P-ISSN 2828-5557
E-ISSN 2829-0364

Volume 2 Nomor 1
Maret 2023

SIMULASI *HACK VS CRACK*: "GAME" PADA SMA NEGERI 3 SEMARANG

Sendi Novianto[1], Indra Gamayanto[2], Ramadhan Rakhmat Sani[3], Setyo Budi[4]*

[1]Teknik Informatika, Universitas Dian Nuswantoro, Semarang, Indonesia
[2,3,4]Sistem Informasi, Universitas Dian Nuswantoro, Semarang, Indonesia

**setyobudi@dsn.dinus.ac.id, JL. Imam Bonjol No. 207, Kota Semarang, Provinsi Jawa Tengah, 50131, Indonesia*

Abstrak

Game adalah salah satu kegiatan yang digemari orang untuk memperoleh hiburan dan kesenangan, juga dapat disebut sebagai sebuah kegiatan informal yang memiliki hasil akhir. Lebih jauh lagi, game juga akan dapat mengubah banyak hal, mulai dari karakter, sikap, dan peningkatan kreativitas jika berada di jalur yang benar. Oleh sebab itu, game merupakan hal penting yang perlu di *manage* dengan baik. SMA Negeri 3 Semarang termasuk dalam SMA terbaik yang berada di kota Semarang. Pada tahapan globalisasi serta perkembangan dari teknologi informasi yang begitu pesat, SMA Negeri 3 Semarang membutuhkan peningkatkan kompetensi sumber daya manusia dengan bekerjasama dengan universitas. Pelatihan, simulasi dan penyuluhan mengenai industri kreatif, sosial media, *data mining*, *hack* vs *crack* merupakan hal yang penting sehingga kompetensi dapat meningkat secara signifikan. Pada simulasi *hack* vs *crack* ini berfokus pada game, dimana game secara umum paling disukai dan digemari dari kalangan muda sampai orang tua. Oleh sebab itu, sangat diperlukan pemahaman tentang game dan hal-hal yang dapat menyebabkan *fraud* pada game. Hasil akhir dari Pengabdian kepada Masyarakat adalah siswa dan guru dapat memahami game dan jenis-jenis *fraud* yang terdapat didalamnya, dan pemahaman ini sangat penting untuk masa depan game dan para pemain game.

Kata Kunci: Fraud, Game, Online, Simulasi, Studi Kasus.

Pendahuluan

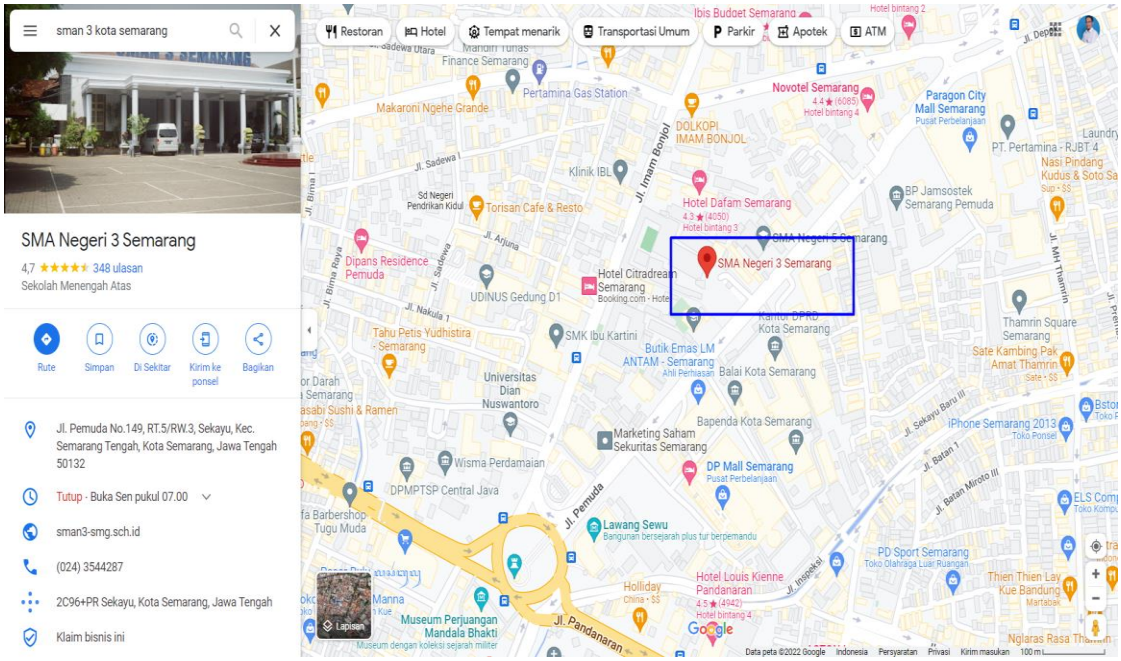
Game adalah jenis aktivitas bermain yang terjadi dalam konteks simulasi tetapi terlihat nyata. Tujuan para pemain adalah untuk memperoleh suatu kemenangan serta dijalankan mengikuti aturan permainan [1]. Atau dalam definisi lain game adalah salah satu kegiatan yang digemari orang untuk memperoleh hiburan dan kesenangan. Lebih jauh lagi, game juga dapat mengubah banyak hal, mulai dari karakter, sikap, dan peningkatan kreativitas jika berada di jalur yang benar. Oleh karena itu, game merupakan hal penting yang harus di *manage* dengan baik.

