**Jurnal Inovasi Artificial Intelligence & Komputasional Nusantara (JIKOMNUS)**
Vol. 2, No. 1, Juli 2025, hlm. 22-26 p-ISSN: 3063-XXXX
SK.ISSN: 30634830/II.7.4/SK.ISSN/09/2024 e-ISSN: 3063-4830

# Analisis Keamanan Sistem Operasi Android terhadap Serangan Phishing pada Aplikasi E-Wallet

**Indra Lesmana Putra[1], Fernando Siahaan[2], M Ihsan Raditya[3], Michael Orlando A. Purba[4] Indra Gunawan[5]**

STIKOM Tunas Bangsa, Pematangsiantar,Indonesia

Email: indralsmana1206@gmail.com[1], siahaanfernando18@gmail.com[2] , muhammadihsanraditya@gmail.com[3], mikaelpurba14@gmail.com[4], indra@amiktunasbangsa.ac.id[4]

**Abstrak**

Penelitian ini menganalisis keamanan sistem operasi Android terhadap serangan phishing yang menargetkan aplikasi e-wallet. Dengan meningkatnya penggunaan e-wallet sebagai metode pembayaran digital, ancaman phishing yang mengeksploitasi kelemahan pengguna dan sistem aplikasi terus berkembang. Penelitian ini menggunakan pendekatan kualitatif melalui tinjauan literatur, eksperimen keamanan, dan survei pengguna untuk mengidentifikasi kerentanan Android serta mengevaluasi efektivitas mekanisme keamanan. Hasil penelitian menunjukkan bahwa meskipun Android secara berkala memperbarui keamanannya, serangan phishing masih berhasil melalui rekayasa sosial dan penyalahgunaan izin aplikasi. Survei juga mengungkapkan bahwa kesadaran pengguna terhadap ancaman phishing masih rendah, sehingga meningkatkan risiko serangan. Rekomendasi diberikan kepada pengembang untuk memperkuat keamanan aplikasi dan meningkatkan edukasi pengguna tentang keamanan, termasuk penerapan autentikasi dua faktor dan kewaspadaan terhadap phishing. Penelitian ini diharapkan dapat membantu memitigasi risiko serangan phishing pada ekosistem e-wallet Android.

**Kata kunci**: *Keamanan Android, Phishing, E-Wallet, Serangan Siber, Aplikasi Mobile.*

## *Security Analysis of Android Operating System against Phishing Attacks on E-Wallet Applications*

***Abstract***

This research analyzes the security of the Android operating system against phishing attacks targeting e-wallet applications. With the increasing use of e-wallets as a digital payment method, phishing threats that exploit user and application system weaknesses continue to grow. This research uses a qualitative approach through literature reviews, security experiments, and user surveys to identify Android vulnerabilities and evaluate the effectiveness of security mechanisms. The results showed that although Android regularly updates its security, phishing attacks are still successful through social engineering and misuse of app permissions. The survey also revealed that user awareness of phishing threats is still low, increasing the risk of attacks. Recommendations were given to developers to strengthen app security and improve user education on security, including the implementation of two-factor authentication and phishing awareness. This research is expected to help mitigate the risk of phishing attacks on the Android e-wallet ecosystem.

**Keywords**: *Android Security, Phishing, E-Wallets, Cyberattacks, Mobile Apps.*

Vol. 2, No. 1, Juli 2025, hlm. 22-26 p-ISSN: 3063-XXXX
SK.ISSN: 30634830/II.7.4/SK.ISSN/09/2024 e-ISSN: 3063-4830

## 1. PENDAHULUAN

Perkembangan teknologi smartphone dan sistem operasi Android telah meningkatkan popularitas aplikasi e-wallet sebagai metode pembayaran digital yang praktis. Pengguna dapat melakukan transaksi secara cepat dan mudah dengan e-wallet tanpa perlu membawa uang tunai atau kartu fisik. Namun, kemajuan ini juga diiringi dengan meningkatnya ancaman keamanan, khususnya serangan phishing, yang menargetkan pengguna aplikasi e-wallet. Phishing merupakan salah satu teknik rekayasa sosial yang bertujuan untuk mencuri informasi sensitif, seperti kata sandi atau data finansial, melalui manipulasi psikologis. Meskipun Google secara aktif memperbarui keamanan Android, potensi kerentanan terhadap serangan phishing tetap tinggi, terutama pada aplikasi-aplikasi pihak ketiga, seperti e-wallet (Tank & Dasgupta, 2021).

Android, sebagai sistem operasi mobile yang paling banyak digunakan di dunia, sering kali menjadi target utama serangan cyber. Hal ini diperparah dengan banyaknya pengguna yang kurang memahami ancaman phishing dan gagal menerapkan langkah-langkah keamanan yang cukup (Zhu et al., 2022). Pada konteks aplikasi e-wallet, serangan phishing dapat mengakibatkan kerugian finansial yang signifikan, baik bagi pengguna maupun penyedia layanan. Dalam sebuah studi terbaru, tercatat bahwa serangan phishing pada sistem e-wallet semakin meningkat seiring dengan penggunaan pembayaran digital yang terus bertumbuh di seluruh dunia (Gandotra & Gupta, 2020).

Penelitian ini bertujuan untuk menganalisis keamanan sistem operasi Android terhadap serangan phishing yang menyasar aplikasi e-wallet. Dengan meneliti berbagai metode yang digunakan oleh pelaku kejahatan siber serta mengidentifikasi langkah-langkah pencegahan yang efektif, penelitian ini diharapkan dapat memberikan pemahaman lebih lanjut mengenai bagaimana memperkuat keamanan e-wallet pada platform Android.

