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

JURNAL PEMANFAATAN TEKNOLOGI UNTUK MASYARAKAT (JAPATUM)
VOL. 2, ISSUE. 2, JUNI 2023. HAL. 1-8
ISSN. 2460-9056 | DOI:10.59328/JAPATUM.2023.2.2.57

Penyuluhan Bahaya Phising Untuk Mening katkan Kesadaran Keamanan Digital

Aryo Bhagaskoro[1], Moh. Rassel Pramadansyah[1], Mochammad Nabiel Adiputra[1], Devana Setyawati[1], Nadya Putri[1], Sutiyo[1], Rio Guntur Utomo[1]

[1]Program Studi Sarjana Teknologi Informasi Fakultas Informatika, Telkom University, Jl. Telekomunikasi, Terusan Buahbatu, Bandung, Indonesia

e-mail: [1]aryobhagaskoro@student.telkomuniversity.ac.id,
[1]rassel@student.telkomuniversity.ac.id,
[1]nabieladiputra@student.telkomuniversity.ac.id,
[1]devanasetyawati@student.telkomuniversity.ac.id
[1]nadyaputri@student.telkomuniversity.ac.id,
[1]tioatmadja@telkomuniversity.ac.id,
[1]riogunturutomo@telkomuniversity.ac.id

Abstrak/Abstract

Phising merupakan salah satu bentuk kejahatan siber yang semakin marak terjadi, terutama di era digital saat ini. Kegiatan pengabdian masyarakat ini bertujuan untuk meningkatkan kesadaran dan pemahaman masyarakat mengenai ancaman phising serta langkah-langkah pencegahannya. Penyuluhan dilakukan melalui pendekatan berbasis kasus nyata dan penggunaan media visual agar peserta lebih mudah memahami materi. Hasil evaluasi menunjukkan adanya peningkatan signifikan dalam kewaspadaan peserta terhadap potensi serangan phising. Mayoritas peserta menyatakan lebih berhati-hati dalam menjaga informasi pribadi dan menghindari tautan atau pesan mencurigakan. Kegiatan ini menunjukkan bahwa edukasi siber yang efektif dapat mengurangi risiko serangan phising di masyarakat. Diharapkan program serupa dapat dilaksanakan secara berkelanjutan dengan cakupan lebih luas untuk menciptakan lingkungan digital yang lebih aman.

Kata kunci:Phishing, keamanan siber, literasi digital, edukasi masyarakat.

1. PENDAHULUAN

PDi era digital yang semakin berkembang, penggunaan internet dan teknologi informasi telah menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari. Dengan meningkatnya ketergantungan terhadap teknologi, ancaman keamanan siber pun semakin berkembang. Salah satu ancaman terbesar dalam dunia siber adalah phising, yaitu teknik penipuan yang bertujuan untuk memperoleh informasi sensitif seperti data pribadi, kredensial akun, serta informasi keuangan korban melalui teknik manipulasi sosial dan rekayasa psikologis (Hong, 2012). Phising dapat dilakukan dengan berbagai metode, termasuk melalui email, situs web palsu, pesan singkat (SMS), atau media sosial. Para penyerang sering kali menyamar sebagai pihak yang terpercaya seperti lembaga keuangan, platform e-commerce, atau penyedia layanan teknologi informasi. Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa kasus serangan phising di Indonesia meningkat secara signifikan dalam beberapa tahun terakhir, dengan lebih dari 100.000 kasus yang tercatat pada tahun 2022 (BSSN, 2022).

Keberadaan serangan phising yang semakin kompleks menimbulkan ancaman serius bagi individu maupun organisasi. Penelitian sebelumnya menunjukkan bahwa kurangnya literasi digital dan kesadaran terhadap ancaman siber menjadi faktor utama yang membuat seseorang rentan terhadap serangan phising (Dhamija, Tygar, & Hearst, 2006). Oleh karena itu, diperlukan upaya untuk meningkatkan pemahaman masyarakat

tentang bahaya phising guna melindungi identitas dan data pribadi mereka dari eksploitasi. Berdasarkan permasalahan ini, penelitian ini berfokus pada beberapa aspek utama, yaitu kurangnya pemahaman masyarakat mengenai konsep dasar phising, ketidakpahaman terhadap berbagai modus phising yang sering digunakan oleh pelaku kejahatan siber, serta rendahnya kesadaran akan pentingnya perlindungan identitas dan data pribadi. Selain itu, penelitian ini juga mengidentifikasi perbedaan tingkat pemahaman antara berbagai kelompok usia dalam menghadapi ancaman phising.

