Attamkiim: Jurnal Pengabdian Masyarakat
e-ISSN 3064-3007
https://ejournal.stais-garut.ac.id/index.php/attamkiim

SOSIALISASI KEAMANAN DIGITAL UNTUK MENGATASI PHISHING DAN APK BERBAHAYA

Emi Sita Eriana[1], Afrizal Zein[2], Fordiana Eka wati[3], Mohammad Satria Arya Buminata[4]
Sistem Informasi, Universitas Pamulang, Banten, Indonesia
Jl. Puspitek Raya No 10, Serpong, Tangerang Selatan.
Email: dosen02692@unpam.ac.id.

Abstrak

Kemajuan teknologi digital membawa kemudahan dalam berbagai aspek kehidupan, namun juga meningkatkan risiko keamanan siber, termasuk serangan phishing dan aplikasi berbahaya (APK). Phishing adalah metode penipuan yang digunakan oleh pelaku kejahatan siber untuk mencuri informasi sensitif dengan menyamar sebagai entitas terpercaya, sedangkan APK berbahaya adalah aplikasi yang mengandung malware yang dapat mencuri data pribadi atau merusak perangkat. Sosialisasi ini bertujuan untuk meningkatkan kesadaran masyarakat terhadap ancaman keamanan digital serta memberikan edukasi tentang cara melindungi diri dari serangan phishing dan APK berbahaya. Metode yang digunakan dalam sosialisasi mencakup seminar, pelatihan interaktif, serta simulasi serangan siber untuk meningkatkan pemahaman peserta. Materi yang disampaikan mencakup cara mengenali situs atau email phishing, pentingnya autentikasi ganda (2FA), serta langkah-langkah aman dalam mengunduh dan menggunakan aplikasi dari sumber terpercaya. Hasil dari sosialisasi ini diharapkan dapat meningkatkan kewaspadaan masyarakat terhadap ancaman digital serta membentuk kebiasaan aman dalam penggunaan teknologi. Dengan pemahaman yang baik tentang ancaman siber, individu dapat lebih proaktif dalam melindungi data pribadi dan menghindari potensi risiko yang ditimbulkan oleh serangan phishing dan aplikasi berbahaya.

Kata Kunci : Keamananan, Digital,Sosialisasi, Siber, Teknologi

Abstract

Advances in digital technology bring convenience in various aspects of life, but it also increases cybersecurity risks, including phishing attacks and malicious applications. Phishing is a deceptive method used by cybercriminals to steal sensitive information by posing as a trusted entity, while malicious APKs are applications that contain malware that can steal personal data or damage devices. This socialization aims to increase public awareness of digital security threats as well as provide education on how to protect themselves from phishing attacks and malicious APKs. The methods used in the socialization included seminars, interactive training, and simulated cyberattacks to improve participants' understanding. The material presented includes how to recognize phishing sites or emails, the importance of double authentication (2FA), and secure steps in downloading and using apps from trusted sources. The results of this socialization are expected to increase public awareness of digital threats and form safe habits in the use of technology. With a good understanding of cyber threats, individuals can be more proactive in protecting personal data and avoiding the potential risks posed by phishing attacks and malicious applications.

Keywords: Security, Digital, Socialization, Cyber, Technology

PENDAHULUAN

Di era digital yang terus berkembang, kejahatan siber seperti phishing dan penyebaran aplikasi berbahaya (APK) menjadi ancaman serius yang tidak dapat diabaikan. Phishing merupakan metode penipuan daring yang dilakukan dengan menyamar sebagai pihak tepercaya untuk mencuri informasi sensitif, sementara APK berbahaya mengandung malware yang dapat merusak perangkat atau mencuri data pribadi. Seiring meningkatnya penggunaan internet di kalangan pelajar, ancaman-ancaman ini menjadi semakin relevan, terutama karena banyak pengguna muda belum dibekali pemahaman yang cukup tentang cara melindungi diri secara digital.

