

Pelatihan dan Sosialisasi Keamanan Digital untuk Meningkatkan Kesadaran Siswa Terhadap Ancaman Phishing di Era Digital

Zuriati ¹, Amanda Bulan Nayla ², Gilang Rizki Ramadhan ³, Syahreza Riatma ⁴
^{1,2,3,4}Teknologi Rekayasa Internet, Politeknik Negeri Lampung

Abstrak

Kegiatan pengabdian kepada masyarakat ini mengangkat topik keamanan digital untuk meningkatkan kesadaran siswa terhadap ancaman phishing di era digital. Phishing merupakan salah satu ancaman signifikan yang dapat menimbulkan kerugian besar, terutama bagi generasi muda yang aktif menggunakan teknologi. Kelompok siswa, khususnya mereka yang sering berinteraksi dengan dunia maya melalui perangkat digital, termasuk golongan yang rentan terhadap serangan ini. Oleh karena itu, kegiatan pelatihan dan sosialisasi ini dirancang untuk memberikan edukasi kepada siswa jurusan Teknik Jaringan Komputer dan Telekomunikasi di SMK Negeri 4 Bandar Lampung mengenai cara mengenali dan menghindari phishing serta pentingnya menjaga keamanan digital. Kegiatan ini diawali dengan wawancara informal sebagai pre-test untuk mengukur tingkat pemahaman awal siswa tentang phishing. Selanjutnya, dilakukan pelatihan dan sosialisasi melalui presentasi interaktif yang membahas berbagai jenis serangan phishing, ciri-ciri serangan, dan langkah-langkah pencegahan yang dapat diambil. Simulasi praktik juga diadakan untuk memberikan pengalaman langsung kepada siswa tentang cara kerja phishing dan strategi melindungi diri dari serangan tersebut. Sebagai penutup, dilakukan sesi tanya jawab, sekaligus menjadi post-test untuk mengevaluasi peningkatan pemahaman siswa setelah mengikuti kegiatan. Hasil evaluasi menunjukkan peningkatan signifikan dalam pemahaman dan kesadaran siswa terhadap ancaman phishing. Siswa menjadi lebih terampil dalam mengenali potensi ancaman dan mampu menerapkan langkah-langkah perlindungan di dunia digital. Dengan pendekatan berbasis teknologi dan simulasi langsung, metode ini terbukti efektif dalam membantu siswa menghadapi tantangan keamanan digital di era modern.

Kata kunci: Sosialisasi, Literasi Digital, Phishing, Keamanan Digital.

Abstract

This community service activity raises the topic of digital security to increase students' awareness of the threat of phishing in the digital era. Phishing is a significant threat that can cause major losses, especially for the younger generation who actively use technology. Student groups, especially those who frequently interact with cyberspace via digital devices, are among the groups vulnerable to this attack. Therefore, this training and outreach activity is designed to provide education to students majoring in Computer Network and Telecommunications Engineering at SMK Negeri 4 Bandar Lampung about how to recognize and avoid phishing and the importance of maintaining digital security. This activity begins with an informal interview as a pre-test to measure students' initial level of understanding about phishing. Furthermore, training and outreach was carried out through interactive presentations discussing various types of phishing attacks, the characteristics of attacks, and preventive steps that can be taken. Practical simulations are also held to give students direct experience of how phishing works and strategies to protect themselves from these attacks. In closing, a question and answer session was held, as well as a post-test to evaluate the increase in students' understanding after participating in the activity. Evaluation results show a significant increase in students' understanding and awareness of phishing threats. Students become more skilled at recognizing potential threats and able to implement protective measures in the digital world. With a technology-based approach and hands-on simulation, this method has proven effective in helping students face digital security challenges in the modern era.

Keywords: Socialization, Digital Literacy, Phishing, Digital Security.



This work is licensed under a [Creative Commons Attribution-Share Alike 4.0](https://creativecommons.org/licenses/by-sa/4.0/) Copyright © 2024 by Author. Published by IDEANova Press.

