Jurnal Pengabdian Kepada Masyarakat
Publisher
Cv Era Digital Nusantara

Program Edukasi *Cyber Crime*: Pencegahan dan Penanggulangan Teknik *Phishing* pada Siswa SD Inpres 13 Kabupaten Sorong

Melda Agnes Manuhutu[1*], Agung[2], Alusius[3], Alfaris Mambrasar[4], Indri[5], Tri[6], Sahidin[7], Yermina[8], Beatrik[9], Lulu Jola Uktolseja[10]
[1-10]Universitas Victory Sorong, Indonesia
*e-mail: melda.a.manuhutu@gmail.com

Abstract: *This community service activity was conducted at SD Inpres 13, Sorong Regency, with the aim of providing elementary school students with education on cybercrime, particularly phishing techniques. The program was implemented through five main stages: socialization, training, technology implementation, mentoring and evaluation, and program sustainability. The activity involved 41 fourth- and fifth-grade students of SD Inpres 13, Sorong Regency. An interactive approach was employed through presentations, question-and-answer sessions, and phishing case simulations. The results of the activity indicated that students were able to understand the basic concept of phishing, identify characteristics of suspicious messages or links, and recognize appropriate steps to protect their personal data. This activity contributes to improving digital security literacy among elementary school students and fostering awareness of the importance of safe technology use in the digital era.*
Keywords: *Cyber Crime, Digital Education, Literation, Phishing, Student.*

Abstrak: *Kegiatan pengabdian kepada masyarakat ini dilaksanakan di SD Inpres 13 Kabupaten Sorong dengan tujuan memberikan edukasi tentang cyber crime, khususnya teknik phishing kepada siswa sekolah dasar. Program ini dilaksanakan melalui lima tahapan utama, yaitu sosialisasi, pelatihan, penerapan teknologi, pendampingan dan evaluasi, serta keberlanjutan program. Kegiatan diikuti oleh 41 siswa kelas 4 dan 5 Sekolah Dasar Inpres 13 Kabupaten Sorong. Metode yang digunakan bersifat interaktif meliputi presentasi, sesi tanya jawab, dan simulasi kasus phishing. Hasil pelaksanaan kegiatan menunjukkan bahwa siswa dapat memahami konsep dasar phishing, mengenali ciri-ciri pesan atau tautan mencurigakan, serta mengetahui langkah yang dapat dilakukan untuk melindungi data pribadi. Kegiatan ini memberikan kontribusi dalam meningkatkan literasi keamanan digital siswa sekolah dasar dan membangun kesadaran mengenai pentingnya penggunaan teknologi secara aman di era digital.*
Kata Kunci: *Edukasi Digital, Kejahatan Siber, Literasi, Siswa, Phishing.*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi saat ini berkembang sangat pesat, termasuk di kalangan pelajar. Teknologi menjadi bagian yang tak terpisahkan dari kehidupan anak. Mulai dari segi akademik, hiburan, komunikasi, dan juga relasi dengan sebaya. Di Indonesia sendiri, penetrasi internet mencapai 79,5% pada 2024 dengan jumlah pengguna sekitar 221,56 juta jiwa (APJII, 2024). Peningkatan tersebut memperluas peluang anak untuk memperoleh informasi dan memanfaatkan berbagai sumber belajar, tetapi pada saat yang sama juga memperbesar paparan terhadap berbagai risiko di ruang digital. Penelitian terhadap sekitar 300 siswa sekolah dasar di Indonesia menunjukkan bahwa literasi digital, mediasi orang tua, dan kemampuan pengendalian diri memiliki keterkaitan dengan tingkat risiko yang dihadapi siswa dalam penggunaan internet, sehingga kemampuan menggunakan teknologi secara aman menjadi bagian penting dari kompetensi digital anak (Arianto et al., 2021).

Risiko tersebut mencakup ancaman terhadap keamanan informasi dan data pribadi. Pada waktu yang bersamaan, hal ini dapat disebabkan oleh interaksi yang tidak aman. Anak merupakan kelompok yang perlu memperoleh perhatian khusus karena kemampuan kognitif dan pengambilan keputusan mereka masih berkembang. Mereka cenderung mudah membuka tautan yang belum jelas sumbernya, membagikan data pribadi, hingga belum memahami pentingnya menjaga kerahasiaan *password* (Hong, 2012). Pendidikan *cybersecurity* di sekolah lebih banyak berfokus pada penggunaan *password*, sedangkan topik yang lebih kompleks seperti *phishing* dan *hacking* cenderung belum diberikan secara konsisten kepada anak usia sekolah dasar (Lamond

et al., 2025). Kondisi tersebut menunjukkan bahwa peningkatan akses anak terhadap teknologi tidak selalu berjalan seiring dengan kesiapan mereka dalam mengenali dan merespons risiko keamanan digital.

