TEKNOVOKASI: Jurnal Pengabdian Masyarakat: **Vol. 1, No.2, Mei 2023**
P-ISSN : 2985-6787 (Media Cetak)
E-ISSN : 2985-6779 (Media *Online)*
http://journal.unm.ac.id/index.php/TEKNOVOKASI

Pengenalan *Cyber Security* Bagi Siswa Sekolah Menengah Atas

[1]Veronika Asri Tandirerung*, [2]Riana T.Mangesa, [3]Syahrul

[1,2,3]Universitas Negeri Makassar, Kota Makassar

Email: veronika.asri@unm.ac.id[1], rianamangesa@unm.ac.id[2], syahrul@unm.ac.id[3]
**Corresponding author*: veronika.asri@unm.ac.id[1]

Received **: 7 April 2023**
Accepted **: 9 Mei 2023**
Published **: 15 Mei 2023**

ABSTRAK

Upaya untuk meningkatkan kesadaran, pengetahuan dan keterampilan anak dan remaja Indonesia dalam kaitannya dengan keamanan berinternet sangat perlu diperhatikan khususnya bagi anak-anak dan remaja. Mengingat Internet telah menjadi bagian yang tidak dapat dipisahkan dari kehidupan sehari-hari anak dan remaja di Indonesia. Hal ini dapat dicapai melalui sosialisasi, pendidikan literasi maupun pelatihan. Pemahaman penggunaan dan keamanan media digital sangat penting khususnya dari perspektif anak-anak dan remaja. Mereka perlu memahami tentang cara menggunakan teknologi digital, komunikasi secara online dan perilaku berisiko atau tidak aman. Selain itu, perlu perhatian khusus untuk memberikan informasi bagi anak dan remaja tentang resiko bahaya yang mungkin timbul dari pertemuan langsung dengan seseorang yang baru dikenal dari dunia maya. Para orangtua dan guru perlu mengetahui dan terlibat dalam program keamanan digital bagi anak dan remaja. Anak-anak dan remaja harus terus dimotivasi untuk memandang dan menjadikan internet sebagai sumber informasi yang berharga, dan untuk memanfaatkan teknologi digital secara maksimal untuk membantu pendidikan, meningkatkan pengetahuan, memperluas kesempatan dan keberdayaan mereka dalam meraih kualitas kehidupan yang lebih baik. Metode Pelaksanaan PKM ini adalah metode model open *Design*. Model *open Design* terdiri atas tiga tahap yaitu perencanaan, pelaksanaan workshop dan evaluasi. Setelah pelaksanaan kegiatan diharapkan siswa dapat menggunakan akun media sosial secara bijaksana dan mengetahui bagaimana melakukan proteksi terhadap diri sendiri dan orang lain.
Kata Kunci: Pelatihan, cyber security, teknologi, siswa

ABTRACT

Efforts to increase awareness, knowledge and skills in internet safety need attention, especially for children and adolescents. They considered that the Internet had become an inseparable part of the daily life of children and adolescents in Indonesia. It can be achieved through outreach, literacy education and training. Understanding the use and safety of digital media is especially important from the perspective of children and adolescents. They must understand how to use digital technology, online communication and risky or unsafe behaviour. In addition, special attention is needed to provide information for children and adolescents about the risks of harm that may arise from a direct encounter with someone they have just met from cyberspace. Parents and teachers must be aware of and involved in digital safety programs for children and youth. Children and youth must continue to be motivated to view and use the internet as a valuable source of information and to make the most of digital technology to assist in education, increase knowledge, expand opportunities and empower them to achieve a better quality of life. This PKM implementation method is an open-design model method. The open design model consists of three stages: planning, workshop implementation and evaluation. After carrying out the activity, it is expected that students can use social media accounts wisely and know how to protect themselves and others.
Keywords: training, cyber security, internet, students