Diterima: 27-12-2024

Direvisi: 20-04-2025

Diterbitkan: 30-04-2025

Penulis Korespondensi:

Amanda Bulan Nayla,
Teknologi Rekayasa Internet/Teknologi Informasi, Politeknik Negeri Lampung
Jl. Soekarno Hatta No.10, Rajabasa Raya, Kec. Rajabasa, Kota Bandar Lampung, Lampung
Email: amandbulan@gmail.com

1. PENDAHULUAN

Di era digital yang berkembang pesat, ancaman phishing menjadi salah satu tantangan besar yang dihadapi oleh masyarakat, terutama generasi muda. Phishing merupakan metode penipuan siber yang bertujuan untuk mendapatkan informasi sensitif, seperti kata sandi dan data pribadi, dengan menyamar sebagai pihak yang dapat dipercaya. Siswa, sebagai pengguna aktif teknologi digital, menjadi salah satu kelompok yang paling rentan terhadap ancaman ini. Tingginya intensitas interaksi mereka dengan dunia maya, ditambah dengan rendahnya kesadaran akan keamanan digital, menjadikan mereka target utama serangan phishing. Survei yang dilakukan oleh Kominfo (Kementerian Komunikasi dan Informatika) menunjukkan bahwa kasus bullying dan judi online menjadi bentuk kekerasan digital pada anak yang paling sering muncul di media sosial. Sekitar 440.000 anak usia 10-20 tahun di Indonesia dilaporkan kecanduan judi online, yang sering kali menjadi pintu masuk bagi serangan phishing dan penipuan daring lainnya (Espelage dkk., 2023). Data terkini menunjukkan bahwa serangan digital di Indonesia meningkat pada kuartal I tahun 2024, dengan peningkatan sebesar 25% dibandingkan periode yang sama tahun sebelumnya (Butler dkk., 2021). Jenis serangan yang paling banyak terjadi adalah phishing, malware, dan ransomware. Hal ini mengindikasikan bahwa ancaman kejahatan digital di Indonesia semakin serius dan membutuhkan penanganan yang komprehensif.

Fakta lain menunjukkan bahwa siswa usia sekolah, termasuk siswa SMK, memang rentan menjadi korban kejahatan digital. Penelitian menunjukkan bahwa siswa yang merasa lebih terhubung dengan sekolah memiliki risiko yang lebih rendah untuk menjadi korban cyberbullying, sedangkan siswa yang melaporkan kesulitan emosional dan masalah dengan teman sebaya lebih mungkin menjadi korban cyberbullying dan viktimisasi tradisional (Livazović & Ham, 2019). Faktor-faktor tingkat sekolah yang terkait dengan perpetrasi cyberbullying termasuk suasana kelas dan pendidikan keamanan siber (Zhou & Li, 2021). Studi lain menyebutkan bahwa berbagai bentuk kejahatan digital yang sering melibatkan anak-anak dan remaja, seperti eksploitasi seksual, cyberbullying, grooming, dan sextortion, telah menjadi ancaman serius bagi penegakan hukum pidana anak di Indonesia (Jauhari, 2023). Hal ini diperparah dengan adanya kesulitan dalam menangani kasus-kasus tersebut karena peraturan yang belum jelas dan komprehensif (Kim, 2023). Upaya untuk mengurangi kejahatan dan kekerasan di sekolah telah mendorong banyak sekolah untuk mengadopsi strategi pencegahan, termasuk bekerja sama dengan departemen kepolisian setempat dan menerapkan petugas sumber daya sekolah, memasang kamera video dan sistem televisi sirkuit tertutup, serta menggunakan sistem deteksi senjata (Shestakova, 2023).

Sebagai institusi pendidikan vokasi, SMK Negeri 4 Bandar Lampung memiliki peran strategis dalam membentuk kompetensi digital siswa sekaligus meningkatkan kesadaran mereka terhadap bahaya ancaman siber. Siswa kelas XI jurusan Teknik Jaringan Komputer dan Telekomunikasi, yang aktif menggunakan teknologi dalam pembelajaran, menunjukkan kebutuhan mendesak untuk diberikan edukasi tentang keamanan digital. Berdasarkan hasil pengamatan awal, sebagian besar siswa memiliki pemahaman yang terbatas terhadap ancaman phishing, seperti kesulitan mengenali tautan palsu dan kecenderungan membagikan informasi pribadi tanpa berpikir panjang. Oleh karena itu, kegiatan pelatihan dan sosialisasi ini dirancang untuk memberikan pemahaman mendalam kepada siswa mengenai ancaman phishing, cara mengenali tanda-tanda serangan, dan langkah-langkah pencegahan yang dapat dilakukan. Pelatihan dilakukan melalui pendekatan berbasis teknologi dengan beberapa tahapan: perencanaan, pelaksanaan, hingga monitoring dan evaluasi. Dengan metode ini, diharapkan siswa dapat lebih terampil dalam mengenali potensi ancaman dan mengambil langkah preventif untuk melindungi diri di dunia digital.

