Jurnal Pengabdian Masyarakat Permata Indonesia (JPMI)
Volume 6, Nomor 1, April 2026, Hal 1-6
P- ISSN 2808 - 7828
E- ISSN 2985 - 377X

Pelatihan Pembuatan Password yang Kuat, Pengenalan Bahaya Phishing dan Prinsip Perlindungan Data Pribadi

Strong Password Creation Training, Introduction to the Dangers of Phishing and Principles of Personal Data Protection

Ahmad Yani Noor[1], Azis Wahyudi[2*], Anas Rahmad Hidayat[2]

[1]Diploma Tiga Administrasi Rumah Sakit, Politeknik Kesehatan Permata Indonesia Yogyakarta
email: noorberbagi@gmail.com
[2]Diploma Tiga Rekam Medis dan Informasi Kesehatan, Politeknik Kesehatan Permata Indonesia Yogyakarta
email: azis@permataindonesia.ac.id, anasrh@permataindonesia.ac.id

Abstrak

Peningkatan pemanfaatan layanan digital di perguruan tinggi dan fasilitas pelayanan kesehatan diikuti oleh kenaikan risiko keamanan siber, terutama serangan *phishing* dan kebocoran data pribadi. Berbagai insiden menunjukkan bahwa faktor manusia masih menjadi titik lemah dominan, sehingga literasi keamanan digital perlu diperkuat melalui intervensi edukatif yang terukur. Kegiatan pengabdian kepada masyarakat ini bertujuan meningkatkan pengetahuan dan kesadaran peserta mengenai (1) karakteristik dan modus *phishing*, (2) praktik penyusunan kata sandi yang kuat (*strong password*) dan *password hygiene*, serta (3) prinsip-prinsip perlindungan data pribadi, khususnya data kesehatan. Kegiatan dilaksanakan daring melalui Zoom pada 14 Maret 2026 selama 3 jam dan diikuti 47 peserta (mahasiswa, dosen, dan praktisi) dari RSKIA Sadewa, RS DKT Dr. Soetarto, dan RSUD Saras Adhyatma Bantul. Metode pelaksanaan meliputi ceramah interaktif, studi kasus dan simulasi, diskusi, serta evaluasi berbasis *pre-test* dan *post-test* menggunakan Google Form. Hasil menunjukkan peningkatan persentase jawaban benar pada indikator pengenalan jenis *phishing* (32% menjadi 88%) dan identifikasi ciri pesan/email *phishing* (28% menjadi 85%). Pemahaman prinsip perlindungan data pribadi meningkat (45% menjadi 80%), serta kemampuan menerapkan praktik keamanan digital sederhana meningkat (41% menjadi 89%). Program ini efektif meningkatkan literasi keamanan digital lintas kelompok peserta dan relevan untuk direplikasi sebagai upaya pencegahan risiko kebocoran data dan penyalahgunaan akun pada lingkungan akademik dan layanan kesehatan

Kata kunci: keamanan siber; phishing; kata sandi kuat; perlindungan data pribadi; pengabdian kepada masyarakat.

Abstract

The increased use of digital services in higher education and healthcare facilities is accompanied by a growing risk of cybersecurity incidents, particularly phishing attacks and personal data leaks. Evidence from multiple incidents suggests that human factors remain a major vulnerability; therefore, digital security literacy should be strengthened through measurable educational interventions. This community service program aimed to improve participants' knowledge and awareness of (1) phishing characteristics and tactics, (2) strong password practices and password hygiene, and (3) personal data protection principles, especially for health data. The online training was conducted via Zoom on March 14, 2026 (3 hours) with 47 participants (students, lecturers, and practitioners) from RSKIA Sadewa, RS DKT Dr. Soetarto, and RSUD Saras Adhyatma Bantul. The program used interactive lectures, case-based simulations, discussion, and pre–post evaluation using Google Forms. Results showed increased correct responses for phishing type recognition (32% to 88%) and phishing message/email identification (28% to 85%). Understanding of personal data protection principles improved (45% to 80%), as did the ability to apply basic digital security practices (41% to 89%). The program effectively improved cybersecurity literacy across participant

P- ISSN 2808 - 7828
E- ISSN 2985 - 377X

groups and is feasible to replicate to mitigate risks of data leakage and account compromise in academic and healthcare contexts.