Internet memberikan banyak manfaat untuk belajar dan hiburan, tetapi di sisi lain juga menyimpan risiko keamanan yang tidak bisa diabaikan. Salah satu ancaman yang relevan dalam konteks tersebut adalah *phishing*. *Phishing* merupakan teknik penipuan dengan cara memancing pengguna untuk memberikan data sensitif seperti *username*, *password*, hingga data kartu kredit, dengan berpura-pura menjadi lembaga atau orang terpercaya (Jagatic et al., 2007). Kurangnya pengetahuan menjadikan siswa sebagai target yang rentan menjadi korban penipuan digital, pembajakan akun *game*, hingga penyebaran konten berbahaya (Chiew et al., 2018). Penelitian Lastdrager et al. (2017) terhadap 353 anak berusia 8–13 tahun menunjukkan bahwa pelatihan anti-*phishing* dapat membantu anak meningkatkan kemampuan dalam mengenali *phishing*. Namun, penelitian tersebut juga menemukan bahwa kemampuan tersebut dapat menurun beberapa minggu setelah pelatihan. Temuan ini menunjukkan bahwa edukasi mengenai *phishing* penting diberikan sejak dini dan perlu dilakukan secara berkelanjutan, bukan hanya melalui penyampaian informasi satu kali.

Kondisi tersebut relevan dengan situasi di SD Inpres 13 Kabupaten Sorong. Hampir seluruh siswa di SD Inpres 13 Kabupaten Sorong sudah memiliki akses terhadap internet melalui *smartphone* maupun komputer. (Gupta et al., 2018). Berdasarkan observasi awal, sebagian besar siswa telah berinteraksi dengan internet melalui smartphone maupun komputer, tetapi pemahaman mengenai keamanan digital masih terbatas. Kondisi ini menunjukkan adanya kesenjangan antara akses terhadap teknologi dan kemampuan menggunakannya secara aman. Anak memang sudah berada di ruang digital, tetapi belum tentu memiliki pengetahuan yang cukup untuk mengenali risiko di dalamnya.

Oleh karena itu, kegiatan pengabdian kepada masyarakat ini dilakukan untuk memberikan edukasi mengenai *cyber crime*, khususnya *phishing*, kepada siswa kelas 4 dan 5 SD Inpres 13 Kabupaten Sorong. SD Inpres 13 Kabupaten Sorong merupakan salah satu sekolah dasar negeri yang terletak di Kabupaten Sorong. Sekolah ini memiliki fasilitas yang cukup memadai dan antusiasme siswa yang tinggi terhadap teknologi. Namun, materi mengenai keamanan digital atau *cyber security* belum secara khusus dan mendalam diajarkan dalam kurikulum sehari-hari (Verizon, 2024). Guru-guru di sekolah juga menyadari pentingnya pembekalan ilmu ini, tetapi dibutuhkan narasumber yang dapat menyampaikan materi dengan bahasa yang sederhana, menarik, dan mudah dipahami oleh anak-anak usia sekolah dasar. Dengan alasan tersebut, sekolah menyambut baik kegiatan pengabdian masyarakat yang dilakukan oleh mahasiswa Universitas Victory Sorong ini (Kaspersky Lab, 2025).

Agenda yang dilakukan adalah pengajaran cara mengenali ciri-ciri penipuan online dan pembekalan siswa dengan langkah-langkah praktis jika menemukan hal mencurigakan di internet. Materi disampaikan melalui presentasi, tanya jawab, dan simulasi kasus *phishing.* Tujuannya agar siswa mengetahui pengertian phishing dan mengenali pesan atau tautan yang mencurigakan serta mengetahui langkah yang harus dilakukan untuk melindungi data pribadi. Kegiatan ini diharapkan dapat memperkuat literasi keamanan digital siswa dan membangun kebiasaan menggunakan teknologi secara lebih aman sejak usia sekolah dasar. Selain itu, kegiatan ini bertujuan untuk mewujudkan bentuk pengabdian mahasiswa kepada masyarakat dalam bidang literasi digital (Symantec, 2023).

