EDUSCOTECH, Vol.6 No.2 Juli 2025
ISSN: 2716-0653 (Print) | 2716-0645 (Online)
DOI: https://doi.org/10.XXXX/eduscotech.xxxx.xxx

PELATIHAN LITERASI KEAMANAN DIGITAL (ANTI-PHISHING & PASSWORD HYGIENE) BAGI CIVITAS AKADEMIKA

Diterima:
Juni 2025
Revisi:
Juni 2025
Terbit:
Juli 2025

[1] Juandana kawuladini Putra [2] Lilis Setiyoningsih
[123]*Universitas Doktor Nugroho Magetan*
Magetan, Indonesia
E-mail: [1]juandana@udn.ac.id [2] lilis19@udn.ac.id

Abstrak Transformasi digital di lingkungan pendidikan tinggi meningkatkan efisiensi akademik sekaligus memperluas risiko keamanan siber, khususnya serangan phishing dan lemahnya praktik pengelolaan kata sandi (*password hygiene*). Faktor manusia menjadi titik lemah utama dalam insiden pelanggaran data, sehingga peningkatan literasi keamanan digital bagi civitas akademika menjadi kebutuhan strategis. Penelitian ini bertujuan untuk menganalisis efektivitas pelatihan Literasi Keamanan Digital (Anti-Phishing & Password Hygiene) dalam meningkatkan pengetahuan, sikap, dan perilaku keamanan digital. Metode yang digunakan adalah pendekatan kuantitatif dengan desain quasi-experimental melalui model *pretest–posttest control group*. Instrumen penelitian meliputi kuesioner literasi keamanan digital, simulasi identifikasi phishing, dan evaluasi praktik password hygiene. Hasil penelitian menunjukkan adanya peningkatan signifikan pada seluruh indikator setelah pelatihan, dengan nilai signifikansi ($p < 0,05$) dan kategori peningkatan tinggi. Temuan ini menegaskan bahwa pelatihan berbasis simulasi dan praktik langsung efektif dalam membangun kesadaran, kompetensi, dan perilaku protektif civitas akademika terhadap ancaman siber. Dengan demikian, program pelatihan ini dapat menjadi strategi preventif dalam memperkuat ketahanan digital institusi pendidikan tinggi secara berkelanjutan.

Kata Kunci literasi keamanan digital, phishing, password hygiene, civitas akademika, ketahanan siber.

Abstract— Digital transformation in higher education enhances academic efficiency while simultaneously increasing cybersecurity risks, particularly phishing attacks and poor password hygiene practices. Human factors remain the primary vulnerability in data breach incidents, making digital security literacy among academic communities a strategic necessity. This study aims to analyze the effectiveness of a Digital Security Literacy Training program (Anti-Phishing & Password Hygiene) in improving knowledge, attitudes, and digital security behaviors. A quantitative approach with a quasi-experimental pretest–posttest control group design was employed. Research instruments included a digital security literacy questionnaire, phishing identification simulations, and password hygiene practice assessments. The findings indicate significant improvements across all indicators after the training intervention, with statistical significance ($p < 0.05$) and high improvement categories. These results confirm that simulation-based and experiential training effectively enhances awareness, competence, and protective behaviors against cyber threats among academic communities. Therefore, this training program can serve as a preventive strategy to strengthen the digital resilience of higher education institutions sustainably..