2. METODE

Tahapan pelaksanaan pelatihan ini terdiri dari tiga fase utama, yaitu perencanaan, pelaksanaan, serta monitoring dan evaluasi. Berikut adalah penjelasan lebih rinci mengenai setiap tahap:

2.1. Tahap Perencanaan

Sebelum pelaksanaan pelatihan dan sosialisasi, sejumlah kegiatan persiapan dilakukan. Langkah pertama adalah menentukan lokasi sosialisasi, diikuti dengan penyusunan administrasi surat-menyurat. Setelah administrasi disiapkan, dilakukan kunjungan untuk menetapkan jadwal kegiatan dan mencari narasumber yang

sesuai. Selanjutnya, materi pelatihan disusun dan persiapan sarana serta prasarana pendukung dilakukan untuk mendukung kelancaran pelaksanaan kegiatan.

2.2. Tahap Pelaksanaan

Tahap pelaksanaan mengikuti jadwal pelaksanaan yang ditentukan. Sosialisasi dilakukan berdasarkan materi yang telah disiapkan, Metode penyampaian materi teori menggunakan pendekatan yang interaktif dan didukung teknologi untuk memperdalam pemahaman siswa mengenai ancaman phishing dan cara pencegahannya. Kegiatan dimulai dengan diskusi interaktif sebagai pre-test untuk mengevaluasi pemahaman awal siswa tentang phishing dan potensi ancaman di dunia maya. Selain itu, dalam diskusi ini, para siswa juga ditanya apakah ada di antara mereka yang pernah menjadi korban serangan phishing, serta bagaimana mereka menangani situasi tersebut. Langkah ini bertujuan untuk mengetahui sejauh mana siswa sudah memahami topik tersebut sebelum materi disampaikan, sekaligus menggali pengalaman nyata mereka terkait serangan phishing. Kemudian, dilakukan presentasi interaktif yang menguraikan konsep phishing, jenis-jenis serangan phishing, serta cara-cara untuk mengenali dan melindungi diri dari serangan tersebut. Dalam sesi ini, berbagai contoh serangan phishing ditampilkan menggunakan media seperti slide, email dan contoh langsung dari situs web atau email phishing yang sering digunakan oleh pelaku kejahatan. Tujuannya adalah agar siswa dapat lebih memahami bagaimana serangan phishing terjadi dan apa saja ciri-cirinya yang perlu diwaspadai.

Pada sesi berikutnya, Dilaksanakan simulasi praktik dan demonstrasi untuk memberikan siswa pengalaman langsung mengenai cara kerja serangan phishing. Dalam simulasi ini, digunakan platform Kali Linux, yang sering dimanfaatkan oleh para profesional keamanan siber, untuk memperlihatkan secara nyata bagaimana serangan phishing dapat dilakukan. Siswa diajak untuk memahami proses teknis, seperti cara informasi dapat dicuri melalui email phishing atau situs web palsu. Simulasi ini bertujuan untuk memberikan pemahaman yang lebih mendalam tentang teknik yang digunakan oleh penyerang dan bagaimana cara menghindari jebakan tersebut. Siswa akan dibimbing untuk melihat tanda-tanda phishing pada situs web atau email, serta langkah-langkah yang perlu diambil untuk menghindarinya, seperti memverifikasi URL, tidak mengklik link mencurigakan, dan tidak memberikan informasi pribadi melalui media yang tidak terpercaya.

Setelah melakukan simulasi, observasi langsung dilakukan untuk melihat bagaimana siswa merespons situasi tersebut dan seberapa baik mereka dapat mengidentifikasi ancaman phishing. Proses ini juga diikuti dengan **post-test** yang berupa tanya jawab untuk mengukur sejauh mana pemahaman siswa setelah melalui simulasi dan demonstrasi. Pada tahap ini, siswa akan dinilai berdasarkan kemampuan mereka untuk menerapkan apa yang telah dipelajari, serta sejauh mana mereka dapat mengenali potensi ancaman phishing dan langkah-langkah pencegahan yang perlu diambil. Proses tanya jawab juga digunakan untuk mengklarifikasi hal-hal yang masih kurang dipahami oleh siswa.

2.3. Tahap Monitoring dan Evaluasi

Setelah sesi presentasi dan demonstrasi mengenai cara kerja phishing melalui Simulasi Phishing dalam Praktik Keamanan Digital, peserta diberikan kuesioner untuk mengevaluasi perubahan pemahaman mereka terkait phishing serta langkah-langkah pencegahan yang dapat diambil untuk melindungi diri dari ancaman tersebut. Kuesioner ini dirancang untuk mengukur sejauh mana pemahaman peserta meningkat setelah mengikuti kegiatan edukasi. Selain itu, kuesioner juga mencakup saran-saran dari peserta yang digunakan sebagai bahan evaluasi untuk meningkatkan kualitas sosialisasi pada kegiatan serupa di masa mendatang.