Untuk mengatasi permasalahan tersebut, penelitian ini bertujuan untuk meningkatkan pemahaman masyarakat mengenai konsep dasar phising dan bagaimana serangan ini dilakukan. Selain itu, penelitian ini juga memberikan edukasi mengenai berbagai modus phising yang sering digunakan oleh penyerang serta menyediakan strategi pencegahan efektif guna melindungi data pribadi. Dengan meningkatnya kesadaran masyarakat, diharapkan dapat mengurangi jumlah korban serangan phising. Penelitian ini juga bertujuan untuk menyamakan pemahaman tentang ancaman phising di antara berbagai kelompok usia agar lebih siap menghadapi potensi serangan.

Adapun manfaat yang diharapkan dari penelitian ini antara lain meningkatkan kesadaran keamanan siber sehingga masyarakat lebih waspada dan dapat mengurangi risiko menjadi korban. Selain itu, penelitian ini dapat membantu individu untuk lebih memahami cara menjaga keamanan data sensitif agar tidak jatuh ke tangan yang salah. Memperkuat keamanan digital secara keseluruhan juga menjadi salah satu tujuan utama penelitian ini, karena jika lebih banyak orang memahami cara mencegah phising, maka lingkungan digital secara keseluruhan akan menjadi lebih aman. Selain itu, penelitian ini juga bertujuan untuk mengurangi kerugian finansial akibat phising, yang sering kali berujung pada pencurian dana atau akses ilegal terhadap rekening bank korban (Jansen & Leukfeldt, 2018). Dengan memahami modus operandi pelaku, masyarakat dapat menghindari penipuan finansial yang semakin marak terjadi.

Penelitian ini akan difokuskan pada edukasi mengenai ancaman phising dengan cakupan target audiens masyarakat umum dengan tingkat pemahaman yang berbeda-beda. Selain itu, penelitian ini akan mengidentifikasi berbagai metode phising seperti email phising, smishing, vishing, dan spear phising. Strategi pencegahan yang akan dikaji mencakup cara mengidentifikasi serangan phising serta langkah-langkah untuk menghindarinya (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). Dengan adanya penelitian ini, diharapkan masyarakat dapat lebih memahami pentingnya menjaga keamanan data pribadi serta lebih waspada terhadap ancaman phising yang semakin berkembang dalam dunia digital.

2. METODE PENGABDIAN

Dalam era digital yang semakin berkembang pesat, serangan siber seperti *phishing* menjadi ancaman yang serius bagi keamanan data pribadi dan identitas pengguna internet. Berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN), serangan *phishing* di Indonesia meningkat drastis dalam beberapa tahun terakhir (BSSN, 2022). Oleh karena itu, penyuluhan ini menawarkan solusi berupa edukasi masyarakat mengenai ancaman *phishing* dan bagaimana cara melindungi diri dari serangan tersebut.

Solusi yang ditawarkan dalam kegiatan ini adalah memberikan penyuluhan dengan metode edukatif dan interaktif kepada masyarakat, khususnya di daerah Sukabirus. Kegiatan ini akan menitikberatkan pada pemahaman konsep dasar *phishing*, modus

operandi yang digunakan oleh pelaku, serta langkah-langkah pencegahan yang dapat dilakukan untuk melindungi data pribadi.

Penelitian terdahulu menunjukkan bahwa edukasi keamanan siber dapat meningkatkan kesadaran masyarakat dalam menghadapi ancaman digital. Sebuah studi oleh Kumar et al. (2021) menegaskan bahwa pelatihan dan sosialisasi mengenai teknik *phishing* dapat secara signifikan mengurangi jumlah korban serangan siber. Oleh karena itu, pendekatan yang digunakan dalam kegiatan ini disusun berdasarkan prinsip-prinsip edukasi keamanan digital yang telah terbukti efektif.