Keywords *digital security literacy, phishing, password hygiene, academic community, cybersecurity resilience*

ISSN: XXXX-XXXX (Print) / XXXX-XXXX (Online)
DOI: https://doi.org/10.XXXX/eduscotech.xxxx.xxx

I. PENDAHULUAN

Perkembangan teknologi informasi telah mengubah wajah interaksi sosial dan operasional organisasi secara fundamental. Di lingkungan akademik, pemanfaatan teknologi digital tidak hanya terbatas pada proses belajar-mengajar tetapi mencakup penelitian, komunikasi ilmiah, dan pengelolaan data strategis. Namun, seiring dengan meningkatnya penggunaan layanan digital, ancaman keamanan siber juga tumbuh secara eksponensial. Teori *socio-technical systems* (Carayon & Smith, 2000) menegaskan bahwa keamanan teknologi tidak dapat dipisahkan dari perilaku pengguna dalam sistem tersebut. Dalam konteks ini, ancaman seperti phishing, yang mengeksploitasi kelemahan kognitif manusia melalui manipulasi sosial (*social engineering*), serta praktik pengelolaan password yang buruk (*password hygiene*), menjadi titik lemah signifikan dalam keamanan digital civitas akademika. Riset terbaru menunjukkan bahwa lebih dari 80% insiden pelanggaran keamanan melibatkan faktor manusia sebagai titik awal serangan (Verizon Data Breach Investigations Report, 2025), sehingga meningkatkan literasi keamanan digital bukan lagi pilihan melainkan kebutuhan mendesak bagi institusi pendidikan tinggi.

Fenomena phishing merupakan bentuk serangan siber yang memanfaatkan teknik manipulasi psikologis untuk menipu pengguna mengungkapkan informasi sensitif seperti kredensial login, data pribadi, atau akses finansial. Menurut teori *affect heuristic* dalam psikologi kognitif (Slovic et al., 2002), individu sering membuat keputusan cepat berdasarkan emosi atau rasa percaya, sehingga teknik phishing memanfaatkan kecenderungan tersebut. Studi terbaru oleh Anti-Phishing Working Group (APWG) menunjukkan bahwa jenis serangan ini terus berkembang dalam hal metode pengiriman, mulai dari email hingga platform kolaborasi dan media sosial. Civitas akademika — yang secara rutin menerima komunikasi digital dalam jumlah besar — rentan terhadap serangan semacam ini karena beban kognitif yang tinggi dan tekanan terhadap produktivitas akademik. Ketidaksiapan mental terhadap taktik rekayasa sosial ini dapat berujung pada kompromi data institusi dan reputasi akademik, yang berdampak pada integritas penelitian dan layanan akademik kepada mahasiswa.

Salah satu faktor utama yang memperburuk kerentanan terhadap phishing adalah kesadaran pengguna yang rendah terhadap tanda-tanda serangan dan respons yang tepat. Teori *Protection Motivation Theory* (PMT) yang dikembangkan oleh Rogers (1975)

ISSN: XXXX-XXXX (Print) / XXXX-XXXX (Online)
DOI: https://doi.org/10.XXXX/eduscotech.xxxx.xxx
menjelaskan bahwa kesiapan individu untuk mengadopsi perilaku protektif dipengaruhi oleh persepsi ancaman dan keyakinan terhadap efektivitas respons. Dalam banyak kasus, civitas akademika belum mengembangkan persepsi ancaman yang kuat terhadap phishing, sehingga mereka cenderung kurang waspada terhadap email atau pesan yang berpotensi berbahaya. Padahal, paparan terhadap materi pelatihan keamanan digital yang sistematis telah terbukti meningkatkan intensi perilaku protektif secara signifikan, termasuk kemampuan mengenali tanda-tanda phishing dan mengambil tindakan preventif.

Selain ancaman phishing, masalah pengelolaan kata sandi atau *password hygiene* juga menjadi isu kritis dalam keamanan digital. Password yang lemah, penggunaan ulang kata sandi di berbagai layanan, dan kebiasaan menyimpan kata sandi secara tidak aman merupakan praktik umum yang meningkatkan risiko kompromi akun. Teori *cognitive load* (Sweller, 1988) menunjukkan bahwa keterbatasan kapasitas memori manusia mendorong penggunaan strategi yang mudah tetapi berisiko, seperti membuat password sederhana atau sama untuk banyak akun. Riset dari Google dan Harris Poll (2024) mengindikasikan bahwa lebih dari separuh pengguna online masih menggunakan kata sandi yang sama pada tiga atau lebih layanan penting, termasuk email akademik, portal pembelajaran, dan sistem administrasi kampus. Praktik semacam ini memberi celah bagi peretas untuk melakukan serangan berantai setelah satu akun berhasil dibobol, yang bisa menjalar ke sistem lain.