2. METODE

Kegiatan pengabdian masyarakat ini dilaksanakan di SD Inpres 13 Kabupaten Sorong, Papua Barat, yang diikuti oleh 41 siswa kelas 4 dan 5. Kegiatan berlangsung pada hari Jumat, 24 April 2026. Metode pelaksanaan menggunakan pendekatan edukatif-partisipatif. Tahapan pelaksanaan program edukasi ini terdiri dari lima fase utama, sebagaimana dijelaskan berikut:

a. **Persiapan:** Rapat koordinasi tim untuk menentukan materi, pembagian tugas, dan jadwal. Pembuatan materi presentasi (*slide*) tentang *phishing* yang disesuaikan untuk siswa SD, serta persiapan alat peraga, laptop, dan perlengkapan dokumentasi.

b. **Sosialisasi:** Pendekatan dan pengenalan kegiatan kepada pihak sekolah, penyampaian maksud dan tujuan kegiatan, serta meminta izin pelaksanaan. Tim memperkenalkan diri kepada siswa dan membangun suasana yang akrab namun kondusif.

c. **Pelaksanaan/Pelatihan:** Penyampaian materi secara interaktif mencakup pengertian *phishing*, ciri-ciri pesan mencurigakan, cara kerja *phishing*, dampak yang ditimbulkan, serta langkah-langkah pencegahan. MC membuka acara, pemateri menyampaikan konten, dan moderator mengatur perpindahan slide.

d. **Penerapan Teknologi:** Siswa diajak melihat contoh tampilan website atau pesan palsu di layar, lalu bersama-sama menganalisis mana yang aman dan mana yang berbahaya. Materi meliputi cara memeriksa keamanan website melalui penggunaan "https" serta pentingnya melakukan pembaruan aplikasi secara berkala.

e. **Evaluasi dan Keberlanjutan:** Sesi tanya jawab untuk mengukur pemahaman siswa dan diskusi internal tim setelah kegiatan selesai. Pada akhir sesi, disampaikan kesimpulan dan pesan-pesan penting agar siswa dapat terus berhati-hati dan menyebarkan informasi positif kepada keluarga dan teman-teman mereka.

3. HASIL DAN PEMBAHASAN

Pelaksanaan Program Edukasi Cyber Crime dengan fokus pada pencegahan dan penanggulangan teknik *phishing* di SD Inpres 13 Kabupaten Sorong dilaksanakan melalui lima tahapan utama. Setiap tahapan memberikan kontribusi terhadap peningkatan pemahaman siswa mengenai keamanan digital.

3.1 Persiapan

Kegiatan diawali dengan mengadakan rapat koordinasi menyeluruh secara internal untuk mematangkan seluruh rencana kerja tim. Dalam pertemuan ini, seluruh anggota berdiskusi secara mendalam untuk menentukan materi apa saja yang akan disampaikan, sekaligus menyusun pembagian tugas yang jelas serta menetapkan jadwal pelaksanaan yang terperinci. Tim juga mempersiapkan seluruh fasilitas pendukung di lapangan, mulai dari pengecekan laptop, pembuatan alat peraga fisik yang edukatif, hingga kesiapan seluruh perlengkapan dokumentasi untuk mengabadikan jalannya kegiatan secara utuh.

Gambar 1. Program Persiapan Edukasi *Cyber Crime*

3.2 Sosialisasi

Tahap sosialisasi merupakan tahap awal yang bertujuan untuk memperkenalkan kegiatan kepada pihak sekolah dan siswa. Pada tahap ini, tim menyampaikan maksud dan tujuan kegiatan serta memberikan gambaran umum mengenai materi yang akan dibahas. Materi yang disampaikan meliputi pengertian *cyber crime*, khususnya *phishing*, contoh kasus yang sering terjadi, tujuan pelaku melakukan *phishing*, serta dampak yang dapat ditimbulkan. Dalam tahap ini diketahui bahwa siswa mulai dapat memahami konsep dasar *phishing* dan menyadari terdapat risiko dalam penggunaan internet yang mereka gunakan sehari-hari.

