GIAT: Teknologi untuk Masyarakat
Vol. 4, No. 1, Mei 2025
Online issn:2829-8268
Print issn:2829-6532

Penyuluhan Keamanan Informasi Terkait Ancaman *Phishing* untuk Meningkatkan Literasi Digital Warga Kompleks Yadara Babarsari Yogyakarta

N Yudistira[*1], E F Lamba[2], R Jauhari[3], F R Farhanna[4], C Y Palangan[5]

[1-5]Program Studi Sistem Informasi, Universitas Atma Jaya Yogyakarta

E-mail: 231712520@students.uajy.ac.id*[1], 231712521@students.uajy.ac.id[2], 231712550@students.uajy.ac.id[3], 231712613@students.uajy.ac.id[4], citra.yayu@uajy.ac.id[5]

Abstrak. Perkembangan teknologi digital yang pesat membawa kemudahan sekaligus tantangan baru, salah satunya adalah kejahatan siber berupa *phishing* yang dapat mengancam kebocoran data pribadi maupun organisasi. Rendahnya kesadaran masyarakat, terutama kalangan orang tua, terhadap ancaman *phishing* menjadi faktor utama tingginya keberhasilan serangan ini. Kegiatan sosialisasi ini bertujuan untuk meningkatkan literasi digital melalui pengenalan keamanan informasi terkait ancaman *phishing* kepada warga Kompleks Yadara Babarsari, Yogyakarta. Metode pelaksanaan menggunakan pendekatan secara penyuluhan dengan metode penyuluhan partisipatif yang melibatkan 35 orang tua sebagai peserta. Kegiatan meliputi pemaparan materi, kuis interaktif, serta evaluasi pemahaman sebelum dan sesudah sosialisasi melalui *pre-test* dan *post-test*. Hasil menunjukkan adanya peningkatan signifikan dalam pemahaman peserta terhadap ciri-ciri *phishing* dan pentingnya menjaga keamanan data pribadi. Kegiatan ini diharapkan dapat menjadi sarana edukasi efektif untuk meningkatkan literasi digital dan kesadaran masyarakat dalam menghadapi ancaman kejahatan siber.

Kata kunci: *phishing*; keamanan informasi; sosialisasi; literasi digital; orang tua

Abstract.. The rapid advancement of digital technology brings both convenience and new challenges, one of which is cybercrime in the form of phishing attacks that threaten the leakage of personal and organizational data. Low awareness among community members, especially older adults, about phishing threats is a major factor contributing to the success of these attacks. This socialization activity aims to enhance digital literacy by introducing information security related to phishing threats to residents of the Yadara Babarsari Complex, Yogyakarta. The implementation method uses a qualitative approach with participatory counseling involving 35 older adult participants. The activity includes material presentation, interactive quizzes, and evaluation of participants' understanding through pre-tests and post-tests. Results show a significant increase in participants' knowledge about phishing characteristics and the importance of safeguarding personal data security. This activity is expected to serve as an effective educational tool to improve digital literacy and public awareness in facing cybercrime threats.

Keywords: *phishing; information security; socialization; digital literacy; parents*

Online issn:2829-8268
Print issn:2829-6532

1. Pendahuluan

Di era modern saat ini, perkembangan teknologi telah mempermudah manusia dalam melakukan berbagai aktivitas. Perkembangan teknologi tersebut telah mengubah cara kita berinteraksi, berkomunikasi, dan bekerja. Seiring dengan perkembangannya, kemampuan digital literasi juga menjadi tuntutan agar individu dapat menggunakan teknologi dan informasi secara akurat. Digital literasi merupakan kemampuan individu untuk mengakses, menggunakan, memahami, dan mengevaluasi informasi melalui teknologi secara bijak dan bertanggung jawab[1]. Oleh karena itu, setiap individu perlu dibekali dengan kemampuan ini. Di sisi lain, kurangnya digital literasi memunculkan sebuah tantangan baru, yaitu timbulnya berbagai bahaya yang mengancam privasi dan keamanan data pribadi[2]. Bentuk ancaman tersebut dapat berupa kejahatan siber yang berusaha mengeksploitasi sistem dan memanfaatkan kurangnya pengetahuan pengguna sistem informasi[3]. Salah satu contohnya adalah tindakan *phishing*, yang dapat mengancam kebocoran data[4].

Phishing merupakan jenis kejahatan siber umum yang melibatkan tindakan penipuan atau pemalsuan dengan tujuan memperoleh informasi rahasia, seperti data pribadi, *password*, dan data finansial seperti rekening bank dan data kartu kredit dari korban[5]. Hal tersebut kerap dilakukan melalui *email*, pesan, dan situs web tiruan yang dirancang agar terlihat meyakinkan untuk menipu korban[6]. Serangan *phishing* tersebut dapat berupa, seperti *email phishing*, *link manipulation*, dan *malware*[7]. Tindakan-tindakan tersebut menimbulkan dampak negatif baik secara finansial maupun non-finansial[8].

Selain itu, *phishing* tidak sebatas menyebabkan kerugian finansial untuk individu serta organisasi, tetapi dapat juga berdampak negatif pada nama baik dan kepercayaan masyarakat[9]. Lebih dari itu, serangan ini juga dapat membuka celah untuk ancaman siber yang lebih membahayakan, seperti peretasan akun ataupun ancaman enkripsi data[6]. Salah satu dampak terbesarnya adalah permasalahan tentang risiko kebocoran data pribadi yang bersifat sensitif dan seharusnya hanya dapat diketahui oleh pemiliknya. Data pribadi tersebut mencakup hal-hal, seperti data pengguna, catatan rahasia dari organisasi atau individu, sehingga data tersebut menjadi hal yang privasi dan harus dijaga kerahasiaannya. Di samping itu, masyarakat masih belum sadar dan tidak memedulikan risiko dari ancaman *phishing* tersebut, serta menganggapnya sebagai permasalahan kecil[10]. Salah satu kelompok masyarakat yang rawan terkena kejahatan digital berupa serangan *phishing* tersebut adalah orang tua [11]. Hal ini disebabkan oleh rendahnya tingkat pemahaman mengenai teknologi pada orang tua, sehingga lebih rawan terkena kejahatan siber[12].