3. HASIL DAN PEMBAHASAN

Kegiatan sosialisasi ini dilaksanakan dalam satu hari dengan tujuan untuk meningkatkan pemahaman siswa mengenai ancaman phishing. Kegiatan tersebut berlangsung di SMK Negeri 4 Bandar Lampung dan diikuti oleh siswa kelas 11 jurusan Teknik Jaringan Komputer dan Telekomunikasi.

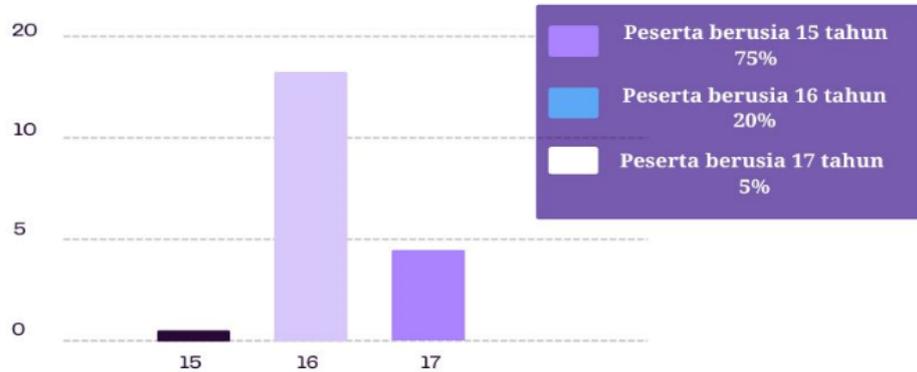


Gambar 1. Peserta kegiatan Sosialisasi

Peserta memiliki rentang usia antara 16 hingga 17 tahun, yang merupakan generasi muda yang aktif menggunakan teknologi digital dalam kehidupan sehari-hari. Hal ini menunjukkan pentingnya pemberian edukasi tentang ancaman phishing kepada kelompok ini, mengingat mereka sering terlibat dalam aktivitas online yang rentan terhadap serangan siber (Gambar 2).

Grafik Umur Peserta

SMK NEGERI 4 BANDAR LAMPUNG



Gambar 2. Umur Peserta Sosialisasi

Kegiatan dimulai dengan diskusi interaktif sebagai pre-test untuk mengevaluasi pemahaman awal siswa tentang phishing dan potensi ancaman di dunia maya. Selain itu, dalam wawancara ini, siswa juga ditanya apakah ada di antara mereka yang pernah menjadi korban serangan phishing, serta bagaimana mereka menangani situasi tersebut. Langkah ini bertujuan untuk mengetahui sejauh mana siswa sudah memahami topik tersebut sebelum materi disampaikan, sekaligus menggali pengalaman nyata mereka terkait serangan phishing, sehingga hasil akhirnya dapat dievaluasi dengan lebih efektif. Pada tabel 1 menunjukkan pertanyaan - pertanyaan diskusi.

Tabel 1. Pertanyaan Diskusi Interaktif

NO	Pertanyaan
1	Apakah siswa, sebelumnya sudah mengetahui materi Phising?
2	Apakah siswa pernah menjadi korban Phising?
3	Jika pernah menjadi korban Phising, langkah apa yang dilakukan?



Gambar 3. Kegiatan Sosialisasi

Pada tahap presentasi materi interaktif mencakup penyampaian materi dasar mengenai phishing secara interaktif. Materi yang disampaikan meliputi pengertian phishing, jenis-jenisnya, teknik yang biasa digunakan, serta dampaknya terhadap korban. Penyampaian dilakukan secara dinamis untuk memastikan siswa terlibat aktif dalam proses pembelajaran.

Setelah pemahaman dasar diberikan, siswa diajak mengikuti simulasi phishing menggunakan perangkat seperti Kali Linux. Dalam simulasi ini, peserta diperlihatkan bagaimana serangan phishing dilakukan secara teknis. Tujuannya adalah untuk memberikan gambaran nyata tentang cara kerja phishing sekaligus mengajarkan cara mengenali tanda-tanda serangan phishing di kehidupan nyata. Kegiatan diakhiri dengan post-test yang berfungsi untuk mengukur sejauh mana pemahaman siswa meningkat setelah mengikuti sosialisasi. Selain itu, siswa juga diminta mengisi kuesioner untuk memberikan umpan balik terkait efektivitas sosialisasi, termasuk kekuatan dan kelemahannya.