Sejumlah studi internasional menunjukkan bahwa pelajar di berbagai negara, termasuk Indonesia, rentan terhadap serangan siber akibat rendahnya kesadaran dan literasi digital. Situasi ini juga tercermin di SMKN 3 Kota Tangerang Selatan, di mana mayoritas siswa aktif menggunakan internet namun belum memahami risiko kejahatan siber yang mereka hadapi. Data internal sekolah menunjukkan bahwa lebih dari 60% siswa pernah mengalami atau hampir menjadi korban phishing dan penipuan online, sementara pengetahuan mereka tentang praktik keamanan digital dasar masih terbatas.

Kondisi ini menandakan perlunya intervensi edukatif yang terstruktur untuk meningkatkan literasi dan keterampilan keamanan digital di kalangan siswa. Dengan dukungan sekolah dan potensi kolaborasi lintas lembaga, program pelatihan keamanan siber dapat menjadi solusi strategis untuk membekali siswa dengan pengetahuan dan keterampilan yang dibutuhkan agar mereka mampu mengenali dan menghindari ancaman digital. Tujuan akhirnya adalah menciptakan lingkungan belajar yang aman secara digital dan membentuk generasi muda yang cakap menghadapi tantangan dunia maya.

Metode

Tahap Persiapan

Pada tahap awal, dilakukan identifikasi kebutuhan dan kesiapan mitra melalui survei dan wawancara untuk mengetahui tingkat pemahaman siswa serta kesiapan sekolah dalam mendukung program. Berdasarkan hasil tersebut, disusun modul pelatihan yang mencakup topik-topik penting seperti ancaman phishing, malware, dan praktik keamanan digital dasar. Modul dirancang menarik dan relevan dengan kurikulum yang ada. Selanjutnya, dilakukan pelatihan untuk guru (Training of Trainers) agar mereka mampu menjadi fasilitator yang efektif dalam menyampaikan materi kepada siswa.

Pelaksanaan Edukasi dan Pembentukan Tim

Pelaksanaan program mencakup sesi pelatihan interaktif selama tiga bulan, dengan pertemuan mingguan berdurasi 90 menit. Materi disampaikan melalui metode aktif seperti simulasi, studi kasus, dan diskusi. Siswa juga mengikuti simulasi ancaman siber untuk mengasah keterampilan praktis dalam mengenali dan merespons serangan digital. Selain itu, dibentuk Tim Keamanan Digital Siswa yang direkrut dan dilatih sebagai "Duta Keamanan Digital" untuk menyebarkan edukasi melalui pendekatan peer-to-peer seperti kampanye dan diskusi kelompok.

Partisipasi Mitra dan Evaluasi Program

Pihak sekolah berperan aktif menyediakan fasilitas, melibatkan guru, serta mempromosikan program di lingkungan sekolah. Evaluasi dilakukan secara bertahap: mulai dari evaluasi proses (monitoring pelaksanaan), evaluasi hasil (tes sebelum dan sesudah pelatihan), hingga evaluasi dampak jangka panjang untuk melihat perubahan perilaku siswa dalam penggunaan internet secara aman. Keberhasilan program juga diukur dari efektivitas Tim Keamanan Digital dalam meningkatkan kesadaran keamanan digital di kalangan siswa.

Keberlanjutan Program

Agar program berkelanjutan, modul pelatihan akan diintegrasikan ke dalam kurikulum mata pelajaran seperti TIK dan PKn. Tim Keamanan Digital Siswa akan terus berfungsi sebagai agen perubahan di sekolah dengan dukungan guru. Sekolah juga didorong untuk menjalin kemitraan dengan pihak eksternal seperti komunitas siber atau perusahaan teknologi guna mendukung pelatihan lanjutan. Monitoring dan evaluasi berkala dilakukan untuk menjaga keberlangsungan dampak program dan menyesuaikan strategi dengan kebutuhan yang berkembang.

HASIL

Program pelatihan interaktif mengenai literasi digital dan keamanan siber telah berhasil dilaksanakan di SMKN 3 Kota Tangerang Selatan dengan melibatkan siswa dari berbagai jurusan. Kegiatan ini dilaksanakan dalam beberapa sesi yang mencakup materi teori dan praktik, seperti cara membuat kata sandi yang kuat, mengenali email phishing, serta mengidentifikasi situs dan aplikasi berbahaya. Peserta juga mengikuti simulasi kasus nyata terkait penipuan online yang dirancang untuk meningkatkan pemahaman secara kontekstual. Respons dari para siswa sangat positif, ditandai dengan tingginya partisipasi dan antusiasme selama sesi berlangsung.