Berdasarkan penelitian sebelumnya, data yang didapat dari Indonesia Anti-*Phishing* Data Exchange (IDADX) menunjukkan bahwa tingginya angka serangan *phishing* telah menimbulkan rasa waspada di kalangan masyarakat. Tercatat, laporan *phishing* di Indonesia mengalami lonjakan dari 3.180 kasus pada kuartal pertama telah menjadi 5.579 kasus pada kuartal kedua tahun 2022. Hal tersebut menunjukkan adanya peningkatan aktivitas kejahatan siber yang semakin masif dan terstruktur[13]. Selain itu, peningkatan aktivitas kejahatan siber tersebut juga disebabkan oleh rendahnya kesadaran masyarakat[14]. Penelitian sebelumnya menyatakan bahwa rendahnya pemahaman masyarakat terhadap ciri-ciri situs web palsu menjadi salah satu faktor utama tingginya keberhasilan serangan *phishing*[15]. Hal tersebut menunjukkan bahwa tingkat kesadaran masyarakat terhadap ancaman *phishing* masih tergolong rendah[13]. Oleh karena itu, untuk memastikan data pribadi dan identitas tersebut terlindungi dari eksploitasi perlu adanya upaya dalam meningkatkan kesadaran masyarakat tentang bahaya *phishing*[11].

Pada beberapa tahun terakhir di Daerah Istimewa Yogyakarta mendapati peningkatan kasus serangan *phishing*. Berdasarkan data yang didapat dari laporan polisi di Subdit V Siber Polda DIY, terjadi peningkatan angka kasus *phishing* pada tahun 2021 dan 2022 yang mencatat 8 kasus serta puncaknya terjadi pada tahun 2023 yang mencatat terjadinya 12 kasus *phishing*. Jumlah kasus *phishing* yang terjadi di Daerah Istimewa Yogyakarta tersebut memperlihatkan adanya ancaman yang dapat menyerang keamanan siber di Daerah Istimewa Yogyakarta[16]. Dalam mengatasi hal tersebut, dibutuhkan kesadaran serta pemahaman mengenai permasalahan *link phishing* pada lingkungan sekitar [17].

Kesadaran dan pengetahuan tentang macam-macam *link phishing* yang terdapat di sekeliling kita merupakan perihal yang diperlukan dalam mengurangi risiko terkenanya serangan *phishing* tersebut. Dalam meningkatkan kesadaran akan bahaya *phishing* tersebut, terdapat sejumlah strategi yang bisa diterapkan,

Online issn:2829-8268
Print issn:2829-6532

seperti menjalankan aktivasi verifikasi dua langkah untuk meningkatkan keamanan dengan meminta kode tambahan yang dikirim ke ponsel atau *email*, serta mengatur privasi dan izin aplikasi yang terpasang untuk memperkecil kesempatan aplikasi dalam mengelola data yang dimiliki sehingga risiko kebocoran data pribadi juga dapat dikurangi[17].

Dalam mengurangi risiko kebocoran data tersebut, penggunaan *Wi-Fi atau Wireless Fidelity* publik perlu juga diperhatikan. Saat menggunakan jaringan *Wi-Fi* publik, aktivitas transaksi yang melibatkan informasi sensitif seperti penggunaan *Mobile Banking* perlu dihindari karena jaringan *Wi-Fi* publik sering kali tidak aman[17]. Lalu, ketelitian juga dibutuhkan dalam mengolah sebuah informasi dari mana pun khususnya internet, kita wajib berhati-hati dengan tautan atau lampiran dari situs, pesan, iklan, grup dalam internet. Oleh karena itu, masyarakat juga wajib memeriksa alamat situs web dengan cermat karena terdapat banyak kasus yang melibatkan alamat situs resmi, tetapi dipalsukan untuk tujuan kejahatan informasi pribadi[18].

Salah satu wilayah yang belum mendapatkan pengetahuan dan pemahaman secara mendalam yaitu Kompleks Yadara Babarsari, Yogyakarta yang terletak di Jl. Komp. Yadara No.5/33, Tambak Bayan, Caturtunggal, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta. Kegiatan pengabdian ini dilakukan dengan memberikan pelatihan berupa sosialisasi kepada para warga, khususnya orang tua dalam menjaga keamanan informasi yang meliputi data pribadi, seperti identitas data diri, nomor telepon, alamat email, kata sandi, dan informasi sensitif lainnya. Dengan adanya sosialisasi ini, diharapkan kalangan orang tua di Kompleks Yadara Babarsari, Yogyakarta dapat menjadi lebih sadar dan waspada terhadap ancaman dari *link phishing.* Selain itu, dengan adanya sosialisasi ini diharapkan para orang tua dapat mengidentifikasi ciri-ciri dari *link phishing* agar tidak terjadinya kebocoran data pribadi maupun organisasi serta mengalami kerugian secara finansial maupun non finansial dari serangan *phishing* tersebut.

