

## Edukasi Bahaya *Link Phishing* Untuk Meningkatkan Kesadaran Keamanan Digital Pada Ibu-Ibu PKK

Rosmalia Anggraeni<sup>1</sup>, Sandikha Bayu Pratama<sup>2</sup>, Diva Nurhafizha Uswendi<sup>3</sup>, Hifni Wafi Abiyya Achmad<sup>4</sup>, Debi Sela<sup>5</sup>, Latifah<sup>6</sup>, Niko Ikmal Wirawan<sup>7</sup>, Fitri Aulia Insani<sup>8</sup>, Avila Marsa Salsabila<sup>9</sup>, Mufida Salsabila<sup>10</sup>, Alan Dharmawan<sup>11</sup>, Shafa Ainun Nabila<sup>12</sup>, Figih Roni Mahendra<sup>13</sup>, Muhammad Kamal Burhanudin<sup>14</sup>, Anaf Rafitno<sup>15</sup>, Hidayatus Sibyan<sup>16\*</sup>

<sup>1</sup>Fakultas Bahasa dan Sastra, Sastra Inggris, Universitas Sains Al-Qur'an, Wonosobo, Indonesia

<sup>2, 3, 4, 7, 8, 11, 13, 14, 15, 16</sup> Fakultas Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Sains Al-Qur'an, Wonosobo, Indonesia

<sup>5, 6, 9, 10</sup> Fakultas Ilmu Tarbiyah dan Keguruan, Pendidikan Agama Islam, Universitas Sains Al-Qur'an, Wonosobo, Indonesia

<sup>12</sup> Fakultas Teknik dan Ilmu Komputer, Teknik Sipil, Universitas Sains Al-Qur'an, Wonosobo, Indonesia

Email: <sup>1</sup>[rosmalia.an@gmail.com](mailto:rosmalia.an@gmail.com), <sup>2</sup>[sandikhabayupratama@gmail.com](mailto:sandikhabayupratama@gmail.com), <sup>3</sup>[divanurhafizha28@mhs.unsiq.ac.id](mailto:divanurhafizha28@mhs.unsiq.ac.id),

<sup>4</sup>[abiyyaachmad@mhs.unsiq.ac.id](mailto:abiyyaachmad@mhs.unsiq.ac.id), <sup>5</sup>[debysella12237@gmail.com](mailto:debysella12237@gmail.com), <sup>6</sup>[latifaah800@gmail.com](mailto:latifaah800@gmail.com),

<sup>7</sup>[nicoikmal@gmail.com](mailto:nicoikmal@gmail.com), <sup>8</sup>[fitriauliainsani2@gmail.com](mailto:fitriauliainsani2@gmail.com), <sup>9</sup>[avilamarsa55@gmail.com](mailto:avilamarsa55@gmail.com),

<sup>10</sup>[mufida2s2s@gmail.com](mailto:mufida2s2s@gmail.com), <sup>11</sup>[dharmawanalan@gmail.com](mailto:dharmawanalan@gmail.com), <sup>12</sup>[shafaainunnabila30@gmail.com](mailto:shafaainunnabila30@gmail.com),

<sup>13</sup>[figihroni@proton.me](mailto:figihroni@proton.me), <sup>14</sup>[kamalburhan185@gmail.com](mailto:kamalburhan185@gmail.com), <sup>15</sup>[arafikno@gmail.com](mailto:arafikno@gmail.com), <sup>16\*</sup>[hsibyan@unsiq.ac.id](mailto:hsibyan@unsiq.ac.id)

(\* : coresponding author)