SMA Negeri 3 Semarang yang termasuk ke dalam salah satu SMA terbaik yang berada di Kota Semarang. Untuk mengembangkan kompetensi siswa/i dan guru, SMA Negeri 3 Semarang bekerjasama dengan universitas dan perguruan tinggi. Kerjasama ini bisa dalam bentuk pelatihan, simulasi, penyuluhan atau yang lainnya di beberapa bidang yang termasuk teknologi informasi seperti *fraud*, *social* media, industri kreatif, data *mining*, dan bidang lainnya agar mampu bersaing dalam menghadapi globalisasi. Saat ini permasalahan di SMA Negeri 3 Semarang yaitu memerlukan pengembangan untuk upaya peningkatan kompetensi siswa/i dan guru dalam menghadapi

globalisasi, terutama terkait *fraud* dan game. Maka di Pengabdian kepada Masyarakat (PkM) ini kegiatan yang dilakukan adalah simulasi *hack* vs *crack* pada game. Harapannya setelah adanya kegiatan ini dapat meningkatkan: 1) kompetensi siswa/i serta guru pada bidang *fraud* dan game; 2) pemahaman yang mendalam tentang *fraud* serta contoh penerapannya dan; 3) mampu menerapkan penanganan awal terhadap *fraud* pada game.

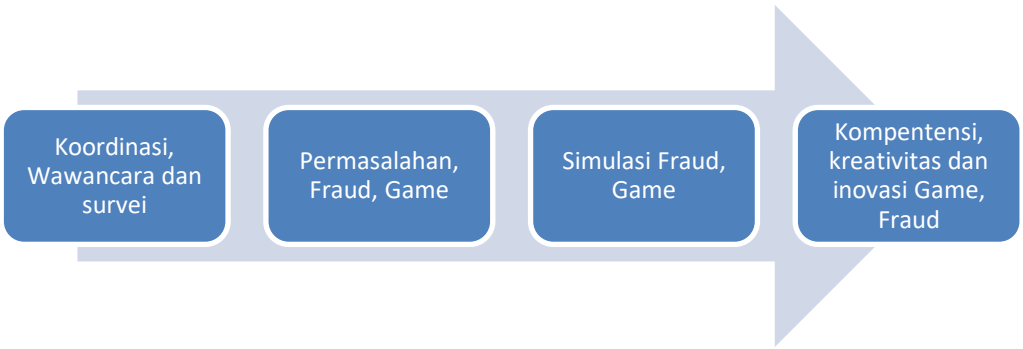
Metode Pelaksanaan

Pelaksanan Pengabdian kepada Masyarakat ini dilaksanakan di SMA Negeri 3 Semarang yang berlokasi di Jl. Pemuda No.149, RT.5/RW.3, Kelurahan Sekayu, Kecamatan Semarang Tengah, Kota Semarang. Apabila dilihat dari google map lokasi sekolah seperti yang ditunjukkan pada gambar 1. Kegiatan simulasi dilakukan sesuai dengan tahapan yang sudah direncanakan seperti ditunjukkan pada gambar 2.



