

## Implementasi Game Mobile Legend Dengan Menggunakan Metode Phising

<sup>1</sup> Muhamad Nur Aliansyah Akbar, <sup>2</sup> Muhammad Rafi Ammar, <sup>3</sup> Muhammad Adha Vanurizaldi <sup>4</sup>Essy Malays Sari Sakti

Informatika, Universitas Persada Indonesia YAI, Jakarta Pusat

E-mail: <sup>1</sup> [Alibabam727@gmail.com](mailto:Alibabam727@gmail.com), <sup>2</sup> [rafiammar58@gmail.com](mailto:rafiammar58@gmail.com),  
<sup>3</sup> [vanurizaldi@gmail.com](mailto:vanurizaldi@gmail.com), <sup>4</sup> [emalays67@gmail.com](mailto:emalays67@gmail.com)

### ABSTRAK

Dalam dunia game online, Mobile Legends telah menjadi salah satu permainan yang paling banyak dimainkan, dengan jutaan pengguna aktif setiap hari. Namun, popularitasnya juga membuatnya rentan terhadap serangan cyber, salah satunya adalah melalui metode phishing. Metode phishing ini memanfaatkan ketidaktahuan dan kepercayaan pengguna dengan menyamar sebagai situs atau aplikasi resmi Mobile Legends untuk mencuri informasi pribadi, seperti kata sandi dan data akun. Penjahat cyber akan menciptakan situs web atau aplikasi palsu yang meniru tampilan dan fungsionalitas Mobile Legends asli untuk menipu pengguna agar memasukkan informasi akun mereka. Dengan menggunakan teknik sosial engineering yang canggih, serangan phishing semacam ini bisa sangat persuasif dan sulit dideteksi oleh pengguna yang kurang waspada. Oleh karena itu, pemain Mobile Legends perlu meningkatkan kesadaran mereka terhadap ancaman keamanan cyber ini dan mengambil langkah-langkah pencegahan, seperti memeriksa URL dengan hati-hati sebelum memasukkan informasi pribadi mereka dan menggunakan otentikasi dua faktor untuk melindungi akun mereka.

**Kata kunci :** *Metode phishing, Mobile Legends, keamanan cyber, kesadaran pengguna.*

### ABSTRACT

In the world of online gaming, Mobile Legends has become one of the most played games, with millions of active users every day. However, its popularity also makes it vulnerable to cyber attacks, one of which is through phishing methods. This phishing method exploits the ignorance and trust of users by impersonating as official Mobile Legends websites or applications to steal personal information, such as passwords and account data. Cyber criminals will create fake websites or applications that mimic the appearance and functionality of the original Mobile Legends to deceive users into entering their account

information. By using sophisticated social engineering techniques, such phishing attacks can be highly persuasive and difficult to detect by less vigilant users. Therefore, Mobile Legends players need to increase their awareness of these cyber security threats and take preventive measures, such as carefully checking URLs before entering their personal information and using two-factor authentication to protect their accounts.

**Keyword :** *Phishing method, Mobile Legends, cyber security, user awareness*

## 1. PENDAHULUAN

Perkembangan teknologi informasi berbasis digital, sangat cepat mempengaruhi dalam kehidupan sehari-hari tak terkecuali dalam bidang permainan (Sari Sakti & Wagiyati.P, 2022)

Mobile Legends telah menjadi fenomena dalam industri game online, menarik jutaan pemain dari seluruh dunia dengan gameplay yang seru dan kompetitif. (Haikal, 2023) Namun, kesuksesan besar ini juga telah menarik perhatian para penjahat cyber yang mencari peluang untuk memanfaatkannya. Salah satu metode yang paling umum digunakan untuk mengeksploitasi pengguna Mobile Legends adalah melalui serangan phishing.

Phishing merupakan praktik cybercrime yang meretas informasi pribadi pengguna dengan menyamar sebagai entitas yang tepercaya, seperti situs web atau aplikasi resmi. (Fauzan Imam et al., 2023) Dalam konteks Mobile Legends, para penjahat cyber menciptakan situs web palsu atau aplikasi yang meniru tampilan dan fungsionalitas asli permainan tersebut, (Sugiono, 2018) dengan tujuan untuk mencuri informasi

sensitif, seperti kata sandi dan data akun. Dengan demikian, pengguna yang kurang waspada rentan menjadi korban serangan phishing ini, terjebak dalam jaringan penipuan yang sulit dideteksi. Oleh karena itu, pemahaman akan metode ini dan upaya pencegahan yang diperlukan sangat penting bagi para pemain Mobile Legends untuk menjaga keamanan akun dan data pribadi mereka. Dalam pendahuluan ini, akan ditinjau lebih lanjut tentang bagaimana metode phishing ini dapat merusak pengalaman bermain Mobile Legends serta tindakan yang dapat diambil untuk melindungi diri dari ancaman cyber semacam itu.

