Jurnal Pengabdian Multidisiplin
Volume 6 Nomor 3, 2026

Kuras Institute
Scidac Plus

Edukasi Pencegahan *Phishing* Melalui Permainan dan Simulasi Kasus bagi Anak Usia Sekolah di RW 07 Kelurahan Kedungsari, Kota Magelang, Indonesia

Achmad Busrotun Nufus*, Habibah Nuraini, Ida Indarwati, Yuki Luciana, Amisha Shahila Divania, Shinta Anggraeni, Khoirunnisa Ayu
Universitas Tidar, Indonesia
busro@untidar.ac.id*

Abstrak

Anak usia sekolah di RW 07 Kelurahan Kedungsari, Kota Magelang, terbiasa memakai ponsel untuk bermain gim, bermedia sosial, dan berkirim pesan, tetapi kemampuan mereka mengenali pesan phishing masih beragam. Kegiatan pengabdian ini bertujuan meningkatkan pemahaman anak tentang ciri-ciri phishing, perlindungan data pribadi, dan tindakan yang tepat saat menerima pesan mencurigakan. Kegiatan dilaksanakan pada 26 September 2026 di Balai RW 07 dan diikuti 22 anak kelas IV SD sampai kelas IX SMP. Pelaksanaannya menggunakan pendekatan partisipatif berbasis pengalaman yang terdiri atas pemaparan materi, permainan "Aman atau Phishing?", simulasi kasus, diskusi kelompok kecil, penguatan melalui poster "5 Langkah Aman dari Phishing", dan refleksi. Pemahaman peserta diukur dengan pretest dan posttest berisi 10 soal, lalu dianalisis menggunakan statistik deskriptif, N-gain, dan uji Wilcoxon. Rata-rata nilai naik dari 51,82 menjadi 91,36 dengan N-gain 0,86 (kategori tinggi). Seluruh peserta mengalami kenaikan nilai dan perbedaannya signifikan ($Z = -4{,}35$; $p < 0{,}001$). Sebanyak 19 dari 22 peserta (86,4%) mencapai nilai minimal 80, sedangkan tiga peserta dengan nilai awal terendah masih memerlukan pendampingan. Latihan memilah contoh pesan secara langsung membantu anak memahami ciri phishing dalam waktu singkat. Pemantauan bersama orang tua dan pengurus RW diperlukan agar pemahaman tersebut berlanjut menjadi kebiasaan aman dalam bermedia digital.

Kata Kunci: *Phishing*, Literasi Digital, Keamanan Siber Anak, Pembelajaran Berbasis Pengalaman, Pengabdian Masyarakat

PENDAHULUAN

RW 07 Kelurahan Kedungsari, Kecamatan Magelang Utara, Kota Magelang, merupakan lingkungan permukiman dengan cukup banyak anak usia sekolah dasar dan menengah pertama. Observasi dan wawancara awal pada 3 Agustus 2026 menunjukkan bahwa anak kelas IV SD hingga IX SMP di wilayah ini aktif memakai ponsel untuk bermain gim, bermedia sosial, berkirim pesan, dan mencari informasi. Sebagian dari mereka sudah tahu bahwa kata sandi tidak boleh dibagikan kepada orang lain. Namun, pemahaman tentang bentuk-bentuk *phishing*, hadiah atau undian palsu, dan cara memeriksa keamanan sebuah tautan masih beragam. Pengurus RW 07 menyambut baik rencana edukasi keamanan digital bagi kelompok usia ini.

Artikel ini menggunakan lisensi Creative Commons Attribution 4.0 International License
© 2026 Penulis

Kondisi di RW 07 sejalan dengan gambaran nasional. Survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII, 2026) mencatat penetrasi internet Indonesia mencapai 80,66%, dengan penetrasi pada Generasi Z sebesar 87,80% dan pada Generasi Alpha sebesar 79,73%. Sebagian besar anak usia SD dan SMP dengan demikian sudah terhubung ke internet, sering kali sebelum mereka dibekali cara mengenali risiko di dalamnya. Livingstone & Stoilova (2021) mengelompokkan risiko daring anak ke dalam empat kategori, yaitu konten, kontak, perilaku, dan kontrak. Penipuan seperti *phishing* masuk ke dalam risiko kontrak, karena anak diperlakukan sebagai konsumen atau pemilik akun yang dapat dieksploitasi secara komersial.

