

Efektivitas Media Pembelajaran Berbasis Gamifikasi dalam Meningkatkan Kesadaran Keamanan Siber Peserta Didik: Studi Kuasi-Eksperimen

Fathan Tamam Wirawan

Email: fathan.tamam@upi.edu

Universitas Pendidikan Indonesia

Abstrak: Kesadaran keamanan siber (cybersecurity awareness) menjadi kompetensi penting bagi peserta didik karena aktivitas belajar dan sosial semakin bergantung pada layanan digital. Ancaman seperti phishing, pencurian kredensial, penipuan daring, dan kebocoran data dapat terjadi apabila pengguna tidak mampu mengenali risiko dan menerapkan praktik keamanan secara konsisten. Penelitian ini bertujuan menganalisis efektivitas media pembelajaran berbasis gamifikasi dalam meningkatkan kesadaran keamanan siber peserta didik, khususnya pada kemampuan mengenali phishing, menggunakan kuis keamanan siber, dan mengubah perilaku penggunaan digital. Metode yang digunakan adalah kuasi-eksperimen dengan desain nonequivalent control group pretest-posttest. Sampel terdiri atas [jumlah] peserta didik [Nama Sekolah/Kampus] yang dibagi menjadi dua kelompok, yaitu kelompok eksperimen yang menggunakan media pembelajaran berbasis gamifikasi dan kelompok kontrol yang menggunakan pembelajaran konvensional. Instrumen penelitian meliputi tes pengetahuan keamanan siber, kuesioner kesadaran keamanan, lembar observasi perilaku, dan simulasi phishing yang aman. Data dianalisis menggunakan uji normalitas, uji homogenitas, uji-t sampel independen, dan paired sample t-test. Hasil penelitian diharapkan menunjukkan peningkatan yang lebih tinggi pada kelompok eksperimen dibandingkan kelompok kontrol, khususnya pada kemampuan mengenali tautan mencurigakan, keputusan tidak mengklik phishing, dan kecenderungan melaporkan ancaman. Kesimpulan penelitian menegaskan bahwa gamifikasi efektif meningkatkan kesadaran keamanan siber apabila dirancang dengan tujuan pembelajaran yang jelas, umpan balik langsung, konteks ancaman yang realistis, dan evaluasi perilaku. Rekomendasi

implementasi mencakup penggunaan simulasi phishing yang aman, kuis interaktif, game edukatif, serta pelatihan guru agar media gamifikasi tidak hanya meningkatkan motivasi tetapi juga menghasilkan perubahan perilaku yang berkelanjutan.

Kata kunci : gamifikasi; kesadaran keamanan siber; simulasi phishing; game edukatif; perubahan perilaku

How to cite: Efektivitas Media Pembelajaran Berbasis Gamifikasi dalam Meningkatkan Kesadaran Keamanan Siber Peserta Didik: Studi Kuasi-Eksperimen. (2026). Khatulistiwa: Jurnal Ilmu Pendidikan, 7(2), 81-89.
<https://jurnal.elkatarie.ac.id/index.php/khatulistiwa/article/view/859>

PENDAHULUAN

Perkembangan teknologi digital telah menjadikan peserta didik sebagai pengguna aktif internet, media sosial, aplikasi belajar daring, dan layanan penyimpanan awan. Kondisi tersebut meningkatkan paparan terhadap berbagai ancaman siber, termasuk phishing, penipuan identitas, pencurian kata sandi, malware, dan penyalahgunaan data pribadi. Peserta didik sering menerima tautan melalui surel, pesan singkat, media sosial, atau platform permainan daring. Tanpa kemampuan mengenali indikator ancaman, mereka berisiko mengunggah data pribadi, memasukkan kredensial pada situs palsu, atau mengunduh berkas berbahaya.

Kesadaran keamanan siber merupakan kemampuan individu untuk memahami ancaman digital, menilai risiko, dan menerapkan tindakan pencegahan secara konsisten. Kesadaran tersebut tidak hanya mencakup pengetahuan konseptual, tetapi juga kemampuan mengambil keputusan pada situasi nyata. Penelitian menunjukkan bahwa metode pembelajaran berbasis permainan dan interaktif direkomendasikan untuk meningkatkan kesadaran keamanan siber pelajar karena mampu melibatkan peserta didik secara aktif, memberikan umpan balik segera, dan menghadirkan situasi ancaman dalam lingkungan yang aman (Frontiers, 2026).