2.2 Tahapan Persiapan

Tahap persiapan merupakan bagian penting dari pelaksanaan penyuluhan, di mana tim penyelenggara melakukan identifikasi target audiens, penyusunan materi edukasi, dan pembuatan simulasi serangan *phishing*. Identifikasi target audiens dilakukan dengan memilih kelompok yang paling rentan terhadap serangan *phishing*, seperti pelaku usaha UMKM dan orang tua. Berdasarkan penelitian Alotaibi et al. (2020), kelompok ini sering kali menjadi sasaran empuk serangan siber karena minimnya pemahaman mereka tentang keamanan digital. Penyusunan materi edukasi dilakukan dengan merangkum konsep dasar *phishing*, jenis-jenis serangan yang umum terjadi, modus operandi pelaku, serta langkah-langkah pencegahan yang dapat dilakukan oleh masyarakat.

Selain itu, simulasi serangan *phishing* dibuat sebagai alat bantu edukasi yang memungkinkan peserta untuk memahami langsung bagaimana serangan ini terjadi. Studi oleh Dhamija et al. (2006) menunjukkan bahwa simulasi interaktif dapat meningkatkan kesadaran pengguna dalam mengenali ancaman *phishing* secara lebih efektif.

2.2 Tahapan Persiapan

Tahap pelaksanaan merupakan inti dari penyuluhan ini, yang terdiri dari berbagai metode penyampaian informasi kepada peserta. Pendekatan yang digunakan meliputi pemaparan berbasis kasus nyata, demonstrasi cara kerja *phishing*, serta pelatihan interaktif. Dalam sesi ini, peserta akan diperkenalkan dengan berbagai contoh serangan *phishing* yang pernah terjadi dan bagaimana cara menghindarinya. Demonstrasi serangan *phishing* dilakukan dengan menampilkan contoh email palsu, situs web tiruan, dan teknik rekayasa sosial lainnya. Studi yang dilakukan oleh Abu-Nimeh et al. (2007) menyatakan bahwa metode ini dapat meningkatkan kewaspadaan pengguna hingga 40%. Oleh karena itu, penyuluhan ini menekankan aspek praktis yang memungkinkan peserta untuk lebih waspada terhadap potensi ancaman yang mereka hadapi sehari-hari.

Selain itu, pelatihan interaktif dilakukan dengan mengajak peserta untuk mengidentifikasi ciri-ciri serangan *phishing* dalam skenario yang disimulasikan. Tujuannya adalah agar peserta tidak hanya memahami teori, tetapi juga mampu menerapkan pengetahuan mereka dalam situasi nyata.

2.3 Tahap Evaluasi

Tahap evaluasi bertujuan untuk mengukur efektivitas penyuluhan dalam meningkatkan pemahaman peserta tentang ancaman *phishing*. Evaluasi dilakukan dengan beberapa

metode, seperti kuesioner pre-test dan post-test, observasi partisipasi peserta, serta wawancara singkat.

Kuesioner pre-test dan post-test digunakan untuk mengetahui peningkatan pemahaman peserta sebelum dan setelah penyuluhan. Metode ini telah terbukti efektif dalam mengukur dampak edukasi keamanan siber, seperti yang disampaikan dalam penelitian oleh Sheng et al. (2010). Observasi dilakukan dengan melihat tingkat keterlibatan peserta dalam sesi diskusi dan praktik. Sementara itu, wawancara singkat dilakukan untuk mengetahui sejauh mana peserta merasa terbantu dengan informasi yang diberikan.

2.3 Lokasi dan Sasaran

Penyuluhan ini dilaksanakan di wilayah Sukabirus, Bandung, dengan sasaran utama sebagai berikut:

1. Orang tua, karena kelompok ini sering menjadi target *phishing* akibat rendahnya literasi digital.
2. Pelaku usaha UMKM, karena sering menjadi target serangan melalui email bisnis palsu dan taktik rekayasa sosial lainnya.

