

## SMART SCHOOL NETWORK, INTERNET SEHAT DAN AMAN”: KEAMANAN WI-FI, PRIVASI DATA, DAN PENCEGAHAN PHISHING

Fitra Yuda<sup>1\*</sup>, Yulia<sup>2</sup>, Mailisa<sup>3</sup>, Fauziah<sup>4</sup>, Cut Mutia<sup>5</sup>, Irzon Meiditra<sup>6</sup>,  
M. Rasyid<sup>7</sup>, Alifia Restu Selvanda<sup>8</sup>

<sup>1,2,3,4,5,6,7,8</sup>Institut Teknologi Rokan Hilir

[fitrayuda110199@gmail.com](mailto:fitrayuda110199@gmail.com)<sup>1</sup>, [mrsyulia98@gmail.com](mailto:mrsyulia98@gmail.com)<sup>2</sup>,  
[mailisamsiuii1711@gmail.com](mailto:mailisamsiuii1711@gmail.com)<sup>3</sup>, [fauziahnurgayo@gmail.com](mailto:fauziahnurgayo@gmail.com)<sup>4</sup>,  
[cutmutia117@gmail.com](mailto:cutmutia117@gmail.com)<sup>5</sup>, [meiditairzon@gmail.com](mailto:meiditairzon@gmail.com)<sup>6</sup>,  
[muhammadrasyid798@gmail.com](mailto:muhammadrasyid798@gmail.com)<sup>7</sup>, [alifiarestu1@gmail.com](mailto:alifiarestu1@gmail.com)<sup>8</sup>

\*corresponding author

Received: 10-02-2026

Revised: 15-03-2026

Approved:30-03-2026

### ABSTRAK

*Kegiatan Pengabdian kepada Masyarakat (PkM) dilaksanakan oleh Dosen Program Studi Sistem Informasi dan Program Studi Teknologi Informasi Institut Teknologi Rokan Hilir ini bertujuan untuk meningkatkan pemahaman siswa mengenai konsep Smart School Network, pentingnya keamanan WI-FI sekolah, perlindungan privasi data pribadi dan akademik, serta pengenalan dan pencegahan phishing. Pengabdian kepada masyarakat (PkM) ini melibatkan 25 peserta, terdiri dari 25 siswa kelas sepuluh, 2 guru di SMA Negeri 3 Tanah Putih. Perkembangan teknologi informasi dan komunikasi telah mendorong pemanfaatan internet dan jaringan sekolah sebagai komponen penting dalam mendukung proses pembelajaran dan pengelolaan administrasi di SMA Negeri 3 Tanah Putih. Penerapan konsep Smart School Network menjadi langkah strategis dalam menciptakan lingkungan sekolah yang modern dan berbasis digital. Namun, meningkatnya penggunaan jaringan internet juga menimbulkan berbagai permasalahan, terutama terkait keamanan Wi-Fi, perlindungan privasi data warga sekolah, serta ancaman kejahatan siber seperti phishing. Kurangnya pengelolaan jaringan dan literasi digital berpotensi menyebabkan gangguan stabilitas jaringan, kebocoran data, dan penyalahgunaan informasi. Berdasarkan hasil kegiatan sosialisasi dan sesi tanya jawab dengan peserta selama kegiatan berlangsung, PkM ini menghasilkan beberapa capaian yaitu meningkatkan kesadaran dan pemahaman siswa sekolah terhadap penggunaan internet yang sehat, aman, dan bertanggung jawab, sehingga diharapkan dapat mendukung terciptanya lingkungan digital sekolah yang aman serta meningkatkan kualitas pembelajaran dan literasi digital.*

