Jurnal Pendidikan dan Teknologi Indonesia (JPTI)
Vol. 5, No. 7, Juli 2025, Hal. 1981-1992
DOI: https://doi.org/10.52436/1.jpti.873
p-ISSN: 2775-4227
e-ISSN: 2775-4219

Analisis Serangan Social Engineering melalui Pretexting, Impersonating, dan Phishing pada Pemain Game Mobile Online

Januponsa Dio Firizqi*[1], Valentinus Putra Setiawan[2]

[1,2]Informatika, Universitas Pradita, Indonesia
Email: [1]januponsa.dio@pradita.ac.id, [2]valentinus.putra@student.pradita.ac.id

Abstrak

Penelitian ini menganalisis metode serangan rekayasa sosial (social engineering) yang terjadi dalam konteks permainan mobile online, khususnya pada **PUBG Mobile** dan **Mobile Legends**. Studi ini bertujuan untuk mengidentifikasi metode serangan seperti *pretexting*, *impersonation*, dan *phishing*, serta faktor-faktor yang mempengaruhi keberhasilannya. Penelitian dilakukan menggunakan metode kuantitatif, melibatkan simulasi serangan melalui platform media sosial, komunitas game, dan komunikasi dalam game. Hasil penelitian menunjukkan bahwa dari 124 responden yang menjadi target serangan, 88 akun berhasil ditembus. Faktor keberhasilan mencakup tekanan sosial, keterbatasan waktu bermain, rendahnya kesadaran pengguna terhadap risiko keamanan, dan daya manipulasi teknik *social engineering*. Sebaliknya, aktivasi fitur keamanan seperti autentikasi dua faktor (2FA) menjadi hambatan utama bagi keberhasilan serangan. Hasil dari penelitian ini memberikan strategis untuk meningkatkan kesadaran dan perlindungan pengguna, termasuk edukasi keamanan digital, peningkatan fitur keamanan pada platform game, dan kolaborasi dengan komunitas game. Dengan implementasi langkah-langkah ini, risiko serangan *social engineering* dapat diminimalkan secara signifikan, menciptakan lingkungan game yang lebih aman bagi pemain.

Kata kunci: *Game Online, Impersonation, Phishing, Pretexting, Social Engineering.*

.

Analysis of Social Engineering Attacks Through Pretexting, Impersonating, and Phishing on Online Mobile Game Players

Abstract

This study analyzes social engineering attack methods occurring in the context of online mobile gaming, specifically targeting PUBG Mobile and Mobile Legends. The aim of this research is to identify attack techniques such as pretexting, impersonation, and phishing, as well as the factors influencing their success. The study adopts a quantitative approach, involving simulated attacks conducted through social media platforms, gaming communities, and in-game communication. The findings reveal that out of 124 respondents targeted in the attacks, 88 accounts were successfully compromised. Contributing factors to the success include social pressure, limited playtime, low user awareness of security risks, and the manipulative nature of social engineering techniques. Conversely, the activation of security features such as two-factor authentication (2FA) served as a major barrier to successful attacks. The results of this study offer strategic insights to enhance user awareness and protection, including digital security education, improved security features in gaming platforms, and collaboration with gaming communities. By implementing these measures, the risk of social engineering attacks can be significantly reduced, creating a safer gaming environment for players.

Keywords: *Game Online, Impersonation, Phishing, Pretexting, Social Engineering*

1. PENDAHULUAN

Teknologi informasi dapat mengubah ekonomi, budaya, politik, dan hukum. Selain menghasilkan manfaat bagi banyak orang, perkembangan teknologi informasi juga memicu kejahatan baru, yaitu serangan *cyber* dari internet [1]. Jumlah pengguna internet yang meningkat juga menimbulkan ancaman terhadap privasi yang dapat membahayakan data pribadi [2]. Pesatnya perkembangan teknologi saat ini sangat membantu orang dalam berkomunikasi dan mengakses berbagai aplikasi online, seperti *fintech*, game online, belanja, kartu kredit, aplikasi perbankan, streaming video, musik, dan lainnya. *Cybercrime* merupakan fenomena yang sangat mengkhawatirkan, mengingat tindakan seperti *carding*, *hacking* penipuan, terorisme, dan penyebaran informasi yang mengganggu menjadi bagian dari aktivitas pelaku *cybercrime* [3].

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Perkembangan teknologi tidak hanya mengubah cara kita berkomunikasi, bekerja, dan mengakses informasi, tetapi juga bagaimana kita bermain game. Game online, terutama yang berbasis daring, telah menjadi bagian penting dari kehidupan sehari-hari banyak orang. Game online sebagai permainan yang menggunakan teknologi internet memiliki dampak positif seperti meningkatkan relasi sosial, namun juga memiliki dampak negatif jika tidak dikontrol [4]. Popularitas game online ini diikuti oleh munculnya berbagai ancaman, salah satunya adalah serangan *social engineering*.

Social engineering dipahami sebagai strategi yang memanfaatkan kelemahan manusia dalam proses manipulasi untuk mendapatkan informasi sensitif atau mengakses data penting, terutama di era digital [5]. Dalam konteks game online, pelaku kejahatan menggunakan teknik *social engineering* untuk mengeksploitasi pemain, mengakses akun mereka, atau mencuri data sensitif seperti informasi login atau pembayaran. Serangan ini sering memanfaatkan perangkat pribadi pengguna, seperti ponsel atau tablet, untuk mengeksploitasi kerentanan manusia dalam memberikan informasi pribadi [6].

Serangan *social engineering* memanfaatkan kesalahan manusia untuk melewati langkah-langkah keamanan teknis, dan terbukti sangat efektif di platform dengan interaksi pengguna tinggi, seperti game online. Temuan ENISA menunjukkan bahwa 84% serangan siber berbasis pada beberapa bentuk *social engineering*, menyoroti peran kesalahan manusia dalam kegagalan keamanan platform, termasuk layanan permainan daring [7].

Komunikasi di dalam komunitas virtual game online sering kali menjadi jalan masuk bagi pelaku serangan *social engineering* untuk memanipulasi korban mereka [8]. Framework yang dirancang untuk memahami pola serangan *social engineering* dapat membantu mengidentifikasi metode yang paling sering digunakan oleh penyerang [9]. Metode serangan yang paling sering digunakan adalah *pretexting*, *impersonation*, dan *phishing*. Taktik rekayasa sosial seperti ini semakin sering digunakan dalam platform game online untuk memanfaatkan kepercayaan pengguna dan mengambil informasi sensitive [10].

Selain itu, popularitas *multiplayer online games* membuat mereka menjadi target utama serangan siber, terutama metode *social engineering* yang menipu pemain untuk mengungkapkan kredensial akun (Mahmor et al., 2024). Serangan ini semakin berbahaya selama pandemi COVID-19, ketika waktu bermain game online meningkat secara signifikan [11].