## 2. LANDASAN TEORI

Teori tentang serangan phishing dalam konteks permainan Mobile Legends dapat merangkum beberapa konsep penting dalam keamanan cyber dan perilaku pengguna. (Yarfa Dzardi, 2024) Pertama-tama, konsep phishing itu sendiri adalah teknik yang digunakan oleh penjahat cyber untuk memperoleh informasi sensitif dari pengguna dengan menyamar sebagai entitas yang tepercaya. (Wijoyo et al., 2023) Teknik ini

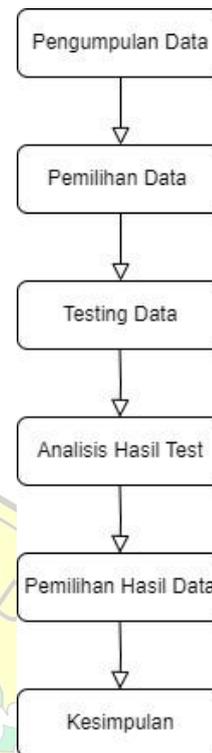
sering kali melibatkan penggunaan email, situs web palsu, atau aplikasi yang meniru tampilan dan fungsionalitas dari platform yang sah, seperti Mobile Legends.

Teori sosial engineering menjadi kunci dalam pemahaman serangan phishing. (Tyas Darmaningrat et al., 2022) Sosial engineering mengacu pada manipulasi psikologis yang dilakukan oleh penjahat cyber untuk memanipulasi pengguna agar melakukan tindakan tertentu, seperti memasukkan informasi pribadi mereka ke dalam situs web palsu. Dalam konteks Mobile Legends, penjahat cyber menggunakan teknik sosial engineering yang canggih untuk membuat serangan phishing mereka lebih meyakinkan, seperti menyediakan imbalan palsu atau menjanjikan manfaat tambahan kepada pengguna yang terpengaruh.

Teori keamanan informasi juga relevan dalam kajian ini. Konsep keamanan informasi mencakup strategi dan praktik yang dirancang untuk melindungi data sensitif dari akses yang tidak sah, manipulasi, atau kerusakan. (Paryati, 2008) Dalam konteks Mobile Legends, keamanan informasi adalah faktor penting dalam menjaga keamanan akun dan data pengguna dari serangan phishing dan ancaman cyber lainnya.

*(Ancaman+Cybercrime+di+Indonesia+dan+Pentingnya+Pemahaman+akan+Fenomena+Kejahatan+Digital+siap+terbit, n.d.)*

### 3. METODOLOGI

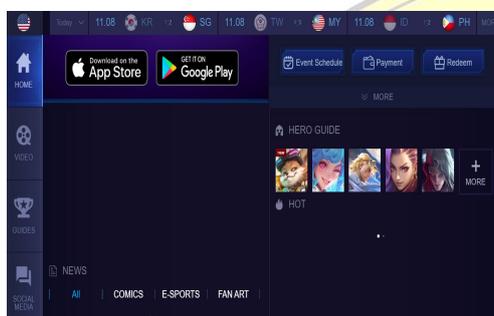


Gambar 1. Langkah Langkah

Metodologi yang digunakan untuk mengkaji serangan phishing dalam konteks permainan Mobile Legends melibatkan tahapan studi literatur untuk memahami dasar-dasar serangan phishing, konsep keamanan cyber, teori sosial engineering, dan perilaku pengguna dalam game online. Setelah itu, dilakukan analisis data dari laporan keamanan, studi kasus, dan survei pengguna untuk mengidentifikasi pola serangan, teknik yang digunakan, serta dampaknya terhadap pengguna. Langkah selanjutnya adalah pengembangan strategi pencegahan yang didasarkan pada temuan analisis data dan teori yang telah dipelajari, seperti peningkatan kesadaran pengguna, penerapan teknologi

keamanan, dan edukasi tentang tindakan pencegahan. Dengan pendekatan ini, dapat diharapkan peningkatan pemahaman tentang serangan phishing dalam Mobile Legends serta upaya perlindungan yang lebih efektif terhadap pengguna game online.