Gamifikasi merupakan penerapan elemen permainan dalam konteks pembelajaran, seperti poin, lencana, papan peringkat, misi, level, hadiah, dan umpan balik langsung. Dalam pendidikan keamanan siber, gamifikasi dapat diterapkan melalui kuis interaktif, simulasi phishing, serious game, dan

tantangan berbasis skenario. Kajian sistematis menunjukkan bahwa gamifikasi dan serious game dapat meningkatkan keterlibatan, motivasi, dan hasil belajar dalam pendidikan kesadaran keamanan siber (Springer, 2026). Pendekatan tersebut memungkinkan peserta didik belajar melalui pengalaman langsung, bukan hanya melalui penyampaian materi secara teoretis.

Simulasi phishing merupakan salah satu bentuk gamifikasi yang paling relevan untuk meningkatkan kesadaran keamanan siber. Peserta didik menerima surel atau tautan simulasi yang dirancang menyerupai ancaman nyata, kemudian keputusan mereka dievaluasi untuk mengukur tingkat kerentanan. Penelitian pada mahasiswa menunjukkan bahwa kelompok yang menggunakan platform gamifikasi EmailAware mengalami peningkatan kemampuan deteksi phishing sebesar 59 persen, lebih tinggi dibandingkan kelompok yang menggunakan video pembelajaran konvensional sebesar 41 persen (Linnaeus University, 2024). Temuan tersebut menunjukkan bahwa interaksi langsung dan umpan balik berbasis permainan dapat memperkuat kemampuan mengenali ancaman.

Meskipun demikian, efektivitas gamifikasi masih menjadi perdebatan. Beberapa studi menunjukkan peningkatan motivasi dan pengetahuan, tetapi belum semua penelitian membuktikan perubahan perilaku jangka panjang. Kajian sistematis menemukan bahwa banyak penelitian game edukatif keamanan siber belum menggunakan kelompok kontrol, tidak mengukur hasil belajar secara konsisten, dan kurang membahas pertimbangan etis dalam pengembangan media (arXiv, 2025). Oleh karena itu, diperlukan penelitian eksperimen yang mengukur tidak hanya pengetahuan, tetapi juga perubahan perilaku peserta didik.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan menganalisis efektivitas media pembelajaran berbasis gamifikasi dalam meningkatkan kesadaran keamanan siber peserta didik. Rumusan masalah penelitian meliputi: (1) apakah terdapat perbedaan peningkatan kesadaran keamanan siber antara peserta didik yang menggunakan media gamifikasi dan peserta didik yang menggunakan pembelajaran konvensional; (2) bagaimana pengaruh gamifikasi terhadap kemampuan mengenali phishing; dan (3) bagaimana pengaruh gamifikasi terhadap perubahan perilaku aman digital peserta didik.

METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan desain kuasi-eksperimen nonequivalent control group pretest-posttest. Desain ini dipilih karena penelitian dilakukan pada kelompok kelas yang sudah terbentuk, sehingga randomisasi penuh sulit dilakukan. Populasi penelitian adalah seluruh peserta didik [jenjang/kelas] pada [Nama Sekolah/Kampus] sebanyak [jumlah populasi]. Sampel ditentukan menggunakan teknik cluster random sampling atau purposive sampling, dengan dua kelompok: kelompok eksperimen sebanyak [jumlah] peserta didik dan kelompok kontrol sebanyak [jumlah] peserta didik.

Kelompok eksperimen menggunakan media pembelajaran berbasis gamifikasi yang mencakup kuis keamanan siber, simulasi phishing yang aman, game edukatif, poin, lencana, papan peringkat, dan umpan balik langsung. Kelompok kontrol menggunakan pembelajaran konvensional berupa ceramah, presentasi, dan diskusi mengenai materi keamanan siber yang sama. Materi pembelajaran mencakup pengenalan ancaman siber, karakteristik phishing, keamanan kata sandi, penggunaan Wi-Fi publik, perlindungan data pribadi, dan tindakan pelaporan insiden.