2. Analisis Situasi

Gambar 1. Kompleks Yadara Babarsari Yogyakarta

Gambar 1 memperlihatkan Kompleks Yadara Babarsari, Yogyakarta adalah Kompleks perumahan yang didirikan pada tahun 1975 oleh Bapak KRT. Tjokronegoro yang berlokasi di Jl. Komp. Yadara No.5/33, Tambak Bayan, Caturtunggal, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta. Kegiatan pengabdian berupa sosialisasi ini akan dilaksanakan di Pendopo yang berlokasi di Kompleks Yadara RT.21/RW.06 Blok.I, Depok, Sleman, Daerah Istimewa Yogyakarta.

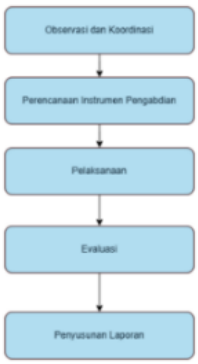
Setelah mengadakan pertemuan dan mengumpulkan informasi dari salah satu ketua RT Kompleks Yadara Babarsari, Yogyakarta, ditemukan bahwa sebagian besar warga di Kompleks ini adalah orang tua yang memiliki tingkat pemahaman yang rendah terkait kesadaran akan bahaya dari *link phishing*. Rendahnya tingkat pemahaman ini disebabkan oleh kurangnya pengetahuan secara mendalam mengenai karakteristik dari *link phishing*. Kurangnya pemahaman tersebut dapat berdampak pada kemampuan orang tua dalam menjaga kerahasiaan informasi data pribadi, terutama dari ancaman pencurian data melalui *link phisihng*. Oleh karena itu, dibutuhkan pendekatan secara efektif melalui sosialisasi. Sosialisasi ini bertujuan untuk meningkatkan kesadaran mengenai ancaman dari *link phishing*, serta memberikan beberapa contoh dari jenis *link phishing*. Sosialisasi ini akan diikuti oleh 35 orang tua dengan gabungan RT.21-26/RW.06 dari Kompleks Yadara Babarsari, Yogyakarta.

Online issn:2829-8268
Print issn:2829-6532

3. Metode

Kegiatan pengabdian ini akan dilaksanakan dengan menggunakan pendekatan secara penyuluhan yang didukung dengan metode partisipatif berupa program sosialisasi. Penyuluhan merupakan aktivitas yang dilaksanakan secara terstruktur, terencana, dan sistematis dengan tujuan mengubah perilaku individu, kelompok, atau masyarakat, berdasarkan kondisi sosial, ekonomi, dan budaya setempat[19]. Sementara itu, metode partisipatif merupakan suatu metode kegiatan pembelajaran yang melibatkan keikutsertaan para peserta. Metode tersebut melibatkan para peserta dalam kegiatan perencanaan, pelaksanaan, dan penilaian mengenai kegiatan pembelajaran[20]. Penggunaan pendekatan dan metode tersebut memungkinkan seluruh anggota tim pengabdian dapat memahami secara langsung mengenai kondisi sosial warga sekaligus dapat terlibat secara aktif dalam proses identifikasi permasalahan. Pendekatan dan metode tersebut dipilih karena kegiatan pengabdian ini berfokus pada upaya peningkatan kesadaran warga, terutama orang tua di Kompleks Yadara Babarsari, Yogyakarta terhadap ancaman *link phishng.*

Pendekatan dalam penelitian ini didukung oleh penelitian yang telah dilakukan sebelumnya pada tahun 2024 yang menggunakan metode partisipatif. Penelitian tersebut melibatkan masyarakat secara langsung dalam seluruh proses pengabdian dan mendapatkan hasil yang menunjukkan kesadaran masyarakat yang meningkat[21]. Dalam mendukung proses pemahaman pada kegiatan pengabdian ini, data akan dikumpulkan melalui formulir *pre-test* dan *post-test* yang akan diberikan kepada peserta sosialisasi yakni orang tua dengan tujuan untuk mengukur tingkat pemahaman terhadap materi yang diberikan. Pelaksanaan kegiatan pengabdian kepada para orang tua di Kompleks Yadara Babarsari, Yogyakarta ini mencakup beberapa tahapan kegiatan yang dilakukan. Berikut adalah tahapan kegiatan pengabdian yang dapat dilihat pada Gambar 2.



Gambar 2. Tahapan Pelaksanaan

3.1. Observasi dan Koordinasi

Pada tahap awal, seluruh anggota tim pengabdian melakukan observasi dan koordinasi di lokasi tempat pengabdian. Kegiatan ini bertujuan untuk memahami kondisi, kebutuhan dasar warga, terutama orang tua dan menetapkan tujuan pelaksanaan pengabdian terkait penggunaan internet dan perangkat digital. Kegiatan ini meliputi beberapa proses yang harus diperhatikan. Tahap pertama adalah melakukan wawancara dengan tujuan untuk mengidentifikasi kebutuhan bersama dengan salah satu perwakilan warga Kompleks Yadara Babarsari, Yogyakarta yakni Ketua RT. Setelah melakukan wawancara, seluruh anggota tim pengabdian akan berdiskusi dan memberikan rekomendasi terkait solusi yang tepat dalam menangani permasalahan yang dihadapi. Lalu, tahap selanjutnya adalah mendapatkan persetujuan dari Ketua RT sekitar mengenai rencana kegiatan pengabdian tersebut.