**Kata kunci :** Smart School Network, Internet, Keamana Wi-fi, Phishing, Privasi data

### PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah memberikan dampak besar terhadap dunia pendidikan, termasuk di SMA Negeri 3 Tanah Putih. Pemanfaatan internet dan jaringan sekolah saat ini menjadi kebutuhan utama dalam mendukung proses pembelajaran, pengelolaan administrasi, serta akses informasi bagi guru dan peserta didik (Azizah, 2023) . Seiring dengan hal tersebut, penerapan konsep Smart School Network menjadi langkah strategis untuk menciptakan lingkungan sekolah yang modern, efektif, dan berbasis teknologi digital (Irfan, 2025). Namun, meningkatnya penggunaan jaringan internet di lingkungan SMA Negeri 3 Tanah Putih juga menimbulkan berbagai tantangan, khususnya dalam aspek keamanan Wi-Fi sekolah. Jaringan yang belum dikelola secara optimal berpotensi disalahgunakan, baik oleh pihak internal maupun eksternal, sehingga dapat mengganggu stabilitas jaringan, memperlambat akses pembelajaran digital, bahkan membuka peluang terjadinya pencurian data (Helmiawan dkk, 2025).

Selain itu, privasi data warga sekolah menjadi hal yang sangat penting untuk diperhatikan. Data pribadi siswa, guru, dan tenaga kependidikan seperti identitas, akun

pembelajaran, serta data akademik harus dilindungi dengan baik (Bate & Prasetyo, 2025). Kurangnya pemahaman mengenai keamanan data digital dapat menyebabkan kebocoran informasi yang berisiko menimbulkan penyalahgunaan dan merugikan pihak sekolah maupun individu (Erikha & Hoesein, 2025).

Ancaman lain yang semakin sering terjadi adalah phishing, yaitu bentuk penipuan digital melalui pesan, email, atau tautan palsu yang bertujuan mencuri data akun dan informasi penting (Sahfitri & Rosmalinda, 2024). Peserta didik dan pendidik yang belum memiliki literasi digital yang memadai rentan menjadi korban phishing, sehingga berpotensi mengganggu aktivitas pembelajaran dan keamanan sistem sekolah (Pohan et al., 2023).

Berdasarkan permasalahan tersebut, kegiatan Pengabdian kepada Masyarakat dengan tema “Smart School Network, Internet Sehat Dan Aman”: Keamanan Wi-Fi, Privasi Data, Dan Pencegahan Phishing” dilaksanakan di SMA Negeri 3 Tanah Putih sebagai upaya edukatif untuk meningkatkan pemahaman dan kesadaran warga sekolah mengenai keamanan Wi-Fi, perlindungan privasi data, serta pencegahan phishing. Melalui kegiatan ini diharapkan tercipta lingkungan digital sekolah yang aman, bijak, dan bertanggung jawab, serta mendukung peningkatan kualitas pendidikan dan literasi digital di SMA Negeri 3 Tanah Putih.

#### **METODE KEGIATAN**

Metode sosialisasi dalam PkM ini dilaksanakan melalui beberapa tahapan sebagai berikut:



Gambar 1. Metode Kegiatan

#### **Tahap Perencanaan**

Persiapan Pada tahap awal, tim pelaksana melakukan serangkaian persiapan yang mencakup:

1. Koordinasi dengan Pihak Sekolah – Berkomunikasi dengan pihak SMA Negeri 3 Tanah Putih yang menjadi target program terkait waktu, tempat dan sasaran kegiatan.
2. Identifikasi Kebutuhan – Melakukan kajian mendalam tentang permasalahan yang dihadapi siswa terkait penggunaan internet dan kemaanan digital.
3. Pembuatan Media Pembelajaran – Mengembangkan slide presentasi, video edukasi, dan perangkat pendukung kegiatan.
4. Pengembangan Materi Sosialisasi – Menyusun materi edukasi yang meliputi smart School Network, keamanan Wi-fi, privasi data dan pencegahan Phising.

#### **Pelaksanaan Sosialisasi**

Sosialisasi dilaksanakan dalam beberapa sesi yang mencakup:

1. Sesi Pengenalan - Pemaparan mengenai pentingnya etika bermedia sosial, dampak jejak digital, serta peran sistem informasi dalam membentuk perilaku

digital yang bertanggung jawab.