Gambar 2. Kegiatan Sosialisasi dan Pembukaan Acara di SD Inpres 13 Kabupaten Sorong

3.2 Pelatihan

Tahap pelatihan merupakan inti dari kegiatan. Sebelum penyampaian materi, siswa terlebih dahulu diberikan simulasi sederhana berupa contoh pesan palsu melalui email atau chat yang sering digunakan oleh pelaku *phishing*. Simulasi ini bertujuan untuk melatih kemampuan awal siswa dalam mengenali tanda-tanda kecurigaan. Selanjutnya, materi disampaikan secara interaktif yang mencakup pengertian *phishing*, ciri-ciri pesan mencurigakan, tujuan *phishing*, cara kerja *phishing*, dampak yang ditimbulkan, serta langkah-langkah pencegahan. Penjelasa disambut dengan baik, para siswa dengan tenang mendengarkan penjelasan materi yang disampaikan. Hasil dari tahap ini menunjukkan bahwa siswa mampu mengenali ciri-ciri *phishing*, lebih berhati-hati terhadap pesan atau tautan yang diterima, serta mulai memiliki kesadaran untuk menjaga data pribadi.

3.3 Penerapan Teknologi

Pada tahap penerapan teknologi, siswa diperkenalkan dengan cara sederhana dalam memanfaatkan teknologi untuk meningkatkan keamanan digital. Materi yang diberikan meliputi cara memeriksa keamanan *website* melalui penggunaan "*https*" serta pentingnya melakukan pembaruan (*update*) aplikasi secara berkala. Melalui tahap ini, siswa diajak memahami bahwa teknologi tidak hanya digunakan untuk hiburan, tetapi juga dapat dimanfaatkan untuk melindungi diri dari ancaman di dunia digital. Hasil yang diperoleh menunjukkan bahwa siswa mulai memahami langkah-langkah dasar dalam menjaga keamanan saat menggunakan internet.

Gambar 3. Kegiatan Penyampaian Materi dan Penerapan Teknologi kepada Siswa

3.4 Pendampingan dan Evaluasi

Tahap pendampingan dan evaluasi dilakukan setelah seluruh materi disampaikan. Pada tahap ini, siswa didampingi untuk mengulang kembali materi serta diberikan kesempatan untuk bertanya dan berdiskusi. Evaluasi dilakukan melalui sesi tanya jawab dan pengamatan terhadap respon siswa selama kegiatan berlangsung. Tim memastikan bahwa siswa benar-benar memahami materi yang telah diberikan. Hasil evaluasi menunjukkan adanya peningkatan pemahaman siswa, yang ditandai dengan kemampuan mereka dalam menjawab pertanyaan, mengidentifikasi pesan mencurigakan, serta menjelaskan kembali konsep *phishing* dengan bahasa sederhana.

3.5 Keberlanjutan Program

Tahap keberlanjutan program bertujuan untuk memastikan bahwa kegiatan yang telah dilakukan tidak berhenti pada satu waktu saja. Pada tahap ini, disampaikan pentingnya menjaga keamanan digital secara berkelanjutan kepada siswa dan pihak sekolah. Siswa didorong untuk menerapkan pengetahuan yang telah diperoleh dalam kehidupan sehari-hari serta membagikan informasi tersebut kepada lingkungan sekitar. Pihak sekolah juga diharapkan dapat melanjutkan edukasi terkait cyber crime sebagai bagian dari pembelajaran tambahan. Dengan demikian, kegiatan ini tidak hanya memberikan dampak jangka pendek, tetapi juga diharapkan mampu menciptakan kesadaran jangka panjang dalam penggunaan teknologi yang aman.

Hasil kegiatan pengabdian masyarakat ini menunjukkan bahwa pendekatan edukatif-interaktif efektif dalam meningkatkan pemahaman siswa sekolah dasar tentang bahaya *phishing*. Temuan ini sejalan dengan penelitian Gupta et al. (2018) yang menyatakan bahwa edukasi langsung kepada pengguna merupakan salah satu strategi paling efektif dalam pertahanan terhadap serangan *phishing*. Pendekatan berbasis simulasi dan contoh nyata terbukti lebih efektif dibandingkan hanya memberikan materi teoritis.

