimiliki oleh pengguna terkait. Hal ini tentu saja sangat mengkhawatirkan bahkan dapat membuat kita yang kehilangan data mengalami kerugian baik secara materiil

maupun non- materiil. Menurut Yuwinanto, (2015) penggunaan perangkat sistem informasi yang terhubung ke jaringan atau online memunculkan isu privasi dan menurutnya ada beberapa langkah yang bisa digunakan untuk menjaga privasi itu yaitu memberikan pengguna mekanisme pengontrolan khususnya pada data atau informasi yang dimiliki.
Sebagaimana yang kita ketahui bahwa siswa/i menengah adalah usia remaja dan merupakan komunitas terbesar dalam masyarakat Indonesia yang menggunakan media sosial secara regular. Alasan awal mereka sangat aktif menggunakan media sosial adalah untuk mencari perhatian, meminta pendapat dan menumbuhkan citra, namun lama kelamaan akhirnya menjadi ketergantungan. Walaupun media sosial memberikan dampak positif pada remaja, namun pada saat mereka sulit melepaskan diri dari kegiatan yang berkaitan dengan media sosial maka akan memberikan dampak yang kurang positif. Sejumlah studi menunjukkan bahwa akibat penggunaan media sosial yang berlebihan, remaja ditemukan mengalami ingkongruensi pada konsep dirinya.

METODE

Melaksanakan solusi yang ditawarkan untuk mengatasi permasalahan tentang sosialisasi tentang keamanan data pribadi memerlukan pendekatan yang terstruktur dan terarah. Berikut adalah tahapan atau langkah-langkah dalam melaksanakan solusi tersebut:

1. Pengembangan Kurikulum Khusus
   - Pertama-tama, langkah awal adalah mengembangkan kurikulum khusus yang mencakup materi tentang prinsip-prinsip keamanan data pribadi. Langkah-langkah yang dapat diambil dalam pengembangan kurikulum ini meliputi:
   - Identifikasi Kebutuhan: Melakukan analisis mendalam terhadap tingkat pemahaman, kebutuhan, dan tantangan yang dihadapi siswa dan siswi PKBM Wong Sing Gesit terkait dengan keamanan data pribadi.
   - Penyusunan Materi Pembelajaran: Menyusun materi pembelajaran yang mencakup konsep dasar keamanan data pribadi, risiko online, praktik keamanan yang aman, serta etika digital. Materi ini harus disesuaikan dengan tingkat pemahaman dan kebutuhan siswa dan siswi.
   - Pengujian Materi: Melakukan uji coba materi pembelajaran dengan melibatkan sejumlah siswa dan siswi PKBM Wong Sing Gesit untuk memastikan keterbacaan, keefektifan, dan kebermanfaatan materi yang disajikan.
2. Pelatihan dan Workshop
   Setelah materi pembelajaran disusun, langkah selanjutnya adalah menyelenggarakan pelatihan dan workshop tentang keamanan data pribadi. Tahapan yang perlu dilakukan dalam pelaksanaan pelatihan dan workshop ini meliputi:
   a. Penentuan Jadwal dan Tempat: Menjadwalkan waktu dan tempat pelatihan yang sesuai dengan jadwal belajar siswa dan siswi PKBM Wong Sing Gesit.
   b. Pemilihan Narasumber: Mengundang narasumber yang kompeten dan berpengalaman dalam bidang keamanan data pribadi untuk memberikan materi dan pemahaman yang lebih mendalam.
   c. Pelaksanaan Pelatihan: Melakukan sesi pelatihan dan workshop yang interaktif, dimana siswa dan siswi diajak untuk berpartisipasi aktif dalam diskusi, simulasi, dan latihan praktis terkait dengan keamanan data pribadi.
3. Penggunaan Materi Pembelajaran Interaktif
   Menggunakan materi pembelajaran interaktif merupakan langkah penting dalam meningkatkan keterlibatan siswa dan siswi dalam pembelajaran tentang keamanan data pribadi. Tahapan yang dapat dilakukan dalam penggunaan materi pembelajaran interaktif adalah sebagai berikut:
   a. Pengembangan Materi: Mengembangkan materi pembelajaran interaktif, seperti video edukatif, permainan digital, atau infografis interaktif, yang menarik dan mudah dipahami oleh siswa dan siswi PKBM Wong Sing Gesit.
   b. Penggunaan Materi: Menggunakan materi pembelajaran interaktif dalam sesi pembelajaran reguler atau sebagai tambahan materi dalam kegiatan ekstrakurikuler di PKBM Wong Sing Gesit.