***Keywords**: cybersecurity; phishing; strong password; personal data protection; community service.*

P- ISSN 2808 - 7828
E- ISSN 2985 - 377X

PENDAHULUAN

Transformasi digital di lingkungan pendidikan tinggi dan fasilitas pelayanan kesehatan telah meningkatkan efisiensi operasional secara signifikan. Namun, perkembangan teknologi digital yang pesat ini juga diiringi dengan meningkatnya risiko terhadap keamanan siber, terutama dalam bentuk serangan phishing dan kebocoran data pribadi (Lubis et al., 2025). Masalah utama yang sering dihadapi adalah serangan phishing yang mengeksploitasi kelemahan kognitif manusia dan rendahnya praktik pengelolaan kata sandi atau password hygiene.

Faktor manusia seringkali menjadi titik lemah utama (the weakest link) dalam insiden pelanggaran data (Juandana & Setiyoningsih, 2025). Kurangnya literasi digital masyarakat, khususnya dalam hal keamanan informasi, menjadi celah yang sering dimanfaatkan oleh pelaku kejahatan siber melalui teknik manipulasi psikologis (Lubis et al., 2025). Serangan phishing bertujuan menipu pengguna agar mengungkapkan informasi sensitif seperti kredensial login atau data pribadi yang dapat berujung pada kerugian finansial maupun reputasi.

Bagi praktisi medis di rumah sakit, kerentanan ini sangat berisiko terhadap keamanan data pasien. Celah dalam pengelolaan kata sandi—seperti penggunaan kata sandi yang lemah atau penggunaan ulang kata sandi di berbagai platform—sering dimanfaatkan untuk meretas sistem informasi kesehatan (Juandana & Setiyoningsih, 2025). Oleh karena itu, penguatan literasi keamanan digital bagi civitas akademika dan praktisi kesehatan melalui pengenalan ancaman siber dan prinsip perlindungan data pribadi merupakan kebutuhan strategis yang mendesak.

METODE PELAKSANAAN

Kegiatan pengabdian ini dilaksanakan secara daring menggunakan platform Zoom Meeting pada tanggal 14 Maret 2026. Peserta Kegiatan dihadiri oleh 47 peserta yang terdiri dari mahasiswa, dosen, Praktisi dari Rumah Sakit Sadewa, Rumah Sakit DKT Soetarto, dan RSUD Saras Adhyatma Bantul. Metode yang digunakan adalah pendekatan edukatif berbasis ceramah interaktif, pemaparan studi kasus dan simulasi (Lubis et al., 2025).

Pelaksanaan PkM dibagi ke dalam dua sesi materi utama yang dipandu oleh Densya Tri, mahasiswi program studi D3 Administrasi Rumah Sakit. Materi ke-1 tentang Prinsip Perlindungan Data Pribadi disampaikan oleh Ahmad Yani Noor, M.H.Kes., yang

P- ISSN 2808 - 7828
E- ISSN 2985 - 377X

memfokuskan pada aspek hukum perlindungan data, khususnya data kesehatan. Materi 2 disampaikan oleh Azis Wahyudi S.T., M.Kom., yang memberikan pelatihan praktis mengenai teknik identifikasi pesan phishing dan langkah-langkah menyusun kata sandi yang kuat. Kegiatan dilaksanakan pukul 10.00 hingga 13.00 WIB melalui zoom meeting.

Evaluasi hasil dilakukan melalui observasi partisipatif dan metode pre-test serta post-test kepada 47 peserta melalui google form untuk mengukur daya tangkap dan pemahaman peserta terhadap materi yang disampaikan (Juandana & Setiyoningsih, 2025).

HASIL DAN PEMBAHASAN

A. HASIL

Pelaksanaan pelatihan berjalan lancar dengan tingkat keterlibatan peserta yang aktif. Pengukuran pemahaman dilakukan melalui kuesioner pre-test dan post-test yang diisi oleh seluruh 47 peserta. Hasil evaluasi menunjukkan adanya peningkatan pengetahuan yang signifikan pada berbagai indikator materi.

Berdasarkan data yang dihimpun, terdapat perbaikan pemahaman peserta secara drastis setelah mengikuti sesi pelatihan:

Tabel 1. Tabel Pre-Test dan Post-Test

No	Indikator Pemahaman	Persentase Pre-test (%)	Persentase Post-test (%)	Keterangan
1	Mengenali jenis-jenis *phishing*	32%	88%	Peningkatan signifikan
2	Mengetahui ciri-ciri email/pesan *phishing*	28%	85%	Peningkatan signifikan
3	Memahami prinsip perlindungan data pribadi	45%	80%	Peningkatan baik
4	Mampu menerapkan praktik keamanan digital sederhana	41%	89%	Meningkat secara signifikan

Berdasarkan Tabel 1, terdapat peningkatan sebesar 56% pada indikator pengenalan jenis phising, pada indikator identifikasi ciri-ciri email/pesan phishing meningkat sebesar 57%, pada indikator prinsip perlindungan data pribadi meningkat 35%, dan indikator praktik keamanan digital sederhana (termasuk pembuatan password yang kuat meningkat 48%.