Cybercriminals juga sering menggunakan teknik seperti *impersonation* dan hadiah palsu untuk memancing pemain ke dalam penipuan. *Deepfake* kini mulai digunakan di lingkungan game virtual untuk menciptakan ilusi identitas palsu, membuka peluang baru bagi serangan *social engineering* [12]. Dalam game online, pelaku serangan sering kali menciptakan skenario atau persona palsu untuk memanipulasi pemain agar memberikan informasi sensitive.

Selain itu, pelatihan berbasis game telah terbukti efektif meningkatkan respons manusia terhadap ancaman keamanan siber, termasuk serangan *social engineering* [13]. Pendekatan berbasis kesadaran seperti model PROTECT (*Prepare, Recognize, Observe, Think, Engage, Communicate*) memungkinkan pemain untuk lebih tanggap terhadap ancaman, sementara mitigasi berbasis riset menjadi penting dalam mengurangi dampak serangan ini [14].

Meskipun sejumlah penelitian telah membahas social engineering dalam konteks umum seperti sistem perbankan, organisasi, dan media sosial [2][5][6], masih sangat terbatas kajian yang secara spesifik meneliti teknik serangan ini dalam lingkungan game online berbasis mobile. Studi seperti oleh Tariq et al. (2023) menyoroti potensi ancaman deepfake dan impersonation di lingkungan gaming, sementara Mahmor et al. (2024) menggarisbawahi tingginya risiko serangan terhadap pemain multiplayer selama pandemi. Namun, tidak banyak yang mengkaji secara langsung strategi pretexting, impersonation, dan phishing dalam konteks dua game mobile populer seperti PUBG Mobile dan Mobile Legends. Oleh karena itu, penelitian ini hadir untuk mengisi kekosongan tersebut dengan pendekatan berbasis simulasi yang sesuai dengan karakteristik pengguna game mobile yang popular.

Fenomena ini menarik untuk diteliti, mengingat banyaknya kasus yang melibatkan *social engineering* di game online. Permainan online menjadi target karena sifatnya yang interaktif dan melibatkan banyak pemain yang mungkin tidak sepenuhnya memahami risiko keamanan. Selain itu, di dalam game mobile, metode serangan ini sering kali lebih efektif karena interaksi pengguna yang cepat dan tidak jarang kurang hati-hati. Kesadaran pengguna terhadap serangan *social engineering* masih rendah, sehingga diperlukan pendekatan pendidikan yang komprehensif [15].

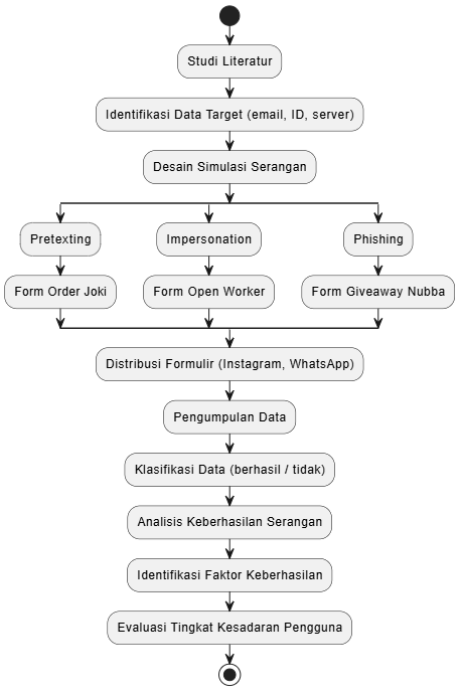
Berdasarkan fenomena tersebut, penelitian ini akan mencoba menganalisis metode-metode serangan *social engineering* yang umum terjadi di game online, khususnya game mobile. Penelitian ini juga akan mengidentifikasi faktor-faktor yang mempengaruhi keberhasilan serangan tersebut serta memberikan rekomendasi untuk meningkatkan kesadaran dan perlindungan pengguna terhadap ancaman *social engineering*.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam studi ini adalah metode kuantitatif dengan pendekatan eksperimental, yang bertujuan untuk menganalisis efektivitas serangan social engineering di game online pada platform mobile, khususnya PUBG Mobile dan Mobile Legends. Penelitian dimulai dengan studi literatur untuk mengumpulkan teori dan referensi terkait, dilanjutkan dengan riset informasi yang mengidentifikasi data target seperti email, password, ID, dan server akun game. Setelah itu, dilakukan simulasi serangan menggunakan tiga pendekatan utama, yaitu pretexting, impersonation, dan phishing, yang dikemas dalam bentuk formulir Google Form untuk mengelabui target agar memberikan informasi sensitif.

Dalam metode pengumpulan data, penguji menggunakan tiga jenis formulir: Form Order Joki untuk pretexting dengan skenario jasa joki akun game, Form Open Worker untuk impersonation dengan skenario perekrutan pekerja joki, dan Form Giveaway Nubba untuk phishing dengan iming-iming hadiah. Ketiga form ini meminta target mengisi data akun mereka dengan format khusus guna menghindari pembatasan dari platform Google Form. Data yang diperoleh kemudian dianalisis untuk mengukur tingkat keberhasilan setiap metode serangan, mengidentifikasi faktor-faktor yang mempengaruhi keberhasilan, serta mengevaluasi tingkat kesadaran player terhadap ancaman social engineering. Hasil dari penelitian ini diharapkan dapat memberikan rekomendasi dalam meningkatkan kesadaran keamanan siber, khususnya di kalangan pemain game online.



Gambar 1. Alur Penelitian

Gambar 1 diatas memperjelas alur penelitian, tahapan metode yang digunakan dimulai dengan studi literatur untuk meninjau referensi terkait *social engineering* dalam konteks game online. Selanjutnya dilakukan identifikasi target dengan menentukan data sensitif seperti email, password, ID akun, dan *server* permainan. Tahap berikutnya adalah pembuatan simulasi serangan dengan tiga pendekatan: pretexting melalui formulir layanan joki, impersonation melalui skenario perekrutan joki, dan phishing melalui penawaran hadiah giveaway palsu, semuanya dikemas dalam bentuk Google Form. Formulir ini kemudian didistribusikan melalui komunitas game seperti WhatsApp, Instagram, dan media sosial. Setelah data terkumpul, dilakukan pengolahan dan klasifikasi berdasarkan keberhasilan serangan, yang diukur dari jumlah akun yang mengisi informasi login secara lengkap dan valid. Faktor-faktor keberhasilan, seperti tekanan sosial, intensitas bermain, dan kepercayaan terhadap persona penyerang, dianalisis secara deskriptif. Dalam hal validitas dan etika penelitian, seluruh partisipasi dilakukan secara sukarela dengan penyampaian disclaimer dan informed consent. Tidak ada data yang disalahgunakan, dan semua informasi dijaga kerahasiaannya serta digunakan hanya untuk analisis statistik dalam rangka keperluan akademik.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

3. HASIL DAN PEMBAHASAN

3.1. Pengujian *Pretexting*

Pengujian pertama yang dilakukan penguji menggunakan social engineering dengan pendekatan teknik sosial berupa pretexting yang menargetkan player PUBG Mobile dan Mobile Legends. Tahapan pengujiannya adalah sebagai berikut:Penguji pertama-tama akan membeli sebuah akun Instagram sebagai store joki game PUBG Mobile dan Mobile Legends, lalu mengubah namanya menjadi Nubba.Corp seperti pada Gambar 2. Nama Nubba.Corp ini diambil karena merupakan salah satu komunitas game yang sangat aktif dengan anggota yang kurang lebih berjumlah 300 orang, sehingga akan memudahkan penguji melakukan pengujian dengan berpura-pura menjadi salah satu pengurus komunitasnya. Alasan lainnya adalah karena kebanyakan player akan lebih tertarik untuk bergabung ke sebuah komunitas tertentu dan memercayai orang-orang di dalamnya.