WAKTU	DURASI	ACARA	PELAKSANA
09.00 – 09.20	20	Persiapan Acara Kegiatan PKM	Panitia
09.20 – 09.25	5	Pembukaan	Panitia
09.25 – 09.35	10	Sambutan Kepala Sekolah SMKN 3 Kota Tangerang Selatan	Hj. Dwi Novy Hardani, S.Pd, M.Pd
09.35 – 09.45	10	Sambutan Perwakilan Dosen Pendamping PKM	Emi Sita Eriana S.Kom., M.Kom
09.45 – 09.50	5	Sambutan Ketua Pelaksana PKM	M Satria Arya Buminata
09.55 – 10.25	30	Materi "Pengenalan tentang Teknologi Kecerdasan Buatan dan ancaman siber seperti Phishing"	Panitia
10.25 – 10.35	10	Sesi Pertanyaan	Panitia & Peserta
10.35 – 11.05	30	Materi " Implementasi Teknologi Kecerdasan Buatan Untuk Pendeteksian Serangan Phishing pada Aplikasi Mobile "	Panitia
11.05 – 11.15	10	Sesi Pertanyaan	Panitia & Peserta
11.05 – 11.25	20	Quiz	Panitia & Peserta
11.25 – 11.30	5	Penutup Acara	Panitia

Gambar 1 Rundown Kegiatan PKM Sosialisasi Keamanan Digital

Berdasarkan hasil evaluasi pre dan post pelatihan, tercatat adanya peningkatan signifikan dalam pemahaman peserta terhadap topik-topik keamanan digital. Dari total peserta yang mengikuti pelatihan, lebih dari 85% menunjukkan peningkatan

skor pemahaman sebesar minimal 20% setelah pelatihan. Hasil ini mengindikasikan bahwa pendekatan edukatif berbasis praktik mampu meningkatkan kesadaran serta keterampilan siswa dalam menghadapi potensi ancaman siber secara lebih kritis dan responsif. Selain itu, diskusi kelompok dan kuis interaktif juga memberikan dampak positif dalam memperkuat pemahaman peserta terhadap materi yang disampaikan.

Gambar 2 Pelaksanaan PKM Keamanan Digital

Secara keseluruhan, kegiatan pengabdian kepada masyarakat ini memberikan dampak yang nyata dalam meningkatkan literasi digital siswa, khususnya terkait keamanan informasi pribadi di dunia maya. Pihak sekolah memberikan apresiasi atas pelaksanaan program ini dan berharap kegiatan serupa dapat terus dilakukan secara berkelanjutan. Hasil pelaksanaan ini juga menunjukkan pentingnya kolaborasi antara institusi pendidikan, akademisi, dan praktisi keamanan siber dalam membangun generasi yang tangguh dan sadar akan bahaya serangan digital di era teknologi saat ini.

Kesimpulan

Kesimpulan Program Edukasi Keamanan Siber di SMKN 3 Kota Tangerang Selatan

a. Urgensi Edukasi Keamanan Siber Program edukasi keamanan siber yang dilaksanakan di SMKN 3 Kota Tangerang Selatan merupakan respons tepat terhadap meningkatnya ancaman kejahatan siber seperti phishing dan aplikasi berbahaya (APK) yang menyasar kalangan pelajar. Data menunjukkan bahwa lebih dari 60% siswa pernah mengalami atau hampir menjadi korban phishing dan penipuan online, menegaskan pentingnya intervensi edukatif.
b. Efektivitas Program Pendekatan interaktif yang diterapkan dalam program terbukti efektif, dengan peningkatan signifikan pada pemahaman siswa, di mana lebih dari 85% peserta menunjukkan peningkatan skor minimal 20% setelah pelatihan. Metode kombinasi teori dan praktik termasuk simulasi kasus nyata secara kontekstual berhasil meningkatkan kesadaran dan keterampilan siswa dalam menghadapi ancaman siber.
c. Implikasi Jangka Panjang Pembentukan Tim Keamanan Digital Siswa dan integrasi modul keamanan siber ke dalam kurikulum regular menjadi langkah strategis untuk keberlanjutan program. Kolaborasi antara institusi pendidikan, akademisi, dan praktisi keamanan siber merupakan faktor kunci dalam membangun generasi yang tangguh di era digital.