Phishing adalah penipuan yang memakai pesan, surel, atau situs palsu agar korban menyerahkan data pribadi atau mengunduh perangkat lunak berbahaya. Pesan semacam ini biasanya dibuat meyakinkan dan mendorong penerimanya segera mengeklik tautan atau membuka lampiran (Federal Trade Commission, 2024). Bagi anak, bentuk yang paling dekat dengan keseharian mereka adalah pengumuman hadiah, tawaran kuota atau item gim gratis, dan permintaan kode OTP. Sheng et al. (2010) bahkan menemukan bahwa kelompok usia 18–25 tahun lebih mudah tertipu *phishing* dibanding kelompok usia yang lebih tua, antara lain karena pengalaman berinternet dan paparan edukasi tentang ancaman ini masih sedikit.

Kemampuan memakai perangkat ternyata tidak otomatis disertai kemampuan mengenali ancaman (Nufus, Novitasari, 2018; Nufus et al., 2024, 2026). Survei terhadap 114 guru sekolah dasar di Skotlandia menemukan bahwa 84% guru mengajarkan keamanan kata sandi, tetapi hanya 42% yang mengajarkan *phishing*, dan topik ini umumnya baru diberikan kepada siswa kelas atas (Lamond et al., 2025). Studi tersebut juga merujuk temuan bahwa anak usia 8–12 tahun memiliki kesadaran keamanan siber yang sangat rendah, terutama terkait *phishing*. Nascimbeni & Vosloo (2019) mengingatkan bahwa literasi digital anak perlu dikembangkan sesuai dengan konteks kehidupan anak, tidak cukup hanya dengan kemahiran menggunakan perangkat.

Literasi digital anak juga tidak dapat dilepaskan dari nilai dan etika. Cathrin et al., (2020) mengangkat konsep *empan papan* dari budaya Jawa sebagai etika komunikasi di media sosial, yang menekankan kemampuan menempatkan diri serta menimbang kebenaran, ketepatan, situasi, dan kondisi sebelum berkomunikasi. Prinsip ini dekat dengan sikap yang diharapkan dari anak ketika menerima pesan asing: berhenti sejenak, menimbang siapa pengirimnya, dan tidak tergesa-gesa membalas atau mengeklik. Dalam tradisi pendidikan Indonesia, Ki Hadjar Dewantara merumuskan ajaran *Tringa*, yakni *ngerti*, *ngerasa*, dan *ngelakoni*. Nufus & Irnawati (2020) menunjukkan bahwa ketiga tahap ini menuntut kesadaran dan pengetahuan, kepedulian yang lahir dari hati nurani, serta tindakan nyata yang dijalankan secara konsisten. Kerangka tersebut mengingatkan bahwa edukasi *phishing* tidak cukup berhenti pada hafalan ciri-ciri penipuan, tetapi perlu sampai pada kebiasaan berhati-hati dalam keseharian anak (Aleroud & Zhou, 2017; Alkhalil et al., 2021).

Sejumlah kegiatan pengabdian telah menguji edukasi keamanan digital bagi pelajar. Pramono et al. (2025) memadukan seminar, praktik pengaturan privasi di ponsel siswa, dan simulasi kasus pada 20 siswa SMA di Semarang; pada *posttest* tidak ada lagi siswa yang bernilai di bawah 80. Ilmiana (2025) di Gunungkidul mencatat kenaikan rata-rata yang lebih kecil, yaitu 9,90%, dan tiga dari 20 siswa justru mengalami penurunan nilai. Agung (2025) juga melaporkan kenaikan pengetahuan pada 30 siswa SMA, termasuk kemampuan mengenali tautan *phishing*. Di luar negeri, Panga et al. (2022) menemukan bahwa remaja yang belajar melalui gim lebih mampu mempertahankan pengetahuan tentang *phishing* daripada remaja yang hanya membaca catatan. Alzahrani et al. (2026) menyoroti bahwa pelatihan *phishing* di sekolah sering hanya berupa sesi singkat yang tidak interaktif.

Bukti dari luar negeri memperlihatkan bahwa format permainan dan pelatihan yang dekat dengan situasi nyata cukup menjanjikan. Gim Anti-Phishing Phil yang dikembangkan Sheng et al. (2007) membantu

pengguna mengenali situs palsu lebih baik daripada materi bacaan biasa. Sheng et al. (2010) menunjukkan bahwa pelatihan PhishGuru, yang disisipkan dalam situasi menyerupai kejadian sebenarnya, membuat pengetahuan peserta tetap bertahan beberapa minggu kemudian. Pada anak, Lastdrager et al. (2017) menguji pelatihan anti-*phishing* di sekolah dasar Belanda. Skor anak naik 14% setelah pelatihan, tetapi kemampuan mengenali *phishing* kembali ke tingkat semula setelah empat minggu. Temuan ini menunjukkan bahwa edukasi untuk anak perlu dirancang interaktif sekaligus disertai pengingat yang berulang.

