

PELATIHAN KEAMANAN CYBER UNTUK ANAK-ANAK DAN ORANG TUA DI MESJID IKHSAN KOTO SIBAUAK

Nurmaliana Pohan^{1*}, Juna Eska², Hidayatullah¹

¹Teknik Informatika, Universitas Putra Indonesia YPTK

²Teknik Komputer, Universitas Putra Indonesia YPTK

¹Teknik Informatika, AMIK Polibisnis Perdagangan

*email: *dosen.junaeska@gmail.com*

Abstract : In the increasingly developing digital era, internet use has become an inseparable part of everyday life. However, with the convenience offered by technology, there are also various cyber security risks that can endanger children and the elderly. To address this problem, the "Cyber Security Training for Children and Parents" project aims to provide a better understanding of online threats and steps that can be taken to protect oneself and one's family in cyberspace. The project will present a series of trainings covering important topics such as safe use of social media, password control and privacy protection. Participants will be taught by facilitators who are experts in the field of cyber security, and they will be given a guide that can be used as a reference to ensure security in their online activities. The training will involve children aged 10-18 years as well as their parents, with the hope that the knowledge gained will provide better protection for the entire community. This project requires financial support to finance facilitators, training materials and promotional activities. With financial assistance and contributions from various parties, we hope to increase awareness about cyber security and provide the skills needed to face challenges in cyberspace.

Keywords: internet of things (IoT); internet technology

Abstrak : Di era digital yang semakin berkembang, penggunaan internet telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari. Namun, dengan kemudahan yang ditawarkan oleh teknologi, muncul pula berbagai risiko keamanan cyber yang dapat membahayakan anak-anak dan orang tua. Untuk mengatasi masalah ini, proyek "Pelatihan Keamanan Cyber untuk Anak-anak dan Orang Tua" bertujuan untuk memberikan pemahaman yang lebih baik tentang ancaman online dan langkah-langkah yang dapat diambil untuk melindungi diri dan keluarga di dunia maya. Proyek ini akan menyajikan serangkaian pelatihan yang mencakup topik-topik penting seperti penggunaan yang aman di media sosial, pengendalian kata sandi, dan perlindungan privasi. Para peserta akan diajarkan oleh para fasilitator yang ahli di bidang keamanan cyber, dan mereka akan diberikan panduan yang dapat digunakan sebagai referensi untuk memastikan keamanan dalam aktivitas online mereka. Pelatihan akan melibatkan anak-anak usia 10-18 tahun serta orang tua mereka, dengan harapan bahwa pengetahuan yang diperoleh akan memberikan perlindungan yang lebih baik bagi seluruh komunitas. Proyek ini memerlukan dukungan dana untuk membiayai fasilitator, materi pelatihan, dan promosi kegiatan. Dengan bantuan dana dan kontribusi dari berbagai pihak, kami berharap dapat meningkatkan kesadaran tentang keamanan cyber dan memberikan keterampilan yang diperlukan untuk menghadapi tantangan di dunia maya.

Kata Kunci : security; cyber; child; parent

PENDAHULUAN

Dalam era digital ini, penggunaan internet telah menjadi bagian tak terpisahkan dari kehidupan sehari-hari. Anak-anak dan orang tua pun semakin terlibat dalam aktivitas online, mulai dari pembelajaran, bermain game, hingga berkomunikasi dengan teman dan keluarga. (Tandirerung et al., 2023) Namun, keamanan cyber menjadi isu kritis karena ancaman seperti penipuan online, kejahatan cyber, dan pelecehan online semakin meningkat. Oleh karena itu, penting untuk memberikan pelatihan keamanan cyber kepada anak-anak dan orang tua untuk melindungi mereka dari potensi risiko yang ada di dunia maya. Dalam rangka menghadapi tantangan dan dinamika kehidupan yang semakin kompleks dan dinamis dalam dunia internet, anak-anak dan orang tua seharusnya terus meningkatkan ilmu pengetahuan salah satunya dengan mengikuti pelatihan. (Budi et al., 2021) Oleh karena itu, program pengabdian kepada masyarakat yang akan kami laksanakan ini merupakan upaya untuk membantu anak-anak dan orang tua dalam meningkatkan kualitas ilmu pengetahuan melalui pelatihan yang berkualitas dalam pemanfaatan teknologi untuk keamanan cyber. Melalui program pengabdian kepada masyarakat ini, kami tim PKM UPI YPTK bertujuan memberikan Pelatihan Keamanan Cyber untuk Anak-anak dan Orang Tua, tujuan utamanya adalah memberikan pelatihan keamanan cyber kepada anak-anak dan orang tua pada lingkungan Mesjid Ikhsan. Pelatihan ini akan membantu mereka memahami risiko online dan bagaimana cara melindungi diri mereka sendiri dan anak-

anak mereka saat beraktivitas di internet. Pelatihan ini akan meliputi pengenalan teknologi digital, pemanfaatan teknologi, dan teknik pengamanan cyber. Anak-anak menaklukkan dunia digital pada usia yang sangat muda. Oleh karena itu, penting bagi mereka untuk menerima pelatihan keamanan cyber yang efektif dan komprehensif. Dengan bantuan proposal ini, diharapkan pihak terkait memberikan dukungan dan persetujuan untuk mempromosikan keamanan cyber yang efektif dan berkelanjutan bagi anak-anak dan orang tua. Dengan cara ini, anak-anak dan orang tua akan memiliki keterampilan yang diperlukan untuk menjadi pengguna teknologi yang cerdas, kritis, dan bertanggung jawab di era digital yang terus berkembang.