Setelah akun Instagram selesai dibuat, penguji membuat Google Form yang harus diisi oleh target untuk menggunakan jasa joki store. Isi dari Google Form tersebut salah satunya akan meminta target untuk memberikan informasi pribadi berupa alamat email (bisa untuk akun media sosial seperti Facebook, Twitter, ataupun TikTok) dan password dari alamat email tersebut untuk digunakan login oleh penjoki (penguji). Sample yang terkumpul akan masuk ke dalam Google Sheets untuk diuji oleh penguji, seperti ditunjukkan pada Gambar 3. Setelah Google Form selesai dibuat, penguji akan menambahkan beberapa detail ke Instagram Nubba.Corp seperti postingan tata cara order joki, testimoni palsu para customer yang sudah memakai jasa store joki, serta beberapa atribut lain agar akun Instagram terlihat seperti sudah lama beroperasi untuk meyakinkan target.

Gambar 2 Instagram Nubba.Corp

Setelah seluruh persiapan selesai, penguji mulai melakukan pengujian. Pertama-tama, penguji mempromosikan store joki melalui berbagai platform komunikasi seperti WhatsApp, Telegram, Discord, serta melalui chat in-game pada masing-masing game yang diuji, dengan tujuan untuk memperoleh lebih banyak data yang dapat dianalisis. Penyerangan ini dilakukan dalam rentang waktu 24 jam, di mana selama periode tersebut berhasil dikumpulkan sebanyak 41 sampel data melalui Google Form yang telah disebarkan.

Setelah data terkumpul, penguji melanjutkan ke tahap berikutnya, yaitu mencoba masuk ke akun target yang telah mengisi form dan memberikan informasi berupa alamat email dan password. Penguji terlebih dahulu melakukan login ke akun media sosial target, kemudian dilanjutkan dengan login ke akun game yang bersangkutan. Pengujian dimulai pada game Mobile Legends, lalu dilanjutkan pada PUBG Mobile. Dalam proses login ke akun game Mobile Legends, ditemukan bahwa target memberikan akses login melalui akun media sosial Facebook. Penguji berhasil mengakses akun media sosial tersebut, dan selanjutnya berhasil masuk ke akun Mobile Legends milik target. Hasilnya, penguji dapat mengakses ID game target secara penuh.

Pengujian yang kedua dilakukan kembali kepada target yang memesan jasa joki game PUBG Mobile, dengan akses login yang berbeda, yaitu melalui email secara langsung. Penguji melakukan login sesuai dengan data yang telah diinput oleh target melalui Google Form, dan berhasil masuk ke akun target. Setelah berhasil mengakses akun email, penguji kemudian melakukan login ke dalam game PUBG Mobile dengan menggunakan opsi login melalui Google Play, dan berhasil masuk ke akun media sosial target. Dalam gambar 3 ini menunjukan penguju berhasil login ke akun game dan akun media sosial target.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Gambar 3 Berhasil *login* ke akun media sosial dan akun *game* target.

3.2. Pengujian Impersonation

Pengujian kedua yang dilakukan oleh penguji menggunakan serangan social engineering dengan pendekatan teknik pretexting, yang menargetkan player PUBG Mobile dan Mobile Legends. Tahapan pengujiannya adalah sebagai dengan langkah pertama, penguji kembali menggunakan akun Instagram Nubba.Corp dan membuat posting dengan tujuan mencari *worker/player* yang bersedia melakukan joki pada game PUBG Mobile dan Mobile Legends, sebagaimana ditunjukkan pada Gambar 4. Selanjutnya, penguji membuat kembali sebuah Google Form yang harus diisi oleh target untuk mendaftar sebagai worker.

Formulir ini sekaligus digunakan untuk mengumpulkan informasi pribadi berupa alamat email (yang dapat digunakan untuk akun media sosial seperti Facebook, Twitter, atau TikTok) dan password dari alamat email tersebut untuk kemudian digunakan oleh penjoki (penguji) dalam proses pengujian. Sampel data yang terkumpul akan secara otomatis masuk ke dalam Google Sheets, yang kemudian akan dianalisis lebih lanjut oleh penguji. Setelah google form selesai dibuat,penguji juga akan melakukan scouting/stalking kepada beberapa target/*player* di discord, whatsapp, instagram, tiktok dan in-*game* untuk memperluas opsi sample data yang di dapat.

Nama & No Whatsapp	Worker Game :	User ID & Nickname	Login Game Via	Usia	Pendidikan Terakhir
Adr 081316401	Mobile Legends	Buzz - 21938540(2039)	Email - Jul	19–24	SMA
Akb 99940	Mobile Legends	RoCCinate - 21938450(1920)	Facebook	19–24	SMA
raul	Mobile Legends	[AFK] - Reaper 0 21838499(0293)	Email - ysu	19–24	S1
Ang 778	Mobile Legends	Shiki 再優 23828326 (2039)	Facebook	19–24	S1
fath 11	Mobile Legends	Chans7Z - 23741993(1290)	Twitter - M	19–24	SMA
ami	Mobile Legends	MGWxMRCL - 21030150(2391)	Email - an	19–24	SMA
has	Mobile Legends	ELCRUZ - 08123744(9012)	Facebook	19–24	S1
fred	Mobile Legends	Keciiii 22903147(9912)	Email - Hu	19–24	S1
abd	Mobile Legends	PUFF2C 23881039(1203)	Twitter - s	19–24	SMP
ima	Mobile Legends	ChoppeRR - 20183347(0012)	Email - no	19–24	S1
Ray 201	Mobile Legends	Rayhan Del Rey - 22934012(1056)	Email - aiic	19–24	S1

Gambar 4 Sample Google Form Worker

Setelah persiapan selesai, penguji kemudian melanjutkan ke tahap pengujian. Pertama-tama, penguji melakukan posting pencarian worker dan mengunggah Instagram Story pada akun Nubba.Corp. Setelah itu, penguji juga mengirimkan pesan langsung (DM) ke beberapa target potensial yang menunjukkan ketertarikan untuk menjadi penjoki di game PUBG Mobile dan Mobile Legends.Penyerangan ini dilakukan dalam rentang waktu 24 jam, di mana setelah waktu tersebut terkumpul sebanyak 42 sampel data dari Google Form joki yang telah disebarkan.