3.1. Hasil Monitoring dan Evaluasi

Dalam kegiatan sosialisasi ini dapat melihat indikator keberhasilan yang meliputi tiga aspek utama, yaitu peningkatan pemahaman, kepuasan peserta, dan perubahan perilaku. Peningkatan pemahaman siswa tentang phishing diukur melalui perbandingan hasil pre-test dan post-test, yang menunjukkan bahwa materi yang disampaikan berhasil meningkatkan pengetahuan mereka mengenai ancaman phishing dan langkah pencegahannya. Tingkat kepuasan peserta juga menjadi tolak ukur penting, di mana sebagian besar siswa menyatakan puas dengan materi yang disampaikan dan menganggapnya relevan berdasarkan kuesioner yang diisi setelah sosialisasi. Selain itu, keberhasilan kegiatan juga terlihat dari perubahan perilaku siswa, yang ditunjukkan melalui kemampuan mereka dalam mengenali tanda-tanda phishing selama simulasi dan praktik langsung. Efektivitas materi dalam sosialisasi ini terlihat dari sejauh mana materi yang disampaikan dapat memenuhi tujuan pembelajaran dan kebutuhan peserta.

Sebagian besar peserta merasa materi yang diberikan relevan dan bermanfaat, terutama terkait dengan phishing, yang menunjukkan bahwa topik yang dipilih sesuai dengan kebutuhan audiens. Selain itu, banyak peserta merasa pemahaman mereka meningkat setelah mengikuti sosialisasi ini, sementara sebagian lainnya merasa ada peningkatan yang cukup baik. Hal ini menunjukkan bahwa sosialisasi ini berhasil memberikan pengetahuan yang lebih dalam kepada peserta mengenai topik yang dibahas. Dalam pelaksanaan sosialisasi, Penggunaan alat bantu dalam terbukti efektif dalam memperjelas materi yang disampaikan. Sebagian besar peserta merasa bahwa alat bantu yang digunakan dalam sosialisasi, seperti slide, handout, dan simulasi phishing, sangat efektif dalam memperjelas topik yang disampaikan. Alat bantu ini berperan penting dalam memvisualisasikan informasi yang mungkin sulit dipahami hanya dengan penjelasan lisan. Sebanyak 50% peserta merasa alat bantu yang disediakan cukup memadai, sementara 40% peserta merasa alat bantu tersebut sangat memadai. Hal ini menunjukkan bahwa mayoritas peserta merasa alat bantu yang digunakan selama sosialisasi membantu mereka memahami materi dengan lebih baik.

Simulasi phishing, khususnya, memainkan peran yang sangat penting dalam mempermudah peserta untuk mengaitkan teori dengan praktik. Dengan memberikan pengalaman langsung mengenai bagaimana serangan phishing dilakukan, peserta bisa lebih mudah melihat hubungan antara pengetahuan yang mereka terima dengan situasi dunia nyata. Penggunaan simulasi ini memberikan kesempatan bagi peserta untuk melihat

secara langsung bagaimana metode-metode phishing dijalankan, serta cara melindungi diri dari ancaman tersebut.

Secara keseluruhan, penggunaan materi yang relevan, penyampaian yang jelas, dan alat bantu yang efektif, memberikan dampak positif terhadap pemahaman peserta. Alat bantu, baik slide, handout, maupun simulasi, bekerja dengan baik dalam mendukung proses pembelajaran dan memperdalam pemahaman peserta mengenai phishing yang dapat dilihat pada gambar 4 dibawah ini :



Gambar 4. Efektivitas materi yang didukung alat bantu (Slide) dalam Meningkatkan Pemahaman Peserta

Berdasarkan hasil kuesioner, sebagian besar siswa melaporkan adanya peningkatan pemahaman yang signifikan. Sebanyak 60% peserta merasa pemahaman mereka sangat meningkat, sementara 35% merasa cukup meningkat. Hanya satu peserta yang merasa netral, menunjukkan bahwa hampir semua peserta merasa memperoleh pengetahuan baru atau pemahaman yang lebih dalam tentang topik yang dibahas dalam sosialisasi. Tidak ada peserta yang melaporkan bahwa pemahaman mereka tidak meningkat atau meningkat sedikit, yang menunjukkan bahwa sosialisasi ini berhasil mencapai tujuan utama, yaitu meningkatkan pemahaman peserta terkait topik phishing yang dapat dilihat pada gambar 5. Dengan demikian, dapat disimpulkan bahwa materi yang disampaikan berhasil memperdalam pengetahuan peserta, dan pendekatan yang digunakan dalam sosialisasi efektif dalam menyampaikan informasi yang relevan dan berguna.