2. Ceramah interaktif - Menyampaikan konsep dasar Smart School Network, internet sehat dan aman, serta risiko keamanan digital.
3. Diskusi dan tanya jawab - Menggali pengalaman peserta terkait penggunaan internet dan permasalahan yang pernah dihadapi.
4. Studi kasus - Contoh nyata khususnya terkait modus phishing dan pelanggaran privasi data yang sering terjadi.
5. Demonstrasi Aplikasi – Demonstrasi langsung menggunakan aplikasi pendeteksi phishing dengan cara melihat apakah link yang dipraktekan termasuk dalam kategori phishing.

### **Evaluasi dan Tindak Lanjut**

Setelah sosialisasi, evaluasi dilakukan untuk mengukur efektivitas kegiatan dengan metode berikut:

1. Diskusi bersama guru dan siswa – Membahas dampak program terhadap perilaku siswa yang menunjukkan sikap lebih waspada terhadap pesan, tautan dan email yang mencurigakan.
2. Penyusunan laporan akhir – Merangkum hasil kegiatan sosialisasi yang sesuai dengan rencana dan diikuti oleh sasaran yang ditentukan serta rekomendasi untuk implementasi lanjutan.

### **HASIL DAN PEMBAHASAN**

Kegiatan PkM Dosen Prodi Sistem informasi dan Prodi Teknologi Informasi dikemas dalam bentuk sosialisasi. Metode yang diaplikasikan kepada siswa selama sosialisasi adalah pemaparan dari tim, demo aplikasi dan tanya jawab antara pemateri dengan siswa (Baiq et al., 2024) . Setiap pemateri menyampaikan materi terkait dengan bidang keahliannya. Kegiatan diawali dengan perkenalan dan penyampaian tujuan kegiatan sosialisasi kepada siswa (Fauziah, Selvanda et al., 2025).

Pemateri pertama memberikan sosialisasi kepada siswa terkait keamanan Wi-Fi memberikan pemahaman kepada siswa mengenai pentingnya penggunaan jaringan sekolah secara bijak dan aman, serta risiko yang dapat timbul akibat akses tidak sah dan penyalahgunaan jaringan. Pada materi privasi data, siswa dibekali pengetahuan mengenai pentingnya menjaga kerahasiaan data pribadi dan akademik, seperti akun email, identitas digital, dan informasi pembelajaran (Mulawarman et al., 2026) . Selain itu, materi pencegahan phishing membantu siswa mengenali berbagai bentuk penipuan digital yang sering terjadi melalui email, media sosial, maupun tautan palsu serta cara mengenali ciri-ciri phishing agar siswa tidak menjadi korban kejahatan siber (Agung, 2025).

Seiring dengan meningkatnya pemanfaatan teknologi informasi dan internet dalam kegiatan pembelajaran, potensi risiko keamanan jaringan dan kebocoran data juga semakin besar (Fauziah et al., 2025). Oleh karena itu, edukasi mengenai *Smart School Network* menjadi langkah penting dalam membangun pemahaman bahwa pemanfaatan teknologi di sekolah harus diimbangi dengan pengelolaan keamanan yang baik. (Meiditra et al., 2025)

Peningkatan pemahaman siswa mengenai keamanan Wi-Fi sekolah diharapkan dapat mendorong penggunaan jaringan internet secara lebih bertanggung jawab dan mengurangi risiko penyalahgunaan jaringan (N & Bisma, 2023). Kesadaran akan pentingnya perlindungan privasi data juga menjadi aspek krusial dalam membentuk

perilaku digital yang aman, mengingat data pribadi dan akademik merupakan aset penting yang harus dijaga kerahasiaannya(Sutarli et al., 2023).