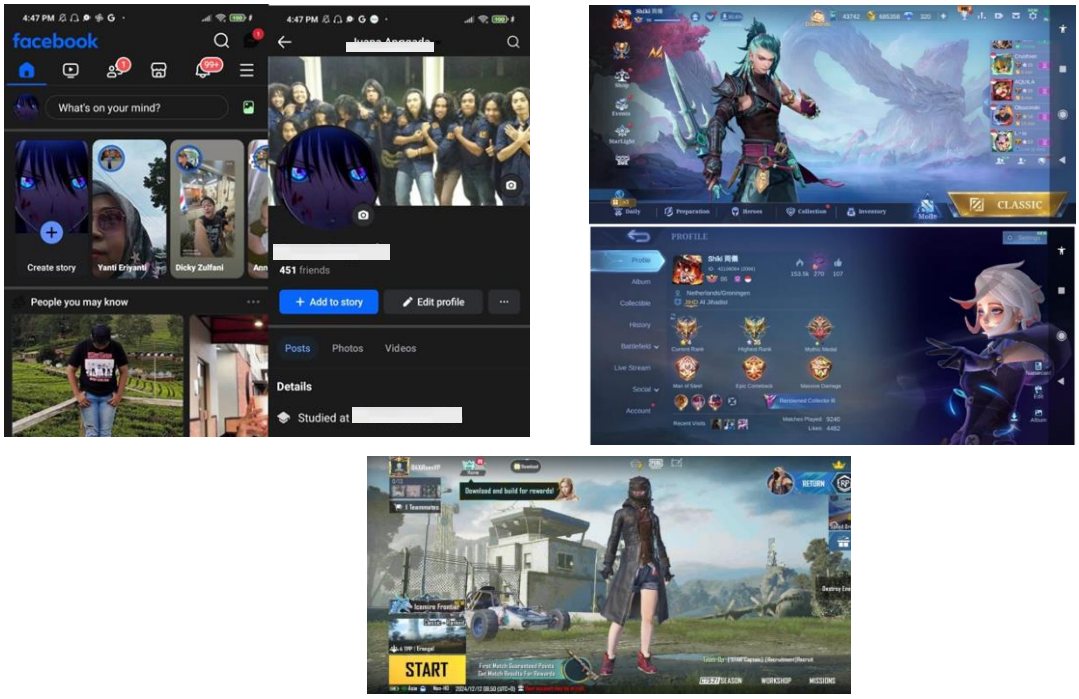
Dari data yang telah terkumpul, penguji kemudian melanjutkan ke tahap selanjutnya, yaitu mencoba masuk ke akun target yang telah mengisi formulir dan memberikan informasi berupa email serta password mereka. Penguji terlebih dahulu melakukan login ke akun media sosial target, kemudian dilanjutkan dengan login ke akun game target. Pengujian pertama dilakukan pada game Mobile Legends, di mana target memberikan akses login melalui akun media sosial Facebook. Penguji berhasil mengakses akun Facebook target, dan setelah berhasil masuk, penguji melanjutkan login ke akun Mobile Legends milik target. Hasilnya, penguji berhasil masuk ke dalam ID game target.

Setelah selesai melakukan pengujian pada akun Mobile Legends, penguji berniat untuk melanjutkan pengujian dengan mencoba login ke game PUBG Mobile milik target berikutnya. Namun, penguji mengalami misclick yang menyebabkan ia secara tidak sengaja melakukan login menggunakan akun Facebook milik target. Ternyata, akun Mobile target juga tertaut dengan akun Facebook tersebut, sebagaimana ditunjukkan pada Gambar

p-ISSN: 2775-4227
e-ISSN: 2775-4219

5. Hal ini secara tidak langsung membuat penguji memperoleh akses ke tiga akun sekaligus, yaitu akun media sosial Facebook, akun Mobile Legends, dan akun PUBG Mobile dalam satu kali pengujian.

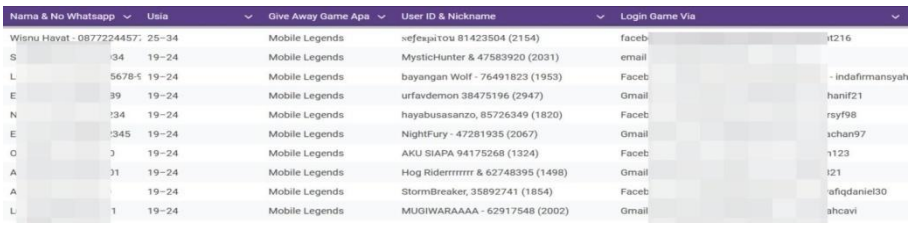
Penguji melanjutkan kembali pengujian terhadap target kedua yang mendaftar sebagai worker untuk game PUBG Mobile, dengan akses login yang berbeda, yaitu melalui Google Play, sehingga mengharuskan penguji untuk terlebih dahulu melakukan login ke akun email target secara langsung. Penguji melakukan login sesuai dengan data yang telah diinput oleh target melalui Google Form, dan berhasil masuk. Setelah berhasil mengakses akun email, penguji kemudian melanjutkan proses login ke dalam game PUBG Mobile dengan menggunakan opsi login melalui Google Play dan akhirnya berhasil masuk ke akun game target.



Gambar 5. Berhasil *login* ke akun media sosial dan akun *game* target.

3.3. Pengujian Phishing

Pengujian ketiga yang dilakukan oleh penguji menggunakan metode social engineering dengan pendekatan teknik sosial berupa phishing, yang menargetkan player PUBG Mobile dan Mobile Legends. Tahapan pengujiannya dangan Langkah awal, penguji kembali menggunakan akun Instagram Nubba.Corp dan membuat sebuah post dengan tujuan menyelenggarakan giveaway berupa UC PUBG Mobile serta Diamonds & Weekly Pass untuk Mobile Legends. Selanjutnya, penguji membuat Google Form yang harus diisi oleh target untuk mengikuti giveaway tersebut. Formulir ini meminta informasi pribadi berupa alamat email (bisa untuk akun media sosial seperti Facebook, Twitter, ataupun TikTok) dan password dari alamat email tersebut agar bisa diakses oleh penguji. Sampel data yang terkumpul dari formulir akan masuk ke dalam Google Sheets dan akan diuji oleh penguji. Setelah Google Form selesai dibuat, penguji menyebarkan posting-an giveaway ini ke berbagai media sosial lainnya untuk memperluas jangkauan dan mengumpulkan lebih banyak data sampel seperti yang ditunjukkan pada Gambar 6.