Gambar 5. Pemahaman Peserta Dalam Kegiatan

Keberhasilan sosialisasi dalam menyampaikan informasi baru yang relevan tercermin dari antusiasme peserta yang merasa mendapatkan wawasan yang sebelumnya mungkin belum mereka ketahui. Pendekatan yang mendalam dalam penyampaian materi serta metode inovatif dalam menjelaskan topik terbukti mampu memotivasi peserta untuk memperdalam pengetahuan mereka tentang phishing. Sosialisasi ini berhasil meningkatkan pemahaman siswa secara signifikan, dengan 95% peserta melaporkan adanya peningkatan pengetahuan mengenai phishing. Hal ini mencerminkan efektivitas metode seperti penjelasan, studi kasus, dan diskusi dalam memperjelas dan memperdalam pemahaman mereka. Namun, terdapat 5% peserta yang merasa tidak mengalami peningkatan pemahaman, yang menunjukkan perlunya evaluasi terhadap kecepatan penyampaian materi atau pendekatan pengajaran yang digunakan.

Tingkat keterlibatan peserta dalam sosialisasi mencerminkan seberapa aktif peserta dalam mengikuti kegiatan yang diselenggarakan. Mayoritas peserta merasa terlibat, dengan 40% mengaku cukup terlibat dan 20% merasa sangat terlibat. Namun, ada 25% peserta yang bersikap netral terhadap tingkat keterlibatan mereka, serta 15% yang merasa kurang terlibat. Meskipun sebagian besar peserta merasa terlibat, masih terdapat peluang untuk meningkatkan partisipasi. Salah satu strategi yang dapat diterapkan adalah memperbanyak interaksi melalui diskusi atau sesi tanya jawab. Selain itu, suasana sosialisasi yang mendukung juga terlihat dari 40% peserta yang merasa nyaman dan 40% lainnya yang merasa sangat nyaman untuk berpartisipasi. Hal ini menunjukkan bahwa lingkungan sosialisasi cukup mendukung bagi peserta untuk berinteraksi dan memberikan kontribusi secara aktif yang dapat dilihat pada gambar 6 dibawah ini.



Gambar 6. Peserta yang terlibat dalam kegiatan

Kepuasan peserta yaitu siswa merupakan salah satu indikator utama untuk menilai keberhasilan suatu sosialisasi. Kepuasan peserta dalam kegiatan dapat dilihat indikator keberhasilan dalam sosialisasi yang dilakukan. Hasilnya menunjukkan bahwa 60% peserta merasa sangat puas, 25% puas, dan 15% berada di kategori netral. Tidak ada peserta yang merasa tidak puas atau sangat tidak puas. Sebagian besar peserta merasa sosialisasi ini sangat bermanfaat dan memenuhi harapan mereka. Tingkat kepuasan yang tinggi menunjukkan bahwa sosialisasi berhasil menyampaikan materi dengan efektif dan sesuai dengan ekspektasi peserta. Keterlibatan peserta dalam sosialisasi dan hasil yang positif dari kuesioner mengindikasikan bahwa materi yang disampaikan sesuai dengan harapan mereka dan bermanfaat. Penyampaian yang interaktif, jelas, dan mudah dipahami menjadi faktor penting dalam mencapai tingkat kepuasan yang tinggi. Meskipun hasilnya sangat positif, ada 15% peserta yang berada pada kategori netral. Hal ini mengindikasikan bahwa masih ada ruang untuk perbaikan dalam meningkatkan kepuasan peserta secara keseluruhan yang bisa dilihat pada gambar 7 dibawah ini.



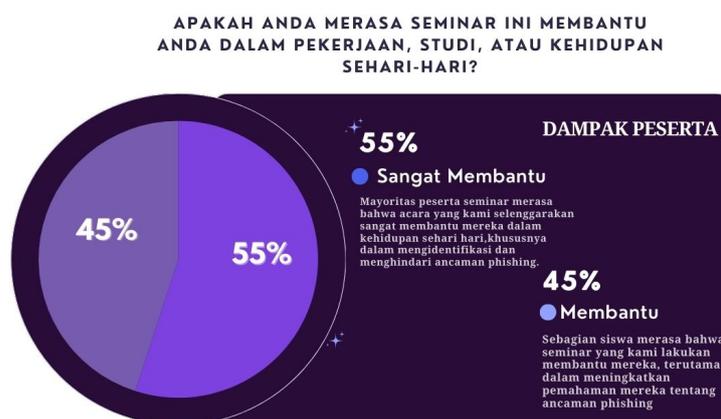
Gambar 7. Kepuasan Peserta terhadap Materi dan Penyampaian dalam Kegiatan Sosialisasi