#### 4. HASIL DAN PEMBAHASAN



Gambar 1. Hasil web yang kita buat

Hasil penelitian tentang serangan phishing dalam Mobile Legends, beberapa aspek penting perlu dipertimbangkan. Pertama, meningkatnya jumlah kasus serangan phishing dalam game tersebut menunjukkan adanya kebutuhan mendesak untuk tindakan pencegahan yang efektif. Pengguna Mobile Legends perlu lebih waspada terhadap upaya-upaya phishing yang semakin canggih dan persuasif. Selanjutnya, ditemukan bahwa faktor kesadaran pengguna memiliki peran krusial dalam mengurangi risiko serangan phishing. Dengan meningkatkan pemahaman mereka tentang taktik-taktik yang digunakan oleh penjahat cyber, pengguna dapat lebih mudah

mengenalinya dan menghindari serangan tersebut. (Prasetya et al., 2023)

Pentingnya kerjasama antara pengembang game dan penyedia layanan keamanan untuk melindungi pengguna dari serangan phishing. Pengembang permainan dapat meningkatkan fitur keamanan dalam aplikasi mereka, seperti memperkuat sistem autentikasi dan memberikan edukasi tentang praktik keamanan cyber kepada pengguna. Selain itu, penyedia layanan keamanan juga dapat bekerja sama dengan pihak-pihak terkait untuk memantau dan memblokir situs web phishing yang muncul. Selanjutnya, dalam konteks solusi, perlu diterapkan pendekatan yang holistik yang mencakup pendidikan pengguna, pengembangan teknologi keamanan, dan penegakan hukum terhadap pelaku serangan phishing. Upaya-upaya ini harus didukung oleh dukungan dari pemerintah, industri game, dan masyarakat secara keseluruhan. (Wijaya et al., 2023) Dengan demikian, dapat diharapkan penurunan jumlah kasus serangan phishing dalam Mobile Legends serta peningkatan kesadaran dan keamanan cyber bagi pengguna game online secara umum.

Pendekatan pencegahan tidak hanya harus bersifat reaktif, tetapi juga proaktif. Ini berarti mengantisipasi serangan phishing yang mungkin terjadi di masa depan dan mengambil langkah-langkah untuk mengurangi kerentanan sistem

serta meningkatkan kesadaran pengguna sebelum serangan terjadi. Selain itu, kerjasama antara pemain industri, pemerintah, dan masyarakat sipil juga sangat penting dalam mengatasi masalah serangan phishing dalam Mobile Legends dan game online lainnya. Dengan bekerja sama secara sinergis, berbagai pihak dapat saling melengkapi dalam upaya melawan ancaman keamanan cyber yang semakin kompleks ini. Dengan demikian, pembahasan ini menyoroti pentingnya mengadopsi pendekatan yang komprehensif dan kolaboratif dalam menanggapi serangan phishing dalam Mobile Legends. Hanya dengan upaya bersama dan komitmen yang kuat dari semua pihak terlibat, kita dapat mengurangi risiko serangan phishing dan menciptakan lingkungan game online yang lebih aman dan terpercaya bagi semua pengguna.

implikasi jangka panjang dari serangan phishing dalam Mobile Legends. Salah satu implikasi utamanya adalah kerugian finansial dan reputasi bagi pengguna yang menjadi korban serangan. Pencurian informasi pribadi seperti kata sandi dan data keuangan dapat mengakibatkan penyalahgunaan akun, pembelian tidak sah, atau bahkan pencurian identitas. Selain itu, pengguna yang terkena dampak serangan phishing juga bisa mengalami kerugian reputasi, terutama jika akun mereka digunakan untuk melakukan tindakan ilegal atau merugikan lainnya.

Selain dampak langsung bagi pengguna, serangan phishing juga dapat merusak reputasi Mobile Legends sebagai platform game online yang aman dan terpercaya. Jika serangan phishing terjadi secara terus-menerus tanpa tindakan yang memadai dari pihak pengembang atau penyedia layanan, hal ini dapat mengurangi kepercayaan pengguna terhadap platform tersebut dan menyebabkan penurunan jumlah pemain aktif.

Phishing bukan hanya masalah keamanan individual, tetapi juga masalah yang berkaitan dengan keamanan platform game secara keseluruhan dan industri game online. Diperlukan upaya kolaboratif dan berkelanjutan dari berbagai pihak terkait untuk mengatasi ancaman ini dan menciptakan lingkungan game online yang lebih aman dan terpercaya bagi semua pengguna.