METODE

Metode yang digunakan dalam PKM ini dalam bentuk seminar atau ceramah. Adapun Lokasi Kegiatan Pengabdian Kepada Masyarakat ini adalah di Mesjid Ikhsan Koto Sibauak Kel. Tanjung Alam Kec. Tanjung Baru, Kab.Tanah Datar. Metode dan langkah yang akan dilakukan dapat dijelaskan sebagai berikut :

1. Melakukan rapat koordinasi bersama Tim PKM Mandiri UPI YPTK Padang dalam waktu yang terukur dan tersistem.
2. Memilih tema dan kebijakan-kebijakan penting terkait bentuk kegiatan yang akan diselenggarakan.
3. Melakukan survei lokasi dengan cara mendatangi langsung tempat

atau lokasi kegiatan. Kegiatan ini di akhiri dengan membuat kerjasama berupa pengagendaaan jadwal kegiatan PKM.

4. Mendata dengan baik seluruh peserta kegiatan dan fasilitas yang dapat digunakan selama berkegiatan.
5. Merealisasikan seluruh agenda di atas secara tertulis dalam naskah proposal kegiatan PKM. (Nadjiha, 2019)
6. Kemudian menyerahkannya kepada LPPM UPI YPTK Padang sesuai dengan arahan dan prosedur yang telah ditentukan.

keluarga (rumah) dan pendidikan (sekolah), dan 3) Literasi digital dan perlindungan online anak sangat membutuhkan dialog dan kerjasama multi stakeholder yang inklusif, setara, transparan dan akuntabel dalam koridor Internet Governance.”



Gambar 1. Penjelasan Cyber security

PEMBAHASAN

Cyber Security merupakan praktik melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari ancaman yang juga dikenal sebagai keamanan teknologi informasi. (Hantoro et al., 2020) terdapat tiga konsep cyber security yaitu (1) confidentiality untuk perlindungan informasi yang belum diotorisasi atau diungkapkan, (2) integrity untuk perbaikan data yang rusak harus secepatnya ditangani, (3) availability untuk menjamin akses yang tepat untuk penggunaan sistem, informasi. Cyber security melindungi data akun pengguna dan membatasi 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

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. (Sacharisa & Shalehah, 2023) 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

Memahami Dan Melindungi Personal Identification Number (Pin) Sering kali 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.(Harahap et al., 2024) 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.

Kemampuan Memahami dan Melindungi Two-Factor Authentication (2fa) Aplikasi surat elektronik saat ini sudah merupakan sebuah kebutuhan dalam setiap aktivitas pekerjaan. Melakukan two factor authentication 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.(Aulia, F., Magistarina, E., & Sukma, 2023) Langkah berikutnya, pengguna dikonfirmasi lagi dengan beberapa faktor sebagai langkah tambahan untuk memastikan. 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 menysar 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 menghungi 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.(Harahap et al., 2024) 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.(Budi et al., 2021)



Gambar 3. Orang tua peserta

SIMPULAN

Kegiatan Pelatihan Keamanan cyber bagi Anak dan Orang tua di Lingkungan Masjid Ikhsan Koto Sibauk, dapat diambil simpulan yang mana Pelatihan Keamanan cyber di Lingkungan Masjid Ikhsan Koto Sibauk sangat penting bagi Anak dan Orang tua, agar mereka bisa menggunakan teknologi dan mengetahui ancaman di dunia teknologi. Kegiatan ini juga membantu orang tua dalam memberikan pemahaman kepada anak-anak untuk cermat lagi dalam memanfaatkan teknologi. Pelatihan keamanan cyber dilakukan dgn tujuan, agar anak dan orang tua dapat melihat dampak positif yang ada atau ditimbulkan dengan mengetahui keamanan dalam ancaman yang ada saat sekarang ini.

DAFTAR PUSTAKA

- Aulia, F., Magistarina, E., & Sukma, D. (2023). Psikoedukasi literasi media sosial untuk meningkatkan parental awareness terhadap cyber threats pada orangtua dan guru. *Pendidikan Tambusai*, 7(1), 3866–3872. <https://jptam.org/index.php/jptam/article/view/5853/4898>
- Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, 3(November), 223–234. <https://doi.org/10.54706/senastindo.v3.2021.141>
- Rasim. (2020). Siber Sosialisasi Keamanan Siber Untuk Anak-Anak di Panti Asuhan Aisyah Bekasi. *Jurnal Sains Teknologi Dalam Pemberdayaan Masyarakat*, 1(1), 1–10. <https://doi.org/10.31599-/jstpm.v1i1.224>
- Harahap, N. M., Islam, U., & Sumatera, N. (2024). *CYBER CRIME DAN ANALISI INOVASI PENCEGAHAN RESIKO CYBER CRIME DI INDONESIA CYBER CRIME INFORMATION AND COMMUNICATION TECHNOLOGY CRIME RISKS AND INNOVATION ANALYSIS OF CYBER CRIME RISK*. 3, 52–59.
- Nadjih, S. (2019). Japs 1. *Jurnal Asia Pacific Studies*, 4 Number 1(1), 33–45. <https://dx.doi.org/10.33541-/japs.v4i1.1640>
- Sacharisa, R. N., & Shalehah, A. Y. (2023). Parasitisme Media Sosial Dalam Konteks Child Cyber Grooming Pada Jejaring Sosial Games Hago. *RELASI: Jurnal Penelitian Komunikasi*, 03(1), 88–100.
- Tandirerung, V. A., Riana T. Mangesa, & Syahrul. (2023). Pengenalan Cyber Security Bagi Siswa Sekolah Menengah Atas. *TEKNOVOKASI: Jurnal Pengabdian Masyarakat*, 1(2), 89–94. <https://doi.org/10.59562/teknovokasi.v1i2.131>
- Hantoro, K., Mahbub, A., Khaerudin, &