1. PENDAHULUAN

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 sehari-hari 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). "Studi ini menemukan bahwa banyak anak-anak yang tidak terlindungi dari konten negatif yang ada di internet, sebagian besar sampai kepada mereka tanpa sengaja melalui pesan pop-up atau melalui link yang menyesatkan. Selain itu, Perlu perhatian khusus untuk memberikan informasi bagi anak dan remaja tentang resiko bahaya yang mungkin timbul dari pertemuan langsung dengan seseorang yang baru dikenal dari dunia maya. Para orangtua dan guru perlu mengetahui dan terlibat dalam program keamanan digital bagi anak dan remaja. Sementara untuk Pesan-pesan tentang keamanan digital harus berimbang dengan menekankan pada kemanfaatan internet bagi pendidikan, penelitian, dan perdagangan. Anak-anak dan remaja harus terus dimotivasi untuk memandang dan menjadikan internet sebagai sumber informasi yang berharga, dan untuk memanfaatkan teknologi digital secara maksimal untuk membantu pendidikan, meningkatkan pengetahuan, memperluas kesempatan dan keberdayaan mereka dalam meraih kualitas kehidupan yang lebih baik. Perlu dikembangkan cara-cara efektif untuk mengkampanyekan keamanan digital secara online maupun offline melalui segala bentuk saluran media tradisional maupun digital, seperti televisi, radio, websites, atau media sosial yang sering digunakan oleh anak dan remaja. Dibutuhkan kader-kader muda teladan dalam keamanan berinternet, yang dapat membagikan hal tersebut kepada teman-temannya melalui media digital, melalui sarana audio dan video di media massa, maupun secara offline di sekolah-sekolah maupun kampus.

Kejahatan di dunia siber terjadi karena kurangnya pengetahuan dari perlindungan data pribadi oleh masyarakat mengakibatkan masyarakat hanya mengabaikan peristiwa yang terjadi dan menganggap hal tersebut sepele sehingga banyak masyarakat mengabaikan kasus ini, Terlepas dari hal-hal ini, faktor penyebab yang lainnya adalah masyarakat masih kesulitan membedakan mana data yang bisa disebarkan ke publik dan mana yang tidak. Perlu diperingatkan bahwa dalam menginstal sebuah aplikasi apapun terutama media sosial jangan pernah menggunakan data pribadi asli jika memang tidak dibutuhkan untuk di publish, gunakan password yang unik sehingga sulit untuk ditebak oleh orang lain, jangan menginstal aplikasi yang tidak diperlukan dan tetap berhati-hati dengan harus mengetahui seluk beluk aplikasi tersebut apakah aman untuk memasukkan data pribadi kita di dalamnya (Garo Pane, 2021)

Untuk mencapai sasaran tersebut perlu dilakukan hal-hal seperti; 1) penyebaran informasi serta sosialisasi terkait isu-isu keamanan informasi serta pencerdasan terkait risiko-risiko dalam penggunaan teknologi informasi guna meningkatkan security awareness pada masyarakat luas. 2) transfer pengetahuan yang berhubungan dengan keamanan siber dapat dimasukkan ke dalam pendidikan formal dalam rangka mempersiapkan generasi penerus dalam menghadapi perkembangan teknologi serta risiko-risiko yang melekat dengannya. (Banyumurti, Indroyatno, 2018).

Penerapan internet juga dalam hal bidang ekonomi yakni dalam *e-commerce* dan *fintech*. Keamanan data dalam bidang ini perlu diperhatikan. Guna melakukan mitigasi terhadap tantangan cybercrime tersebut diperlukan cybersecurity melalui tindakan proaktif, penguatan regulasi dan pembentukan kerangka kerja atau prosedur cybersecuriy yang handal, efektif dan efisien (Anggono & Riskiyadi, 2021).

SMA Katolik Cenderawasih merupakan salah satu sekolah menengah atas yang berada di Kota Makassar. Sekolah ini memiliki kelas berasrama yang memiliki aturan dan disiplin yang tinggi. Kelas berasrama tersebut adalah Seminari Menengah St. Petrus Claver Makassar. Merupakan bagian dari pendidikan para calon imam di keuskupan Agung Makassar. Pola pendidikan di tempat ini sangat berbeda dengan pola pendidikan sekolah menengah atas pada umumnya. Mereka tidak diijinkan menggunakan handphone (HP) dan penggunaan komputer yang terbatas hanya pada waktu tertentu saja. Hal positif dari pola pendidikan ini adalah mereka tidak terkontaminasi dengan perkembangan dunia bidang teknologi informasi dan komunikasi. Namun, tentu saja ada hal negatifnya yakni kurangnya informasi yang mereka dapatkan terkait TIK sehingga mereka kurang memahami perkembangan dunia luar baik sisi positif maupun sisi negatif perkembangan TIK. Tujuan dari kegiatan ini adalah memberikan pengetahuan terhadap siswa SMA agar lebih bijak dalam menggunakan sarana media sosial. Selain itu memperkenalkan kepada siswa hal-hal yang perlu dijaga keamanannya dalam dunia internet dan pengenalan etika-etika dalam berinteraksi dalam dunia maya.