**Abstrak** – Perkembangan teknologi digital yang semakin pesat memberikan kemudahan dalam kehidupan sehari-hari, namun juga membuka peluang terjadinya kejahatan digital, salah satunya *phishing*. *Phishing* merupakan upaya penipuan dengan memanfaatkan tautan atau pesan palsu untuk mencuri data pribadi pengguna. Kelompok dewasa dan lanjut usia, termasuk ibu-ibu PKK, menjadi kelompok yang rentan karena tingginya penggunaan aplikasi pesan instan tanpa diimbangi pemahaman keamanan digital yang memadai. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan kesadaran dan pemahaman ibu-ibu PKK Desa Salam terhadap bahaya *link phishing*, khususnya yang tersebar melalui aplikasi WhatsApp. Metode yang digunakan adalah pendekatan deskriptif kualitatif melalui kegiatan sosialisasi dan diskusi interaktif. Data dikumpulkan melalui observasi, tanya jawab, serta dokumentasi kegiatan. Hasil kegiatan menunjukkan adanya respons positif dan peningkatan pemahaman peserta terhadap ciri-ciri *phishing* serta langkah pencegahan yang dapat dilakukan. Dengan demikian, sosialisasi keamanan digital ini dinilai efektif sebagai upaya preventif dalam meningkatkan literasi keamanan digital masyarakat desa.

**Kata Kunci:** *Phishing*, Keamanan Digital, Literasi Digital, Ibu-Ibu PKK, WhatsApp

**Abstract** – The rapid development of digital technology provides convenience in daily life but also increases the risk of digital crimes, one of which is *phishing*. *Phishing* is a fraudulent attempt that exploits fake links or messages to steal users' personal information. Adults and the elderly, including PKK women, are considered vulnerable groups due to their high use of instant messaging applications without sufficient digital security awareness. This community service activity aims to enhance awareness and understanding of the dangers of *phishing* links among PKK women in Salam Village, particularly those spread through WhatsApp. A qualitative descriptive approach was employed through socialization activities and interactive discussions. Data were collected through observation, question-and-answer sessions, and documentation. The results indicate positive responses and improved participants' understanding of *phishing* characteristics and preventive measures. Therefore, this digital security socialization activity is considered effective as a preventive effort to improve digital security literacy in rural communities.

**Keywords:** *Phishing*, Digital Security, Digital Literacy, PKK Women, WhatsApp

## 1. PENDAHULUAN

Perkembangan teknologi telah memberi banyak manfaat bagi kehidupan manusia. Kemajuannya telah menyediakan berbagai fitur yang mempermudah dan memberikan kenyamanan dalam hidup manusia. Tak bisa dipungkiri bahwa kemajuan teknologi berkembang begitu pesat, maka masyarakat perlu memiliki kemampuan untuk memahami sekaligus menyesuaikan kemajuan teknologi. Edukasi terkait dunia digital tak hanya mencakup bagaimana cara menggunakannya dengan benar, tetapi juga mencakup pemahaman bahwa terdapat risiko dan ancaman di balik kemutakhirannya. Teknologi memang memberikan banyak sekali kemudahan. Tetapi kemudahan

itu pula yang mempermudah pihak tak bertanggungjawab untuk melakukan aksi kejahatan. Salah satunya adalah kejahatan *phishing*.

*Phishing* adalah tindakan memperdaya seseorang agar dapat memperoleh informasi pribadi seperti *username*, kata sandi, bahkan informasi perbankan yang dilakukan dengan cara mengirim pesan, email, atau *website* palsu (Tabrani, Safitri, Nayla P, & Hosnah, 2024). Biasanya pesan disamarkan dalam bentuk yang dapat dipercaya, seolah-olah dikirim oleh pihak resmi seperti instansi pemerintah, perbankan, atau layanan publik lainnya (*National Institute of Standards and Technology*, 2023). Bahkan dalam kasus terbaru, modus *phishing* telah berkembang ke dalam bentuk yang lebih bervariasi, seperti akun *customer service* palsu, QRIS palsu, dan lampiran *file .apk* yang sedang marak terjadi (Anwari, 2025). Pelaku semakin kreatif merancang berbagai skenario yang menyerupai aktivitas sehari-hari, seperti pesan undangan digital, informasi bantuan sosial, pemberitahuan paket, hingga akun yang mengatasnamakan layanan pelanggan. Selain tautan mencurigakan, pesan-pesan tersebut seringkali disertai lampiran *file* yang tampak meyakinkan sehingga sulit diidentifikasi sebagai penipuan oleh masyarakat awam.