Nama & No Whatsapp	Usia	Give Away Game Apa	User ID & Nickname	Login Game Via
Wisnu Havat - 0877224457;	25-34	Mobile Legends	81423504 (2154)	faceb
S	34	Mobile Legends	MysticHunter & 47583920 (2031)	email
L	5678-9	19-24	Mobile Legends	bayangan Wolf - 76491823 (1953)
E	39	19-24	Mobile Legends	urfavdemon 38475196 (2947)
N	34	19-24	Mobile Legends	hayabusasanzo, 85726349 (1820)
E	345	19-24	Mobile Legends	NightFury - 47281935 (2067)
O	)	19-24	Mobile Legends	AKU SIAPA 94175268 (1324)
A	1	19-24	Mobile Legends	Hog Riderrrrrrrr & 62748395 (1498)
A		19-24	Mobile Legends	StormBreaker, 35892741 (1854)
L	1	19-24	Mobile Legends	MUGIWARAAAA - 62917548 (2002)

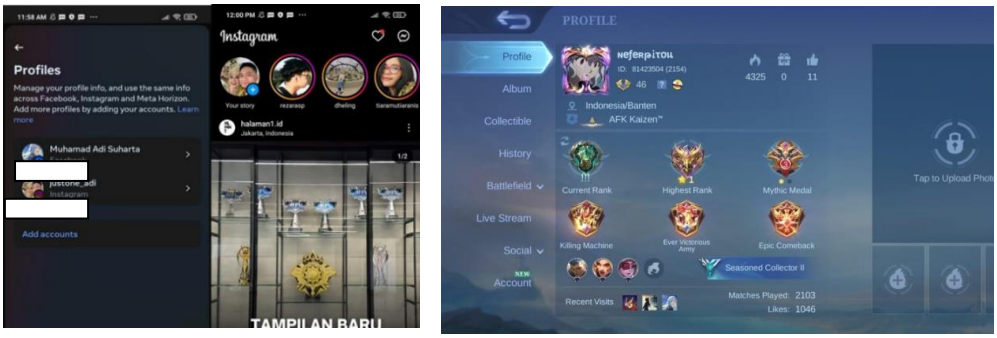
Gambar 6. Sample Google Form Giveaway

Setelah persiapan selesai, penguji mulai melakukan pengujian. Pertama-tama, penguji mempublikasikan post giveaway dan mengunggah story di akun Instagram. Penyerangan ini dilakukan dalam rentang waktu 24 jam, di

p-ISSN: 2775-4227
e-ISSN: 2775-4219

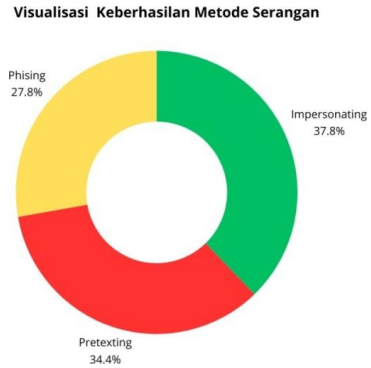
mana setelah 24 jam terkumpul sebanyak 41 sampel data dari Google Form yang telah disebarkan. Dari data yang telah terkumpul, penguji kemudian melanjutkan ke tahap berikutnya, yaitu mencoba masuk ke akun target yang telah mengisi form dan memberikan email serta password mereka.Penguji pertama-tama melakukan login ke akun media sosial target, kemudian dilanjutkan dengan login ke akun game target, dimulai dari game Mobile Legends, lalu dilanjutkan ke PUBG Mobile. Dalam pengujian, penguji mencoba masuk ke akun target yang mendaftar untuk giveaway game Mobile Legends. Dalam kasus ini, target memberikan akses login ke akun Mobile Legends melalui akun media sosial Facebook, namun tidak mencantumkan alamat email secara eksplisit dan hanya memberikan username serta nomor telepon. Meskipun demikian, penguji berhasil mengakses akun media sosial milik target.

Dalam tahap ini, penguji telah melakukan cross-check terhadap profil akun Facebook target dan memastikan bahwa akun tersebut memang tidak memiliki atau menautkan alamat email, melainkan menggunakan nomor telepon sebagai opsi login. Setelah berhasil masuk ke akun instagram target, penguji kemudian melanjutkan proses login ke akun game Mobile Legends milik target dan berhasil masuk seperti pada gambar 7.



Gambar 7 Berhasil *login* ke akun media sosial dan akun *game* target.

3.4. Visualisasi dan Analisis Keberhasilan Metode Serangan



Gambar 8 Grafik tingkat keberhasilan metode serangan

Berdasarkan Gambar 8, grafik tersebut menggabarkan dari tiga jenis serangan yang telah dilakukan dengan total 124 responden, metode impersonation memperoleh 42 responden dengan 33 akun berhasil diakses oleh penguji. Kemudian, metode pretexting menghasilkan 41 responden dengan 31 akun yang berhasil dimasuki. Terakhir, metode phishing juga memperoleh 41 responden, dan sebanyak 24 akun berhasil diakses oleh penguji. Dengan demikian, total sebanyak 88 akun yang meliputi akun email pribadi, akun media sosial, serta akun game milik target berhasil diakses oleh penguji.Penguji memberikan analisa bahwa serangan social engineering terhadap pemain dalam game online sangat mudah dilakukan, bahkan hanya dengan menggunakan metode yang relatif sederhana.

1. Tekanan Lingkungan Sosial & Kompetisi

   Banyak pemain merasa terdorong untuk menjaga atau meningkatkan peringkat mereka dalam permainan, terutama jika mereka aktif di komunitas game. Pemain yang memiliki peringkat tinggi akan mendapatkan pengakuan dan prestise. Prestasi tinggi dalam game sering kali memberikan rasa bangga dan meningkatkan status di mata teman-teman atau komunitas online mereka.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

2. Keterbatasan Waktu

   Banyak pemain, terutama yang berada pada usia produktif, memiliki kesibukan seperti kuliah atau pekerjaan, sehingga waktu bermain menjadi terbatas. Game seperti *PUBG Mobile* dan *Mobile Legends* memiliki durasi permainan yang cukup lama. Menggunakan jasa joki dianggap sebagai cara cepat untuk mencapai target dalam game tanpa harus meluangkan banyak waktu bermain.
3. Minimnya Kesadaran terhadap Risiko

   Tidak semua pemain memahami risiko menggunakan jasa joki atau mengikuti giveaway yang meminta data pribadi akun mereka. Potensi risiko seperti akun terkena banned, pencurian data pribadi, atau penyalahgunaan akun sering kali diabaikan. Banyak pemain merasa bahwa penyedia jasa joki dapat dipercaya atau menganggap risikonya kecil. Selain itu, beberapa pemain tergiur dengan hadiah giveaway tanpa memverifikasi keaslian penyelenggara.
4. Pengaruh Teknik Social Engineering