Gambar 1. Lokasi SMA Negeri 3 Semarang dilihat dari Google Map

Pada gambar 2 dijelaskan tahapan pelaksanaan dari kegiatan PkM, yaitu melakukan simulasi berupa tutorial, dimana pemateri akan menjelaskan tentang *fraud* secara umum kemudian dilanjutkan dengan penjabaran dan penerapannya. Secara detail pelaksanaan kegiatan simulasi ini ditunjukkan pada tabel 1.



Gambar 2. Tahapan Kegiatan Simulasi *Fraud*-Game

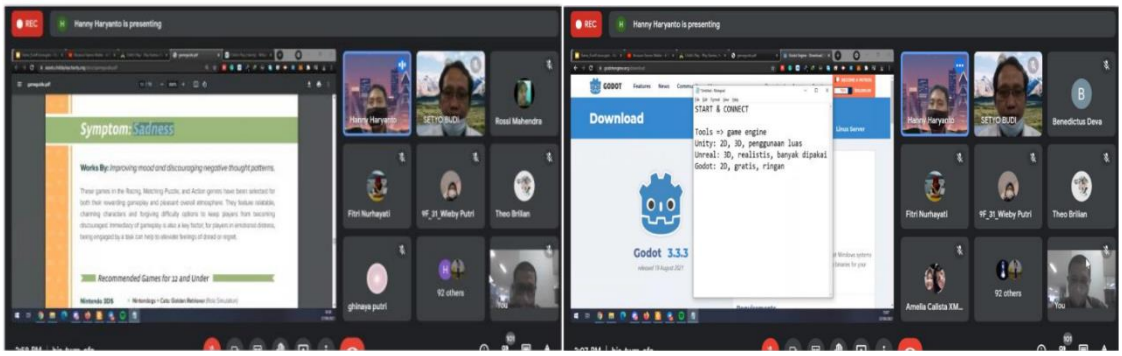
Tabel 1. Penjelasan Detail Tahapan PkM

No	Tahapan	Keterangan
1	Melakukan koordinasi dengan SMA Negeri 3 Semarang	dilaksanakan untuk mendata daftar peserta yang dapat mengikuti program simulasi serta evaluasi masalah yang lebih spesifik
2	Menentukan dan membuat detail materi yang akan diberikan	
3	Menentukan waktu dan tempat penyelenggaraan kegiatan simulasi	waktu dijadwalkan mengikuti waktu luang peserta dan pemberi materi
4	Membuat undangan bagi mitra	undangan diserahkan pada peserta untuk mengetahui waktu, tempat dan agenda kegiatan
5	Menyiapkan sarana dan prasarana kegiatan, termasuk laboratorium komputer, konsumsi, laptop, dan LCD jika dilakukan secara *offline*, tetapi jika dilakukan secara *online*, maka akan dipersiapkan *link* untuk pertemuan baik melalui google meet, zoom, maupun lewat *live* Youtube.	hal ini dilaksanakan sehingga pelaksanaan kegiatan berjalan dengan baik dan lancar
6	Pelaksanaan tutorial dan bimbingan serta konsultasi dilakukan sebagai cara membantu peserta yang mengalami kesulitan	
7	Melakukan pengarsipan dan dokumentasi	administrasi yang meliputi undangan peserta, surat menyurat, dokumentasi foto, dan daftar hadir diarsipkan dan untuk pembuatan laporan
8	Membuat laporan	hal ini dilaksanakan untuk memberi laporan kepada instansi bahwa kegiatan telah benar-benar dilakukan
9	Menyiapkan tim pendamping untuk *monitoring*	hal ini dimanfaatkan untuk memantau keterampilan serta perkembangan hasil simulasi

Peran yang dilaksanakan oleh Tim pengabdian pada pemberian materi adalah: (1) Menjelaskan tentang dasar-dasar *fraud*; (2) Menerangkan langkah-langkah yang praktis secara detail untuk memulai aktivitas *fraud*, (3) Memberikan sesi tanya jawab sehingga dapat menjelaskan lebih detail tentang kegiatan yang sedang berlangsung agar bisa memperjelas materi yang sudah disampaikan.