Salah satu media yang sering digunakan sebagai media penyebaran *phishing* adalah WhatsApp. Aplikasi ini telah digunakan secara masif oleh berbagai usia, termasuk kalangan dewasa bahkan lansia. Fitur praktis dalam WhatsApp dimanfaatkan masyarakat sebagai sarana berkomunikasi dalam kehidupan sehari-hari. Namun tingginya tingkat penggunaan WhatsApp menjadikannya sasaran yang empuk untuk mencari korban yang dapat diperdaya kejahatan digital. Pesan-pesan menipu tersebut seringkali disertai tautan ataupun aplikasi

Berdasarkan konteks tersebut, edukasi mengenai keamanan digital menjadi kebutuhan yang mendesak. Khususnya bagi masyarakat yang sudah aktif menggunakan layanan digital tetapi belum memiliki pemahaman yang cukup mengenai potensi ancaman di dalamnya. Kegiatan pengabdian kepada masyarakat merupakan kesempatan yang tepat untuk berbagi pengetahuan yang dapat disampaikan dengan praktis dan kontekstual, sehingga lebih mudah diterima dan dipahami oleh masyarakat.

Bahkan individu yang memiliki pengetahuan baik tentang teknologi tetap dapat menjadi korban *phishing*, apalagi jika tidak paham dan awam dengan perkembangan teknologi. Sebuah studi menunjukkan bahwa kecenderungan seseorang terjebak tautan *phishing* tidak melihat latar belakang pendidikan maupun pengalaman seseorang secara teknis dalam bidang teknologi (Aljeaid, Alzhirani, Alrougi, & Almalki, 2020).

Data dari Otoritas Jasa Keuangan menunjukkan sebagian besar laporan penipuan *online* yang masuk pada tahun 2025 didominasi oleh kaum perempuan terutama ibu-ibu (WartaEkonomi, 2025). Hal ini menjadikan kalangan Ibu-ibu menjadi kaum yang cukup rentan terhadap modus kejahatan *online*. Hal ini mempertimbangkan ibu rumah tangga sebagai pengelola komunikasi dan pemegang keuangan keluarga. Maka dari itu, penting bagi masyarakat umum terutama ibu-ibu untuk memiliki pengetahuan mengenai kejahatan digital seperti *phishing*.

*Phishing* memiliki dampak yang serius bagi siapa pun yang menjadi korbannya. Dampak yang dapat dialami berupa kerugian finansial, kerusakan reputasi, stress, dan trauma (Fathonah, Firganefi, Jatmiko, Muda, & Diana, 2025). Kerugian finansial dapat terjadi secara langsung setelah informasi perbankan korban bocor. Korban dapat mengalami kerusakan reputasi setelah pelaku *phishing* menyalahgunakan identitas korban dan melakukan tindakan tidak pantas. Korban juga akan mengalami stress dan tekanan mental karena kejadian tidak menyenangkan tersebut. Setelah terkena dampak *phishing*, korban baik individu maupun bisnis dapat menjadi lebih rentan menjadi target untuk serangan lebih lanjut.

Kelompok dewasa dan lanjut usia termasuk salah satu kelompok yang rentan terhadap kejahatan digital. Hal ini dipertimbangkan dengan penggunaan perangkat digital yang sudah umum di kalangan dewasa ke atas, tapi tidak diiringi dengan adaptasi terhadap modus kejahatan digital yang terus berubah. Hal ini mengakibatkan adanya kesenjangan antara penggunaan dan pemahaman terhadap keamanannya.

Berangkat dari kondisi tersebut, tim pengabdian menyusun sebuah program kerja unggulan guna meningkatkan pemahaman masyarakat terhadap keamanan digital, khususnya *phishing* yang menyebar di aplikasi populer seperti WhatsApp. Tim pengabdian bertempat di Desa Salam, Kecamatan Gebang, Kabupaten Purworejo.

Desa Salam adalah sebuah desa kecil dengan jumlah penduduk sebanyak 581 jiwa. Mata pencaharian kebanyakan penduduk mengandalkan pertanian dan perkebunan. Berdasarkan hasil observasi awal, banyak dari penduduk di Desa Salam berasal dari kalangan dewasa dan lanjut usia yang aktif menggunakan gawai. Dalam hal ini juga aplikasi pesan instan dan media sosial, termasuk WhatsApp sebagai aplikasi yang sangat umum digunakan sebagai aplikasi utama yang digunakan untuk berkomunikasi. Dengan hasil pengamatan tersebut serta komposisi tim pengabdian yang didominasi oleh mahasiswa program studi Teknologi Informasi, kegiatan yang berfokus pada peningkatan literasi keamanan digital menjadi program yang potensial untuk dilaksanakan di desa tersebut. Tak hanya menjadi potensi, tapi dengan adanya mahasiswa dengan latar belakang keilmuan di bidang teknologi informatika, penyampaian materi dapat disampaikan secara tepat dan terstruktur.