Siswa kelas 4 dan 5 SD Inpres 13 menunjukkan antusiasme yang tinggi dalam mengikuti seluruh rangkaian kegiatan. Mereka aktif bertanya dan mampu mengidentifikasi ciri-ciri *phishing* setelah mengikuti pelatihan. Hal ini mendukung temuan Jagatic et al. (2007) bahwa faktor sosial dan pendekatan berbasis komunitas sangat berperan dalam meningkatkan kesadaran keamanan digital. Dengan metode yang menyenangkan dan mudah dipahami, siswa tidak hanya memperoleh pengetahuan tetapi juga termotivasi untuk berbagi kepada teman dan keluarga mereka.

Menurut Chiew et al. (2018), serangan *phishing* terus berkembang dalam berbagai vektor dan teknik yang semakin canggih. Oleh karena itu, pembekalan literasi digital sejak dini di tingkat sekolah dasar merupakan langkah strategis yang perlu didukung oleh berbagai pihak, termasuk perguruan tinggi melalui program pengabdian masyarakat seperti yang telah dilakukan oleh Tim Universitas Victory Sorong ini. Data dari Verizon (2024) menunjukkan bahwa faktor manusia

masih menjadi celah utama dalam insiden keamanan siber, sehingga edukasi berkelanjutan sangat diperlukan.

4. KESIMPULAN

Program Edukasi *Cyber Crime* yang dilaksanakan di SD Inpres 13 Kabupaten Sorong telah berhasil meningkatkan pemahaman siswa tentang bahaya *phishing* dan cara mencegahnya. Melalui lima tahapan pelaksanaan yang terstruktur: sosialisasi, pelatihan, penerapan teknologi, pendampingan dan evaluasi, serta keberlanjutan program, siswa memperoleh pengetahuan dan keterampilan dasar dalam menjaga keamanan digital. Kegiatan ini juga memberikan manfaat bagi mahasiswa dalam melatih kemampuan komunikasi, kepemimpinan, dan pengabdian kepada masyarakat. Diharapkan sekolah dapat melanjutkan edukasi terkait keamanan digital sebagai bagian dari pembelajaran di era digital yang terus berkembang.

UCAPAN TERIMA KASIH

Tim pelaksana mengucapkan terima kasih kepada Universitas Victory Sorong, Ucapan terima kasih juga disampaikan kepada Kepala Sekolah dan seluruh guru SD Inpres 13 Kabupaten Sorong yang telah memberikan izin dan dukungan penuh dalam pelaksanaan kegiatan pengabdian masyarakat ini, serta kepada seluruh siswa yang telah berpartisipasi aktif dalam program edukasi ini.

DAFTAR REFERENSI

Arianto, I. M., Suyanto, S., & Suyanto, E. (2021). Digital literacy and online risk among elementary school students in Indonesia. Heliyon, 7(7), e07406. https://doi.org/10.1016/j.heliyon.2021.e07406

Chiew, K. L., Yong, S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications, 106, 1–20. https://doi.org/10.1016/j.eswa.2018.03.050

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. Telecommunication Systems, 67, 497–510. https://doi.org/10.1007/s11235-017-0334-z

Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74–81. https://doi.org/10.1145/2063176.2063197

IBM Security. (2024). What is phishing? IBM Security Intelligence. Retrieved from https://www.ibm.com/topics/phishing

Imperva. (2024). Phishing attacks: Types, techniques and prevention. Imperva Blog. Retrieved from https://www.imperva.com/learn/application-security/phishing-attack/

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94–100. https://doi.org/10.1145/1290958.1290968

Kaspersky Lab. (2025). Phishing attacks in 2025: Trends and statistics. Kaspersky Security Bulletin. Retrieved from https://www.kaspersky.com/resource-center/threats/phishing

Lamond, M., Prior, S., Renaud, K., & Wood, M. (2025). Teachers' perspectives and practice of cybersecurity education in primary schools. Discover Education, 4. https://doi.org/10.1007/s44217-025-00471-0

Lastdrager, E. E. H., Mengerink, J., Keijzer-Broers, W., & Renaud, K. (2017). How effective is anti-phishing training for children? Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), 237–249. USENIX Association.

Symantec. (2023). Internet security threat report. Broadcom Symantec Enterprise Blogs. Retrieved from https://symantec-enterprise-blogs.security.com

Trend Micro. (2024). What is social media phishing? Trend Micro Security Intelligence. Retrieved from https://www.trendmicro.com/vinfo/us/security/definition/phishing

Verizon. (2024). 2024 data breach investigations report. Verizon Enterprise. Retrieved from https://www.verizon.com/business/resources/reports/dbir/