OPEN ACCESS
japatum.matradipti.org
DITERIMA PADA SEPTEMBER, 2023

JURNAL PEMANFAATAN TEKNOLOGI UNTUK MASYARAKAT (JAPATUM)
VOL. 3, ISSUE. 4, SEPTEMBER, 2023. HAL. 19-26
ISSN. 2460-9056 | DOI:10.59328/ JAPATUM.2023.2.3.65

Masyarakat Cakap Digital: Sosialisasi Bahaya dan Pencegahan Serangan Phishing

M. Naufal Hafizh Jatsono[1], Filza Fadia Suri[1], Ragil Deantika Rohmaniar[1], Muhammad Ardhi Al-Fatih[1], Verindra Hernanda Putra[1], Deril Wijdan Falih[1], Samuel Andi Kristyan[2], Rahmat Yasirandi[3]

[1,2,3]Program Studi Sarjana Teknologi Informasi Fakultas Informatika, TelkomUniversity,Jl. Telekomunikasi, Terusan Buahbatu, Bandung, Indonesia

e-mail: [1]jatsyn@student.telkomuniversity.ac.id,
[1]bluekitten@student.telkomuniversity.ac.id,
[1]ragildntika@student.telkomuniversity.ac.id,
[1]ardialpat@student.telkomuniversity.ac.id,
[1]verindrahp@student.telkomuniversity.ac.id,
[1]derilwjdf@student.telkomuniversity.ac.id, [2]samuelandi@telkomuniversity.ac.id,
[3]batanganhitam@telkomuniversity.ac.id

Abstrak/Abstract

Kegiatan penyuluhan ini bertujuan untuk meningkatkan kesadaran masyarakat terhadap ancaman serangan phishing yang semakin marak di era digital. Phishing merupakan bentuk kejahatan siber yang menargetkan informasi pribadi dengan menyamar sebagai entitas terpercaya. Kegiatan dilaksanakan di lingkungan sekitar Telkom University dengan metode penyampaian materi edukatif, penyebaran poster, serta lokakarya interaktif. Peserta diberikan pemahaman mengenai cara mengenali ciri-ciri phishing, strategi pencegahan, serta langkah yang harus diambil jika menjadi korban. Evaluasi dilakukan melalui survei sebelum dan sesudah penyuluhan, yang menunjukkan adanya peningkatan signifikan dalam pemahaman peserta terhadap keamanan digital. Penyuluhan ini juga mendorong tumbuhnya inisiatif peserta untuk berbagi pengetahuan kepada lingkungan sekitarnya. Hasil kegiatan menunjukkan bahwa pendekatan edukatif langsung mampu meningkatkan literasi keamanan digital masyarakat. Diharapkan kegiatan ini dapat berkontribusi dalam menciptakan komunitas yang lebih waspada, cakap, dan tanggap terhadap ancaman siber. Dengan pengembangan program yang berkelanjutan, masyarakat dapat lebih siap menghadapi tantangan di era transformasi digital.
Kata kunci: phishing, penyuluhan, keamanan digital, literasi siber, masyarakat

1. METODE PENGABDIAN

Di era digital saat ini, serangan siber telah menjadi ancaman yang sangat nyata dan merugikan, salah satunya adalah phishing. Phishing merupakan metode penipuan yang bertujuan untuk mendapatkan informasi sensitif seperti kata sandi atau data keuangan dengan menyamar sebagai pihak yang terpercaya. Kejahatan ini memanfaatkan kelemahan manusia, bukan hanya celah teknis, sehingga pelatihan dan edukasi menjadi sangat penting sebagai bentuk pertahanan utama.

Lingkungan perguruan tinggi seperti Telkom University juga tidak terlepas dari risiko ini. Banyak mahasiswa dan staf belum sepenuhnya menyadari bentuk dan bahaya dari phishing. Kurangnya penyuluhan atau edukasi langsung menyebabkan mereka lebih rentan menjadi korban. Padahal, efek dari serangan phishing bisa sangat luas, mulai dari pencurian data pribadi hingga gangguan pada operasional institusi.

Program penyuluhan keamanan digital yang berfokus pada phishing menjadi langkah awal yang strategis dalam menumbuhkan kesadaran dan meningkatkan keterampilan mengenali serta menanggapi ancaman siber. Studi oleh Carella et al. (2017) menunjukkan bahwa pelatihan kesadaran keamanan informasi secara signifikan mengurangi jumlah pengguna yang mengklik tautan phishing, menandakan efektivitas pendekatan edukatif dalam mengurangi kerentanan terhadap serangan siber (Carella dkk., 2017).