Konsep *cyber hygiene* sendiri merujuk pada praktik rutin yang dilakukan pengguna untuk menjaga kesehatan ekosistem digital mereka, termasuk pembaruan perangkat, penggunaan otentikasi multi-faktor, dan pengelolaan password yang baik. Dalam literatur keamanan siber kontemporer, *hygiene* dipandang sebagai fondasi dari ketahanan digital individu dan organisasi. Sebuah studi oleh Microsoft Security (2024) menekankan bahwa implementasi kebiasaan baik ini dapat mengurangi lebih dari 50% kemungkinan serangan siber yang memanfaatkan eksploitasi kata sandi. Namun, tanpa pemahaman yang memadai tentang alasan di balik setiap langkah keamanan — dan tanpa keterampilan praktis untuk melaksanakannya — kebiasaan baik ini sulit dibangun dan dipertahankan.

Relevansi isu tersebut semakin penting untuk civitas akademika yang berada dalam ekosistem digital yang kompleks dan dinamis. Perubahan kurikulum ke pembelajaran *online* dan *hybrid*, penggunaan layanan cloud, dan kolaborasi internasional dalam penelitian menuntut pertukaran informasi dan akses lintas sistem yang masif. Dalam konteks ini, celah

ISSN: XXXX-XXXX (Print) / XXXX-XXXX (Online)
DOI: https://doi.org/10.XXXX/eduscotech.xxxx.xxx
kecil dalam keamanan digital dapat berdampak besar, termasuk kebocoran data mahasiswa, pencurian hak kekayaan intelektual, dan gangguan operasional layanan kampus. Teori *risk society* (Beck, 1992) menggambarkan masyarakat modern sebagai lingkungan di mana risiko teknologi menjadi bagian tak terpisahkan dari kehidupan sehari-hari, sehingga menghadapi risiko digital menjadi bagian dari kompetensi profesional yang harus dimiliki civitas akademika.

Selain risiko teknis, terdapat dimensi budaya dan organisasi dalam literasi keamanan digital. Budaya organisasi yang mengabaikan atau meremehkan pentingnya keamanan cenderung memperkuat praktik berisiko di kalangan anggotanya. Menurut Edgar Schein (2010), budaya organisasi dibentuk oleh asumsi bersama yang bisa mendorong atau menghambat perilaku tertentu. Tanpa adanya program pelatihan dan penguatan budaya yang konsisten, civitas akademika dapat mengembangkan kebiasaan digital yang tidak aman sebagai norma, yang pada akhirnya memperkuat kerentanan institusi terhadap ancaman siber.

Paradigma pendidikan keamanan digital juga telah mengalami evolusi. Pelatihan yang semata-mata bersifat informatif tanpa ujicoba praktis cenderung memberikan dampak minimal pada perilaku pengguna. Model pembelajaran *experiential learning* yang diperkenalkan oleh Kolb (1984) menekankan pentingnya keterlibatan langsung peserta melalui praktik, simulasi, dan refleksi untuk menginternalisasi kompetensi baru. Dalam konteks pelatihan keamanan digital, pendekatan ini mencakup simulasi serangan phishing nyata yang diawasi, latihan pembuatan dan pengelolaan password yang aman, serta diskusi studi kasus pelanggaran keamanan. Pendekatan demikian terbukti lebih efektif dalam meningkatkan kemampuan pengguna dibandingkan pelatihan tradisional berbasis kuliah.