3.2. Perencanaan Instrumen Pengabdian

Pada tahap ini, seluruh anggota tim pengabdian akan mulai menyusun instrumen kegiatan pengabdian dengan menyiapkan materi edukasi dalam bentuk presentasi yang berisi penjelasan tentang *phishing*, cara mengenalinya, dan langkah pencegahan dengan menggunakan bahasa sederhana dan contoh-contoh nyata

Online issn:2829-8268
Print issn:2829-6532

agar mudah dipahami oleh orang tua. Penyusunan materi akan menggunakan referensi yang diambil dari beberapa sumber seperti jurnal, berita, dan Youtube. Selain itu, materi akan disampaikan dalam bentuk PowerPoint *Presentation*. Dalam mendukung penyampaian materi tersebut, tim pengabdian juga akan menyusun soal *pre-test*, *post-test*, dan kuis dengan tujuan untuk menguji tingkat pemahaman para peserta sebelum dan sesudah penyampaian materi. Sebagai pelengkap, akan dibuat media pendukung seperti gambar ilustratif mengenai ciri-ciri *phishing* dalam presentasi.

3.3. Pelaksanaan

Setelah menyusun instrumen penelitian, tahapan selanjutnya adalah seluruh anggota tim pengabdian melaksanakan kegiatan pengabdian ini secara langsung kepada warga khususnya orang tua di Kompleks Yadara Babarsari, Yogyakarta. Pada tahap ini, seluruh anggota tim pengabdian akan memaparkan dan menjelaskan materi tentang *link phishing*, ciri-cirinya, dan cara menghindari serta mengatasinya. Penyampaian materi akan dilakukan selama 100 menit dalam satu kali pertemuan dengan interaktif agar para orang tua lebih mudah memahami dan sadar mengenai ancaman *link phishing* yang muncul melalui internet atau pesan singkat. Sebelum menyampaikan materi, seluruh anggota tim pengabdian akan membagikan formulir *pre-test* untuk mengukur tingkat pemahaman para peserta mengenai tindakan penipuan berupa *link phishing*. Selanjutnya, tim pengabdian akan memberikan kuis sederhana kepada peserta sebelum sesi penyampaian materi berakhir. Setelah materi selesai disampaikan secara keseluruhan, tim pengabdian akan menyebarkan formulir *post-test* kepada para peserta dengan tujuan untuk mengetahui tingkat pemahaman peserta dalam membedakan *link phishing*.

3.4. Evaluasi

Setelah melaksanakan kegiatan pengabdian, tim pengabdian akan melakukan evaluasi terhadap kegiatan pengabdian ini. Evaluasi tersebut akan diukur dari hasil pengerjaan *post-test* saat kegiatan pengabdian tersebut. Hasil pengerjaan *post-test* yang menggunakan skala Likert berupa evaluasi yang nantinya menjadi pedoman dasar dalam mengetahui efektivitas kegiatan pengabdian yang telah dilaksanakan.

3.5. *Penyusunan Laporan*

Pada tahap terakhir, seluruh anggota tim akan melakukan penyusunan laporan kegiatan pengabdian yang mencakup seluruh tahapan yang dimulai dari observasi hingga evaluasi secara lengkap. Laporan tersebut akan disertai dengan dokumentasi dan hasil kegiatan pengabdian yang telah dilaksanakan.

Tabel 1. *Timeline* Pengabdian

Kegiatan	**Maret**				**April**			
	1	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Melakukan Observasi dan Koordinasi								
Perencanaan Instrumen Pengabdian								
Pelaksanaan								
Evaluasi								
Penyusunan Laporan								

Tabel 1 menunjukkan *timeline* kegiatan pengabdian yang dilakukan oleh tim pengabdian yang dimulai dari tahap observasi dan koordinasi sampai dengan tahap penyusunan laporan pada minggu pertama bulan Maret sampai dengan minggu keempat bulan April. Kegiatan observasi dan koordinasi mencakup aktivitas

Online issn:2829-8268
Print issn:2829-6532

wawancara identifikasi kebutuhan dan koordinasi persetujuan dengan perwakilan warga Kompleks Yadara Babarsari, Yogyakarta yaitu Ketua RT pada hari Senin, 24 Maret 2025 selama 90 menit pada pukul 08.00-09.30 WIB. Selanjutnya, tim pengabdian merancang instrumen pendukung kegiatan pengabdian berupa materi, soal *pre-test*, soal *post-test*, dan kuis sederhana pada minggu kedua sampai dengan minggu keempat bulan Maret. Kemudian, pada hari Rabu, 16 April 2025 tim pengabdian melaksanakan kegiatan pengabdian berupa sosialisasi selama 100 menit yang dimulai dari pukul 15.50 WIB sampai dengan pukul 17.30 WIB dan dilanjutkan dengan kegiatan evaluasi berupa peninjauan pelaksanaan pengabdian dan hasil *pre-test* dan *post-test* di hari Sabtu, 19 April 2025. Setelah melakukan evaluasi kegiatan, tim pengabdian mulai menyusun laporan dari minggu ketiga sampai dengan minggu keempat bulan April.

Tabel 2. Target dan Luaran

Aspek	Kegiatan	Target Luaran	Spesifikasi
Pemahaman mengenai keamanan informasi	Pengenalan mengenai pengetahuan dasar keamanan informasi dan ancaman *link phishing*	Orang tua dapat memahami tentang pentingnya menjaga data pribadi dan dapat mengenali ciri-ciri *link phishing*	Penggunaan media presentasi berupa *PowerPoint* yang menggunakan bahasa sederhana dan disertakan kasus nyata yang mudah dipahami
Kemampuan mengidentifikasi dan menghindari *link phishing*	Memberikan pelatihan interaktif untuk menguji dan mengetahui tingkat pemahaman dengan menggunakan contoh yang didapat dari pesan *Whatsapp*, internet, media sosial, dan *email*	Orang tua memiliki keterampilan dasar dalam mengidentifikasi ancaman *phishing* yang mencurigakan dan mengetahui tindakan pencegahan dan penanganannya	Penggunaan kuis interaktif berbasis gambar yang memuat contoh *link phishing* sebagai sarana pelatihan.