   Penyedia jasa joki sering kali berpura-pura bekerja sama dengan pemain profesional untuk membangun kepercayaan calon pelanggan. Mereka membuat toko palsu yang menyerupai atau seolah terafiliasi dengan toko terkenal. Janji-janji seperti "dijamin aman" atau "berpengalaman dengan banyak testimoni" sering memengaruhi keputusan pemain. Beberapa penyedia juga menggunakan tautan palsu untuk mencuri informasi akun korban. Fenomena ini diperkuat oleh banyaknya toko joki yang aktif membuat konten di TikTok atau Instagram, memungkinkan teknik impersonation digunakan untuk mencuri identitas dan konten yang diunggah.
5. Budaya Instan & FOMO (Fear of Missing Out)

   Generasi muda cenderung menginginkan hasil yang instan. Menggunakan jasa joki untuk meningkatkan peringkat atau mendapatkan hadiah giveaway tanpa mengeluarkan uang sendiri dianggap sebagai solusi cepat. Faktor psikologis seperti rasa putus asa akibat kekalahan beruntun, kesulitan naik peringkat, serta rasa takut tertinggal (FOMO) karena tidak memiliki aksesori in-game yang sama bagusnya dengan pemain lain, mendorong pemain untuk mencari bantuan eksternal.
6. Kurangnya Edukasi tentang Bahaya Social Engineering

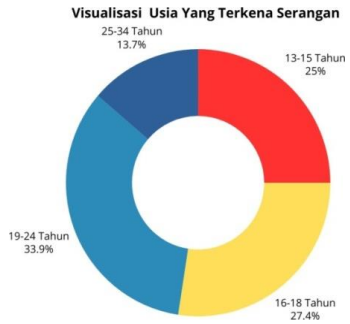
   Banyak pemain belum memahami ancaman manipulasi psikologis yang dilakukan pelaku melalui teknik seperti pretexting, impersonation, dan phishing. Berdasarkan hasil pengujian terhadap 124 responden menggunakan tiga metode serangan social engineering (impersonation, pretexting, dan phishing), sebanyak 88 akun berhasil ditembus oleh penguji. Namun, terdapat 36 akun yang tidak berhasil ditembus, yang dapat dijelaskan melalui beberapa faktor pengaman berikut:
7. Pengaktifan Verifikasi Dua Langkah (2FA)

   Salah satu faktor utama yang menyebabkan kegagalan dalam menembus akun adalah penggunaan verifikasi dua langkah (2FA) pada akun game, media sosial, dan email. Fitur ini mengharuskan pemain memasukkan kode verifikasi tambahan yang dikirim ke perangkat atau nomor telepon terdaftar, selain dari kata sandi utama. Fitur ini secara signifikan mengurangi kemungkinan pengambilalihan akun, meskipun pelaku memiliki data login. Pengguna yang mengaktifkan 2FA akan menerima notifikasi atau kode sementara yang tidak dapat digunakan kembali oleh pelaku.
8. Penggunaan Verifikasi Perangkat

   Beberapa akun menggunakan sistem verifikasi perangkat, yang meminta autentikasi tambahan saat login dari perangkat baru. Misalnya, jika login dilakukan dari perangkat tidak dikenal, sistem akan mengirimkan kode ke nomor telepon atau aplikasi otentikasi pengguna. Ini menjadi penghalang besar bagi penguji, karena mereka tidak memiliki akses ke perangkat yang biasa digunakan pemilik akun, sehingga login gagal dilakukan meskipun data login telah diperoleh.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

3.5. Visualisasi dan Analisis Usia Yang Terkena Serangan

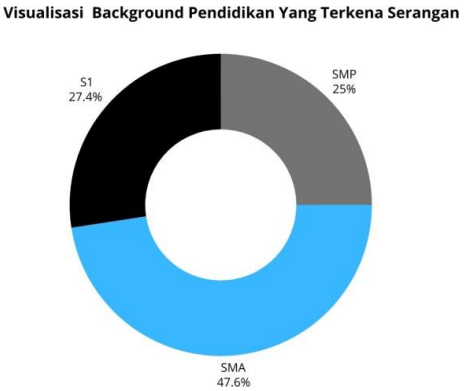


Gambar *9* Grafik usia yang terkena serangan

Berdasarkan data yang divisualisasikan pada Gambar 9, dari total tiga formulir yang disebarkan dengan jumlah keseluruhan 124 responden, penguji melakukan analisis terhadap distribusi usia pengguna yang menjadi korban serangan social engineering pada game online *PUBG Mobile* dan *Mobile Legends*. Adapun hasil analisis tersebut disajikan sebagai berikut: Berdasarkan data pada Gambar, berikut merupakan analisis distribusi usia dari 124 responden yang terkena serangan social engineering pada game online *PUBG Mobile* dan *Mobile Legends*:

1. Usia 19–24 Tahun (33,9%)
   Kelompok usia ini merupakan yang paling banyak menjadi korban serangan. Hal ini dapat dikaitkan dengan tingginya intensitas bermain game online, ditambah motivasi untuk mencapai peringkat atau level tertentu. Namun, keterbatasan waktu akibat aktivitas produktif seperti kuliah atau pekerjaan serta tekanan sosial dari lingkungan komunitas game menjadi faktor pendorong mereka untuk menggunakan jasa joki atau mengikuti giveaway, meskipun berisiko.
2. Usia 16–18 Tahun (27,4%)
   Kelompok usia ini merupakan kelompok terbesar kedua yang menjadi korban. Player pada rentang usia ini cenderung memiliki waktu bermain yang lebih banyak, namun masih kurang memiliki pemahaman dan kewaspadaan terhadap risiko serangan social engineering. Tingkat kehati-hatian yang rendah membuat mereka lebih mudah menjadi target manipulasi.
3. Usia 13–15 Tahun (25%)
   Meskipun tergolong usia muda, kelompok ini juga menunjukkan kerentanan yang cukup tinggi. Minimnya edukasi terkait keamanan digital serta faktor psikologis seperti emosional yang masih labil menjadikan mereka mudah termanipulasi. Keinginan untuk mendapatkan aksesori atau prestasi dalam game secara instan memperkuat kerentanan kelompok ini terhadap tipu daya pelaku.
4. Usia 25–34 Tahun (13,7%)
   Kelompok usia ini tercatat sebagai yang paling sedikit menjadi korban. Kemungkinan besar hal ini disebabkan oleh tingkat kedewasaan dan pengalaman yang lebih tinggi dalam mengenali potensi ancaman digital. Selain itu, prioritas hidup yang lebih beragam di luar dunia game juga membuat mereka lebih berhati-hati dalam berbagi informasi pribadi secara daring.