Kegiatan-kegiatan tersebut umumnya berlangsung di sekolah dengan peserta dari satu jenjang. Edukasi *phishing* di lingkungan tempat tinggal, dengan peserta yang beragam usia dan kelas, masih jarang dilaporkan. Padahal di lingkungan rumahlah anak paling sering memegang ponsel tanpa pengawasan guru, sehingga pengurus RW dan orang tua memiliki peran yang tidak kalah penting dibanding sekolah. Sebagian besar laporan juga hanya mengukur pemahaman sesaat setelah kegiatan, sehingga belum banyak yang membahas bagaimana pengetahuan itu dijaga ketika anak kembali ke rumah.

Rancangan kegiatan ini bertumpu pada siklus belajar pengalaman Kolb (1984), yang terdiri atas pengalaman konkret, observasi reflektif, konseptualisasi abstrak, dan eksperimentasi aktif. Siklus tersebut diwujudkan dalam permainan memilah pesan, diskusi kasus, perumusan langkah aman, dan komitmen di akhir sesi. Pola ini sejalan dengan model RIAS (*Reading, Identification, Analysis, Self-reflection*) yang dikembangkan Muhlisin et al. (2021) untuk pendidikan karakter. Dalam model tersebut, peserta membaca situasi, mengenali masalah, menganalisisnya, lalu merefleksikan diri.

Berdasarkan kebutuhan tersebut, tim mahasiswa PPG Pendidikan IPA Universitas Tidar melaksanakan Sosialisasi Pencegahan *Phishing* (*Cyber Literacy*) dengan pendekatan pembelajaran berbasis pengalaman. Pendekatan ini menempatkan keterlibatan aktif, konteks nyata, dan refleksi sebagai inti proses belajar (Morris, 2020). Kegiatan bertujuan meningkatkan pemahaman anak tentang ciri-ciri *phishing*, perlindungan data pribadi, dan langkah yang perlu diambil saat menerima pesan mencurigakan. Artikel ini melaporkan pelaksanaan kegiatan beserta perubahan pemahaman peserta sebelum dan sesudahnya.

METODE

Kegiatan menggunakan pendekatan partisipatif dan berbasis pengalaman (*experiential learning*). Pengurus RW 07 dilibatkan sejak penentuan sasaran, waktu, dan tempat, sedangkan peserta terlibat aktif melalui permainan, simulasi, dan diskusi. Seluruh rangkaian berlangsung dari 3 Agustus sampai 30 September 2026 dan terbagi ke dalam tahap perencanaan, pelaksanaan, serta evaluasi. Tim pelaksana terdiri atas mahasiswa PPG Pendidikan IPA dengan pembagian peran sebagai ketua, sekretaris, bendahara, koordinator pelaksana, humas, dan dokumentasi, serta didampingi dosen pembimbing.

Pada tahap perencanaan, tim berkoordinasi dengan pengurus RW 07 pada 3 Agustus 2026, mengidentifikasi kebutuhan pada 6 Agustus, dan menyusun konsep kegiatan pada 7 Agustus. Materi, permainan "Aman atau *Phishing*?", bahan simulasi kasus, poster "5 Langkah Aman dari *Phishing*", serta instrumen *pretest* dan *posttest* disiapkan pada 5–6 September 2026. Contoh kasus dipilih dari situasi yang akrab bagi anak, misalnya pesan hadiah palsu, permintaan kode OTP, tawaran kuota gratis, dan pembelian item gim.

Persiapan teknis meliputi penyusunan materi presentasi, pembuatan contoh pesan dan tautan untuk permainan, pencetakan poster, serta penyiapan laptop, proyektor, dan alat tulis. Pengumuman kegiatan disebarkan melalui humas tim dan pengurus RW, sedangkan peserta melakukan registrasi sebelum acara dimulai. Sebelum acara, tim memeriksa kesiapan perangkat dan tempat serta melakukan koordinasi akhir dengan pengurus RW.

Tahap pelaksanaan berlangsung pada Sabtu, 26 September 2026, pukul 07.30–10.20 WIB di Balai RW 07. Peserta berjumlah 22 anak dari kelas IV SD sampai kelas IX SMP. Urutan kegiatan disajikan pada Tabel 1. Selama permainan dan simulasi, peserta dibagi ke dalam kelompok kecil yang masing-masing didampingi anggota tim agar peserta dari jenjang yang lebih rendah tidak tertinggal.