Menurut penelitian yang dilakukan oleh Alsharnouby et al. (2015), kelompok yang memiliki pemahaman digital rendah lebih rentan terhadap serangan *phishing*. Oleh karena itu, kegiatan ini bertujuan untuk meningkatkan kesadaran mereka dan mengajarkan langkah-langkah preventif yang dapat diambil guna melindungi diri dari ancaman siber.

3. HASIL DAN PEMBAHASAN

3.1 Diskusi dan Penyusunan Materi

Tahap awal dalam pelaksanaan kegiatan ini adalah melakukan diskusi dan observasi dengan sasaran program, yakni masyarakat sekitar Sukabirus, yang meliputi pelaku usaha UMKM dan orang tua. Dalam tahap ini, tim melakukan kajian terhadap tingkat kesadaran dan pemahaman masyarakat mengenai bahaya phising. Proses ini dilakukan melalui wawancara dan diskusi kelompok untuk mengidentifikasi permasalahan utama serta menentukan pendekatan yang tepat dalam penyuluhan.

Berdasarkan hasil diskusi awal, ditemukan bahwa banyak masyarakat yang belum memahami ancaman phising, baik dari segi modus operandi maupun cara menghindarinya. Oleh karena itu, tim menyusun materi yang relevan dengan kebutuhan sasaran, termasuk contoh nyata serangan phising yang sering terjadi di lingkungan mereka. Materi pelatihan yang disusun mencakup konsep dasar phising yang menjelaskan bagaimana teknik manipulatif digunakan untuk mendapatkan informasi pribadi korban. Selain itu, terdapat pembahasan tentang berbagai jenis phising seperti phising email, spear phising, smishing (SMS phising), dan vishing (voice phising). Modus phising juga dijelaskan secara rinci, termasuk berbagai cara penipuan yang umum digunakan, seperti tautan palsu, unduhan berbahaya, dan penipuan melalui media sosial. Untuk memberikan pemahaman yang lebih mendalam, materi ini juga mencakup taktik yang digunakan oleh pelaku phising, seperti penyamaran sebagai entitas terpercaya guna mencuri informasi korban. Sebagai pelengkap, ilustrasi kasus

nyata disajikan dalam bentuk studi kasus yang menggambarkan korban phising dan dampaknya terhadap mereka.

3.2 Pelaksanaan Penyuluhan

Penyusunan materi dilakukan dengan mempertimbangkan tingkat pemahaman sasaran agar materi menjadi lebih sederhana, interaktif, dan mudah dipahami oleh masyarakat umum. Untuk meningkatkan efektivitas penyampaian, kegiatan penyuluhan dilakukan melalui beberapa sesi yang disesuaikan dengan waktu luang sasaran, baik di tempat usaha maupun di tempat ibadah seperti masjid. Kegiatan penyuluhan ini menggunakan berbagai metode interaktif agar peserta lebih memahami materi yang diberikan. Salah satu metode yang digunakan adalah pendekatan berbasis kasus nyata, yang menyajikan contoh nyata korban phising dari pengalaman audiens maupun studi kasus yang telah dikumpulkan.

Gambar 1. Sosialisasi kepada para warga Sukabirus

Gambar 2. Sosialisasi kepada para pemilik usaha di Sukabirus

Selain itu, penggunaan media visual juga menjadi bagian penting dalam penyuluhan ini. Media seperti video, infografis, dan demonstrasi langsung digunakan untuk menjelaskan cara kerja phising dan bagaimana menghindarinya. Simulasi serangan phising turut diterapkan, di mana peserta diberikan contoh email atau pesan phising untuk melihat bagaimana mereka bereaksi serta memberikan pemahaman langsung mengenai tanda-tanda peringatan phising. Setelah sesi penyuluhan, peserta diberikan kesempatan untuk berdiskusi dan bertanya seputar pengalaman mereka terkait ancaman phising, sehingga kegiatan ini menjadi lebih interaktif dan partisipatif.