Pada Tabel 2, dijelaskan bahwa kegiatan pengabdian berfokus untuk meningkatkan pemahaman orang tua dalam menjaga keamanan informasi dan mengenali ancaman *link phishing*. Kegiatan dilakukan secara langsung yang meliputi dua aktivitas utama, yaitu penyampaian materi presentasi dengan PowerPoint dan pelatihan interaktif dengan menggunakan kuis yang didukung media berupa contoh *link phishing.*

Seluruh materi dirancang sedemikian rupa dan disampaikan dengan bahasa yang sederhana, mudah dimengerti, serta dilengkapi contoh kasus nyata yang sering ditemui sehari-hari, seperti pesan mencurigakan di *WhatsApp*, *email*, dan *Short Message Service* atau SMS. Kegiatan sosialisasi akan didukung dengan pelatihan interaktif berbasis kuis dan pertanyaan sederhana, sehingga para orang tua dapat lebih mudah memahami ciri-ciri *phishing* dan cara menanganinya.

4. Hasil dan Pembahasan

Peningkatan Literasi Digital melalui Pelatihan Keamanan Informasi Terkait Ancaman *Link Phishing* di Kompleks Yadara Babarsari, Yogyakarta dilaksanakan pada tanggal 16 April 2025 selama 100 menit.

Tabel 3. *Rundown* Pengabdian

Waktu (WIB)	Jumlah Peserta	Kegiatan	Penanggung Jawab
15.50-16.00	35 Orang tua	Pengerjaan *Pre-test*	Erlan Frylin Lamba, Faiz Rizq Farhanna, Noel Yudistira, dan Robin Jauhari
16.00-17.15		Pemaparan Materi	
17.15-17.20		Pengerjaan Kuis	
17.20-17.30		Pengerjaan *Post-test*	

Online issn:2829-8268
Print issn:2829-6532

Pada Tabel 3 menunjukkan bahwa sosialisasi tentang peningkatan literasi digital melalui pelatihan keamanan informasi terkait ancaman *link phishing* di Kompleks Yadara Babarasari Yogyakarta dilakukan secara langsung atau tatap muka. Sosialisasi ini dilaksanakan di Pendopo Kompleks Yadara Babarsari, Yogyakarta selama 100 menit dan diikuti oleh 35 orang tua yang tinggal di Kompleks Yadara Babarsari, Yogyakarta. Sosialisasi ini meliputi 4 kegiatan, yaitu pengerjaan *pre-test*, pemaparan materi, pengerjaan kuis, dan pengerjaan *post-test*. Tujuan dari sosialisasi ini adalah untuk meningkatkan digital literasi keamanan informasi dan menyampaikan pemahaman yang lebih luas tentang ancaman dari *link phishing*, sehingga para orang tua dapat mengenali dan paham akan ancaman *link phishing* serta dapat meningkatkan keamanan data dan informasi pribadi sebagai kebutuhan sehari-hari.

Dalam mendukung kegiatan pengabdian ini, seluruh anggota tim membuat materi sosialisasi, soal *pre-test* dan *post-test*, serta kuis sederhana yang dirancang sesuai dengan kebutuhan dan kriteria orang tua di Kompleks Yadara Babarsari, Yogyakarta.

4.1. Materi Sosialisasi Ancaman Link Phishing

Materi Sosialisasi mengenai tindakan penipuan berupa *phishing* disusun dengan memanfaatkan Aplikasi Canva sebagai media utama. Materi ini ditujukan untuk warga khususnya orang tua di Kompleks Yadara dengan tujuan meningkatkan pemahaman tentang penipuan *phishing* serta solusi dari penipuan *phishing*. Dalam materi ini, peserta akan diperkenalkan pada pengertian, jenis-jenis, karakteristik, cara kerja, dan solusi dari ancaman *link phishing*. Selain itu, materi ini menyertakan contoh nyata dari penipuan berupa *link phishing* sebagai pedoman dan panduan dalam mengerjakan soal *pre-test* dan *post-test*, serta kuis sederhana. Untuk memperjelas pemahaman, materi ini dilengkapi dengan kasus nyata dan solusinya yang bisa diterapkan audiens. Referensi yang digunakan berasal dari berbagai sumber seperti jurnal, berita, dan video pembelajaran di YouTube.

Gambar 3. Pembuatan Materi dengan Canva

Gambar 4. Pembuatan Materi dengan Canva

4.2. Soal Pre-test, Post-test, dan Kuis Sederhana

Soal *pre-test* dirancang dengan tujuan untuk mengukur pengetahuan dan pemahaman para peserta mengenai ancaman dari *link phishing* sebelum kegiatan pemaparan materi, sedangkan soal *post-test* dirancang untuk menguji tingkat pemahaman para peserta dalam mengenali *link phishing*. Hasil dari *post-test* ini akan menjadi bahan evaluasi bagi seluruh anggota tim pengabdian dalam mengukur tingkat keberhasilan sosialisasi peningkatan kesadaran keamanan informasi terkait ancaman *link phishing* ini. Soal *pre-test* berisi lima pertanyaan yang mencakup pemahaman peserta tentang *link phishing*, ciri-ciri tautan mencurigakan, pengetahuan mengenai tindakan yang harus dilakukan saat menerima *link* mencurigakan, serta pemahaman umum mengenai keamanan informasi di internet. Sementara itu, soal *post-test* juga berisi lima pertanyaan yang menilai tentang kemudahan memahami materi, kesesuaian waktu kegiatan, kejelasan penyampaian, manfaat materi bagi peserta, serta peningkatan pemahaman peserta dalam menghindari *link* penipuan setelah dilakukannya penyampaian materi. Kedua instrumen tersebut disusun dengan menggunakan skala Likert lima poin yaitu: sangat tidak setuju, tidak setuju, netral, setuju, dan sangat setuju. Selain itu, terdapat soal kuis sederhana sejumlah 1 soal yang digunakan untuk memperkuat pemahaman para peserta saat kegiatan sosialisasi. Kuis tersebut akan ditampilkan setelah pemaparan materi, dan peserta akan menjawabnya secara langsung.