Tabel 1. Rangkaian Kegiatan Edukasi Pencegahan *Phishing*

Sesi	Kegiatan	Tujuan
1	Pembukaan, *ice breaking*, *pretest*	Membangun suasana dan mengukur pemahaman awal
2	Pemaparan materi interaktif	Mengenalkan pengertian *phishing*, ciri pesan dan tautan mencurigakan, serta perlindungan data pribadi
3	Permainan "Aman atau *Phishing*?"	Melatih peserta memilah contoh pesan yang aman dan yang berbahaya
4	Simulasi kasus dan diskusi kelompok kecil	Menentukan tindakan yang tepat untuk kasus hadiah palsu, tautan mencurigakan, dan permintaan data
5	Penguatan dengan poster "5 Langkah Aman dari *Phishing*", *posttest*	Merangkum langkah aman dan mengukur pemahaman akhir
6	Refleksi dan penutupan	Peserta menyampaikan hal yang dipelajari dan komitmen memakai ponsel secara aman

Keterkaitan setiap sesi dengan tahapan belajar yang menjadi dasar rancangan disajikan pada Tabel 2. Pemetaan ini memastikan peserta tidak hanya menerima informasi, tetapi juga mencoba, merenungkan, dan memutuskan tindakan.

Tabel 2. Pemetaan Sesi Kegiatan Pada Siklus Belajar Kolb dan Ajaran *Tringa*

Sesi	Siklus belajar Kolb	Tahap *Tringa*
Pemaparan materi interaktif	Konseptualisasi abstrak	*Ngerti*
Permainan "Aman atau *Phishing*?"	Pengalaman konkret	*Ngerti*
Simulasi kasus dan diskusi kelompok kecil	Eksperimentasi aktif	*Ngerasa*
Penguatan dengan poster "5 Langkah Aman dari *Phishing*"	Konseptualisasi abstrak	*Ngelakoni*
Refleksi dan penutupan	Observasi reflektif	*Ngerasa* dan *ngelakoni*

Pemahaman peserta diukur dengan 10 soal pilihan ganda yang sama pada *pretest* dan *posttest*. *Pretest* dikerjakan melalui Google Forms, sedangkan *posttest* melalui Kahoot. Nilai diperoleh dari jumlah jawaban benar dikali 10, sehingga rentangnya 0–100. Peserta dikategorikan berpemahaman baik apabila nilainya minimal 80. Soal disusun tim berdasarkan materi yang disampaikan, meliputi pengertian *phishing*, ciri pesan dan tautan mencurigakan, perlindungan data pribadi, serta langkah yang tepat saat menerima pesan mencurigakan.

Data dianalisis dengan statistik deskriptif, N-*gain*, dan uji peringkat bertanda Wilcoxon. N-*gain* dihitung dengan rumus (nilai *posttest* – nilai *pretest*) / (100 – nilai *pretest*), lalu dikategorikan tinggi ($\geq$ 0,70), sedang (0,30–0,69), atau rendah (< 0,30) mengikuti Hake (1998). Uji Wilcoxon dipilih karena selisih nilai tidak berdistribusi normal (uji Shapiro-Wilk, $p < 0{,}001$). Keaktifan peserta dicatat melalui observasi, sedangkan refleksi di akhir sesi dipakai untuk menggali pemahaman yang belum tertangkap oleh tes. . Besar efek uji Wilcoxon dihitung dengan rumus $r = Z/\sqrt{n}$ dan ditafsirkan sebagai efek besar apabila $r \geq 0{,}50$.

HASIL DAN PEMBAHASAN

Hasil

Pelaksanaan Kegiatan

Kegiatan dihadiri 22 anak dari target 30 peserta (73,3%). Beberapa peserta datang bertahap karena bertepatan dengan kegiatan lain, sehingga tim menyesuaikan *rundown* tanpa memangkas materi, permainan, maupun *posttest*. Rentang kelas yang lebar menjadi tantangan utama karena peserta datang dengan pengalaman digital yang berbeda-beda. Pendampingan dalam kelompok kecil membantu peserta dari semua jenjang mengikuti kegiatan sampai selesai.

Observasi tim mencatat peserta aktif dan antusias sejak permainan "Aman atau *Phishing*?" hingga sesi refleksi. Dalam permainan, peserta menebak apakah sebuah contoh pesan aman atau berbahaya, kemudian menjelaskan alasannya. Simulasi kasus memakai situasi hadiah palsu, tautan mencurigakan, dan permintaan data pribadi, lalu peserta berdiskusi untuk menentukan tindakan yang tepat.

Sesi pembukaan diawali perkenalan dan *ice breaking*. Pada pemaparan materi, tim memakai contoh yang dekat dengan keseharian anak, seperti pemberitahuan hadiah, tawaran kuota gratis, dan permintaan kode OTP, lalu menjelaskan tanda-tanda yang perlu dicurigai. Ketika konsentrasi peserta mulai menurun, tim menyelipkan *ice breaking* singkat sebelum melanjutkan ke permainan. Pada akhir rangkaian, tiga peserta dengan capaian *posttest* terbaik menerima penghargaan sebagai bentuk apresiasi.