Gambar 1. Pembukaan oleh Densya Tri melalui zoom meeting

P- ISSN 2808 - 7828
E- ISSN 2985 - 377X

Gambar 2. Pemaparan materi oleh Narasumber 2 Azis Wahyudi S.T., M.Kom.

Gambar 3. Foto Narasumber 1 Ahmad Yani Noor M.H.Kes dan Narasumber 2 Azis Wahyudi S.T., M.Kom. pada saat sesi diskusi

B. PEMBAHASAN

Melalui simulasi identifikasi, peserta menjadi lebih peka terhadap ciri-ciri serangan phishing, seperti permintaan data mendesak atau tautan yang mencurigakan. Hal ini sejalan dengan temuan bahwa edukasi yang terarah dengan metode evaluasi pre-test dan post-test efektif dalam mengukur perubahan kognitif peserta dalam menghadapi rekayasa sosial.

Selain itu, pemahaman mengenai password meningkat, di mana peserta memahami pentingnya penggunaan kombinasi karakter yang kompleks untuk mempersulit upaya peretasan. Bagi praktisi rumah sakit, materi mengenai prinsip perlindungan data pribadi memberikan pemahaman mengenai batasan legal dan etis dalam mengelola rekam medis elektronik. Penguatan literasi ini diharapkan dapat membentuk budaya digital yang aman di lingkungan kerja masing-masing. Kesadaran untuk menjaga kerahasiaan kredensial akses sistem informasi rumah sakit menjadi poin krusial yang berhasil ditekankan dalam diskusi.

KESIMPULAN

Kegiatan ini berhasil meningkatkan pemahaman dan keterampilan 47 peserta mengenai keamanan siber dan langkah-langkah preventif yang diperlukan. Evaluasi melalui *pre-test* dan *post-test* membuktikan bahwa terdapat peningkatan pemahaman prinsip keamanan data dan praktik pembuatan password yang kuat.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Mahasiswa Program Studi D3 Administrasi Rumah Sakit dan

P- ISSN 2808 - 7828
E- ISSN 2985 - 377X

HIMARS.
2. Poltekkes Permata Indonesia Yogyakarta yang telah mendukung pelaksanaan kegiatan pengabdian masyarakat ini.
3. Seluruh peserta kegiatan dari berbagai elemen masyarakat yang telah berpartisipasi dengan antusias.
4. Semua pihak yang tidak dapat disebutkan satu persatu yang telah berkontribusi dalam kesuksesan kegiatan ini.

DAFTAR PUSTAKA

Juandana Kawuladini Putra, & Lilis Setiyoningsih. (2025). Pelatihan Literasi Keamanan Digital (Anti-Phishing & Password Hygiene) Bagi Civitas Akademika. EDUSCOTECH: Scientific Journal of Education, Economics, and Engineering, 6(2), Juli 2025. ISSN: 2716-0653.

Lubis, H., Awaludin, D. T., Sari, D. P., Milasari, L. A., & Sofyan. (2025). Edukasi Keamanan Siber: Pelatihan Dasar Mengenali Phishing dan Proteksi Data Pribadi di Dunia Digital. JIPITI: Jurnal Pengabdian kepada Masyarakat, 2(2), 101-105. ISSN: 3063-573X.

Prasepta, F., & Surbakti, S. (2024). Edukasi Keamanan Siber Berdigital dengan Aman. Prima Abdika: Jurnal Pengabdian Masyarakat, 4(4), 868-878. https://doi.org/10.37478/abdika.v4i4.4967

Putra, J. L., Raharjo, M., & Fitri, E. (2024). Analisis Ancaman Siber dan Persiapan Pemuda Karang Taruna Kelurahan Rengas dalam Menghadapi Risiko Keamanan Siber. Indonesian Journal for Social Responsibility, 6(2), 151-163. https://doi.org/10.36782/ijsr.v6i02.258

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2002). The affect heuristic. In T. Gilovich, D. Griffin, & D. Kahneman (Eds.), Heuristics and Biases: The Psychology of Intuitive Judgment (pp. 397-420). Cambridge University Press. https://doi.org/10.1017/CBO9780511808098.025

Sugiharto, B., Parulian, E., & Marwan, A. (2024). Pelatihan Penangkalan Peretasan Data Kegiatan UMKM untuk Meningkatkan Pertumbuhan Ekonomi di Kecamatan Medan Perjuangan Kota Medan. JIIP: Jurnal Ilmiah Ilmu Pendidikan, 7(8), 9347-9351. https://doi.org/10.54371/jiip.v7i8.5810