Hasil dan Pembahasan

Secara umum pelaksanaan pelatihan berjalan dengan baik, hal ini ditandai dengan selesainya semua agenda acara kegiatan simulasi. Walaupun simulasi dilaksanakan secara *daring* menggunakan media google meet, akan tetapi antusias peserta cukup baik. Pada gambar 3 ditunjukkan beberapa foto kegiatan PkM Simulasi *Hack* Vs *Crack*: "Game" di SMA Negeri 3 Semarang.

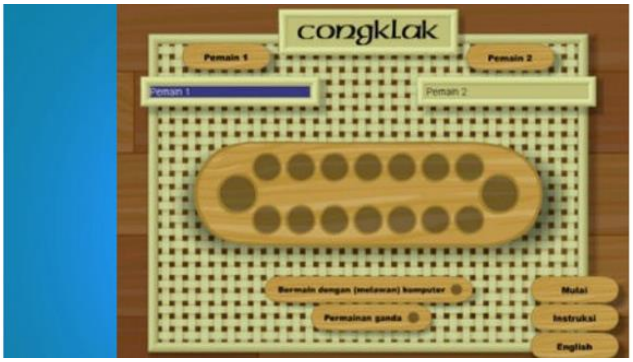


Gambar 3. Kegiatan PkM menggunakan Google Meet

Kegiatan diawali dengan *joint*-nya peserta melalui google meet dari *link* yang sudah diberitahukan pada hari sebelumnya. Pada hari pelaksanaannya diawali oleh moderator untuk memulai kegiatan. Kegiatan dimulai dengan doa yang langsung dipimpin oleh moderator dengan harapan Tuhan YME memberikan kelancaran dan manfaat di dalam kegiatan tersebut. Selama penyampaian materi, peserta dimohon untuk mematikan *microfon* agar materi yang diberikan dapat di dengar oleh peserta dengan baik. Saat tahap tanya jawab, moderator menyediakan kesempatan untuk peserta agar dapat mengajukan pertanyaan. Pertanyaan yang disampaikan oleh peserta bisa ditanggapi langsung oleh pemateri. Beberapa materi yang disampaikan pada kegiatan simulasi ditunjukkan pada gambar-gambar dan penjelasan di bawah ini.

Gambar 4. Contoh Permainan Anak-anak Jaman Dulu

Gambar 4, merupakan salah contoh permainan anak-anak jaman dulu yang kemudian dikonversi dalam bentuk game *digital*. Pada waktu dulu permainan ini dilakukan oleh beberapa anak, dengan game *digital* permainan ini bisa dilakukan hanya satu anak saja. Hasil konversi permainan di tunjukkan pada gambar 4.



Gambar 5. Salah satu contoh Game *Digital* Hasil Pengembangan dari Permainan Jaman Dulu

Gambar 6. Beberapa Dokumentasi Materi Simulasi

Gambar 6 menunjukkan beberapa materi yang disampaikan oleh pemateri, pada materi tersebut menjelaskan tentang contoh beberapa game dan contoh modus penipuan game *online*.

Fraud - Game

Aplikasi game adalah sumber serangan *phishing* yang paling mungkin terjadi pada jaringan perangkat perusahaan. Dalam kasus permainan, peretas dapat membuat salinan palsu dari aplikasi populer dan menggunakan *platform* mereka untuk mengumpulkan informasi tentang pengguna, sementara aplikasi perpesanan dapat memberi kepada peretas akses ke data bisnis sensitif dengan memalsukan domain perusahaan yang sah untuk menipu pengguna perusahaan agar merespon [1],[2].

Mengapa Game *Online* Menarik bagi Penipu

Platform game menghadapi peningkatan kasus penipuan sebelum pandemi dimulai. Sebuah laporan baru-baru ini menunjukkan bahwa skema terhadap *platform* semacam itu naik 30 persen pada Q1 2020 dibandingkan kuartal sebelumnya. Serangan yang diluncurkan melalui akun yang baru terdaftar, sebagian besar mengalami kenaikan, meningkat lebih dari 70%. Data tersebut menyimpulkan bahwa penipu memulai serangan dengan berbagai kompleksitas untuk mencuri informasi pembayaran, mengambil alih akun, dan bahkan mencuri serta menjual aset video game [3].