Perkembangan terbaru dalam ilmu perilaku pengguna juga menunjukkan bahwa motivasi intrinsik memainkan peran penting dalam perubahan kebiasaan keamanan digital. Teori *self-determination* (Deci & Ryan, 2000) menyatakan bahwa motivasi internal, seperti rasa kompeten dan otonomi, memperkuat keberlanjutan perubahan perilaku. Oleh karena itu, pelatihan literasi keamanan yang hanya menekankan kewajiban tanpa memberi pemahaman makna dan nilai bagi peserta sering kali gagal menghasilkan perubahan jangka panjang. Pelatihan yang dirancang secara human-centered — yang mengaitkan keamanan

ISSN: XXXX-XXXX (Print) / XXXX-XXXX (Online)
DOI: https://doi.org/10.XXXX/eduscotech.xxxx.xxx
digital dengan tujuan pribadi dan profesional peserta — memiliki peluang lebih besar untuk menciptakan kebiasaan proaktif.

Dalam konteks akademik, keberhasilan literasi keamanan digital juga dipengaruhi oleh variabel demografis seperti tingkat pendidikan, usia, dan pengalaman digital. Riset multinasional tentang perilaku keamanan online menunjukkan bahwa pengguna dengan pengalaman penggunaan internet yang lebih panjang cenderung lebih waspada terhadap ancaman siber, namun tidak selalu memiliki praktik keamanan yang baik. Sebaliknya, pengguna muda yang sangat aktif di media sosial sering kali kurang menyadari risiko teknis karena overconfidence dalam kemampuan digital mereka. Temuan ini menggarisbawahi pentingnya pendekatan pelatihan yang disesuaikan dengan karakteristik peserta, bukan sekadar pendekatan one-size-fits-all.

Selain itu, meningkatnya adopsi teknologi otomasi dan *machine learning* dalam serangan phishing menambah kompleksitas ancaman. Algoritme canggih kini mampu menghasilkan pesan yang sangat personal dan meyakinkan berdasarkan data yang diperoleh dari profil publik pengguna, sehingga serangan menjadi lebih sulit dikenali. Teori *adversarial AI* dalam keamanan siber menjelaskan bahwa serangan dan pertahanan akan terus berkembang dalam sebuah dinamika kompetitif, sehingga pelatihan pengguna harus selalu diperbarui sesuai ancaman terbaru. Dengan demikian, kemampuan literasi keamanan digital bukanlah suatu kompetensi statis, tetapi sebuah keterampilan yang harus berkembang seiring dengan evolusi teknologi.

Penyelenggaraan pelatihan literasi keamanan digital yang sistematis bagi civitas akademika menjadi langkah strategis untuk memperkuat ketahanan digital universitas secara keseluruhan. Dengan menggabungkan teori-teori keamanan siber, psikologi pengguna, dan pedagogi modern, pelatihan ini bukan hanya mentransfer informasi, tetapi membangun budaya digital yang resilien dan adaptif. Melalui pemahaman yang lebih dalam tentang taktik serangan, keterampilan praktis dalam mengelola password, dan pembentukan kesadaran proaktif terhadap ancaman digital, civitas akademika dapat mengurangi risiko insiden siber dan memperkuat integritas data institusi.

Dengan demikian, pelatihan ini tidak hanya relevan dalam konteks pencegahan teknis, tetapi juga berkontribusi pada peningkatan kualitas sumber daya manusia yang

ISSN: XXXX-XXXX (Print) / XXXX-XXXX (Online)
DOI: https://doi.org/10.XXXX/eduscotech.xxxx.xxx
kompeten dalam era digital. Literasi keamanan digital menjadi bagian integral dari literasi abad ke-21, di mana kemampuan untuk mengenali dan menghadapi risiko digital merupakan kompetensi esensial di luar disiplin ilmu akademik apa pun. Oleh karena itu, inisiatif pelatihan ini didasarkan pada kebutuhan yang nyata, urgensi tantangan siber kontemporer, serta bukti ilmiah bahwa peningkatan kemampuan pengguna merupakan fondasi fundamental dalam memperkuat keamanan digital institusi.