3.6. Visualisasi dan Analisis Pendidikan Yang Terkena Serangan



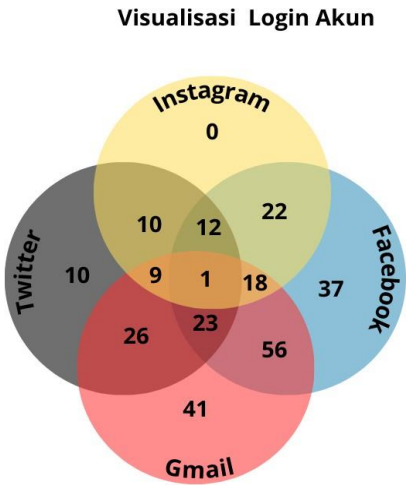
Gambar 10 Grafik pendidikan yang terkena serangan

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Berdasarkan data yang divisualisasikan dalam Gambar 10 dari total 124 responden yang diperoleh melalui tiga form berbeda, penguji melakukan analisis terhadap latar belakang pendidikan pengguna yang rentan terhadap serangan *social engineering*. Berikut adalah rincian dan interpretasinya:

1. Pendidikan SMA (47,6%)
   Kelompok ini merupakan mayoritas dari korban serangan. Hal ini dapat dikaitkan dengan tingginya populasi pelajar SMA yang aktif dalam komunitas game online serta memiliki waktu luang yang relatif lebih banyak. Kurangnya kesadaran terhadap pentingnya keamanan siber serta pengalaman digital yang masih terbatas menjadikan mereka sasaran empuk bagi pelaku.
2. Pendidikan S1 (27,4%)
   Responden dengan latar belakang pendidikan perguruan tinggi menunjukkan tingkat kerentanan yang cukup signifikan. Meskipun secara akademik lebih tinggi, player dari kelompok ini sering terlibat dalam aktivitas kompetitif seperti turnamen dan transaksi dalam game. Ketertarikan terhadap fitur eksklusif dan reward dalam game menjadikan mereka lebih mudah tergiur oleh metode phishing, impersonation, atau pretexting.
3. Pendidikan SMP (25%)
   Meskipun proporsinya lebih kecil, kelompok ini tetap menunjukkan tingkat kerentanan yang perlu diperhatikan. Minimnya pemahaman terkait ancaman digital serta kecenderungan untuk mudah percaya pada informasi yang diterima secara daring menjadi faktor utama penyebab kerentanan pada kelompok ini.

3.7. Visualisasi dan Analisis Akun Yang di Masuk ke Luar Gmail & Game



Gambar 11 Grafik login akun

Berdasarkan data yang divisualisasikan dalam Gambar 11, dari total tiga form yang telah disebarkan, terdapat 88 akun yang berhasil diakses oleh penguji melalui metode social engineering. Menariknya, dari 88 akun tersebut, beberapa di antaranya memiliki keterkaitan atau integrasi dengan akun lain, seperti akun Gmail dan media sosial (Facebook, Twitter, TikTok, dll.) yang tidak dicantumkan secara eksplisit oleh responden saat mengisi Google Form.Hal ini menunjukkan bahwa integrasi akun lintas platform (misalnya login ke game menggunakan akun Google atau Facebook yang juga terhubung ke aplikasi lain) menciptakan celah tambahan yang dapat dimanfaatkan oleh pelaku. Dengan hanya mendapatkan satu akses (misalnya email dan kata sandi dari satu akun), penguji dapat menelusuri dan masuk ke beberapa layanan lain yang terhubung, bahkan tanpa sepengetahuan target.

Berdasarkan visualisasi yang diperoleh dari hasil pengujian terhadap 88 akun yang berhasil diakses, penguji mengidentifikasi beberapa temuan dan pola umum terkait kerentanan keamanan pengguna game online (PUBG Mobile dan Mobile Legends), sebagai berikut:

1. Penggunaan Kredensial yang Sama di Berbagai Platform
   Banyak pengguna menggunakan alamat Gmail dan kata sandi yang sama untuk berbagai platform media sosial dan aplikasi. Hal ini disebabkan oleh:
   a. Kemudahan Akses:
      Dengan hanya mengingat satu kombinasi alamat email dan kata sandi, pengguna merasa lebih praktis dan tidak perlu mengingat banyak informasi login.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

b. Rendahnya Pemahaman Keamanan:
Banyak pengguna tidak sepenuhnya menyadari risiko besar yang muncul jika kredensial ini diretas, terutama jika data tersebut digunakan untuk mengakses akun lainnya.

Kondisi ini menjadi peluang besar bagi pelaku kejahatan melalui teknik credential stuffing, yaitu memanfaatkan kredensial hasil kebocoran data untuk mencoba masuk ke berbagai platform lain. Jika pengguna menggunakan kata sandi yang sama di berbagai akun, kemungkinan keberhasilan pelaku dalam mencuri akses menjadi sangat tinggi.

2. Persepsi Keamanan yang Keliru
   a. Anggapan Gmail adalah Layanan Aman:
   Gmail dikenal luas memiliki sistem keamanan yang baik, sehingga pengguna sering kali merasa kredensial mereka aman digunakan di berbagai platform tanpa mempertimbangkan risikonya.
   b. Kurangnya Pemahaman Risiko Social Engineering:
   Mayoritas pengguna tidak menyadari bahwa pelaku kejahatan dapat dengan mudah memanfaatkan manipulasi psikologis, seperti serangan phishing atau menyamar sebagai pihak terpercaya, untuk mencuri informasi sensitif mereka.
3. Keterhubungan Akun Melalui Gmail
   Sebagai layanan utama untuk mendaftar dan memverifikasi akun pada berbagai platform, Gmail sering kali menjadi pintu masuk ke akun lainnya. Ketika pelaku berhasil mendapatkan akses ke akun Gmail korban, mereka dapat:
   a. Mereset Kata Sandi:
   Mengubah kredensial di akun-akun lain yang terhubung ke email tersebut.
   b. Mengakses Akun Terhubung:
   Masuk ke platform lain melalui email verifikasi tanpa hambatan.

   Keadaan ini menciptakan efek domino, di mana satu pelanggaran akun dapat berujung pada akses ke banyak akun lain yang dimiliki korban. Meskipun Gmail memiliki sistem keamanan yang baik, pengguna sering kali merasa kredensial mereka aman digunakan di berbagai platform tanpa mempertimbangkan risikonya.
4. Minimnya Penggunaan Autentikasi Dua Faktor (2FA)
   Sebagian besar pengguna tidak mengaktifkan fitur autentikasi dua faktor (2FA), yang sebenarnya dapat memberikan perlindungan tambahan. Dengan tidak adanya 2FA, akses ke akun hanya bergantung pada kombinasi nama pengguna dan kata sandi. Jika kredensial tersebut bocor, pelaku dapat langsung mendapatkan akses tanpa hambatan tambahan.

4. DISKUSI

Hasil penelitian ini menunjukkan bahwa metode social engineering seperti impersonation, pretexting, dan phishing sangat efektif dalam lingkungan game online. Tingkat keberhasilan tertinggi ditemukan pada teknik impersonation, yang menunjukkan bahwa pemain lebih mudah percaya pada figur yang dianggap memiliki otoritas, seperti toko joki atau perekrut komunitas. Temuan ini sejalan dengan studi sebelumnya yang menunjukkan bahwa manipulasi identitas adalah salah satu teknik paling berhasil dalam social engineering [6].