4. Kolaborasi dengan Pihak Eksternal
   Kerjasama dengan pihak eksternal, seperti lembaga pendidikan formal, perusahaan teknologi, atau organisasi non-pemerintah, dapat memperluas akses siswa dan siswi PKBM Wong Sing Gesit terhadap sumber daya dan pelatihan tentang keamanan data pribadi. Langkah-langkah yang dapat dilakukan dalam kolaborasi ini antara lain:
   a. Penyediaan Sumber Daya: Mengadakan pertemuan dengan pihak eksternal untuk membahas kemungkinan penyediaan sumber daya, seperti fasilitas, dana, atau tenaga pengajar tambahan.
   b. Pengorganisasian Kegiatan Bersama: Menyelenggarakan kegiatan bersama, seperti lokakarya atau seminar tentang keamanan data pribadi, yang melibatkan pihak eksternal sebagai narasumber atau fasilitator.
5. Pelaksanaan Kampanye Kesadaran
   Mengadakan kampanye kesadaran secara berkala di lingkungan PKBM Wong Sing Gesit merupakan langkah penting dalam meningkatkan kesadaran siswa dan siswi tentang pentingnya keamanan data pribadi. Tahapan-tahapan yang perlu dilakukan dalam pelaksanaan kampanye kesadaran ini meliputi:
   a. Perencanaan dan Persiapan: Merencanakan tema, kegiatan, dan materi kampanye kesadaran yang sesuai dengan kebutuhan dan minat siswa dan siswi PKBM Wong Sing Gesit.
   b. Pelaksanaan Kegiatan: Melakukan kegiatan seperti penyuluhan, lomba poster, atau diskusi panel tentang keamanan data pribadi untuk mengedukasi siswa dan siswi dan meningkatkan kesadaran mereka.
6. Evaluasi dan Pemantauan Berkelanjutan
   Evaluasi dan pemantauan berkelanjutan terhadap efektivitas program edukasi keamanan data pribadi sangat penting untuk mengetahui sejauh mana tujuan telah tercapai dan untuk menemukan area perbaikan yang diperlukan. Langkah-langkah yang dapat dilakukan dalam evaluasi dan pemantauan berkelanjutan ini antara lain:
   a. Penyusunan Indikator Keberhasilan: Menetapkan indikator keberhasilan yang jelas dan terukur untuk mengevaluasi efektivitas program edukasi keamanan data pribadi.
   b. Pelaksanaan Evaluasi Periodik: Melakukan survei, kuesioner, atau tes pengetahuan secara berkala untuk mengukur tingkat pemahaman dan kesadaran siswa dan siswi PKBM Wong Sing Gesit tentang keamanan data pribadi.
   c. Analisis dan Tindak Lanjut: Menganalisis hasil evaluasi dan menggunakan temuan tersebut untuk membuat perbaikan dan penyesuaian terhadap program edukasi keamanan data pribadi yang sedang berjalan.