## 5. KESIMPULAN

Penelitian ini menyoroti pentingnya pemahaman dan kesadaran pengguna tentang serangan phishing dalam permainan Mobile Legends. Ditemukan bahwa serangan phishing merupakan ancaman yang nyata dalam ekosistem game online, dengan peningkatan kasus yang dilaporkan dari waktu ke waktu. Pola serangan yang canggih dan persuasif menuntut adanya upaya pencegahan yang lebih proaktif dan kolaboratif dari berbagai pihak terkait, termasuk pengembang permainan, penyedia layanan keamanan, pemerintah, dan

masyarakat sipil. Langkah-langkah pencegahan yang efektif mencakup peningkatan kesadaran pengguna, pengembangan teknologi keamanan, dan kerjasama antar pemangku kepentingan. Dengan mengadopsi pendekatan yang holistik dan kolaboratif, diharapkan dapat mengurangi tingkat keberhasilan serangan phishing dalam Mobile Legends dan meningkatkan keamanan cyber bagi para pengguna game online.

## 6. UCAPAN TERIMA KASIH

Saya ingin mengucapkan terima kasih yang sebesar-besarnya atas kesempatan untuk mempublikasikan penelitian kami tentang serangan phishing dalam permainan Mobile Legends. Kerjasama dan dukungan dari tim redaksi sangat berarti bagi kami dalam memperluas pemahaman tentang ancaman keamanan cyber dalam lingkungan game online. Kami berharap hasil penelitian ini dapat memberikan kontribusi positif bagi komunitas akademis dan industri dalam upaya melawan serangan phishing yang semakin meningkat. Terima kasih atas kerja keras dan dedikasi Anda dalam menjaga standar keunggulan dalam publikasi ilmiah. Kami berharap dapat terus berkolaborasi di masa depan.

## DAFTAR PUSTAKA

*Ancaman+Cybercrime+di+Indonesia+dan+Pentingnya+Pemahaman+akan+Fenomena+Kejahatan+Digital+siap+terbit.* (n.d.).

- uzan Imam, Iqbal Aditya Ferryanto, & Hardika Khusnuliawati. (2023). Sosialisasi Pishing Guna Mengedukasi Ibu-Ibu Pkk Dukuh Brajan Dalam Antisipasi Kejahatan Siber. *Jurnal Pengabdian Masyarakat Sains Dan Teknologi*, 2(4). <https://doi.org/10.58169/jpmsaintek.v2i4.289>
- aikal. (2023). Mobile Legends. *Mamat Tobi*, 11(12–17).
- ryati. (2008). Keamanan Sistem Informasi. *Seminar Nasional Informatika 2008 (SemnasIF 2008) UPN "Veteran" Yogyakarta, 24 Mei 2008, 2008(semnasIF)*.
- asetia, O., Machfud, S., & ... (2023). Sosialisasi Pengenalan Pentingnya Cyber Security Guna Menjaga Keamanan Data di Era Digital Pada Siswa/i SMK Bakti Idhata Jakarta. *JIPM: Jurnal Inovasi ...*, 2.
- ri Sakti, E. M., & Wagiyati, P., S. (2022). Pengembangan Sistem Informasi Persediaan Barang Berbasis Android ( Kasus Cv Berkah Ananda ). *Ikraith-Informatika*, 7(1). <https://doi.org/10.37817/ikraith-informatika.v7i1.2232>
- igiono, L. A. (2018). Trash-talking dalam game online padau user game online di Indonesia (Etnografi virtual game online mobile legends dan arena of valor). *Departemen Ilmu Komunikasi FISIP Universitas Airlangga*.
- as Darmaningrat, E. W., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. *Sewagati*, 6(2). <https://doi.org/10.12962/j26139960.v6i2.92>
- ijaya, Y. I., Rahman, M. S., Chandra, H. A., & ... (2023). Pelatihan Cyber Security Untuk Menjaga Keamanan Dan Privasi Siswa Smk Negeri 4 Banjarmasin. *Jurnal Nusantara ...*, 1(4).
- ijoyo, A., Saputra, A., Pratama, M. R. A., & Rahman, R. (2023). Analisis Serangan Phising dan Strategi Deteksinya. *JRIIN: Jurnal Riset Informatika Dan Inovasi*, 1(4).
- arfa Dzardi. (2024). Analisis Cyber Fraud Pada Platform Jual Beli Game Online. *Doktrin: Jurnal Dunia Ilmu Hukum Dan Politik*, 2(2). <https://doi.org/10.59581/doktrin.v2i2.2546>