Meskipun masyarakat sudah aktif menggunakan gawai, belum tentu pemahaman mengenai keamanan digital sejalan dengan penggunaannya. Dengan perkembangan teknologi yang berdampak berevolusinya kejahatan digital menjadi semakin canggih dan beragam, masyarakat riskan menjadi korban. Terlebih jika tidak dibekali dengan pengetahuan yang memadai terkait keamanan digital.

Oleh karena itu, dibutuhkan upaya edukatif yang bersifat preventif yang dapat meningkatkan kesadaran dan kewaspadaan masyarakat terhadap bahaya *link phishing*. Melalui kegiatan sosialisasi, diharapkan masyarakat menjadi lebih waspada dalam mengakses tautan dan mengunduh aplikasi yang berpotensi berbahaya. Sehingga hal ini dapat meminimalisir risiko terjadinya kejahatan beserta kerugian.

## **2. METODE PELAKSANAAN**

### **2.1 Bentuk dan Pendekatan Kegiatan**

Kegiatan ini adalah kegiatan pengabdian masyarakat yang dilaksanakan dalam bentuk sosialisasi bertema bahaya *link phishing*. Edukasi disampaikan dalam bentuk pemaparan materi yang disertai dengan diskusi dan demonstrasi langsung. Pendekatan yang diterapkan adalah pendekatan partisipatif dimana peserta turut dilibatkan dalam diskusi dan pendekatan kontekstual dimana materi disampaikan mengambil contoh kasus yang dekat dengan kehidupan nyata dan disampaikan dengan bahasa sehari-hari sehingga akan mudah dipahami oleh peserta. Pendekatan diperkuat dengan adanya demonstrasi secara langsung, sehingga peserta dapat mengamati secara langsung bagaimana praktik *phishing* dilakukan dan betapa menakutkannya dampaknya.

### **2.2 Lokasi dan Peserta Kegiatan**

Kegiatan dilakukan di balai Desa Salam dengan jumlah peserta sebanyak 24 orang. Mayoritas peserta merupakan ibu-ibu yang aktif menggunakan WhatsApp sebagai sarana komunikasi di kehidupan sehari-hari. Lokasi balai desa dipilih karena balai desa merupakan sebuah fasilitas desa dimana semua kegiatan warga Desa Salam terpusat. Ibu-ibu dipilih menjadi peserta selain karena ketersediaan dalam salah satu kegiatan PKK, para ibu dalam rentang usia dewasa sampai lansia merupakan salah satu golongan yang rentan terkena jebakan *phishing* karena kurangnya pemahaman mengenai keamanan digital.

### **2.3 Tahapan Pelaksanaan Kegiatan**

#### **a. Tahap Persiapan**

Persiapan diawali dengan koordinasi dengan pihak desa, tentunya disertai dengan observasi terhadap lingkungan dan warga desa. Setelah menemui berbagai perangkat desa dan tokoh-tokoh masyarakat, komunikasi juga dilakukan dengan ketua Tim Penggerak PKK Desa Salam. Setelah pihak PKK menyetujui adanya sosialisasi dan menentukan tanggal, materi mulai disusun. Materi disusun dalam slide presentasi dan dilengkapi dengan contoh kasus. Simulasi untuk demonstrasi juga dipersiapkan. Tak hanya menyiapkan isi materi, tapi lokasi beserta perangkat untuk melakukan

sosialisasi juga disiapkan dengan sebaik mungkin. Di lokasi disiapkan meja dan kursi untuk peserta. Sedangkan perangkat untuk presentasi dan demonstrasi berupa *laptop*, proyektor, dan *mic*. Tim pengabdian juga berkoordinasi mengenai teknis pelaksanaan acara.

b. Tahap Pelaksanaan

Pelaksanaan sosialisasi direncanakan akan dilaksanakan di balai desa pada hari Senin, 26 Januari 2026. Acara diawali dengan pembukaan dari pembawa acara. Kemudian, tentu saja acara dilanjutkan oleh sambutan oleh Ibu Niken Werdiningtyas selaku ketua Tim Penggerak PKK Desa Salam. Tanpa berbasabasi lagi, acara langsung dilanjutkan dengan sosialisasi yang dibawakan oleh narasumber dari tim pengabdian.