Selain itu, edukasi mengenai pencegahan phishing memberikan kontribusi signifikan dalam meningkatkan kewaspadaan siswa terhadap berbagai bentuk penipuan digital(Sutabri, 2023). Dengan mengenali ciri-ciri phishing, siswa diharapkan mampu menghindari tautan mencurigakan, pesan palsu, dan upaya pencurian data yang dapat merugikan individu maupun institusi sekolah.



Gambar. 1 Proses Penyampaian Materi

Selain materi mengenai konsep smart school network serta pemahaman mengenai keamanan jaringan, pada sosialisasi ini juga melakukan demonstrasi program aplikasi yang telah dikembangkan untuk membantu mendeteksi apakah suatu tautan terindikasi sebagai phishing atau tidak. Aplikasi ini dirancang sebagai alat bantu edukatif yang sederhana dan mudah digunakan oleh siswa, sehingga dapat meningkatkan pemahaman praktis mengenai upaya pencegahan kejahatan siber di lingkungan sekolah.

Pada sesi demonstrasi, pemateri memperlihatkan cara kerja aplikasi dengan memasukkan contoh tautan ke dalam sistem. Aplikasi kemudian melakukan proses pengecekan dan menampilkan hasil analisis berupa status keamanan tautan, apakah tergolong aman atau berpotensi phishing. Melalui demonstrasi ini, siswa dapat memahami bahwa tidak semua tautan yang diterima melalui pesan singkat, email, atau media sosial bersifat aman untuk diakses.

Demo aplikasi ini bertujuan untuk memberikan pengalaman langsung kepada siswa dalam mengenali ancaman phishing secara lebih konkret. Dengan melihat proses deteksi secara langsung, siswa diharapkan mampu meningkatkan kewaspadaan sebelum mengklik tautan yang mencurigakan serta lebih berhati-hati dalam membagikan informasi pribadi dan data akun.

Kegiatan PkM ini diakhiri dengan sesi diskusi serta tanya jawab oleh siswa kepada pemateri dan sebaliknya. Dalam sesi ini dapat dilihat bahwa siswa sangat antusias dalam mengikuti pemaparan materi sosialisasi mengenai phishing dan privasi data. siswa juga memberikan respon positif dan menunjukkan ketertarikan terhadap

penggunaan aplikasi tersebut dengan memberikan umpan balik berupa mencoba tautan yang di dapat langsung oleh siswa apakah terdeteksi phishing atau tautannya termasuk kategori aman. Kegiatan ini diharapkan dapat di praktikan oleh siswa, kegiatan ini diharapkan dapat meningkatkan keaktifan dan efektifitas dalam menggunakan internet di SMA N 3 Tanah Putih.



Gambar. 2 Proses Diskusi dan Tanya Jawab serta pemberian doorprize



Gambar. 3 sesi foto bersama

## KESIMPULAN

Dari kegiatan PkM tim Dosen Prodi Sistem informasi dan Prodi Teknologi Informasi Institut Teknologi Rokan Hilir kepada siswa SMK Al-Muhajirin dapat disimpulkan bahwa adanya Peningkatan pengetahuan dan pemahaman Siswa tentang pentingnya pentingnya keamanan jaringan Wi-Fi, perlindungan privasi data, serta cara mengenali dan mencegah serangan phishing. Implementasi konsep Smart School Network yang aman dapat mendukung terciptanya lingkungan sekolah digital yang produktif, aman, dan beretika.