Selain pendekatan konvensional, pelatihan berbasis permainan atau gamifikasi seperti yang dilakukan dalam proyek Phishy juga terbukti meningkatkan kemampuan pengguna dalam mengidentifikasi tautan phishing melalui pengalaman yang interaktif dan menarik (Gokul dkk., 2018). Penerapan pelatihan yang melibatkan partisipasi aktif seperti ini bukan hanya membuat pembelajaran lebih efektif, tetapi juga meningkatkan daya ingat terhadap materi yang diajarkan.

Efektivitas pelatihan phishing juga terbukti dalam sektor keuangan, di mana kesadaran sosial rekayasa melalui pelatihan secara langsung menurunkan risiko serangan yang ditargetkan kepada pegawai (Ayoola dkk., 2024). Studi lain juga menegaskan pentingnya penggunaan simulasi dan reinforcement dalam pelatihan phishing, yang dapat memperkuat respons pengguna melalui mekanisme pembelajaran berulang (Yeoh dkk., 2021).

Lebih lanjut, pendekatan berbasis teknologi canggih juga mulai digunakan. Penelitian terbaru menunjukkan bahwa pelatihan yang disesuaikan menggunakan kecerdasan buatan dan model bahasa besar (LLM) dapat meningkatkan efektivitas pelatihan phishing secara signifikan dengan mengadaptasi konten berdasarkan profil pengguna (Greco dkk., 2024).

Berdasarkan konteks tersebut, kegiatan penyuluhan tentang phishing di kalangan sivitas akademika merupakan kebutuhan mendesak. Program ini tidak hanya bertujuan untuk meningkatkan pemahaman peserta tentang phishing dan cara menanggulanginya, tetapi juga diharapkan dapat menciptakan agen perubahan dalam ekosistem kampus yang turut menyebarkan pengetahuan digital yang aman dan bertanggung jawab. Kesadaran dan keterampilan ini penting agar masyarakat kampus tidak hanya menjadi pengguna teknologi, tetapi juga pelindung data dan informasi digital di era informasi ini.

2. METODE PENGABDIAN

2.1 Target Luaran

Program pelatihan pemrograman dasar ini dirancang dengan sejumlah target luaran yang relevan dengan kebutuhan peningkatan literasi digital remaja. Target utama dari kegiatan ini adalah agar para peserta, khususnya siswa SMP/SMA, mampu mengenali dan memahami konsep dasar dalam pemrograman komputer. Dengan memperkenalkan logika algoritmik, struktur data sederhana, serta penggunaan bahasa pemrograman Python, diharapkan peserta memiliki keterampilan awal dalam pengembangan aplikasi atau proyek digital sederhana. Selain itu, kegiatan ini juga bertujuan untuk menumbuhkan kepercayaan diri dan rasa ingin tahu peserta terhadap dunia teknologi. Peserta diharapkan tidak hanya menjadi pengguna teknologi, tetapi juga kreator yang mampu menciptakan solusi digital. Dalam jangka panjang, pelatihan ini bertujuan untuk menciptakan lingkungan belajar yang mendorong kolaborasi dan inovasi, sehingga remaja dapat terus mengeksplorasi potensi mereka di bidang teknologi informasi.

Beberapa penelitian telah menunjukkan bahwa pelatihan yang dimulai sejak usia muda dapat membentuk kemampuan berpikir kritis dan problem solving yang baik. Misalnya, Weintrop (2019) menyatakan bahwa pembelajaran berbasis blok visual memudahkan pemahaman konsep pemrograman bagi pemula (Weintrop, 2019). Hal ini sejalan dengan tujuan pelatihan ini yang juga menekankan pentingnya membangun dasar logika dan literasi teknologi sejak dini.

2.2 Solusi

Solusi yang diusulkan dalam program pelatihan ini dirancang secara strategis untuk menjawab tantangan rendahnya literasi digital dan keterampilan pemrograman di kalangan remaja. Salah satu strategi utama adalah penyebaran media pembelajaran yang mudah dipahami seperti poster edukatif yang menjelaskan konsep dasar pemrograman secara visual. Media ini berguna untuk menarik perhatian peserta sekaligus menyampaikan pesan kunci dengan cara yang sederhana. Selain itu, kegiatan inti berupa pelatihan langsung akan dilaksanakan dengan pendekatan praktik yang interaktif. Materi akan difokuskan pada pengenalan bahasa Python sebagai alat eksplorasi berpikir komputasional, dibarengi dengan praktik menggunakan perangkat edukatif seperti micro:bit.

Agar dampak pelatihan dapat terukur, dilakukan pre-test dan post-test untuk mengevaluasi peningkatan pemahaman peserta. Langkah ini juga telah digunakan dalam penyuluhan keamanan digital di kegiatan sebelumnya dan terbukti efektif untuk mengukur hasil pembelajaran. Penelitian oleh Nurhopipah dkk. (2021) mendukung pendekatan ini, menunjukkan bahwa metode berbasis proyek mampu mengembangkan kemampuan computational thinking secara signifikan (Nurhopipah dkk., 2021).