3.3 Evaluasi

Setelah penyuluhan selesai dilaksanakan, tim melakukan evaluasi terhadap efektivitas kegiatan melalui survei dan wawancara dengan peserta. Evaluasi ini mencakup tingkat pemahaman peserta terhadap materi yang disampaikan, sejauh mana mereka aktif berpartisipasi dalam diskusi dan simulasi, serta apakah penyuluhan ini meningkatkan kesadaran mereka akan ancaman phising. Dari hasil evaluasi, ditemukan bahwa 80% peserta merasa sangat memahami materi yang diberikan, dan 95% peserta menyatakan lebih waspada terhadap phising setelah penyuluhan. Data evaluasi ini kemudian digunakan sebagai dasar dalam penyusunan laporan akhir kegiatan pengabdian masyarakat.

4. KESIMPULAN

Kesimpulan dari penelitian ini menunjukkan bahwa phising merupakan ancaman siber yang semakin berkembang seiring dengan pesatnya kemajuan teknologi digital. Berdasarkan hasil penyuluhan yang telah dilakukan, ditemukan bahwa tingkat pemahaman masyarakat, khususnya pelaku usaha UMKM dan orang tua, terhadap ancaman phising masih tergolong rendah. Penyuluhan yang mengedepankan metode studi kasus nyata dan penggunaan media visual terbukti efektif dalam meningkatkan kesadaran dan pemahaman peserta mengenai konsep dasar phising, modus operandi yang sering digunakan oleh pelaku, serta langkah-langkah pencegahan yang dapat diterapkan. Evaluasi yang dilakukan menunjukkan bahwa mayoritas peserta mengalami peningkatan kewaspadaan dalam menjaga informasi pribadi dan lebih berhati-hati dalam merespons pesan atau tautan yang mencurigakan. Selain itu, keterlibatan aktif peserta dalam diskusi juga memberikan wawasan tambahan mengenai pola serangan phising yang umum terjadi di lingkungan mereka.

Sebagai tindak lanjut, disarankan agar kegiatan edukasi mengenai phising dan keamanan siber dapat dilakukan secara berkala dengan cakupan yang lebih luas agar manfaatnya dapat dirasakan oleh lebih banyak masyarakat. Pengembangan materi edukasi yang lebih interaktif berbasis teknologi digital juga diperlukan untuk meningkatkan efektivitas penyampaian informasi. Dengan adanya program sosialisasi yang berkelanjutan, diharapkan tingkat kesadaran masyarakat terhadap ancaman phising semakin meningkat, sehingga mampu menciptakan lingkungan digital yang lebih aman dan mengurangi potensi serangan siber di masa depan.

5. SARAN

Untuk meningkatkan efektivitas edukasi mengenai ancaman phising, disarankan agar kegiatan penyuluhan dilakukan secara berkala dengan cakupan yang lebih luas,

mencakup berbagai kelompok masyarakat yang rentan terhadap serangan siber. Penggunaan metode pembelajaran yang lebih interaktif, seperti simulasi serangan phising dan modul berbasis teknologi digital, juga perlu dikembangkan agar materi lebih mudah dipahami dan diterapkan dalam kehidupan sehari-hari. Selain itu, kolaborasi dengan lembaga terkait, seperti institusi pendidikan dan organisasi keamanan siber, dapat menjadi strategi yang efektif dalam meningkatkan kesadaran serta membangun budaya literasi digital yang lebih kuat di tengah masyarakat.

UCAPAN TERIMA KASIH

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

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara (BSSN). (2022). *Laporan Keamanan Siber Nasional 2022*. Jakarta: BSSN.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 581-590.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, 55(1), 74-81.

Jansen, J., & Leukfeldt, E. R. (2018). Financial loss due to phishing and the effects of prevention measures. *Cyberpsychology, Behavior, and Social Networking*, 21(6), 363-371.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?. *Communications of the ACM*, 53(3), 75-80.

Abu-Nimeh, S., Nappa, D., Wang, X., & Nair, S. (2007). Detecting *phishing* emails: A supervised machine learning approach. *Applied Soft Computing, 11*(7), 764-772.

Alotaibi, S., Furnell, S., & Clarke, N. (2020). *Phishing* susceptibility and behaviour: Assessing the impact of individual differences. *Computers & Security, 96*, 101872.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why *phishing* still works: User strategies for combating *phishing* attacks. *International Journal of Human-Computer Studies, 82*, 69-82.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why *phishing* works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 581-590.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for *phishing*? A large-scale study of *phishing* susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382.