Online issn:2829-8268
Print issn:2829-6532

Gambar 5. Kuis sederhana

Para peserta akan mengerjakan *pre-test* secara langsung dan dibantu oleh tim pengabdian dengan durasi pengerjaannya selama 10 menit sebelum kegiatan pemaparan materi. Setelah pemaparan materi selesai, terdapat kuis sederhana berjumlah 1 soal untuk mengukur tingkat pemahaman peserta dalam mengenali ciri-ciri *link phishing*. Kuis tersebut ditujukan untuk semua peserta secara langsung dan interaktif dengan durasi selama 5 menit. Selanjutnya, para peserta akan mengerjakan soal *post-test* secara mandiri selama 10 menit setelah dilaksanakannya kegiatan pemaparan materi dan penyampaian kuis sederhana.

Gambar 6. Pemaparan Materi

Gambar 7. Pemaparan Materi

Gambar 6 dan Gambar 7 memperlihatkan dokumentasi kegiatan pemaparan materi yang dilakukan oleh tim pengabdian. Gambar tersebut menunjukkan tim pengabdian menjelaskan materi tentang ancaman *link phishing* kepada para peserta selama 75 menit. Pada kegiatan ini, komitmen dan keterlibatan tim pengabdian dalam penyampaian materi tercermin dengan baik, sehingga para peserta diharapkan dapat memperoleh pengetahuan mengenai pemahaman secara komprehensif tentang peningkatan digital literasi keamanan informasi terkait ancaman *link phishing.*

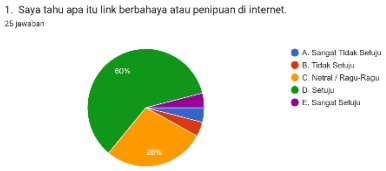
Gambar 8. Pengerjaan *Pre-test*

Gambar 9. Pengerjaan *Post-test*

Gambar 8 dan 9 menunjukkan dokumentasi saat para peserta sedang mengerjakan soal *pre-test* dan *post-test* dengan bantuan dan pantauan dari tim pengabdian. Pada gambar tersebut, terlihat para peserta secara aktif terlibat dalam mengerjakan soal yang diberikan dengan bantuan tim pengabdian jika dibutuhkan. Hal ini menunjukkan komitmen tim pengabdian dalam memastikan bahwa setiap warga mendapatkan dukungan atau bantuan yang diperlukan selama proses sosialisasi, sehingga para warga dapat mendapatkan pemahaman yang mendalam tentang peningkatan literasi digital melalui keamanan informasi terkait ancaman *link phishing*.

Online issn:2829-8268
Print issn:2829-6532

Pre-test

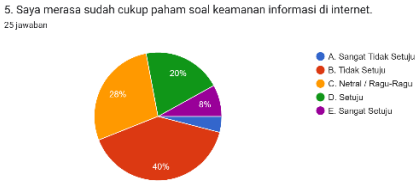


Gambar 10. Hasil *pre-test* pengetahuan *link* berbahaya atau penipuan di internet

Gambar 11. Hasil *pre-test* kesadaran membuka *link* sembarangan bisa berbahaya

Gambar 12. Hasil *pre-test* mengenali ciri-ciri *link* mencurigakan

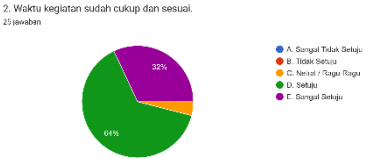
Gambar 13. Hasil *pre-test* mengetahui tindakan yang harus dilakukan jika menerima *link* mencurigakan



Gambar 14. Hasil *pre-test* pemahaman keamanan informasi di internet

Post-test

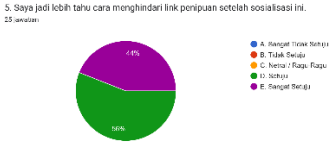
Gambar 15. Hasil *post-test* penjelasan sosialisasi mudah dimengerti



Gambar 16. Hasil *post-test* waktu kegiatan sosialisasi sudah cukup dan sesuai

Gambar 17. Hasil *post-test* penyampaian materi jelas dan menarik

Gambar 18. Hasil *post-test* penyampaian materi bermanfaat untuk para peserta



Gambar 19. Hasil *post-test* lebih tahu cara menghindari *link phishing* setelah sosialisasi

Online issn:2829-8268
Print issn:2829-6532

Sosialisasi peningkatan kesadaran informasi terkait ancaman *link phishing* memperlihatkan hasil yang positif dalam meningkatkan kesadaran dan pemahaman peserta tentang pentingnya menjaga keamanan informasi terhadap ancaman *link phishing* dan cara menerapkan pencegahannya dalam kehidupan sehari-hari. Hasil *pre-test* menunjukkan bahwa sebagian besar responden (96%) menyatakan setuju dan sangat setuju bahwa mereka sadar membuka *link* sembarangan dapat berbahaya. Mayoritas responden (64%) juga menyatakan paham mengenai *link* berbahaya atau penipuan di internet. Namun demikian, hanya sebagian kecil responden (24%) yang setuju dan sangat setuju bahwa mereka dapat mengenali ciri-ciri *link* yang mencurigakan. Selain itu, hanya 48% responden yang menyatakan paham tindakan yang harus dilakukan jika menerima *link* mencurigakan, dan sebanyak 28% responden menyatakan memahami konsep dasar keamanan informasi.