Dari gambar yang dilihat diatas sebagian besar peserta (85%) merasa bahwa sosialisasi ini tidak hanya memenuhi, tetapi juga melebihi harapan mereka. Hal ini menunjukkan bahwa sosialisasi tersebut berhasil memberikan nilai lebih dari yang diharapkan peserta. Topik yang disampaikan mungkin lebih menarik, lebih relevan, atau lebih mendalam dari yang mereka bayangkan sebelumnya. Keberhasilan sosialisasi dalam memenuhi atau bahkan melebihi harapan peserta yaitu siswa menunjukkan bahwa materi yang dibahas sangat relevan dengan kebutuhan para siswa. Namun, dengan 15% peserta yang merasa netral, penting bagi penyelenggara untuk melakukan evaluasi lebih lanjut untuk memahami alasan ketidakpuasan atau ketidakjelasan yang mungkin muncul. Mengidentifikasi dan memperbaiki area yang masih bisa ditingkatkan akan memastikan keberhasilan sosialisasi yang lebih besar di masa depan yang akan datang.

3.2. Dampak Sosialisasi dalam Kehidupan sehari-hari

Melalui sosialisasi, siswa dapat diberikan pemahaman yang lebih baik tentang teknologi dan pendidikan, serta bagaimana keduanya dapat berkolaborasi untuk menghindari ancaman tersebut. penelitian menunjukkan bahwa pendidikan di era digital harus beradaptasi dengan metode yang lebih inovatif dan interaktif untuk mempersiapkan generasi muda menghadapi tantangan yang ada (Wahidah dkk., 2022). Salah satu pendekatan yang dapat diambil adalah dengan mengintegrasikan literasi digital ke dalam kurikulum pendidikan. literasi digital tidak hanya mencakup kemampuan teknis dalam menggunakan perangkat digital, tetapi juga pemahaman tentang risiko yang terkait dengan penggunaan teknologi, termasuk phishing (Fachmi, 2023). Dengan meningkatkan literasi digital siswa, mereka akan lebih mampu mengenali dan menghindari potensi ancaman yang ada di dunia maya (Sandika dkk., 2022).

Selain itu, sosialisasi dapat menjadi platform untuk berbagi informasi dan strategi pencegahan yang efektif. Melalui kolaborasi antara pendidik, orang tua, dan pihak berwenang, sosialisasi dapat menyajikan informasi terkini mengenai teknik-teknik phishing dan cara-cara untuk menghindarinya. Pendekatan kolaboratif ini penting untuk menciptakan lingkungan yang aman bagi siswa dalam menggunakan teknologi. Sosialisasi ini tidak hanya memberikan wawasan baru, tetapi juga relevan dan aplikatif, membantu peserta menghadapi tantangan dunia digital. Mayoritas peserta (55%) merasa sosialisasi ini sangat membantu mereka dalam aktivitas sehari-hari, baik di bidang profesional, akademik, maupun pribadi. Materi yang disampaikan terbukti relevan dengan kebutuhan peserta, terutama dalam memberikan panduan praktis untuk mengidentifikasi dan menghindari ancaman phishing. Dengan hasil ini, sosialisasi berhasil mendorong peserta untuk mengimplementasikan pengetahuan yang diperoleh dalam berbagai aspek kehidupan mereka, memperkuat dampak positif yang dihasilkan yang dapat dilihat pada gambar 8 dibawah.



Gambar 8. Pengaruh Kegiatan terhadap Pemahaman Peserta

4. KESIMPULAN

Sosialisasi mengenai ancaman phishing yang diadakan di SMK Negeri 4 Bandar Lampung berhasil mencapai tujuan utama, yaitu meningkatkan pemahaman siswa tentang keamanan siber, khususnya ancaman phishing, dan langkah-langkah pencegahannya. Berdasarkan hasil pre-test dan post-test, peserta mengalami peningkatan yang signifikan dalam pemahaman mereka mengenai konsep phishing, jenis-jenisnya, serta cara mengidentifikasi dan menghindarinya. Penggunaan materi yang relevan, pendekatan interaktif, dan simulasi

praktik menggunakan alat seperti Kali Linux terbukti sangat efektif dalam memperdalam pemahaman peserta. Sebagian besar peserta merasa puas dengan penyampaian materi dan menganggapnya sangat berguna untuk kehidupan digital mereka. Hasil kuesioner menunjukkan bahwa mayoritas peserta merasa sosialisasi ini melebihi harapan mereka, baik dari segi pengetahuan yang didapatkan maupun keterlibatan mereka dalam sesi praktis.