Kendala yang muncul selama persiapan dan pelaksanaan beserta cara tim menanganinya dirangkum pada Tabel 3.

Tabel 3. Tantangan, Solusi, dan Hasil Pelaksanaan Kegiatan

Tantangan	Solusi yang diterapkan	Hasil
Perbedaan tingkat pemahaman karena rentang kelas IV SD sampai IX SMP	Materi singkat dengan contoh sehari-hari, permainan, simulasi kasus, dan pendampingan kelompok kecil	Peserta dari semua jenjang dapat mengikuti kegiatan sampai selesai
Konsentrasi anak menurun karena sesi berlangsung sekitar dua jam	*Ice breaking* di awal dan di sela kegiatan, permainan, serta diskusi interaktif	Peserta tetap aktif sampai sesi refleksi
Jadwal anak berbenturan dengan kegiatan lain	Koordinasi dengan pengurus RW, pengumuman melalui humas, dan registrasi sebelum acara	22 peserta hadir dan acara berjalan sesuai jadwal
Anggaran dan perangkat terbatas	Anggaran efisien, poster dicetak secukupnya, dan perangkat diperiksa sebelum acara	Kebutuhan inti kegiatan terpenuhi
Pengetahuan dapat memudar dan pendampingan di rumah belum merata	Kartu pengingat, informasi bagi orang tua atau wali, dan rencana pemantauan 1–2 minggu	Peserta memiliki pengingat visual; pemantauan belum dilaporkan

Tabel 3 memperlihatkan bahwa sebagian besar kendala dapat diatasi di lapangan. Kendala yang belum tuntas adalah keberlanjutan, karena pengetahuan anak dapat memudar jika tidak diingatkan dan pendampingan di rumah belum merata.

Perubahan Pemahaman Peserta

Ringkasan nilai *pretest* dan *posttest* disajikan pada Tabel 4. Rata-rata nilai naik sebesar 39,54 poin, dari 51,82 menjadi 91,36.

Tabel 4. Nilai *Pretest* dan *Posttest* Peserta (N = 22)

Ukuran	*Pretest*	*Posttest*
Rata-rata	51,82	91,36
Simpangan baku	13,32	11,67
Median	50	95
Nilai terendah – tertinggi	20 – 70	60 – 100
Peserta bernilai ≥ 80	0 (0%)	19 (86,4%)

Seluruh peserta mengalami kenaikan nilai; tidak ada yang tetap atau turun. Uji Wilcoxon menunjukkan perbedaan yang signifikan antara *pretest* dan *posttest* ($Z = -4{,}35$; $p < 0{,}001$). Rata-rata N-*gain* sebesar 0,86 termasuk kategori tinggi, dengan 18 peserta pada kategori tinggi dan 4 peserta pada kategori sedang. Pada *pretest* belum ada peserta yang mencapai nilai 80, sedangkan pada *posttest* 19 peserta mencapainya dan 11 di antaranya memperoleh nilai sempurna. Dengan demikian, target bahwa minimal 80% peserta berpemahaman baik tercapai. Besar efeknya $r = 0{,}93$, yang termasuk kategori besar.

Rincian nilai setiap peserta disajikan pada Tabel 5. Nama peserta diganti dengan kode untuk menjaga kerahasiaan identitas anak. Sebagian besar peserta naik 40 poin, tetapi peserta dengan *pretest* 70 hanya dapat naik paling banyak 30 poin. Karena itu, N-*gain* dipakai agar kenaikan peserta dengan nilai awal berbeda dapat dibandingkan secara adil. Sebelas peserta memperoleh N-*gain* 1,00 karena mencapai nilai sempurna, dan tujuh peserta berada pada rentang 0,80–0,83. Empat peserta lainnya memperoleh N-*gain* antara 0,50 dan 0,67, dan keempatnya merupakan peserta dengan nilai *pretest* 20–40.