Dalam pelaksanaannya, sosialisasi diawali dengan pertanyaan pembuka yaitu apakah peserta menggunakan Whatsapp sebagai kebutuhan komunikasi sehari-hari. Materi *phishing* disampaikan melalui tayangan slide dan fokus kepada penyebarannya di WhatsApp. Berbagai contoh kasus ditunjukkan kepada peserta, seperti undangan nikah online atau pemberitahuan paket. Kemudian dilakukan praktik demonstrasi secara langsung yang mensimulasikan bagaimana hacker mencuri data korban *phishing*. Setelah pemaparan materi, dilakukan sesi diskusi dan tanya jawab.

c. Tahap Evaluasi

Tahap evaluasi dilakukan secara kualitatif melalui observasi terhadap respons dan partisipasi peserta selama kegiatan berlangsung. Evaluasi memperhatikan antusiasme peserta, pertanyaan yang muncul, dan kemampuan peserta dalam memahami materi yang sudah disampaikan. Hal ini dapat dilihat melalui reaksi ketika materi dijelaskan dan interaksi yang terjadi saat sesi diskusi. Evaluasi dilakukan secara kualitatif sebagai alternatif *pre-test* dan *post-test* mengingat keterbatasan waktu dan karakteristik peserta.

## 2.4 Teknik Pengumpulan Data

Data diperoleh melalui observasi langsung selama kegiatan berlangsung, diskusi dan tanya jawab dengan peserta, serta dokumentasi kegiatan. Data yang dikumpulkan bersifat kualitatif dan digunakan untuk menggambarkan respons, pemahaman, serta antusiasme peserta terhadap materi yang disampaikan.

## 3. HASIL DAN PEMBAHASAN

### 3.1 Pelaksanaan Kegiatan Sosialisasi

Kegiatan sosialisasi bertajuk Sosialisasi Keamanan Digital: Mengetahui Bahaya *Link Phishing* Khusus WhatsApp adalah salah satu dari program kerja unggulan yang direncanakan oleh tim pengabdian. Sosialisasi ini diadakan demi meningkatkan pemahaman masyarakat setempat mengenai keamanan digital. Ibu-ibu PKK menjadi sasaran utama dalam kegiatan sosialisasi ini. Alasan dipilihnya para ibu PKK sebagai target audiens adalah peran mereka sebagai salah satu pengguna gawai dan aplikasi pesan instan yang aktif.

Acara sosialisasi diadakan di balai desa pada tanggal 26 Januari 2026, merangkap dengan pertemuan rutin PKK Desa Salam. Sebelumnya acara diawali dengan sambutan, kemudian langsung diarahkan ke sosialisasi.





**Gambar 1.** Foto Sambutan Ketua TP PKK



**Gambar 2.** Foto Kegiatan Sosialisasi



**Gambar 3.** Foto Setelah Kegiatan Sosialisasi

Sosialisasi dilaksanakan dalam bentuk penyampaian materi melalui tayangan *slide* presentasi. Kemudian dilanjutkan dengan diskusi. Dengan hal ini, diharapkan peserta tidak hanya mendapat materi searah, tapi juga dapat berbagi pengalaman tersendiri mengenai penggunaan media

digital serta berkontribusi aktif dalam kegiatan. Selain itu, interaksi dua arah dimaksudkan agar peserta lebih tertarik, menghidupkan suasana agar tidak terlalu monoton.

Selain pemaparan materi dengan metode ceramah, informasi juga disampaikan melalui demonstrasi langsung. Demonstrasi ini mensimulasikan sudut pandang *hacker* yang telah berhasil menjebak korban dalam skema *phishing*. Salah satu presentator berperan menjadi korban yang lengah menekan tautan *phishing* dan sengaja mengunduh aplikasi *phishing*. Apa pun yang *hacker* dapatkan setelah korban tertipu, ditayangkan dengan jelas dalam demonstrasi. Metode demonstrasi berfungsi untuk memberikan pengalaman nyata dan menekankan urgensi untuk menghindari *phishing*.