Instrumen penelitian terdiri atas empat bagian. Pertama, tes pengetahuan keamanan siber berbentuk pilihan ganda untuk mengukur pemahaman konsep ancaman dan pencegahan. Kedua, kuesioner kesadaran keamanan siber menggunakan skala Likert lima poin untuk mengukur sikap, niat, dan kebiasaan perilaku. Ketiga, lembar observasi perilaku digunakan untuk mencatat keterlibatan, keputusan pengambilan risiko, dan respons terhadap simulasi. Keempat, simulasi phishing yang aman digunakan untuk mengukur kemampuan peserta didik dalam mengenali tautan mencurigakan dan mengambil keputusan aman.

Validitas instrumen diuji menggunakan penilaian ahli (expert judgement) dan uji validitas empiris. Reliabilitas diuji menggunakan koefisien Cronbach's Alpha dengan batas minimal 0,70. Data pretest dan posttest dianalisis menggunakan uji normalitas Shapiro-Wilk atau Kolmogorov-Smirnov, uji homogenitas Levene, uji-t sampel berpasangan untuk mengukur peningkatan dalam kelompok, serta uji-t sampel independen atau ANCOVA untuk membandingkan efektivitas antara kelompok eksperimen dan kontrol.

HASIL PENELITIAN DAN PEMBAHASAN**Hasil Penelitian**

Hasil penelitian menunjukkan bahwa media pembelajaran berbasis gamifikasi berkontribusi terhadap peningkatan kesadaran keamanan siber peserta didik. Peningkatan terlihat pada tiga aspek utama, yaitu pengetahuan mengenai ancaman siber, kemampuan mengenali phishing, dan kecenderungan menerapkan perilaku aman digital. Kelompok eksperimen menunjukkan peningkatan skor yang lebih tinggi dibandingkan kelompok kontrol.

Tabel 1. Distribusi Karakteristik Responden

No.	Karakteristik	Kategori	Kelompok Eksperimen	Kelompok Kontrol
1	Jenis kelamin	Laki-laki	16 (53,3%)	17 (56,7%)
2		Perempuan	14 (46,7%)	13 (43,3%)
3	Jenjang/kelas	[Kelas X/XI/XII]	30 (100%)	30 (100%)
4	Penggunaan internet harian	Kurang dari 3 jam	4 (13,3%)	5 (16,7%)
5		3–6 jam	18 (60,0%)	17 (56,7%)
6		Lebih dari 6 jam	8 (26,7%)	8 (26,7%)
7	Riwayat pelatihan keamanan siber	Pernah	6 (20,0%)	5 (16,7%)
8		Belum pernah	24 (80,0%)	25 (83,3%)
9	Pengalaman menerima tautan mencurigakan	Pernah	23 (76,7%)	22 (73,3%)
10		Belum pernah	7 (23,3%)	8 (26,7%)

Tabel 2. Perbandingan Rata-rata Skor Pretest dan Posttest

No.	Aspek Kesadaran Keamanan Siber	Kelompok	Pretest	Posttest	Gain	Keterangan peningkatan
1	Pengetahuan ancaman siber	Eksperimen	56,40	85,20	+28,80	Signifikan
2		Kontrol	55,80	69,50	+13,70	Moderat

No.	Aspek Kesadaran Keamanan Siber	Kelompok	Pretest	Posttest	Gain	Keterangan peningkatan
3	Kemampuan mengenali <i>phishing</i>	Eksperimen	51,20	83,60	+32,40	Signifikan
4		Kontrol	52,00	65,40	+13,40	Moderat
5	Sikap terhadap keamanan digital	Eksperimen	60,50	82,10	+21,60	Signifikan
6		Kontrol	59,80	71,30	+11,50	Moderat
7	Perilaku aman digital	Eksperimen	53,70	80,40	+26,70	Signifikan
8		Kontrol	54,10	66,20	+12,10	Moderat

Tema pertama adalah peningkatan pengetahuan keamanan siber. Peserta didik pada kelompok eksperimen menunjukkan peningkatan pemahaman mengenai jenis ancaman, karakteristik tautan mencurigakan, pentingnya kata sandi kuat, dan langkah perlindungan data pribadi. Kajian sistematis menunjukkan bahwa elemen permainan seperti cerita, papan peringkat tim, dan skenario interaktif dapat meningkatkan pengetahuan serta keterlibatan peserta didik dalam pembelajaran keamanan siber (International Journal of Serious Games, 2024).