Tabel 5. Nilai *Pretest* (Pre), *Posttest* (Post), dan N-*Gain* Setiap Peserta

Kode	*Pre*	*Post*	N-*gain*	Kategori	Kode	*Pre*	*Post*	N-*gain*	Kategori
P1	60	100	1,00	Tinggi	P12	50	90	0,80	Tinggi
P2	70	100	1,00	Tinggi	P13	70	100	1,00	Tinggi
P3	60	100	1,00	Tinggi	P14	60	100	1,00	Tinggi
P4	50	90	0,80	Tinggi	P15	40	80	0,67	Sedang
P5	70	100	1,00	Tinggi	P16	30	70	0,57	Sedang
P6	50	90	0,80	Tinggi	P17	20	60	0,50	Sedang
P7	40	90	0,83	Tinggi	P18	60	100	1,00	Tinggi
P8	50	100	1,00	Tinggi	P19	50	90	0,80	Tinggi
P9	60	100	1,00	Tinggi	P20	60	100	1,00	Tinggi
P10	50	90	0,80	Tinggi	P21	30	70	0,57	Sedang
P11	60	100	1,00	Tinggi	P22	50	90	0,80	Tinggi

Media Edukasi bagi Lingkungan Mitra

Poster "5 Langkah Aman dari *Phishing*" dicetak empat lembar dan ditempel di lingkungan RW 07, sementara versi kartu pengingatnya dibawa pulang oleh peserta. Materi presentasi dan poster digital juga dapat disebarkan ulang melalui grup WhatsApp warga sehingga orang tua bisa ikut mengingatkan anak di rumah. Langkah-langkah pada poster dirumuskan sebagai tindakan sederhana yang mudah diingat anak, antara lain berhenti sebelum mengeklik, tidak membagikan data pribadi atau kode OTP, dan memberi tahu orang tua atau orang dewasa yang dipercaya ketika menerima pesan mencurigakan.

Respons dan Sikap Peserta

Selain kenaikan nilai, observasi selama kegiatan memperlihatkan perubahan sikap peserta. Peserta tampak lebih kritis ketika diminta menilai contoh pesan. Dalam sesi refleksi, mereka mampu menyebutkan kembali tindakan yang perlu diambil saat menerima pesan mencurigakan, yaitu berhenti, tidak mengeklik, tidak membagikan data, dan menyampaikannya kepada orang tua atau orang dewasa. Orang tua atau wali juga menerima informasi untuk mendampingi anak, sehingga kegiatan ini membuka peluang percakapan di rumah tentang penggunaan gawai dan keamanan data pribadi.

Dampak ekonominya bersifat pencegahan. Anak yang mampu menghindari tautan hadiah palsu, permintaan OTP, atau penipuan pembelian kuota dan item gim ikut mencegah kerugian finansial keluarga, meskipun besarnya belum dapat dihitung.

Pembahasan

Kenaikan nilai pada kegiatan ini jauh lebih besar daripada yang dilaporkan Ilmiana (2025) dan sejalan dengan Pramono et al. (2025), yang juga memakai simulasi dan praktik. Perbedaan dengan Ilmiana (2025) kemungkinan berkaitan dengan porsi latihan. Peserta di RW 07 tidak hanya mendengar ciri-ciri *phishing*, tetapi berulang kali memilah contoh pesan dan memutuskan tindakan yang akan diambil. Pola belajar seperti ini sesuai dengan pandangan bahwa pengalaman langsung yang diikuti refleksi memperkuat pemahaman (Morris, 2020). Temuan Panga et al. (2022) bahwa gim membantu remaja mengingat konsep *phishing* juga mendukung pilihan format permainan, meskipun daya ingat jangka panjang belum diuji dalam kegiatan ini.

Besarnya kenaikan perlu dibaca bersama waktu pengukurannya. Lastdrager et al. (2017) mencatat kenaikan skor 14% pada anak sekolah dasar setelah pelatihan anti-*phishing*, tetapi kemampuan itu menurun kembali dalam empat minggu. *Posttest* dalam kegiatan ini diberikan tidak lama setelah sesi berakhir, sehingga rata-rata 91,36 lebih tepat dipahami sebagai pemahaman segar, bukan bukti bahwa pengetahuan tersebut akan bertahan. Meski demikian, rancangan berbasis permainan memiliki dukungan yang cukup kuat. Sheng et al. (2007) menemukan bahwa gim Anti-Phishing Phil lebih efektif daripada materi tertulis,

Capaian tersebut tidak merata pada semua peserta. Tiga nilai *posttest* terendah, yaitu 60, 70, dan 70, dimiliki peserta yang nilai *pretest*-nya juga paling rendah (20, 30, dan 30). Pola ini mirip dengan temuan Ilmiana (2025) bahwa sebagian siswa memerlukan pendampingan yang lebih intensif. Bagi anak dengan pemahaman awal rendah, satu kali sesi tampaknya belum cukup.