Keberhasilan serangan juga dipengaruhi oleh faktor psikologis dan sosial, seperti tekanan komunitas game, keinginan instan untuk naik peringkat, serta rendahnya kesadaran keamanan digital. Hal ini konsisten dengan temuan [12], yang menunjukkan bahwa pemain muda cenderung mengabaikan risiko keamanan demi kenyamanan atau keuntungan cepat. Kondisi ini diperparah oleh maraknya penggunaan media sosial dan komunikasi in-game sebagai jalur distribusi serangan.

Meskipun sebagian besar serangan berhasil, fitur keamanan seperti autentikasi dua faktor (2FA) dan verifikasi perangkat terbukti efektif mencegah akses tidak sah. Ini mendukung laporan ENISA yang menyebutkan bahwa 2FA dapat memblokir sebagian besar upaya peretasan berbasis kredensial [7]. Dengan demikian, temuan ini menegaskan pentingnya edukasi keamanan dan penerapan fitur protektif yang lebih luas pada platform game online.

5. KESIMPULAN

Penelitian ini menunjukkan bahwa serangan social engineering melalui teknik pretexting, impersonation, dan phishing terbukti efektif dalam mengeksploitasi kerentanan pemain game online, khususnya PUBG Mobile dan Mobile Legends. Dari total 124 responden, sebanyak 88 akun berhasil diakses melalui simulasi yang dilakukan, yang mencakup akun media sosial, email, dan akun game.

Tingkat keberhasilan serangan dipengaruhi oleh beberapa faktor utama, seperti tekanan sosial dalam komunitas game, keterbatasan waktu bermain, dan rendahnya kesadaran terhadap keamanan digital. Di sisi lain,

p-ISSN: 2775-4227
e-ISSN: 2775-4219

fitur keamanan seperti autentikasi dua faktor (2FA) dan verifikasi perangkat terbukti mampu mengurangi keberhasilan serangan secara signifikan.

Secara keseluruhan, temuan ini menegaskan bahwa pemain game mobile, khususnya pada kelompok usia muda, memiliki tingkat kerentanan yang tinggi terhadap manipulasi sosial digital, sehingga penting untuk terus mengkaji dan memahami pola-pola serangan yang berkembang di ranah tersebut.

DAFTAR PUSTAKA

[1] J. Ahmad, A. ul Hasan, T. Naqvi, and T. Mubeen, "A Review on Software Testing and Its Methodology," *Manag. J. Softw. Eng.*, vol. 13, no. 1, pp. 32–38, 2019, doi: 10.26634/jse.13.3.15515.

[2] I. K. O. Kharisma Putra, I. M. A. Darmawan, I. P. G. Juliana, and Indriyani, "Tindakan kejahatan pada dunia digital dalam bentuk phishing," Cyber Security dan Forensik Digital, vol. 5, no. 2, pp. 77–82, 2023, doi: 10.14421/csecurity.2022.5.2.3797.

[3] S. A. Aklani, Haeruddin, and N. Putri, "Implementasi Mail Gateway Security dalam meningkatkan sistem informasi Universitas Internasional Batam: Abstraksi Development Life Cycle (NDLC)," J. Inf. Syst. Manag. (JOISM), vol. 5, no. 2, 2024. [Online]. Available: https://jurnal.amikom.ac.id/index.php/joism/article/view/1378

[4] A. S. Gulo, S. Lasmadi, and K. Nawawi, "Cyber crime dalam bentuk phishing berdasarkan Undang-Undang Informasi dan Transaksi Elektronik," PAMPAS: J. Crim. Law, vol. 1, no. 2, pp. 68–81, 2021, doi: 10.22437/pampas.v1i2.9574.

[5] A. Andoyo, "Sosialisasi dampak positif dan negatif game online bagi anak sekolah dasar," J. PKM Pemberdayaan, vol. 2, no. 1, pp. 33–40, 2021. [Online]. Available: https://jurnalpkmpemberdayaan.yhmm.or.id/index.php/PkMLP3K/article/view/33

[6] R. Triwahono, A. Fauzi, A. Adzansyah, B. Yulivio, M. Y. Fito, R. G. P. Yuntama, and S. W. Azhar, "Pencegahan penipuan social engineering pada masa 4.0," J. Ilmu Multidisiplin, vol. 2, no. 1, pp. 68–74, 2023, doi: 10.38035/jim.v2i1.232.

[7] H. Aldawood and G. Skinner, "A taxonomy for social engineering attacks via personal devices," Int. J. Comput. Appl., vol. 178, no. 50, pp. 19–26, Sep. 2019, doi: 10.5120/ijca2019919411.

[8] I. Stamelos and G. Hatzivasilis, "Active honeyfiles for ransomware encryption mitigation," IEEE International, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10679432/

[9] M. Zakaria, Z. Harahap, and A. Irawan, "Analysis of pretexting and social engineering in online communities," IOP Conf. Ser.: Mater. Sci. Eng., vol. 1174, no. 1, p. 012027, 2022, doi: 10.1088/1757-899X/1174/1/012027

[10] R. F. Abu Hweidi and D. Eleyan, "Social engineering attack concepts, frameworks, and awareness: A systematic literature review," *Int. J. Comput. Digit. Syst.*, 2023, doi: 10.12785/ijcds/1570789805.

[11] L. Nyusti and J. E. Simensen, "Emerging threat of deepfakes: Viability, risks, impacts, and mitigations through a practical use case," in T. Ahram and W. Karwowski, Eds., Human Factors in Design, Engineering, and Computing, AHFE (2024) Int. Conf., vol. 159, AHFE Int., USA, 2024, doi: 10.54941/ahfe1005592

[12] D. L. King, P. H. Delfabbro, J. Billieux, and M. N. Potenza, "Problematic online gaming and the COVID-19 pandemic," J. Behav. Addict., vol. 9, no. 2, pp. 184–186, 2020.

[13] S. Tariq, A. Abuadbba, and K. Moore, "Deepfake in the metaverse: Security implications for virtual gaming, meetings, and offices," in Proc. 2nd Workshop on Security Implications of Deepfakes and Cheapfakes, 2023, pp. 16–19.

[14] F. Muhly, "Improving human responses to cyberdefense by serious gaming," in Cyberdefense: The Next Generation, Cham, Switzerland: Springer Int. Publ., 2023, pp. 183–194.

[15] L. Goeke, A. Quintanar, K. Beckers, and S. Pape, "PROTECT – an easy configurable serious game to train employees against social engineering attacks," in Proc. Int. Workshop on Information and Operational Technology Security Systems, Cham, Switzerland: Springer Int. Publ., 2019, pp. 156–171.

[16] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, "Social engineering attacks prevention: A systematic literature review," IEEE Access, vol. 10, pp. 39325–39343, 2022.