Materi sosialisasi disusun berdasarkan fenomena kasus *phising* yang terjadi di masyarakat. Namun materinya lebih fokus ke kasus *phishing* yang sedang marak yaitu menyebarnya tautan mencurigakan serta bujukan untuk mengunduh aplikasi tak diketahui melalui WhatsApp. Tak hanya marak, namun kompleksitasnya bahkan berada di tingkat dimana pengguna gawai yang cakap teknologi pun dapat terkecoh. Melalui pemaparan contoh kasus dalam bentuk visual beserta ciri-ciri *phishing*, diharapkan para peserta dapat mengenali modus penipuan serupa di kemudian hari.

Penyampaian sosialisasi dikemas dalam bahasa yang sederhana namun tetap informatif. Hal itu menyesuaikan latar belakang peserta yang beragam. Contoh-contoh yang diambil berdasarkan kasus yang nyata terjadi di kehidupan sehari-hari sehingga peserta merasa dekat dan merasakan urgensi untuk berhati-hati dengan bahaya *phishing*.

### **3.2 Respons dan Reaksi Peserta**

Pelaksanaan sosialisasi bahaya *link phishing* mendapat respon positif dari peserta ibu-ibu PKK. Hal ini terlihat dari antusiasme peserta selama kegiatan berlangsung.

Pada mulanya, para peserta terlihat duduk dengan tenang sambil memperhatikan dengan seksama. Ketika ditanya mengenai penggunaan aplikasi WhatsApp dalam kehidupan sehari-hari, para peserta reaktif dan mengiyakan bahwa mereka memang aktif menggunakan aplikasi tersebut. Hal ini menunjukkan bahwa aplikasi pesan instan tersebut merupakan sarana komunikasi tak terpisahkan dari aktivitas masyarakat sehari-hari, bahkan di desa.

Antusiasme naik ketika dilakukan demonstrasi langsung praktik nyata *phishing*. Para peserta terlihat terkejut sekaligus kagum saat diperlihatkan bagaimana pelaku bisa mendapatkan informasi pribadi korban setelah tautan ditekan dan aplikasi diunduh. Respon ini menunjukkan dampak yang kuat untuk meningkatkan pemahaman peserta.

Reaksi peserta menunjukkan bahwa ibu-ibu tertarik sekaligus merasa membutuhkan informasi mengenai keamanan digital, khususnya kejahatan berbasis teknologi.

### **3.3. Peningkatan Pemahaman Peserta**

Setelah materi selesai disampaikan, beberapa peserta terlihat aktif mengajukan pertanyaan, salah satunya adalah mengenai cara mengetahui tanda bahwa ponsel telah diretas.

Dalam sesi diskusi, dijelaskan bahwa saat ini ponsel modern biasanya sudah dilengkapi sistem keamanan dasar yang cukup memadai. Salah satunya adalah indikator kamera yang akan menyala ketika diakses oleh aplikasi tertentu. Sistem peringatan juga dapat mendeteksi virus secara otomatis ketika aplikasi asing terunduh dari sumber yang tidak resmi. Penjelasan ini membantu peserta memahami tanda-tanda awal adanya ancaman keamanan digital pada perangkat mereka.

Ada pula yang berbagi pengalaman tersendiri mengenai keamanan digital seperti munculnya notifikasi tagihan hutang padahal peserta tidak merasa berhutang kepada siapapun. Hal ini menunjukkan bahwa *phishing* dan penipuan digital memang sudah terjadi secara nyata di masyarakat sehingga menjadikan sosialisasi relevan dengan permasalahan dalam masyarakat.

Peserta juga menunjukkan tanda telah lebih memahami ciri-ciri tautan mencurigakan. Beberapa peserta mampu mengidentifikasi ciri-ciri *phishing* seperti permintaan yang mendesak, permintaan data pribadi, dan tautan yang tidak jelas asalnya dari mana.