## DAFTAR PUSTAKA

- Agung, H. (2025). Efektivitas Edukasi Cybersecurity dalam Meningkatkan Pengetahuan Siswa tentang Ancaman Digital pada Siswa Menengah Atas. *Jurnal Ilmu Komputer (JUIK)*, 5(2), 104. <https://doi.org/10.31314/juik.v5i2.4436>
- Azizah, P. N. (2023). *MENUNJANG MUTU PENDIDIKAN SEKOLAH Pendahuluan Perkembangan teknologi informasi di era globalisasi ini berkembang*. 8(1), 11–28.
- Baiq, Y. W., Alimuddin, N., Suranti, N. M. Y., & Rahmatih, A. N. (2024). Sosialisasi Model Pembelajaran Interaktif Bagi Calon Guru Sekolah Dasar Untuk Meningkatkan Pengetahuan Dan Keterampilan Siswa. *Jurnal Interaktif: Warta Pengabdian Pendidikan*, 4(1), 8–14. <https://doi.org/10.29303/interaktif.v4i1.138>
- Bate, A. P., & Prasetyo, K. (2025). Pengamanan Jejak Digital Jejak Digital: Pelatihan dan Edukasi Keamanan Data Pribadi bagi Siswa SMAN 1 Cimarga, Kabupaten Lebak, Provinsi Banten. *Jurnal Abdi Masyarakat Indonesia*, 5(5), 2033–2042. <https://doi.org/10.54082/jamsi.2055>
- Erikha, A., & Hoesein, Z. A. (2025). *Strategi Pencegahan Kebocoran Data Pribadi melalui Peran Kominfo dan Gerakan Siberkreasi dalam Edukasi Digital*. 07, 48–64.
- Fauziah, Selvanda, A. R., Mutia, C., Ramadhani, F., Yuda, F., Meiditra, I., & Rasyid, M. (2025). *STRATEGI MANAJEMEN SUMBER DAYA MANUSIA DIGITAL*. 3(3), 639–646.
- Fauziah, Mutia, C., Meiditra, I., Yuda, F., & Rahmansyah, R. (2025). *Analysis of Teaching Material Delivery Techniques by Lecturers Based on E-Learning at Universitas Pembangunan Panca Budi Medan*. 05. <https://pubs.ascee.org/index.php/iota/article/view/908>
- Helmiawan, M. A. Y. H. A. F. M. (2025). *Keamanan Teknologi Informasi: Teori, Risiko, dan Strategi Pertahanan di Era Digital*. PT Penerbit Naga Pustaka.
- Irfan. (2025). *Pemanfaatan Teknologi Digital Dalam Manajemen Pendidikan Untuk Meningkatkan Kualitas Pembelajaran*. 2(1), 19–24.
- Meiditra, I., Fauziah, Mutia, C., & Yuda, F. (2025). *DESIGN OF A HOTSPOT NETWORK WITH A PREPAID SYSTEM USING MIKROTIK AT REDZ GAMING INTERNET CAFE*. 2(1), 104–116. <https://journal.ppmi.web.id/index.php/jdaics/article/view/1866/1236>
- Mulawarman, U., Mulawarman, U., Mulawarman, U., Mulawarman, U., Mulawarman, U., & Mulawarman, U. (2026). *EVALUASI KEAMANAN DAN MANAJEMEN DATA PADA SISTEM INFORMASI SEKOLAH DI ERA TRANSFORMASI DIGITAL*. 8.
- N, M. H., & Bisma, R. (2023). *Persepsi Keamanan Data Dan Privasi Pada Pengguna Layanan Wifi Gratis Di Coffee Shop*. 04(02), 164–172.
- Pohan, S., Mardivta, H., & Damanik, R. S. (2023). *PROGRAM SOSIALISASI KEAMANAN EMAIL AKADEMIK MAHASISWA TERHADAP ANCAMAN PHISHING BERBASIS SOCIAL ENGINEERING*. 1(November).
- Sahfitri, A., & Rosmalinda, R. (2024). Penipuan Digital Melalui Tautan Phishing. *Jurnal Dialektika Hukum*, 6(2), 92–107. <https://doi.org/10.36859/jdh.v6i2.2881>
- Sutabri, T. (2023). *Analisis kejahatan online phising pada institusi pemerintah / pendidik sehari-hari*. 06(01), 29–34.
- Sutarli, A. F., Hukum, F., & Maranatha, U. K. (2023). *Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi dalam Menanggulangi Phising di Indonesia*. 3, 4208–4221.