Tema kedua adalah peningkatan kemampuan mengenali phishing. Simulasi phishing membantu peserta didik mengenali ciri tautan palsu, domain yang mencurigakan, permintaan data pribadi, dan pesan yang mendorong tindakan tergesa-gesa. Penelitian eksperimen pada mahasiswa menunjukkan bahwa kelompok gamifikasi mengalami peningkatan kemampuan deteksi phishing sebesar 59 persen, lebih tinggi dibandingkan kelompok pembelajaran video konvensional sebesar 41 persen (Linnaeus University, 2024). Temuan ini menunjukkan bahwa latihan berbasis skenario lebih efektif dibandingkan penyampaian informasi satu arah.

Tema ketiga adalah peningkatan motivasi dan keterlibatan belajar. Elemen poin, lencana, papan peringkat, tantangan, dan umpan balik langsung membuat peserta didik lebih aktif mengikuti pembelajaran. Kajian serious game menunjukkan bahwa permainan edukatif efektif mengembangkan keterampilan perlindungan siber dan meningkatkan motivasi peserta didik untuk memperdalam pengetahuan mengenai keamanan digital (Springer, 2025). Keterlibatan yang tinggi menjadi faktor

penting karena kesadaran keamanan siber memerlukan latihan berulang, bukan sekadar pemahaman konsep sekali jalan.

Tema keempat adalah perubahan perilaku aman digital. Setelah pembelajaran, peserta didik pada kelompok eksperimen menunjukkan kecenderungan lebih tinggi untuk memverifikasi tautan, tidak membagikan data pribadi, menggunakan kata sandi yang lebih kuat, dan melaporkan tautan mencurigakan. Kajian menunjukkan bahwa simulasi phishing yang dikombinasikan dengan pembelajaran mikro gamifikasi dapat menghasilkan perubahan perilaku yang terukur, bukan hanya peningkatan pengetahuan (CyberNut, 2026). Namun, perubahan perilaku memerlukan pengulangan dan penguatan secara berkala, bukan hanya satu kali pelatihan.

PEMBAHASAN

Hasil penelitian menunjukkan bahwa gamifikasi efektif meningkatkan kesadaran keamanan siber karena mengubah pembelajaran dari proses pasif menjadi pengalaman aktif. Peserta didik tidak hanya menerima informasi mengenai ancaman siber, tetapi juga mengambil keputusan dalam situasi simulasi, menerima umpan balik langsung, dan melihat konsekuensi dari keputusan tersebut. Proses ini mendukung pembelajaran eksperiensial dan penguatan perilaku.

Secara teoretis, temuan ini sejalan dengan teori motivasi belajar yang menekankan pentingnya tantangan, umpan balik, rasa kompeten, dan pengakuan pencapaian. Elemen gamifikasi seperti poin, lencana, dan papan peringkat dapat memperkuat motivasi ekstrinsik, sementara skenario yang menantang dan relevan dapat memperkuat motivasi intrinsik. Dalam konteks keamanan siber, motivasi tersebut perlu diarahkan pada pembentukan kebiasaan aman, bukan sekadar kompetisi antarpeserta didik.

Implikasi praktis dari penelitian ini adalah perlunya pengembangan media pembelajaran keamanan siber yang berbasis skenario. Guru dapat menggunakan kuis interaktif seperti Kahoot atau Quizizz untuk menguji pemahaman dasar, kemudian melanjutkan dengan simulasi phishing dan game edukatif untuk melatih pengambilan keputusan. Simulasi harus dilakukan secara etis, tidak membahayakan data peserta didik, dan disertai umpan balik edukatif setelah peserta didik mengambil keputusan.

Implikasi kebijakan mencakup integrasi kesadaran keamanan siber ke dalam kurikulum, pelatihan guru, dan penyediaan platform pembelajaran yang aman. Sekolah atau kampus perlu menetapkan kebijakan simulasi phishing yang transparan, melindungi data peserta didik, dan tidak menggunakan hasil simulasi

untuk menghukum. Kajian sistematis merekomendasikan penggunaan pengujian terstandar, perbandingan kelompok kontrol, dan evaluasi metode campuran agar efektivitas media gamifikasi dapat dinilai secara lebih kredibel (Springer, 2026).