Temuan ini mengindikasikan bahwa disampaikan materi ini efektif untuk mengedukasi peserta supaya dapat menghindari kejahatan *phishing*. Para peserta setuju bahwa sangat penting untuk menghindari *phishing* agar tidak terkena dampaknya.

### **3.4. Faktor Pendukung dan Hambatan Kegiatan**

Salah satu keuntungan yang dimiliki kelompok pelaksana adalah mendominasinya mahasiswa program studi Teknologi Informatika dalam kelompok. Dengan pengetahuan dan keahlian di bidangnya, materi disampaikan dengan dasar yang kuat dan demonstrasi yang mumpuni.

Informasi tersebut disampaikan dengan bahasa yang sederhana, sehingga tak hanya mudah untuk dipahami peserta, bahasa yang sederhana juga mempermudah pelaksana dalam menyampaikan materi. Selain itu, para peserta yang bersedia meluangkan waktu untuk hadir dan berpartisipasi dengan aktif juga membuat sosialisasi ini dapat berjalan dengan semestinya.

Meski kegiatan sudah berjalan dengan baik, kegiatan ini juga tak luput dari hambatan. Terdapat peningkatan pemahaman, tetapi ada sebagian peserta belum terbiasa dengan istilah-istilah teknis dalam dunia teknologi dan digital. Terdapat *gap* pengetahuan karena adanya perbedaan generasi dan umur. Walaupun sudah dijelaskan dengan perkiraan bahwa peserta akan dapat memahami materi dengan penuh kesadaran dan keyakinan, masih terdapat peserta yang ragu.

### **3.5. Pembahasan Materi Sosialisasi dan Temuan Kegiatan**

Materi sosialisasi yang disampaikan didasarkan pada fenomena penipuan digital yang marak terjadi di masyarakat dan disesuaikan dengan konteks penggunaan gawai oleh peserta. Materi tersebut mencakup pengertian *phishing*, cara kerja tautan *phishing*, dan media yang sering digunakan pelaku penipuan. Pesan *phishing* juga biasa ditemukan di aplikasi pesan instan seperti WhatsApp. Materi yang mengkhususkan aplikasi WhatsApp relevan dengan kondisi lapangan mengingat mayoritas peserta merupakan pengguna aktif aplikasi tersebut.

Contoh kasus *phishing* yang ditampilkan dekat dengan kehidupan sehari-hari, seperti pesan undangan digital dan pemberitahuan paket. Hal ini dapat membantu peserta mengaitkan materi dengan pengalaman pribadi. Hal ini terlihat dari meningkatnya partisipasi peserta dalam sesi diskusi.

Demonstrasi langsung mengenai cara kerja *phishing* yaitu diperlihatkannya informasi apa saja yang dapat diintip pelaku *phishing* menjadi bagian yang paling menarik perhatian peserta dan memicu rasa ingin tahu.

Penggunaan nomor tidak dikenal, pengatasnamaan instansi resmi, dan kalimat mendesak dalam *link phishing* telah terbukti membantu peserta mengaitkan materi dengan pengalaman pribadi. Setelah materi disampaikan, beberapa peserta bahkan mampu mengidentifikasi pola penipuan yang pernah mereka lakukan sebelumnya. Hasil ini sejalan dengan informasi sebelumnya bahwa pelaku *phishing* sering menggunakan WhatsApp, karena semua orang aktif menggunakan aplikasi tersebut.

Respon positif serta meningkatkannya pemahaman peserta menjadi tolok ukur efektivitas kegiatan sosialisasi ini. Hal ini menunjukkan bahwa kegiatan sosialisasi keamanan digital ini relevan dengan kebutuhan masyarakat di desa ini. Materi yang disampaikan secara kontekstual dan praktis terbukti lebih mudah diterima oleh audiens yang merupakan kalangan dewasa maupun lanjut usia.

Efektivitas penyampaian kontekstual dan penuh empati sejalan dengan penelitian terdahulu, terutama untuk kawula dewasa sampai lansia. Edukasi dilakukan tanpa menghakimi karena pembelajar dewasa memerlukan pengakuan terhadap pengalaman mereka selama hidup dan juga harga diri. Materi yang dirancang kontekstual juga dapat menjawab kebutuhan langsung audiens dalam kehidupan sehari-hari (Tjiptasari & Azizah, 2025). Dalam penelitian lain, adanya diskusi interaktif dalam sosialisasi juga terbukti dapat meningkatkan literasi digital peserta (Amarullah, et al., 2025).