Lebih lanjut, Setiawan dkk. (2023) menekankan bahwa penggunaan alat bantu visual dan proyek nyata seperti CRUD berbasis web atau robotik membantu meningkatkan minat belajar coding di kalangan remaja (Setiawan dkk., 2023). Komponen penting lainnya adalah dukungan terhadap peningkatan kepercayaan diri peserta. Skala self-efficacy yang dikembangkan oleh Tsai dkk. (2019) membuktikan bahwa rasa percaya diri dalam kemampuan coding sangat mempengaruhi keberhasilan belajar remaja (Tsai dkk., 2019).

Program ini juga menjawab kesenjangan akses pendidikan teknologi yang masih terjadi di berbagai daerah. Sebagaimana diungkapkan oleh Purnandi et al. (2024), pelatihan pemrograman dasar yang dirancang dengan materi sederhana namun menarik mampu menjangkau lebih banyak remaja, termasuk mereka yang tidak memiliki akses pendidikan teknologi yang memadai (Purnandi et al., 2024). Oleh karena itu, solusi yang ditawarkan dalam pelatihan ini tidak hanya mencakup aspek teknis, tetapi juga aspek sosial berupa inklusivitas dan keberlanjutan pembelajaran.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Kegiatan

Kegiatan penyuluhan tentang bahaya phishing dilaksanakan dengan pendekatan langsung kepada masyarakat sekitar lingkungan Telkom University. Tujuan utama dari kegiatan ini adalah meningkatkan kesadaran masyarakat mengenai risiko serangan siber dan memberikan edukasi praktis tentang cara pencegahan serta penanggulangan phishing.

Pelaksanaan kegiatan ini berlangsung secara interaktif, di mana mahasiswa sebagai pelaksana menyampaikan materi melalui penyuluhan lisan dan media visual seperti poster. Materi yang disampaikan meliputi pengenalan phishing, jenis-jenis serangan, ciri-ciri email palsu, serta langkah konkret dalam menghadapi dan melaporkan serangan phishing. Masyarakat menunjukkan antusiasme yang tinggi selama penyuluhan dan aktif dalam sesi diskusi serta tanya-jawab.

Sebagai dampak dari kegiatan ini, peserta mulai memahami pentingnya menjaga keamanan data pribadi, mengenali ancaman phishing, dan menerapkan prinsip kehati-hatian saat menggunakan layanan digital. Selain itu, partisipasi masyarakat juga mendorong terbentuknya kesadaran kolektif untuk berbagi informasi terkait keamanan digital kepada lingkungan sekitarnya.

Gambar 1. Dokumentasi Kegiatan

Gambar 2. Penyerahan Poster

3.2 Olahan dan Analisis Survei

Evaluasi terhadap kegiatan dilakukan dengan membandingkan hasil survei sebelum dan sesudah penyuluhan. Survei ini mencakup pemahaman dasar tentang phishing, sikap waspada terhadap email mencurigakan, serta kesiapan masyarakat dalam menghadapi potensi serangan siber.

Hasil survei menunjukkan adanya peningkatan signifikan dalam aspek pemahaman dan sikap kehati-hatian terhadap phishing setelah pelaksanaan kegiatan. Mayoritas peserta menyatakan bahwa mereka menjadi lebih mengerti bagaimana mengidentifikasi ciri-ciri email phishing dan lebih siap dalam menghadapi potensi ancaman digital. Data ini menunjukkan keberhasilan penyuluhan dalam memberikan dampak positif terhadap peningkatan literasi keamanan digital masyarakat.

4. KESIMPULAN

Kegiatan penyuluhan mengenai pencegahan serangan phishing yang dilaksanakan oleh tim pengabdian masyarakat dari Program Studi S1 Teknologi Informasi Universitas Telkom telah memberikan kontribusi signifikan dalam meningkatkan kesadaran keamanan digital masyarakat sekitar kampus. Melalui pendekatan edukatif berbasis partisipatif, peserta mendapatkan pemahaman menyeluruh tentang apa itu phishing, bagaimana modus ini dijalankan, serta langkah-langkah konkret untuk mengidentifikasi dan menanggulanginya.

Penyuluhan yang dilakukan mencakup penyebaran poster edukatif, pelaksanaan lokakarya interaktif, dan asesmen sebelum serta sesudah kegiatan. Hasil evaluasi menunjukkan peningkatan signifikan dalam pemahaman peserta terkait taktik phishing dan kemampuan mereka dalam mengenali serta menghindari ancaman digital tersebut. Partisipasi masyarakat yang aktif juga menandakan antusiasme tinggi terhadap isu keamanan siber, serta munculnya kesadaran kolektif akan pentingnya proteksi data pribadi.