Melawan Penipuan Game

Identifikasi biometrik adalah salah satu bentuk otentikasi yang dapat mencegah penipu mencuri informasi pribadi dan keuangan yang sensitif, dan banyak perusahaan yang ingin mengadopsi pendekatan keamanan tersebut. Teknologi ini menggunakan kredensial biometrik unik individu, seperti sidik jari atau pemindaian wajah untuk memverifikasi identitas mereka sebelum mengizinkan mereka untuk masuk ke *platform* [4].

Yang perlu di Ketahui tentang Menanggulangi Penipuan Game Pengambilalihan Akun (ATO)

Industri game mengalami banyak sekali pola penipuan yang mirip dengan industri *e-commerce*. Pengambilalihan akun dalam bentuk paling sederhana adalah pencurian identitas. Dalam skenario ini, penjahat menargetkan pemain

game terkenal dengan kredensial yang sangat baik, kekuatan khusus, mata uang game dalam jumlah besar, dll. Meretas akun mereka dan kemudian melanjutkan untuk "menjual" akun mereka kepada pemain amatir yang tidak menaruh curiga. Di gunakan kata amatir karena mereka paling mudah ditargetkan dan dijadikan korban. Bagaimana korban mengetahuinya? dalam kebanyakan kasus, dia tidak menerima pembelian bahkan setelah pembayaran dilakukan atau langsung dikeluarkan dari akun yang dia 'beli' karena aktivitas yang mencurigakan. Salah satu cara untuk mengatasi masalah ini adalah dengan mengaktifkan keamanan dua faktor untuk masuk dan memantau aktivitas akun secara teratur untuk setiap aktivitas yang mencurigakan [5],[6].

Situs Palsu

Situs palsu pada dasarnya adalah bentuk lain dari pengambilalihan akun. Seperti halnya di industri e-bisnis, penipu membuat situs permainan palsu yang meniru tampilan dan nuansa situs aslinya. Dalam kasus ini, pengguna yang tidak curiga memasukkan kredensial game mereka ke situs berbahaya. Data mereka kemudian dijual ke perusahaan penipu dan bahkan diunggah di web gelap, setelah itu kredensial dijual ke pemain yang tidak bersalah. Situs web game harus berhati-hati untuk mengautentikasi identitas mereka sebelum pemain masuk agar tidak ada data dalam jumlah besar yang dikompromikan dan digunakan untuk niat buruk [7].

Tagihan Balik (atau) Penipuan Ramah

Pada tingkat yang lebih kecil, industri game dihadapkan pada sejumlah besar penipuan tolak bayar. Terkait dengan industri e-bisnis, tolak bayar berkaitan dengan prosedur yang terkait dengan keaslian pembelian. Tagihan balik terjadi ketika pembelian *digital* dilakukan untuk membeli produk, fisik atau *online*, dan karena alasan tertentu penbelian tersebut tidak terpenuhi. Artinya produk tidak pernah sampai ke pembeli, atau rusak atau tidak memenuhi janji yang dibuat oleh penjual. Tagihan yang dikembalikan ke kartu pembayaran setelah pelanggan berhasil menyengketakan item dalam laporan rekening atau laporan transaksi mereka, inilah yang disebut tolak bayar [8]. Ada dua alasan mengapa ini terjadi :

1. Alasan pertama adalah karena pemegang kartu asli kebingungan ditagih pembayaran dari sumber yang tidak dikenal. Ini dapat dengan mudah diperbaiki dengan memastikan bahwa pernyataan kartu kredit mencerminkan permainan tertentu daripada perusahaan induknya.
2. Alasan kedua sedikit lebih rumit, ini adalah saat tagihan balik disalahgunakan oleh pelanggan karena alasan jahat. Dalam kasus ini, pemain game menolak untuk membayar biaya yang sah dengan klaim palsu.

Karena industri game berurusan dengan kasus utama transaksi 'cepat' yang nilainya rendah, hal ini mempersulit perusahaan untuk benar-benar membuktikan bahwa setiap transaksi terjadi. Jenis penipuan ini dapat membebani waktu dan sumber daya perusahaan secara signifikan.