### **3.6. Implikasi Kegiatan Bagi Masyarakat**

Sosialisasi diharapkan memberi dampak yang positif bagi peserta, yaitu meningkatnya kesadaran tentang keamanan digital. Setelah sosialisasi peserta akan sadar betapa berbahayanya jika

pun hanya lengah sedikit saja melakukan tindakan sesepel menekan link mencurigakan. Dengan didedukasinya para ibu, diharapkan juga dapat menjadi pelopor edukasi dalam keluarga.

Kegiatan ini diharapkan tak hanya memberikan manfaat sekali pakai, tapi juga dampak jangka panjang bagi masyarakat. Dalam hal ini, bukan hanya *phishing* tapi segala bentuk penipuan online dan kejahatan digital yang semakin canggih. Dampak lainnya juga termasuk mendorong terbentuknya budaya penggunaan teknologi yang lebih aman dan masyarakat yang melek digital.

#### **4. KESIMPULAN**

Kegiatan sosialisasi bahaya *link phishing* yang menargetkan ibu-ibu PKK sebagai peserta dilaksanakan dengan tujuan untuk meningkatkan pemahaman masyarakat setempat mengenai bahaya kejahatan digital. Hal ini sebagai tindakan preventif kepada kejahatan digital yang semakin canggih dan berkembang mengikuti teknologi.

Dalam hasil kegiatan, peserta menunjukkan respons positif serta peningkatan pemahaman terhadap *link phishing* dan langkah-langkah pencegahan yang dapat dilakukan apabila menemuinya dalam kehidupan nyata. Pendekatan dilakukan dengan bahasa sederhana dan contoh kasus yang dekat dengan dengan audiens. Penggunaan media visual juga membantu peserta memahami materi dalam sosialisasi.

Kesimpulannya, kegiatan pengabdian ini dapat menjadi salah satu upaya efektif dalam meningkatkan literasi keamanan digital masyarakat desa, khususnya bagi kelompok dewasa dan lanjut usia.

#### **REFERENCES**

- Aljeaid, D., Alzhrani, A., Alrougi, M., & Almalki, O. (2020). Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating *Phishing* Attacks. *Information*, 11(12), 547.
- Amarullah, M. H., Ricky, M., Haq, M. G.-d., Wardana, B. K., Kurniawan, Y., & Tegar, M. (2025). Edukasi dan Sosialisasi Bahaya Phising serta Perlindungan Data Pribadi untuk Meningkatkan Pengamanan Digital di Kalangan Masyarakat. *APPA: Jurnal Pengabdian kepada Masyarakat*, 3(2), 270-273.
- Anwari, F. (2025, December 04). Apa Itu Phising? Cara Kerja, Contoh & Tips Menghindarinya. *Mekari Sign*.
- Fathonah, R., Firganefi, F., Jatmiko, G., Muda, C., & Diana, D. (2025). Analisis Dampak Kerugian Tindak Pidana Pengelabuan (*Phishing*) Melalui Sosial Media. *Causa: Jurnal Hukum dan Kewarganegaraan*, 11(9), 51-60.
- National Institute of Standards and Technology. (2023). NIST. Diambil kembali dari *Phishing*: <https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing>
- Tabrani, S., Safitri, V., Nayla P, P. A., & Hosnah, A. U. (2024). Kejahatan *Phishing* Ditinjau dari Perspektif Hukum dan Kejahatan Siber. *Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan*, 3(1), 1-13.
- Tjiptasari, F., & Azizah, R. N. (2025). Transformasi Pendidikan Literasi Digital Lansia: Dari Akses Teknologi menuju Pemberdayaan Kontekstual. *DIKLUS: Jurnal Pendidikan Luar Sekolah*, 9(2), 154-169.
- WartaEkonomi. (2025, December 22). Ibu-Ibu Jadi Target Penipuan Online, Kerugian Tembus Rp1,14 Triliun. *Warta Ekonomi*.