HASIL DAN PEMBAHASAN

Hasil dari kegiatan pengabdian kepada masyarakat ini dapat diuraikan lebih detail. Secara keseluruhan, hasil ini mencakup beberapa komponen penting, yaitu:1.Keberhasilan target jumlah peserta sosialisasi: Target awal adalah mengundang 20 siswa/siswi PKBM Wong Sing Gesit untuk mengikuti sosialisasi. Dalam pelaksanaannya, kegiatan ini berhasil diikuti oleh 20 peserta, mencapai 100% dari target yang telah ditetapkan. Hal ini menunjukkan bahwa kegiatan pengabdian kepada masyarakat ini dapat dianggap berhasil dan sukses, karena jumlah peserta yang sesuai dengan rencana.2.Ketercapaian target materi yang telah direncanakan: Selama kegiatan pengabdian kepada masyarakat, materi yang telah direncanakan berhasil disampaikan dengan baik. Peserta menunjukkan pemahaman yang baik terhadap materi yang disampaikan, seperti yang terlihat dari tingginya tingkat antusiasme mereka selama sesi diskusi dan tanya jawab. Mereka mampu mengerti dan merespons materi tersebut, serta menerapkan pengetahuan yang didapat dalam kehidupan sehari-hari.Untuk memastikan keberhasilan kegiatan ini, persiapan yang matang dilakukan sebelum pelaksanaan PKM. Ini termasuk melakukan briefing kepada seluruh panitia yang terlibat dalam pelaksanaan kegiatan, termasuk rekan-rekan mahasiswa yang turut serta dalam kegiatan ini.Solusi yang diimplementasikan dalam kegiatan ini terdiri dari empat tahap penting, yaitu perencanaan, pelaksanaan, monitoring dan evaluasi (monev), serta refleksi dan tindak lanjut. Pendekatan ini membantu memastikan bahwa kegiatan berjalan dengan lancar

dan mencapai hasil yang diharapkan. Khalayak sasaran dari kegiatan pengabdian kepada masyarakat ini adalah guru dan siswa/siswi PKBM Wong Sing Gesit. Mereka adalah fokus utama dalam upaya penyampaian materi dan solusi yang telah disiapkan.Tempat pelaksanaan kegiatan ini adalah di PKBM Wong Sing Gesit, dan kegiatan ini berlangsung pada hari Minggu, 6 Oktober 2024. Dengan demikian, waktu dan lokasi pelaksanaan telah ditentukan dengan jelas untuk memastikan kesuksesan dan efektivitas kegiatan ini dalam memberikan manfaat kepada khalayak sasaran yang dituju.

Gambar 1. Pengabdian Kepada Masyarakat PKBM Wong Sing Gesit

KESIMPULAN

Dari kegiatan yang telah dilaksanakan dapat disimpulkan bahwa para peserta merasa senang karena bisa mendapatkan pengetahuan tentang pentingnya menjaga keamanan data pribadi agar terhindar dari kejahatan-kejahatan dunia maya di era digital seperti sekarang ini serta mereka mendapatkan wawasan baru diluar kegiatan belajar mengajar di kelas.

DAFTAR PUSTAKA

Banyumurti, Indroyatno, D. (2018). Kebijakan Cyber Security Dalam Perspektif Multi Stakeholder

Garo Pane, C. G. (2021). Edukasi Kepada Siswa Sma Negeri 1 Mimika Untuk Mengatasi Ancaman Media Online Pada Data Pribadi. KONSTELASI: Konvergensi Teknologi Dan Sistem Informasi, 1(2), 412–418. https://doi.org/10.24002/konstelasi.v1i2.4166.

Pugu, M. R., Riyanto, S., & Haryadi, R. N. (2024). *Metodologi Penelitian; Konsep, Strategi, dan Aplikasi*. PT. Sonpedia Publishing Indonesia

Rahmadi, G., & Pratama, A. R. (2020). Analisis Kesadaran Cyber Security pada Kalangan Pelaku e-Commerce di Indonesia. Automata, 1(2), 7. Retrieved from https://journal.uii.ac.id/AUTOMATA/article/view/15399

Ramadhan, I. (2019). Strategi Keamanan Cyber Security di Kawasan Asia Tenggara.Jurnal Asia Pacific Studies,3(2), 181-192

Rudi Natamiharja, "A Case Study on Facebook Data Theft in Indonesia," FIAT JUSTISIA 12, N (2018): 3.

Salim, S. C. (2017). Analisis Cyber Security pada Instagram untuk mengukur customer trust. (227), 1–23.

Triandi, B. (2019). Keamanan informasi secara aksiologi dalam menghadapi era revolusi industri 4.0. JURIKOM (Jurnal Riset Komputer), 6(5), 477-483

Wahyu Tisno Atmojo, M. E. (2021). Pengenalan Cyber Security Dalam Revousi Industri 4.0 Dan Menyongsong Era Society 5.0. Prosiding PKM-CSR, 39-45