Berdasarkan temuan ini, dapat disimpulkan bahwa meskipun tingkat kesadaran akan bahaya *link* sembarangan cukup tinggi, kemampuan mengenali dan menindaklanjuti ancaman tersebut masih tergolong rendah. Oleh karena itu, perlu dilakukan kegiatan penyuluhan dan pelatihan terkait *link phishing* dan keamanan informasi bagi kalangan orang tua di Kompleks Yadara Babarsari, Yogyakarta.

Setelah kegiatan penyuluhan dilaksanakan, hasil *post-test* menunjukkan peningkatan yang signifikan. Sebagian besar responden (98%) menyatakan setuju dan sangat setuju bahwa mereka menjadi lebih memahami cara menghadapi serangan *link phishing* setelah mengikuti sosialisasi. Selain itu, sebagian besar (96%) responden juga menyatakan bahwa materi yang disampaikan bermanfaat bagi mereka. Temuan ini menunjukkan bahwa penyuluhan dan pelatihan terkait *link phishing* bagi kalangan orang tua di Kompleks Yadara Babarsari, Yogyakarta, telah memberikan dampak positif.

Kegiatan pengabdian berupa penyuluhan tersebut telah mencapai target luaran yaitu orang tua di Kompleks Yadara Babarsari, Yogyakarta dapat memahami tentang pentingnya menjaga data pribadi dan dapat mengenali ciri-ciri *link phishing* berdasarkan temuan sebelumnya yakni hasil *pre-test* dan *post test* yang ditunjukkan sebagai indikator keberhasilan dalam mencapai target luaran di kegiatan pengabdian ini.

Gambar 20. Foto bersama dengan Ketua RT dan Ketua RW

Dengan demikian, kegiatan penyuluhan keamanan informasi terkait ancaman *phishing* untuk meningkatkan literasi digital pada warga Kompleks Yadara Babarsari Yogyakarta berhasil dilaksanakan dengan baik dan mendapat respons positif dari warga Kompleks Yadara Babarsari, Yogyakarta. Sebagai penutup, tim pengabdian melakukan sesi foto bersama dengan perwakilan warga yaitu Ketua RT dan Ketua RW di Kompleks Yadara Babarsari, Yogyakarta sebagai bentuk dokumentasi atas selesainya kegiatan ini.

5. Kesimpulan

Hasil *pre-test* di Kompleks Yadara Babarsari, Yogyakarta menunjukkan bahwa sebagian besar orang tua belum memiliki pemahaman yang mendalam mengenai kesadaran informasi dalam menghadapi ancaman *link phishing.* Dalam mengatasi hal tersebut, dilakukan kegiatan penyuluhan dan pelatihan yang melibatkan 35 orang tua serta didukung dengan media pembelajaran secara sederhana dan kreatif. Hasil *post-test* menunjukkan peningkatan yang signifikan dalam pengetahuan orang tua mengenai pentingnya menjaga keamanan informasi dalam menghadapi ancaman *link phishing*. Persentase orang tua yang mengetahui ciri-ciri *link* mencurigakan meningkat dari 16% menjadi 56% menunjukkan keberhasilan dalam penyampaian

Online issn:2829-8268
Print issn:2829-6532

materi secara efektif. Selain itu, persentase sebagian besar responden sebanyak (96%) yang menyatakan sangat setuju dan setuju memperlihatkan bahwa materi yang disampaikan bermanfaat bagi para peserta.

Meskipun kegiatan sosialisasi menunjukkan hasil yang positif, masih terdapat ruang untuk perbaikan dalam pelaksanaannya. Memperpanjang durasi kegiatan penyuluhan serta melakukan kegiatannya menjadi beberapa temuan merupakan saran dari tim pengabdian untuk kegiatan sosialisasi kedepannya. Sementara itu, berdasarkan temuan yang didapat hasil *pre-test* dan *post-tes*t menunjukkan bahwa kegiatan pelatihan berupa sosialisasi efektif dalam meningkatkan literasi digital melalui pelatihan keamanan informasi pada orang tua dalam menghadapi ancaman *link phishing.* Selain itu, aktivitas evaluasi kegiatan juga bermanfaat untuk mengidentifikasi kebutuhan perbaikan, khususnya terkait durasi sosialisasi dan strategi penyampaian materi dengan tujuan menjadikan kegiatan sosialisasi menjadi lebih menarik dan efektif di masa mendatang.

6. Ucapan Terima Kasih

Kelancaran pelaksanaan kegiatan pengabdian ini tentunya berkat dukungan dan bantuan dari pihak yang telah bekerja sama dengan baik. Ucapan terima kasih untuk dosen pengampu mata kuliah Teknologi Informasi Untuk Masyarakat, Ibu Kristina Wulandari, S.T., M.Kom, dosen pembimbing Ibu Citra Yayu' Palangan, S.T., M.Sc, pihak Universitas Atma Jaya Yogyakarta, dan kepada seluruh pihak Kompleks Yadara Babarsari, Yogyakarta yang telah menerima dan memberikan respons positif terhadap kegiatan pengabdian ini.

7. Referensi

[1] P. Reddy, B. Sharma, and K. Chaudhary, "Digital literacy: A review of literature," *Int J Technoethics*, vol. 11, no. 2, pp. 65–94, 2020, doi: 10.4018/IJT.20200701.oa1.

[2] S. T. Zahwani[1], M. Irwan, and P. Nasution[2], "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital," *Analisis Kesadaran Masyarakat (Zahwani, dkk.) JoSES: Journal of Sharia Economics Scholar*, vol. 2, no. 2, pp. 105–109, 2023, [Online]. Available: https://doi.org/10.5281/zenodo.12608751

[3] N. Vadila and A. R. Pratama, "Analisis Kesadaran Keamanan Terhadap Ancaman Phishing," *Automata*, vol. 2, no. 2, pp. 1–4, 2021.