2. METODE PELAKSANAAN

Metode yang digunakan dalam pelaksanaan program kemitraan masyarakat ini adalah menggunakan model open Design. Model *open Design* terdiri atas tiga langkah yaitu:

1. Perencanaan. Dalam tahap perencanaan ini tim melakukan analisis kebutuhan, penyusunan desain program pelatihan dan penyusun perangkat pelatihan. Perangkat pelatihan yang dihasilkan dalam tahap ini adalah berupa modul Pengenalan Konsep *Cybersecurity* dan jenis kejahatan, media sosial yang marak digunakan serta kelebihan dan kekurangannya.
2. Pelaksanaan workshop. Dalam tahap pelaksanaan ini, kegiatan yang dilakukan adalah membuat setting (pengaturan) pada akun-akun media sosial yang digunakan serta bagaimana membuat konten positif pada media sosial dan bagaimana memblock sumber berita hoax. Pada workshop ini dijelaskan bagaimana mengoptimalkan media sosial sehingga dapat menjadi media pendidikan dan juga untuk meningkatkan jiwa wirausaha sebagai penerapan mata pelajaran prakarya.
3. Evaluasi pasca pelatihan, pada tahap ini dilaksanakan implementasi program tindak lanjut dan monitoring dan evaluasi. Monitoring dilakukan dengan mendampingi anggota komunitas dalam menghasilkan produk yang didesain oleh siswa sendiri dan membentuk kelompok siswa dalam pembentukan produk andalan untuk selanjutnya menjadi produk usaha. Setiap tahap kegiatan ini dilakukan evaluasi berupa kuesioner tentang keterlaksanaan program mulai dari awal hingga tahap monitoring dan evaluasi.

3. HASIL DAN PEMBAHASAN

3.1 Menyampaikan materi tentang Cybersecurity

Cyber Security merupakan praktik melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari ancaman yang juga dikenal sebagai keamanan teknologi informasi (Rahmadi & Pratama, 2020). Menurut ISACA dalam (Salim, 2017) terdapat tiga konsep *cyber security* yaitu (1) *confidentially* untuk perlinfungan informasi yang belum diotorisasi atau diungkapan, 2) *integrity* untuk perbaikan data yang rusak harus secepatnya ditangani, 3) *availability* untuk menjamin akses yang tepat untuk penggunaan siste, informasi. *Cybersecurity* melindungi *data akun pengguna dan membatasai hak akses pengguna*.

Untuk mempromosikan kebebasan berekspresi di internet secara aman dan bijaksana, melalui beberapa pendekatan berikut: 1) Konten online yang positif, bermanfaat dan menarik harus dikembangkan dari-oleh-untuk anak-anak, remaja dan masyarakat lokal, 2) Inisiatif *self-filtering* di internet hanya dapat dilakukan di level keluarga (rumah) dan pendidikan (sekolah), dan 3) Literasi digital dan perlindungan online anak sangat membutuhkan dialog dan kerjasama multistakeholder yang inklusif, setara, transparan dan akuntabel dalam koridor Internet Governance."

Gambar 1. Penjelasan *Cyber security*

3.2 Memahami dan Melindungi dengan Fitur *Back-up Data*

Data dapat diakses dan disimpan melalui aplikasi seluler. Mengakses dan memulihkan file cadangan juga dapat melalui aplikasi seluler. Dengan adanya *cloud computing* , backup dalam jaringan dapat dilakukan. User dapat memastikan dengan memberikan enkripsi pada data yang digunakan dan data yang dikirim serta data yang disimpan. Data dalam setiap bidang pekerjaan dapat dilakukan penyimpanan sistem cloud dan aman dari kerusakan perangkat keras. Layanan penyedia yang cukup banyak digunakan adalah *google drive* dan *one drive* milik Microsoft. Dengan memiliki akun pada cloud tersebut, data dapat disimpan dengan aman dan tidak dapat dibuka oleh orang lain. Kapasitas penyimpanan juga dapat diupgrade sesuai dengan kebutuhan.

Sedangkan untuk data-data pekerjaan, saat ini layanan penyimpanan cloud sudah cukup populer digunakan sebagai penyimpanan data daring yang aman dari potensi kerusakan perangkat keras. Banyak layanan penyedia layanan penyimpanan cloud. Beberapa yang cukup familiar adalah Google Drive dan OneDrive milik Microsoft. Tinggal membuat akun dan kita bisa memanfaatkan fitur ini untuk mencadangkan data-data pekerjaan kita. Pastikan menggunakan kata sandi yang aman agar penyimpanan daring ini tidak dibuka orang lain.