Mencari Jalan Keluar

Meskipun mekanisme yang tepat tidak ditetapkan untuk menangani penipuan game, ada banyak perusahaan seperti Razorpay Thirdwatch yang mengembangkan standar yang ditetapkan untuk menangani penipuan. Salah satu kontributor terbesar penipuan permainan adalah preferensi pemain game *online* untuk tetap anonim atau menggunakan 'nama permainan' dan banyak

situs web berfungsi dengan baik untuk memfasilitasi hal ini. Akibatnya, praktik ini membuka wawasan mereka terhadap semua jenis penipuan pembayaran. Salah satu cara situs game untuk melindungi diri dari penipuan pembayaran adalah dengan menerapkan protokol keamanan yang memverifikasi identitas pengguna [9]. Mereka juga dapat memanfaatkan kecerdasan buatan *(artificial intelligence/AI*) dan pembelajaran mesin (*machine learning*) untuk mengamati pola pengguna dan menganalisis efek jaringan di berbagai situs web. Bagaimanapun, perusahaan game harus mencari solusi yang layak untuk memerangi penipuan agar mereka tidak kehilangan banyak uang [10]. Razorpay Thirdwatch menggunakan mesin AI-nya untuk membuat profil pengguna yang berisiko dari ratusan situs web, juga menemukan bahwa mengamati aktivitas pengguna melalui identitas seperti nomor ponsel, ID Perangkat, nomor IMEI, dll. Teknik ini terbukti sebagai standar untuk mengidentifikasi aktivitas kriminal. Karena industri game terus tumbuh secara eksponensial, penting juga untuk membuat solusi dinamis yang tumbuh bersamanya [11],[12],[13].

Evaluasi Hasil Kegiatan Pengabdian kepada Masyarakat

Indikator keberhasilan di dalam kegiatan simulasi ini dapat dilihat dari tabel *pre test* dan *post test* seperti yang ditunjukkan pada tabel 2.

Tabel 2. Indikator Keberhasilan Kegiatan Simulasi

No	Pertanyaan	Presentase Kuisioner Peserta			
		Pre Test		*Post Test*	
		Ya	Tidak	Ya	Tidak
1	Apakah kalian merasa tidak nyaman kalau tidak bermain game?	30	70	10	90
2	Apakah Anda baik-baik saja selama bermain game?	50	50		
3	Setelah bermain game, apakah ada yang mencurigakan terhadap email atau akun lain Anda?	60	40		
4	Apakah Anda pernah kehilangan saldo keuangan setelah sering bermain game?	30	70		
5	Apakah Anda tahu apa yang Anda lakukan apabila dirugikan setelah bermain game?	20	80	90	10
6	Apakah Anda tahu cara menanggulangi *fraud* yang merugikan setelah bermain game?	10	90	90	10
7	Apakah Anda merasa terbantu setelah mengikuti kegiatan simulasi ini?	40	60	95	5
8	Apakah akan Anda terapkan pengetahuan dari kegiatan simulasi ini?	20	80	90	10
9	Apakah Anda memahami materi yang di simulasikan pada kegiatan ini?	15	85	95	5
10	Apakah Anda setuju apabila kegiatan simulasi *hack* vs *crack*: "game" diadakan lagi di lain waktu untuk lebih memahami tentang *fraud* pada game?			100	0

Tabel 2 menunjukkan bahwa hasil *pre test* dan *post test* sekitar 20% peserta yang memahami bagaimana cara menanggulangi apabila terjadi *fraud* pada game, dan 80% belum mengerti tentang penipuan di game. Hal ini beresiko terhadap generasi muda terutama siswa/i SMA Negeri 3 Semarang. kemudian setelah kegiatan simulasi *crack* vs *hack* pada game ada peningkatan

yang cukup baik, yaitu 90% siswa/i sudah mengetahui bagaimana cara paling dasar untuk mengantisipasi penipuan di game.

Kesimpulan

Dari kegiatan PkM yang di aplikasikan dalam bentuk Simulasi *Hack* vs Crack: "Game" pada SMA Negeri 3 Semarang dapat diambil kesimpulan yaitu meningkatkan pemahaman siswa/i dan guru tentang *hack Vs crack* terutama *fraud* pada game, hal ini ditunjukkan pada tabel indikator keberhasilan simulasi. Dari tabel 2 dijelaskan bahwa ada sekitar 85% peserta yang belum memahami tentang *fraud* pada game, tetapi setelah mengikuti kegiatan simulasi ini mengalami peningkatan cukup tinggi yaitu 95% yang mengerti *fraud* pada game. Kedepannya kegiatan ini akan diadakan lagi dilain waktu untuk memahami lebih dalam tentang *fraud* pada game.