Namun, meskipun hasil keseluruhan sangat positif, terdapat beberapa area yang masih dapat diperbaiki. Sebagian kecil peserta merasa kurang terlibat dalam sosialisasi, yang menunjukkan bahwa interaksi lebih lanjut atau variasi metode pengajaran mungkin perlu dipertimbangkan untuk meningkatkan keterlibatan peserta. Selain itu, meskipun sebagian besar peserta merasa bahwa sosialisasi ini berhasil meningkatkan pemahaman mereka, beberapa peserta masih merasa perlu adanya evaluasi lebih lanjut mengenai kecepatan dan kedalaman materi yang disampaikan. Untuk pengembangan lebih lanjut, akan sangat bermanfaat jika sosialisasi ini dikembangkan dengan melibatkan orang tua dan pendidik untuk menciptakan pendekatan yang lebih holistik dan berkelanjutan dalam membangun kesadaran keamanan siber, serta memperluas platform berbasis digital untuk simulasi dan materi pendidikan lebih lanjut. Dengan langkah-langkah ini, generasi muda dapat semakin siap dalam menghadapi ancaman siber yang terus berkembang.

Ucapan Terima Kasih

Kami mengucapkan terima kasih yang sebesar-besarnya kepada seluruh pihak yang telah mendukung terlaksananya sosialisasi mengenai ancaman phishing di SMK Negeri 4 Bandar Lampung. Terutama kepada para peserta yang telah antusias mengikuti acara ini dari awal hingga akhir, serta aktif berpartisipasi dalam setiap sesi. Tanpa keterlibatan aktif kalian, sosialisasi ini tidak akan berjalan dengan sukses. Tak lupa, kami ucapkan terima kasih kepada pihak sekolah dan semua yang telah membantu dalam persiapan dan pelaksanaan acara ini. Dukungan kalian sangat berarti dalam mewujudkan sosialisasi yang bermanfaat ini.

DAFTAR PUSTAKA

- Butler, L. C., Graham, A., Fisher, B. S., Henson, B., & Reyns, B. W. (2021). Examining the Effect of Perceived Responsibility on Online Bystander Intervention, Target Hardening, and Inaction. *Journal of Interpersonal Violence*, 37(21–22). <https://doi.org/10.1177/08862605211055088>
- Espelage, D. L., Harper, C. R., Ingram, K. M., Basile, K. C., Leemis, R. W., & Nickodem, K. K. (2023). Hostile home environment predicting early adolescent sexual harassment perpetration and potential school-related moderators. *Journal of Research on Adolescence*, 33(2), 530–546. <https://doi.org/10.1111/jora.12823>
- Fachmi, N. M. (2023). Model Inquiry Learning Berbasis Literasi Digital Untuk Meningkatkan Minat Belajar Siswa Di Sekolah Dasar. *Jurnal Educatio Fkip Unma*, 9(4), 1646–1652. <https://doi.org/10.31949/educatio.v9i4.5558>
- Jauhari, H. (2023). *Thread and Challenge of Juvenile Criminal Law in the Digital Era*. <https://doi.org/10.4108/eai.28-10-2023.2341667>
- Kim, H. (2023). The Current State and Legal Issues of Online Crimes Related to Children and Adolescents. *Journal of the Korean Academy of Child and Adolescent Psychiatry*, 34(4), 222–228. <https://doi.org/10.5765/jkacap.230049>
- Livazović, G., & Ham, E. (2019). Cyberbullying and Emotional Distress in Adolescents: The Importance of Family, Peers and School. *Heliyon*, 5(6), e01992. <https://doi.org/10.1016/j.heliyon.2019.e01992>
- Sandika, I. K. B., Bisena, I. K. A., & Monny, M. O. E. (2022). Implementasi Pembelajaran Tik Dalam Peningkatan Literasi Digital Siswa SDN 6 Desa Pecatu. *Jurnal Pendidikan Dan Sastra Inggris*, 2(2), 1–5. <https://doi.org/10.55606/jupensi.v2i2.222>
- Shestakova, T. (2023). *Child, Family, School in the Information Space*. 1(1), 162–162. <https://doi.org/10.61365/forum.2023.136>
- Wahidah, B. Y. K., Ramdhani, M., & Wahyuni, W. (2022). Sosialisasi Literasi Digital Di Komunitas Baca Lumbung Literasi. *Darma Diksani Jurnal Pengabdian Ilmu Pendidikan Sosial Dan Humaniora*, 2(2), 70–78. <https://doi.org/10.29303/darmadiksani.v2i2.1953>
- Zhou, L., & Li, C. (2021). Factors Associated With Cyberbullying Among Vocational Students Based on the Ecological System Model in an Ethnic Minority Area. *Medicine*, 100(40), e27226. <https://doi.org/10.1097/md.0000000000027226>