Gambar 2. Pelatihan *Backup Data*

3.3 Memahami Dan Melindungi *Personal Identification Number (Pin)*

Seringkali untuk memudahkan kita menggunakan beragam platform digital, kita menggunakan angka sandi atau Personal Identification Number (PIN) yang sama. Sebaiknya hindari memilih kombinasi angka yang mudah ditebak, misalnya tanggal dan tahun lahir. Pilihlah kombinasi angka yang potensi keamanannya tinggi dengan selalu membuat PIN yang susah untuk diprediksi orang lain. Kedua, sebaiknya kita tidak menuliskan PIN di kartu identitas kita ataupun secarik kertas yang ditaruh di dompet. Dengan begitu, jika dompet kita tertinggal atau hilang, tidak ada potensi kerugian yang bisa ditimbulkan. Ketiga, gunakan PIN yang berbeda untuk kepentingan yang berbeda supaya tingkat keamanannya.

3.4 Kemampuan Memahami Dan Melindungi *Two-Factor Authentication (2fa)*

Aplikasi surat elektronik saat ini sudah merupakan sebuah kebutuhan dalam setiap aktivitas pekerjaan. Melakukan *two factor authentification* dilakukan untuk memastikan bahwa user yang login adalah user yang sesungguhnya dengan memberikan pertanyaan tambahan atau dengan permintaan kode untuk memastikan bahwa pengguna adalah pengguna yang terdaftar. Permintaan kode dapat dikirim melalui *short message services* (SMS) atau melalui verifikasi ke HP user.

Proses autentikasi dua faktor ini dilakukan dengan cara identifikasi pengguna berdasarkan dua faktor sebagai komponen informasi yang hanya diketahui oleh pengguna dan sistem. Biasanya langkah pertama adalah pengguna login melalui username atau email untuk masuk ke sistem. Langkah berikutnya, pengguna dikonfirmasi lagi dengan beberapa faktor sebagai langkah tambahan untuk memastikan.

3.5 Mengenali Dan Memahami Penipuan Digital

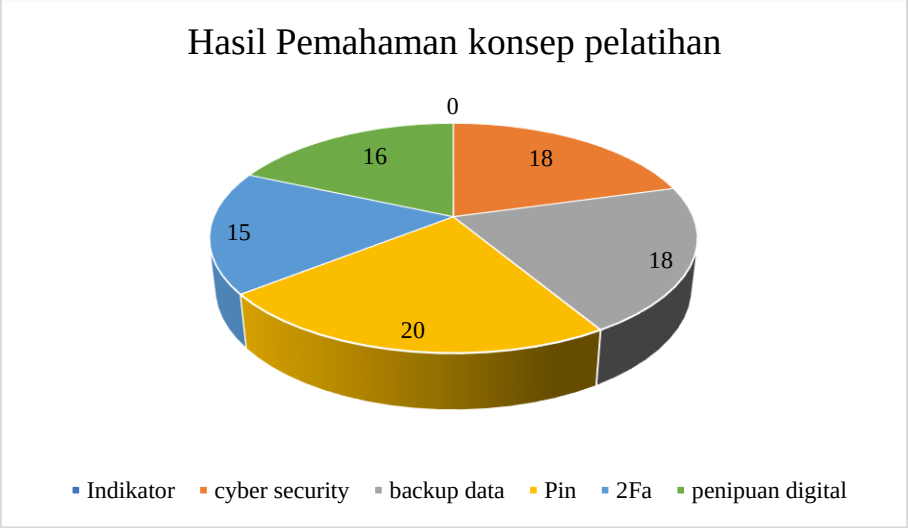
Kemajuan teknologi internet memudahkan berbagai hal mulai dari berbagi informasi hingga proses jual beli barang atau jasa melalui berbagai macam aplikasi. Namun demikian, terdapat oknum-oknum yang memanfaatkan kemajuan teknologi tersebut dengan melakukan kejahatan siber/kejahatan digital. Berbelanja daring rentan menjadi incaran para pelaku kejahatan digital karena aktivitas ini memiliki beragam celah yang bisa dimanfaatkan, terutama dengan memanfaatkan kelengahan pengguna teknologi digital.

Penipuan daring memanfaatkan seluruh aplikasi pada platform media internet untuk menipu para korban dengan berbagai modus. Penipuan jenis ini menggunakan sistem elektronik (komputer, internet, perangkat telekomunikasi) yang disalahgunakan.