Lastdrager et al. (2017) juga menemukan bahwa usia berpengaruh positif terhadap skor, karena anak yang lebih tua cenderung lebih mampu mengenali *phishing*. Pola serupa mungkin terjadi di RW 07 mengingat pesertanya berasal dari rentang kelas yang lebar, meskipun data jenjang setiap peserta belum dianalisis. Tahap refleksi diri dalam model RIAS (Muhlisin et al., 2021) dapat dimanfaatkan untuk peserta seperti ini. Anak diminta menjelaskan kembali alasan di balik pilihannya, sehingga pendamping bisa segera melihat bagian mana yang belum dipahami.

Bagi mitra, hasil ini penting karena edukasi berlangsung di tempat anak paling sering memakai ponsel, yaitu lingkungan rumah. Lamond et al. (2025) mencatat bahwa *phishing* jarang diajarkan kepada siswa kelas rendah, sedangkan peserta kegiatan ini sebagian masih duduk di kelas IV SD. Kehadiran poster di lingkungan RW dan keterlibatan pengurus RW membuka peluang pengingat berkala yang tidak bergantung pada jadwal sekolah.

Dari sisi nilai, kegiatan ini paling kuat menyentuh tahap *ngerti* dalam ajaran *Tringa*, karena tes memang mengukur pengetahuan. Tahap *ngerasa* dan *ngelakoni* belum terukur oleh instrumen yang ada, padahal kedua tahap itulah yang menentukan apakah anak benar-benar menahan diri ketika menerima pesan hadiah palsu. Nufus & Irnawati (2020) menegaskan bahwa pengetahuan saja tidak cukup tanpa kepedulian

dan tindakan nyata yang konsisten. Prinsip *empan papan* yang diuraikan Cathrin et al. (2020) dapat menjadi bahasa yang akrab bagi orang tua di Magelang untuk meneruskan pesan ini di rumah. Anak diajak menimbang siapa pengirim pesan, apakah isinya masuk akal, dan apakah situasinya tepat sebelum menanggapi. Dengan cara ini, keamanan digital tidak terasa sebagai aturan asing, melainkan bagian dari tata krama yang sudah dikenal keluarga.

Kegiatan ini memiliki beberapa keterbatasan. *Posttest* dilakukan langsung setelah sesi sehingga hasilnya menggambarkan pemahaman jangka pendek. Format *posttest* melalui Kahoot berbeda dari *pretest* melalui Google Forms, dan suasana kompetitif Kahoot dapat memengaruhi nilai. Kegiatan juga tidak memakai kelompok pembanding. Pemantauan 1–2 minggu setelah kegiatan sudah direncanakan, tetapi hasilnya belum tersedia, sehingga perubahan perilaku peserta belum dapat disimpulkan. Kegiatan berikutnya disarankan menggunakan format tes yang setara, melakukan tes ulang beberapa minggu setelah sesi, dan memberi sesi tambahan bagi peserta dengan nilai awal rendah. Temuan Lastdrager et al. (2017) tentang menurunnya kemampuan anak setelah empat minggu memperkuat perlunya pengingat berkala, misalnya kuis singkat melalui grup WhatsApp warga atau sesi penyegaran setiap beberapa bulan.

KESIMPULAN

Edukasi pencegahan *phishing* melalui permainan dan simulasi kasus meningkatkan pemahaman 22 anak kelas IV SD sampai IX SMP di RW 07 Kelurahan Kedungsari. Rata-rata nilai naik dari 51,82 menjadi 91,36 dengan N-*gain* 0,86, seluruh peserta mengalami kenaikan, dan 86,4% peserta mencapai nilai minimal 80. Latihan memilah contoh pesan secara langsung menjadi bagian penting dari capaian ini, sedangkan peserta dengan pemahaman awal paling rendah masih memerlukan pendampingan tambahan.

Bagi masyarakat sasaran, kegiatan ini menunjukkan bahwa edukasi keamanan digital dapat dijalankan di tingkat RW dengan biaya kecil dan media sederhana. Pengurus RW dapat memanfaatkan poster dan grup WhatsApp warga sebagai pengingat berkala, sementara orang tua dapat meneruskan langkah-langkah aman di rumah. Pengabdian selanjutnya disarankan menyertakan pemantauan beberapa minggu setelah kegiatan, melibatkan orang tua sejak awal, dan memperluas materi ke topik perundungan siber serta etika bermedia sosial. Nilai lokal seperti *empan papan* dan ajaran *Tringa* dapat dipakai sebagai jembatan agar pesan keamanan digital mudah diteruskan dalam keluarga.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Ketua RW 07 beserta pengurus dan warga Kelurahan Kedungsari atas izin dan dukungannya, kepada para peserta beserta orang tua atau wali, serta kepada Program Studi Pendidikan Profesi Guru Pendidikan IPA Universitas Tidar yang memfasilitasi kegiatan ini.