Ucapan Terima Kasih

Terima kasih diucapkan kepada LPPM Universitas Dian Nuswantoro dan SMA Negeri 3 Semarang yang memberi kami kesempatan serta kerjasama dalam hal meningkatkan pemahaman tentang game. Kami juga menyampaikan terima kasih kepada penitia kegiatan yang telah mengatur kegiatan sehingga berjalan lancar.

Referensi

[1] M. R. Rahadi, K. I. Satoto, and I. P. Windasari, "Perancangan Game Math Adventure Sebagai Media Pembelajaran Matematika Berbasis Android," *J. Teknol. dan Sist. Komput.*, vol. 4, no. 1, 2016, doi: 10.14710/jtsiskom.4.1.2016.44-49.

[2] T. Grassegger and D. Nedbal, "The role of employees' information security awareness on the intention to resist social engineering," in *Procedia Computer Science*, 2021, vol. 181, no. 2019, pp. 59–66. doi: 10.1016/j.procs.2021.01.103.

[3] A. H. Washo, "An interdisciplinary view of social engineering: A call to action for research," *Comput. Hum. Behav. Reports*, vol. 4, p. 100126, 2021, doi: 10.1016/j.chbr.2021.100126.

[4] D. Alharthi and A. Regan, "Social Engineering Infosec Policies (SE-IPS)," *Comput. Sci. Inf. Technol. (CS IT)*, pp. 57–74, 2021, doi: 10.5121/csit.2021.110104.

[5] A. Purohit, A. Mounika, V. S. Madhumala, K. Umarani, and A. S. T. Reddy, "Cyber Threats in Internet of Thing systems and Impact reduction," *Math. Stat. Eng. Appl.*, vol. 71, no. 4, 2022.

[6] M. Hijji and G. Alam, "A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats during the COVID-19 Pandemic: Challenges and Prospective Solutions," in *IEEE Access*, 2021, vol. 9, pp. 7152–7169. doi: 10.1109/ACCESS.2020.3048839.

[7] I. Shammugam, G. N. Samy, P. Magalingam, N. Maarop, S. Perumal, and B. Shanmugam, "Information security threats encountered by Malaysian public sector data centers," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 3, pp. 1820–1829, 2021, doi: 10.11591/ijeecs.v21.i3.pp1820-1829.

[8] M. H. Alsulami *et al.*, "Measuring awareness of social engineering in the educational sector in the kingdom of saudi arabia," *Inf.*, vol. 12, no. 5, pp. 1–13, 2021, doi: 10.3390/info12050208.

[9] E. E. Odokuma and M. O. Musa, "Internet Threats and Mitigation Methods

in Electronic Businesses Post Covid-19," *Int. J. Comput. Appl.*, vol. 184, no. 19, pp. 1–4, 2022, doi: 10.5120/ijca2022922195.

[10] C. B. Mateus-Coelho, "Advanced Research on Information Systems Security , an International Detection and Handling of Threats in Pre-Established Networks Through a Junior Perspective in Internship," *Adv. Res. Inf. Syst. Secur. an Int. J.*, vol. 01, no. 01, pp. 41–49, 2021.

[11] P. R. Brandao and H. S Mamede, "Phishing and Advanced Persistent Threats," *J. Math. Comput. Appl.*, vol. 2022, no. June, pp. 1–4, 2022, doi: 10.47363/jmca/2022(1)105.

[12] Z. Wang, H. Zhu, P. Liu, and L. Sun, "Social engineering in cybersecurity: a domain ontology and knowledge graph application examples," *Cybersecurity*, vol. 4, no. 1, 2021, doi: 10.1186/s42400-021-00094-6.

[13] S. Venkatesha, K. R. Reddy, and B. R. Chandavarkar, "Social Engineering Attacks During the COVID-19 Pandemic," *SN Comput. Sci.*, vol. 2, no. 2, pp. 1–9, 2021, doi: 10.1007/s42979-020-00443-1.