Phishing adalah istilah penipuan yang menjebak korban dengan target menyasar kepada orang-orang yang percaya bahwa informasi yang diberikannya jatuh ke orang yang tepat. Biasanya, phishing dilakukan dengan menduplikat situs web atau aplikasi bank atau provider. Ketika kita memasukkan informasi rahasia, uang kita akan langsung dikuras oleh cracker tadi. Kejahatan phishing ini dilakukan oleh oknum dengan menghubungi kita sebagai calon korbannya melalui email, telepon, atau pesan teks dengan mengaku dari lembaga sah. Biasanya oknum-oknum yang melakukan phishing akan menanyakan beberapa data sensitif seperti identitas pribadi, detail perbankan, kartu kredit, dan juga kata sandi. Bagi kita yang terjebak dalam kejahatan ini, informasi yang diperoleh pelaku dapat ia gunakan untuk mengakses akun penting yang kita miliki dan mengakibatkan pencurian identitas hingga kerugian finansial. Selain melalui email dan situs web, phishing juga bisa dilakukan melalui suara (vishing), SMS (smishing) dan juga beberapa teknik lainnya yang terus-menerus akan diperbarui oleh para penjahat dunia maya. Selain itu phishing ini juga biasanya dilakukan melalui media-media sosial yang terhubung ke jaringan internet seperti melalui email/SMS dan situs web. Modus perbuatannya yang melalui email/SMS mengirimkan pesan. Kita mungkin pernah mendapatkan telepon dari orang yang mengaku teman lama. Mungkin juga telepon dari orang yang mengaku pegawai bank dan menyatakan bahwa kita sudah menerima hadiah. Setelah itu korban akan dipandu sehingga tanpa sadar membocorkan data pribadinya sendiri. Hal semacam ini juga lumrah dalam praktik phishing (Gulo, Lasmadi, & Nawawi, 2021). Jadi phishing dapat kita bedakan sesuai dengan tanda-tanda yang umum sering terjadi diantaranya adanya email phishing yang biasanya berisi tautan situs web phishing atau kata kunci seperti permintaan sandi, login, dan lain-lain. Setidaknya ada beberapa hal yang dapat dilakukan untuk mendeteksi phishing yaitu melalui kesadaran kita untuk mengenali email/SMS/situs web phishing atau melalui piranti lunak yang tersedia seperti PhiGARo maupun Honeypot yang memang telah dipasang untuk mendeteksi adanya serangan phishing pada perangkat digital kita, di mana piranti lunak ini tentu saja akan terus dikembangkan oleh para ahli siber untuk mendeteksi serangan phishing yang semakin waktu semakin canggih cara dan modusnya.

Gambar 3. Peserta Pelatihan

Data persentasi hasil kegiatan pelatihan ini menunjukkan data sebagai berikut:



Gambar 4. Hasil Pemahaman Pelatihan

4. KESIMPULAN DAN SARAN

Kegiatan Pengenalan *cyber security* bagi Siswa sekolah menengah atas sangat penting. Dalam era *big data* yang sangat maju tentu ada peluang maka ada ancaman. Oleh karena itu setiap organisasi khususnya sekolah perlu memahami dan menerapkan praktek keamanan *cyber* yang baik. Melalui pelatihan *cyber security* di sekolah, Siswa mengetahui bagaiamana agar data diri, kelurga, lingkungan sekolah dan data penting lainnya agar aman ketika dibagikan di media berbasis internet. Siswa juga mengetahui bagaimana mengecek kebenaran atas data yang tersebar di internet. Siswa dapat mengetahui bahaya dari media internet dan bagaiamana menggunakan media internet ke hal-hal yang positif dan bermanfaat. Selain itu, siswa dapat melindungi diri dari serangan cyber, mengelola resiko kemanan dan meningkatkan kesadaran keamanan. Pengenalan *cyber security* perlu dilanjutkan pada materi lebih rinci mengenai etika digital agar siswa dapat mengetahui hal-hal yang dapat dibagikan maupun hal-hal yang tidak dapat dibagikan dalam media berbasis internet. Dengan pelatihan yang tepat, setiap siswa maupun pihak-pihak sekolah dapat meningkatkan keamanan dan mengurangi risiko serangan *cyber*.

REFERENSI

Anggono, A., & Riskiyadi, M. (2021). Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis Cybercrime and Cybersecurity at Fintech: A Systematic Literature Review. *Jurnal Manajemen Dan Organisasi (JMO)*, *12*(3), 239–251.

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

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, *1*(2), 68–81. https://doi.org/10.22437/pampas.v1i2.9574

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

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