DAFTAR PUSTAKA

Achmad Busrotun Nufus, Novitasari, S. M. (2018). *Pendidikan Pancasila sebagai paradigma pembangunan* (1st ed.). Madani.

Agung, H. (2025). Efektivitas edukasi cybersecurity dalam meningkatkan pengetahuan siswa tentang ancaman digital pada siswa menengah atas. *Jurnal Ilmu Komputer (JUIK)*, *5*(2), 104–113.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160–196.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

Alzahrani, S., Badri, S., & Nadeem, F. (2026). Design and Development of Anti-Phishing AG: A Web-Based

3D Serious Game to Improve Phishing Awareness Among Students in Saudi Arabia. *Engineering, Technology & Applied Science Research*, *16*(3), 35270–35280.

APJII. (2026). *Survei penetrasi internet dan perilaku pengguna internet Indonesia 2026*. Asosiasi Penyelenggara Jasa Internet Indonesia. https://survei.apjii.or.id/survei

Cathrin, S., Wikandaru, R., Nufus, A. B., Sudarsih, S., & Saraswati, D. (2020). EMPAN PAPAN: ETIKA KOMUNIKASI DI MEDIA SOSIAL DALAM PERSPEKTIF BUDAYA JAWA. *Jurnal Lensa Mutiara Komunikasi*, *4*(2), 165–183.

Commission, F. T. (2024). *How to recognize and avoid phishing scams*. Federal Trade Commission. https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Ilmiana, I. R. (2025). Peningkatan literasi keamanan dan etika berinternet di SMP Muhammadiyah Al Mujahidin Gunungkidul. *GERVASI: Jurnal Pengabdian Kepada Masyarakat*.

Kolb, D. A. (1984). Experiential learning: Experience as the source of learning and development. *EC.: Prentice Hall*.

Lamond, M., Prior, S., Renaud, K., & Wood, L. A. (2025). Teachers' perspectives and practice of cybersecurity education in primary schools. *Discover Education*, *4*(1), 312.

Lastdrager, E., Gallardo, I. C., Hartel, P., & Junger, M. (2017). How effective is {anti-phishing} training for children? *Thirteenth Symposium on Usable Privacy and Security (Soups 2017)*, 229–239.

Livingstone, S., & Stoilova, M. (2021). *The 4Cs: Classifying online risk to children*.

Morris, T. H. (2020). Experiential learning–a systematic review and revision of Kolb's model. *Interactive Learning Environments*, *28*(8), 1064–1077.

Muhlisin, A., Sarwanti, S., Jalunggono, G., Yusliwidaka, A., Mazid, S., & Nufus, A. B. (2021). RIAS Learning Model: a Character Education Innovation. *AL-ISHLAH: Jurnal Pendidikan*, *13*(1), 660–667.

Nascimbeni, F., & Vosloo, S. (2019). *Digital literacy for children: Exploring definitions and frameworks*. UNICEF Office of Global Insight and Policy. https://www.unicef.org/innocenti/reports/digital-literacy-children-exploring-definitions-and-frameworks

Nufus, A. B., & Irnawati, I. (2020). PENGAMALAN NILAI-NILAI AJARAN "TRINGA" KI HADJAR DEWANTARA DALAM MENYIKAPI PANDEMI COVID 19. *JURNAL KALACAKRA: Ilmu Sosial Dan Pendidikan*, *1*(1), 41–50.

Nufus, A. B., Malihah, E., Darmawan, C., Anggraeni, L., Budimansyah, D., & Sehadun, F. (2024). Cultural Diversity and Harmony of Tionghoa Good Character: Towards Unity with Incremental Change of Citizenship. *Jurnal Moral Kemasyarakatan*, *9*(1), 41–52.

Nufus, A. B., Widiyanto, D., Sholikhah, N., Mazid, S., & Ayu, K. (2026). Pendidikan Karakter Toleransi Beragama dan Kearifan Lokal dalam Praktik Sekolah: Survei Pendidik di Magelang. *ARMADA: Jurnal Penelitian Multidisiplin*, *4*(10), 7010–7020.

Panga, R. C. T., Marwa, J., & Ndibwile, J. D. (2022). A game or notes? The use of a customized mobile game to improve teenagers' phishing knowledge, case of Tanzania. *Journal of Cybersecurity and Privacy*, *2*(3), 466–489.

Pramono, B. A., Nugroho, A., & Christioko, B. V. (2025). Edukasi Keamanan Data Pribadi dalam Media Sosial untuk Siswa SMA Masehi 2 PSAK Semarang. *Jurnal DIMASTIK*, *3*(2), 169–177.

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

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish.

Proceedings of the 3rd Symposium on Usable Privacy and Security, 88–99.