[4] N. B. Putri and A. W. Wijayanto, "Analisis Komparasi Algoritma Klasifikasi Data Mining Dalam Klasifikasi Website Phishing," *Komputika : Jurnal Sistem Komputer*, vol. 11, no. 1, pp. 59–66, 2022, doi: 10.34010/komputika.v11i1.4350.

[5] B. Wibowo and T. Hidayat, "Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ," *Jurnal Pengabdian Masyarakat Sultan Indonesia*, vol. 2, no. 1, pp. 1–9, 2024, doi: 10.58291/abdisultan.v2i1.294.

[6] L. A. Febrika Ardy, I. Istiqomah, A. E. Ezer, and S. N. Neyman, "Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial," *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 11, 2024, doi: 10.47134/pjise.v1i4.2753.

[7] M. A. Al Fadillah, M. G. Ramadhan, and M. Erza, "Analisis Ancaman Phishing terhadap Penggunaan E-Commerce di Indonesia," vol. 5, no. 2, pp. 85–96, 2024.

[8] N. Beu *et al.*, "Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation," *Comput Secur*, vol. 131, p. 103313, 2023, doi: 10.1016/j.cose.2023.103313.

[9] E. Ginting, M. P. Sinaga, M. R. Nurdin, and M. D. Putra, "Analisis Ancaman Phising Terhadap Layanan Online Perbankan (Studi Kasus Pada Bank BRI)," *UNES Journal of Scientech Research*, vol.

Online issn:2829-8268
Print issn:2829-6532

8, no. 1, pp. 41–47, 2023, [Online]. Available: https://www.bantenraya.com/nasional/pr-1275958726/awas-penipuan-whatsapp-kurir-paket-pakai-metode-phising-kirim-foto-berisi-aplikasi

[10]A. Ramadhan, M. Alwi Alhafidh, and M. Diki Firmansyah, "Penyebaran Link Phising Kuota Kemendikbud Terhadap Kesadaran," *KAMPRET Jurnal*, vol. 1, no. 2, pp. 11–16, 2022, [Online]. Available: https://plus62.isha.or.id/index.php/kampret/article/view/9

[11]A. Bhagaskoro, M. R. Pramadansyah, and M. N. Adiputra, "Penyuluhan Bahaya Phising Untuk Mening katkan Kesadaran Keamanan Digital," vol. 2022, 2023, doi: 10.59328/JAPATUM.2023.2.2.57.

[12]M. W. A. Prastya, M. Tahir, A. A. Ningrum, and A. P. Zaibintoro, "Analisis Ancaman Pishing melalui Aplikasi WhatsApp : Review Metode Studi Analisis Ancaman Pishing melalui Aplikasi WhatsApp : Review Metode Studi Literatur," no. May, 2024, doi: 10.32672/jnkti.v7i3.7551.

[13]I. Hadi Ramadhan and E. Kumalasari Nurnawati, "Analisis Ancaman Phishing Dalam Layanan E-Commerce," *Prosiding Snast*, no. November, pp. E31-41, 2022, doi: 10.34151/prosidingsnast.v8i1.4169.

[14]W. R. Hendra, M. A. Imam, and S. P. Lindiasari, "Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19," *Iptek-Kom*, vol. 22, no. 2, pp. 143–158, 2020, [Online]. Available: https://jurnal.kominfo.go.id/index.php/iptekkom/article/view/3505

[15]A. Muftiadi, T. P. M. Agustina, and M. Evi, "Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking," *Hexatech: Jurnal Ilmiah Teknik*, vol. 1, no. 2, pp. 60–65, 2022, doi: 10.55904/hexatech.v1i2.346.

[16]H. Sampul, "SKRIPSI Oleh : Maharlina Darni Purwandari FAKULTAS BISNIS DAN EKONOMIKA UNIVERSITAS ISLAM INDONESIA YOGYAKARTA," 2024.

[17]P. N. Islam, R. D. Ahwadti, M. Rizky, and A. Prakoso, "Analisis Dampak Kesadaran Keamanan Informasi User Whatsapp terhadap penyebaran Phising Malware ' Undangan . APK ,'" pp. 524–530, 2024.

[18]B. A. Souhoka, R. A. Fadillah, and M. Fathan, "Analisis Strategi Pencegahan Phising Studi Kasus Pada Media Sosial Facebook," vol. 3, no. 1, pp. 10–22, 2025.

[19]K. Sulandjari, A. Abubakar, and D. Agustina, "Penyuluhan Pengolahan Ikan Bandeng Menjadi Aneka Produk Olahan Dalam Rangka Meningkatkan Pendapatan Masyarakat Desa Karyamakmur," *Abdi Masyarakat*, vol. 4, no. 2, 2022, doi: 10.58258/abdi.v4i2.4244.

[20]A. Hadita, R. Yusuf, and E. D. Darmawan, "Metode Partisipatif Pada Pelatihan Financial Life Skills Untuk Meningkatkan Literasi Keuangan Pengajar Tridaya Group Bandung," *Sebatik*, vol. 25, no. 1, pp. 188–194, 2021, doi: 10.46984/sebatik.v25i1.1266.

[21]M. Atik and S. Ekowati, "Sosialisasi Tentang Pemberdayaan Masyarakat Desa Berbudaya Dalam Meningkatkan Pembelajaran Menuju Desa Unggul (Studi Kasus Desa Gedangsasri , Kab Gunung Kidul)," vol. 2, no. 6, pp. 162–177, 2024.