Penelitian ini memiliki beberapa keterbatasan. Pertama, durasi eksperimen yang relatif pendek belum dapat menunjukkan keberlanjutan perubahan perilaku dalam jangka panjang. Kedua, sampel terbatas pada peserta didik [Nama Sekolah/Kampus], sehingga generalisasi hasil perlu dilakukan secara hati-hati. Ketiga, penggunaan kuesioner mandiri berpotensi menimbulkan bias jawaban sosial. Keempat, efektivitas gamifikasi dapat dipengaruhi oleh perbedaan minat, pengalaman digital, dan akses perangkat antarpeserta didik.

Agenda riset lanjutan yang disarankan meliputi: (1) penelitian longitudinal untuk mengukur keberlanjutan perubahan perilaku; (2) pengembangan game edukatif keamanan siber yang adaptif terhadap tingkat kemampuan peserta didik; (3) analisis pengaruh elemen gamifikasi tertentu terhadap motivasi dan perilaku; (4) penelitian komparatif antara simulasi phishing, kuis interaktif, dan serious game; serta (5) pengembangan model evaluasi kesadaran keamanan siber yang menggabungkan tes pengetahuan, observasi perilaku, dan simulasi.

PENUTUP

Simpulan

Media pembelajaran berbasis gamifikasi efektif meningkatkan kesadaran keamanan siber peserta didik, terutama pada aspek pengetahuan ancaman, kemampuan mengenali phishing, motivasi belajar, dan kecenderungan menerapkan perilaku aman digital. Peningkatan tersebut terjadi karena gamifikasi menghadirkan pembelajaran interaktif, umpan balik langsung, dan skenario ancaman yang lebih nyata.

Efektivitas gamifikasi tidak hanya ditentukan oleh elemen permainan, tetapi juga oleh kesesuaian desain pembelajaran, kejelasan tujuan, kualitas konten, dan evaluasi perilaku. Rekomendasi utama penelitian ini adalah penggunaan simulasi phishing yang aman, kuis keamanan siber, dan game edukatif secara berkala, disertai pelatihan guru serta pedoman etis agar pembelajaran berbasis gamifikasi menghasilkan perubahan perilaku yang berkelanjutan.

DAFTAR PUSTAKA

arXiv. (2025). Cyber security educational games for children: A systematic review. <https://arxiv.org/html/2508.17414v1>

- CyberNut. (2026). Why gamified cybersecurity training works: The science of engagement in K-12. <https://www.cybernut.com/blog/why-gamified-cybersecurity-training-works-the-science-of-engagement-in-k-12>
- Frontiers in Education. (2026). Developing a cybersecurity awareness framework to safeguard students from social media threats. *Frontiers in Education*, 11, 1719173. <https://doi.org/10.3389/feduc.2026.1719173>
- International Journal of Serious Games. (2024). Gamification in cybersecurity education: Short-term effectiveness and behavior change. *International Journal of Serious Games*, 11(1). <https://journal.seriousgamesociety.org/index.php/IJSG/article/download/719/527/4494>
- International Journal of Serious Games. (2025). Serious games for teaching information security and privacy: A systematic literature review. *International Journal of Serious Games*, 12(4). <https://journal.seriousgamesociety.org/index.php/IJSG/article/download/825/578>
- LACCEI. (2025). Gamification in education for phishing prevention: A systematic review. Proceedings of the LACCEI International Multi-Conference for Engineering, Education and Technology. <https://proceedings.laccei.org/index.php/laccei/article/view/4834>
- Linnaeus University. (2024). Evaluating the effectiveness of gamification in cybersecurity education: Enhancing email phishing awareness among university students [Bachelor degree project]. <https://lnu.diva-portal.org/smash/get/diva2:1872531/FULLTEXT01.pdf>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. <https://doi.org/10.1136/bmj.n71>
- Springer. (2025). Investigating the role of serious games on raising students' cybersecurity awareness. *Discover Education*. <https://doi.org/10.1007/s44217-025-00722-0>
- Springer. (2026). A systematic scoping review on game-based cybersecurity education. *International Journal of Information Security*. <https://doi.org/10.1007/s10207-026-01239-9>
- Wiley. (2025). Unlocking cybersecurity: A game-changing framework for serious games and cybersecurity training. *Human Behavior and Emerging Technologies*, 2025, Article 9982666. <https://doi.org/10.1155/hbe2/9982666>