Saran

a. Perluasan Jangkauan Program
   Memperluas program ke sekolah-sekolah lain di wilayah Tangerang Selatan untuk menciptakan jaringan keamanan siber yang lebih luas.Mengembangkan materi pelatihan berdasarkan tingkat pendidikan dan karakteristik demografi siswa.
b. Penguatan Kolaborasi
   Menjalin kemitraan formal dengan perusahaan teknologi dan komunitas keamanan siber untuk mendapatkan dukungan teknis dan materi terkini.Melibatkan orang tua dalam program edukasi untuk menciptakan ekosistem keamanan siber yang terintegrasi antara sekolah dan rumah.
c. Pengembangan Konten dan Metode
   Mengembangkan platform e-learning khusus keamanan siber yang dapat diakses siswa secara mandiri.Menyelenggarakan kompetisi keamanan siber antar kelas atau antar sekolah untuk meningkatkan keterlibatan dan minat siswa.
d. Evaluasi dan Pengembangan Berkelanjutan
   Melakukan evaluasi berkala dengan metode yang lebih komprehensif untuk mengukur perubahan perilaku digital siswa dalam jangka panjang.

Program edukasi keamanan siber ini telah menunjukkan hasil yang menjanjikan dalam meningkatkan kesadaran dan keterampilan siswa menghadapi ancaman digital. Dengan penguatan strategi dan komitmen dari berbagai pemangku kepentingan, program ini berpotensi memberikan dampak lebih luas dalam membangun generasi yang cakap dan aman di dunia digital

Daftar Pustaka

Badan Siber dan Sandi Negara (BSSN). (2023). "Laporan Tahunan Keamanan Siber Indonesia 2023". Jakarta: BSSN.

CERT (Computer Emergency Response Team) Indonesia. (2023). "Modul Pelatihan Pengenalan dan Pencegahan Phishing". Jakarta: BSSN.

Firmansyah, G. & Wahyudi, R. (2021). "Keamanan Aplikasi Mobile: Identifikasi Ancaman dan Pencegahan". Penerbit Lokomedia.

Hidayat, T. (2022). "Mengenal dan Mencegah Phishing di Era Digital". Penerbit Andi.

Kementerian Komunikasi dan Informatika. (2024). "Panduan Sosialisasi Keamanan Digital untuk Pemerintah Daerah". Jakarta: Kominfo.

Kusuma, R. & Hartanto, B. (2023). "Identifikasi dan Mitigasi Aplikasi Berbahaya di Perangkat Mobile". Jurnal Keamanan Siber Indonesia, 7(1), 78-95.

Nugroho, A. (2023). "Keamanan Digital untuk Semua: Panduan Praktis Menghindari Serangan Siber". Penerbit Informatika.

Pratama, D. & Wijaya, S. (2022). "Efektivitas Program Edukasi Anti-Phishing pada Kalangan Pekerja Kantoran". Jurnal Sistem Informasi dan Teknologi, 14(3), 230-245.

Seri Webinar "Safe Digital Indonesia" oleh Indonesia Security Response Team (ID-SIRT), 2023-2024.

Siregar, J., & Saputra, M. (2022). "Model Pelatihan Keamanan Digital untuk Mencegah Penipuan Online". Jurnal Komunikasi dan Informatika, 11(4), 300-315.

Sosialisasi "Waspada Phishing dan Aplikasi Berbahaya" oleh Asosiasi Pengguna Jasa Internet Indonesia (APJII), 2023.

Widyanto, A. (2023). "Strategi Sosialisasi Keamanan Digital untuk Masyarakat Indonesia". Jurnal Keamanan Siber Indonesia, 8(2), 45-62.

Workshop "Keamanan Digital untuk UMKM" oleh Kementerian Komunikasi dan Informatika, 2024.