Efektivitas program ini tercermin dari hasil kuesioner yang menunjukkan peningkatan kesadaran dan pemahaman peserta pasca penyuluhan. Selain itu, penyuluhan ini juga mendorong terjadinya diseminasi pengetahuan secara informal di lingkungan masyarakat, sehingga memperluas dampak edukatif program ini.

Secara keseluruhan, kegiatan penyuluhan phishing ini berhasil menjawab kebutuhan literasi keamanan digital masyarakat dan memperkuat kemampuan mereka dalam menghadapi ancaman siber yang semakin kompleks. Program ini diharapkan menjadi fondasi awal bagi pelaksanaan edukasi keamanan digital yang lebih luas, berkelanjutan, dan berdampak di masa depan.

5. SARAN

Berdasarkan pelaksanaan kegiatan dan hasil evaluasi, terdapat beberapa hal yang dapat menjadi masukan untuk pengembangan program serupa di masa mendatang. Pertama, kegiatan penyuluhan mengenai phishing ini memiliki potensi besar untuk diperluas ke komunitas-komunitas lain di luar lingkungan Telkom University agar semakin banyak masyarakat yang mendapatkan pemahaman mengenai ancaman keamanan siber. Selain itu, program ini sebaiknya dikembangkan secara berkelanjutan dalam bentuk pelatihan berjenjang, sehingga peserta dapat terus memperdalam pemahaman mereka melalui materi lanjutan yang lebih kompleks. Untuk memperkaya pengalaman belajar, penggunaan media edukatif yang lebih variatif seperti video

simulasi, infografis, atau permainan interaktif juga dapat menjadi strategi efektif dalam meningkatkan keterlibatan dan pemahaman peserta. Di sisi lain, kolaborasi dengan pihak eksternal seperti lembaga pemerintah atau penyedia layanan teknologi informasi dapat memperluas jangkauan kegiatan serta menambah nilai edukatif dari materi yang disampaikan. Terakhir, agar dampak dari penyuluhan ini dapat diukur secara menyeluruh, perlu dilakukan evaluasi lanjutan dalam jangka waktu tertentu guna menilai perubahan perilaku dan peningkatan kewaspadaan peserta terhadap serangan phishing di kehidupan sehari-hari.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Telkom University yang telah memberi dukungan terhadap keberhasilan pengabdian ini.

DAFTAR PUSTAKA

Borglet, C, 2003, Finding Asscociation Rules with Apriori Algorithm,

Carella, A., Kotsoev, M., & Truta, T. (2017). *Impact of security awareness training on phishing click-through rates*. In 2017 IEEE International Conference on Big Data (Big Data) (pp. 4458–4466). IEEE.

Gokul, C., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., & Lodha, S. (2018). *PHISHY - A serious game to train enterprise users on phishing awareness*. In Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts. ACM.

Ayoola, V. B., James, U. U., Idoko, P. I., Ijiga, O. M., & Olola, T. M. (2024). *Effectiveness of social engineering awareness training in mitigating spear phishing risks in financial institutions from a cybersecurity perspective*. Global Journal of Engineering and Technology Advances.

Yeoh, W., Huang, H., Lee, W.-S., Al Jafari, F., & Mansson, R. (2021). *Simulated phishing attack and embedded training campaign*. Journal of Computer Information Systems, 62(6), 802–821.

Greco, F., Desolda, G., & Viganò, L. (2024). *Supporting the design of phishing education, training and awareness interventions: An LLM-based approach*.

Nurhopipah, A., Nugroho, I. A., & Suhaman, J. (2021). Pembelajaran pemrograman berbasis proyek untuk mengembangkan kemampuan *computational thinking* anak. *Jurnal Pengabdian Kepada Masyarakat, 27*(1), 6–13.

Purnandi, M., Wibawa, M. B., Yusian, D. R. T. B., & Sayuti, M. S. M. (2024). Pelatihan pemrograman dasar bagi remaja untuk mendorong minat di bidang teknologi. *Jurnal Pengabdian Masyarakat (INOTEC, 6*(2), 57–60.

Setiawan, I., Artha, F. D., & Iktisom, R. W. A. (2023). Peningkatan kemampuan coding anak usia remaja dengan metode CRUD generator berbasis web. *Jurnal PEDAMAS, 1*(2), 331–337.

Tsai, M.-J., Wang, C.-Y., & Hsu, P.-F. (2019). Developing the computer programming self-efficacy scale for computer literacy education. *Journal of Educational*

Computing Research, 56(8), 1345–1360.
https://doi.org/10.1177/0735633118785973

Weintrop, D. (2019). Block-based programming in computer science education. *Communications of the ACM, 62*(8), 22–25.