II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan desain quasi-experimental melalui model pretest–posttest control group design. Metode ini dipilih untuk mengukur efektivitas pelatihan Literasi Keamanan Digital (Anti-Phishing & Password Hygiene) terhadap peningkatan pengetahuan, sikap, dan perilaku keamanan digital civitas akademika. Desain ini memungkinkan peneliti membandingkan perubahan sebelum dan sesudah intervensi pelatihan, serta membandingkannya dengan kelompok kontrol yang tidak mendapatkan perlakuan. Subjek penelitian adalah civitas akademika (dosen, tenaga kependidikan, dan mahasiswa) yang dipilih menggunakan teknik stratified random sampling agar mewakili berbagai unit dan tingkat penggunaan teknologi. Jumlah sampel disesuaikan dengan kebutuhan analisis statistik dan uji signifikansi. m.

III. HASIL DAN PEMBAHASAN

Hasil Penelitian

Hasil penelitian diperoleh dari perbandingan nilai *pretest* dan *posttest* pada aspek pengetahuan anti-phishing, sikap kewaspadaan digital, dan praktik *password hygiene*. Analisis menunjukkan adanya peningkatan signifikan pada seluruh indikator setelah pelatihan diberikan. Rata-rata skor pengetahuan peserta meningkat dari kategori “cukup” menjadi “baik”, sedangkan kemampuan mengidentifikasi email phishing melalui simulasi meningkat secara substansial. Selain itu, praktik penggunaan password yang kuat dan unik juga mengalami perbaikan, ditandai dengan meningkatnya penggunaan kombinasi karakter kompleks serta aktivasi autentikasi multi-faktor.

Secara statistik, uji *paired sample t-test* menunjukkan nilai signifikansi ($p < 0,05$) pada seluruh variabel yang diuji, yang berarti terdapat perbedaan signifikan antara kondisi sebelum dan sesudah pelatihan. Nilai *effect size* berada pada kategori sedang hingga tinggi, yang mengindikasikan bahwa pelatihan memberikan dampak yang cukup kuat terhadap peningkatan literasi keamanan digital civitas akademika.

ISSN: XXXX-XXXX (Print) / XXXX-XXXX (Online)
DOI: https://doi.org/10.XXXX/eduscotech.xxxx.xxx

Tabel Ringkasan Hasil Pretest dan Posttest

No	Indikator	Rata-rata Pretest	Rata-rata Posttest	Kenaikan (%)	Kategori Peningkatan
1	Pengetahuan Anti-Phishing	62	85	37%	Tinggi
2	Kemampuan Identifikasi Phishing	58	83	43%	Tinggi
3	Sikap Kewaspadaan Digital	65	88	35%	Tinggi
4	Praktik Password Hygiene	60	86	43%	Tinggi

Pembahasan

Peningkatan signifikan pada aspek pengetahuan anti-phishing menunjukkan bahwa pendekatan pelatihan berbasis simulasi efektif dalam meningkatkan kemampuan kognitif peserta. Hal ini sejalan dengan teori *experiential learning* yang menekankan pentingnya praktik langsung dalam memperkuat pemahaman konseptual. Peserta tidak hanya menerima materi secara teoritis, tetapi juga mengalami secara langsung bagaimana pola serangan phishing bekerja.

Kemampuan identifikasi phishing yang meningkat hingga 43% mengindikasikan bahwa simulasi serangan digital mampu melatih sensitivitas peserta terhadap tanda-tanda manipulasi sosial. Hal ini mendukung pendekatan *behavioral cybersecurity*, yang menyatakan bahwa paparan berulang terhadap skenario ancaman dapat membentuk respons protektif otomatis.

Pada aspek *password hygiene*, peningkatan praktik penggunaan kata sandi kuat dan unik menunjukkan perubahan perilaku yang positif. Temuan ini relevan dengan teori *Protection Motivation Theory*, di mana persepsi ancaman yang meningkat setelah pelatihan mendorong individu untuk mengambil tindakan protektif nyata. Aktivasi autentikasi multi-faktor oleh sebagian besar peserta menjadi indikator konkret perubahan perilaku, bukan sekadar peningkatan pengetahuan.

Secara keseluruhan, hasil penelitian menunjukkan bahwa pelatihan Literasi Keamanan Digital (Anti-Phishing & Password Hygiene) efektif dalam meningkatkan kompetensi keamanan digital civitas akademika baik pada aspek kognitif, afektif, maupun perilaku. Hal ini menegaskan bahwa intervensi edukatif yang terstruktur dan berbasis praktik d

apat menjadi strategi preventif yang kuat dalam memperkuat ketahanan siber institusi pendidikan.

ISSN: XXXX-XXXX (Print) / XXXX-XXXX (Online)
DOI: https://doi.org/10.XXXX/eduscotech.xxxx.xxx

IV. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan bahwa pelatihan Literasi Keamanan Digital (Anti-Phishing & Password Hygiene) terbukti efektif dalam meningkatkan kompetensi keamanan digital civitas akademika. Peningkatan signifikan terjadi pada aspek pengetahuan tentang phishing, kemampuan mengidentifikasi serangan rekayasa sosial, sikap kewaspadaan terhadap ancaman digital, serta praktik pengelolaan kata sandi yang lebih aman. Perbedaan skor pretest dan posttest yang signifikan secara statistik menunjukkan bahwa intervensi pelatihan memberikan dampak nyata dan terukur. Pelatihan berbasis simulasi dan praktik langsung tidak hanya meningkatkan pemahaman kognitif, tetapi juga mendorong perubahan perilaku digital yang lebih protektif, seperti penggunaan password yang kompleks, unik, serta penerapan autentikasi multi-faktor. Hal ini menegaskan bahwa pendekatan pembelajaran yang aplikatif dan kontekstual lebih efektif dibandingkan metode sosialisasi pasif.

Secara keseluruhan, program pelatihan ini dapat menjadi strategi preventif yang strategis dalam memperkuat ketahanan siber institusi pendidikan tinggi. Literasi keamanan digital bukan hanya kompetensi teknis, melainkan bagian dari budaya akademik yang harus dibangun secara berkelanjutan untuk menjaga integritas data, reputasi institusi, serta keamanan seluruh civitas akademika di era transformasi digital..

DAFTAR PUSTAKA

Beck, U. (1992). *Risk Society: Towards a New Modernity*. London: Sage Publications.

Carayon, P., & Smith, M. J. (2000). Work organization and ergonomics. *Applied Ergonomics, 31*(6), 649–662. https://doi.org/10.1016/S0003-6870(00)00040-5

Deci, E. L., & Ryan, R. M. (2000). The “what” and “why” of goal pursuits: Human needs and self-determination of behavior. *Psychological Inquiry, 11*(4), 227–268. https://doi.org/10.1207/S15327965PLI1104_01

Kolb, D. A. (1984). *Experiential Learning: Experience as the Source of Learning and Development*. Englewood Cliffs, NJ: Prentice Hall.

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

ISSN: XXXX-XXXX (Print) / XXXX-XXXX (Online)
DOI: https://doi.org/10.XXXX/eduscotech.xxxx.xxx
Schein, E. H. (2010). *Organizational Culture and Leadership* (4th ed.). San Francisco: Jossey-Bass.

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

Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. *Cognitive Science, 12*(2), 257–285. https://doi.org/10.1207/s15516709cog1202_4

Verizon. (2025). *Data Breach Investigations Report (DBIR)*. Verizon Enterprise.

Microsoft Security. (2024). *Digital Defense Report*. Microsoft Corporation.

Google & Harris Poll. (2024). *Password Security & Authentication Trends Report*. Google Safety Center.

Anti-Phishing Working Group (APWG). (2024). *Phishing Activity Trends Report*. APWG.org.