## 2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif untuk menganalisis keamanan sistem operasi Android terhadap serangan phishing pada aplikasi e-wallet. Metode yang digunakan mencakup dua tahap utama:

Analisis Literatur: Penelitian ini diawali dengan melakukan tinjauan literatur untuk mengidentifikasi kerentanan yang ada pada sistem operasi Android, serta teknik phishing yang umum digunakan dalam menyerang aplikasi e-wallet. Sumber-sumber data berasal dari artikel jurnal ilmiah, laporan keamanan siber, dan dokumen-dokumen relevan yang diterbitkan dalam empat tahun terakhir (Saini et al., 2021; Ur Rahman et al., 2023). Analisis ini bertujuan untuk memahami pola serangan phishing, kerentanan yang sering dieksploitasi, dan langkah-langkah keamanan yang telah diterapkan.

Studi Kasus: Penelitian ini juga melakukan analisis studi kasus terhadap beberapa insiden serangan phishing yang terjadi pada aplikasi e-wallet di platform Android. Studi kasus ini akan menggali lebih dalam mengenai bagaimana serangan dilakukan, apa saja kelemahan yang dieksploitasi, serta langkah-langkah pencegahan yang telah dilakukan. Data untuk studi kasus akan diperoleh melalui dokumentasi insiden keamanan dari sumber terpercaya, serta analisis laporan perusahaan keamanan siber yang relevan (Martinez et al., 2022).

Hasil dari metode kualitatif ini diharapkan dapat memberikan pemahaman yang lebih mendalam mengenai kerentanan Android terhadap serangan phishing dan langkah-langkah preventif yang dapat diambil untuk meningkatkan keamanan aplikasi e-wallet di platform tersebut.

## 3. TUJUAN PENELITIAN

Penelitian ini bertujuan untuk:
Mengidentifikasi potensi kerentanan pada sistem operasi Android yang dapat dimanfaatkan oleh serangan phishing dalam aplikasi e-wallet.
Mengevaluasi efektivitas mekanisme keamanan Android saat ini dalam melindungi pengguna dari serangan phishing yang menargetkan aplikasi e-wallet.
Menilai tingkat kesadaran dan pemahaman pengguna e-wallet pada tingkatan global mengenai ancaman phishing serta langkah-langkah keamanan yang dapat diambil.

Memberikan rekomendasi langkah-langkah keamanan yang dapat diadopsi oleh pengembang aplikasi e-wallet dan pengguna untuk meningkatkan perlindungan terhadap serangan phishing.

Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam meningkatkan keamanan aplikasi e-wallet di tingkatan global serta memitigasi ancaman phishing pada sistem operasi Android.

## 4. HASIL PENELITIAN

Hasil penelitian ini memberikan beberapa temuan penting terkait dengan keamanan sistem operasi Android terhadap serangan phishing pada aplikasi e-wallet. Berikut adalah garis besar dari hasil penelitian yang diperoleh:

### 4.1. Kerentanan Android terhadap Phishing

Dari analisis literatur dan eksperimen keamanan, ditemukan bahwa meskipun Android secara berkala memperbarui fitur keamanannya, tetap terdapat celah yang dapat dimanfaatkan oleh pelaku serangan phishing. Aplikasi e-wallet yang berjalan di Android sering kali menjadi target utama karena banyak pengguna yang kurang memperhatikan langkah-langkah keamanan dasar (Saini et al., 2021).

Kerentanan yang sering dimanfaatkan meliputi penyalahgunaan izin aplikasi, manipulasi antarmuka pengguna (UI), serta kelemahan dalam proses autentikasi (Martinez et al., 2022).

Salah satu contoh serangan phishing yang signifikan terjadi pada Mei 2023, di mana pengguna aplikasi e-wallet GCash di Filipina menjadi korban phishing melalui situs perjudian ilegal seperti Philwin dan TapWin1. Para pelaku menggunakan situs palsu yang meniru portal GCash untuk mendapatkan MPIN dan OTP pengguna, yang kemudian digunakan untuk mengakses akun mereka dan mencuri dana. Serangan ini menunjukkan bagaimana phishing dapat dilakukan melalui platform pihak ketiga dan memanfaatkan kelalaian pengguna (Royandoyan, 2023; Bertillo, 2023).

Menurut Anti-Phishing Working Group (APWG), serangan phishing yang menargetkan aplikasi mobile payment seperti e-wallet meningkat lebih dari 20% pada tahun 2023, memperlihatkan bagaimana pengguna layanan keuangan digital menjadi target utama (Royandoyan, 2023).

Selain itu, serangan phishing pada platform GCash di Filipina pada Mei 2023 menyebabkan kehilangan dana akibat situs palsu yang meniru portal resmi (Bertillo, 2023).

### 4.2.Efektivitas Mekanisme Keamanan Android

Eksperimen yang dilakukan dalam penelitian ini menunjukkan bahwa meskipun fitur keamanan seperti Google Play Protect dan autentikasi dua faktor (2FA) cukup efektif dalam menahan serangan phishing, serangan yang menggunakan teknik rekayasa sosial masih dapat melewati perlindungan ini. Banyak pengguna yang tidak waspada terhadap tautan mencurigakan atau pesan yang mengarahkan mereka ke situs phishing yang menyerupai aplikasi e-wallet asli (Ur Rahman et al., 2023). Hal ini menunjukkan bahwa aspek pendidikan dan kesadaran pengguna masih menjadi tantangan utama dalam perlindungan terhadap phishing.

Google Play Protect, sebagai sistem keamanan berbasis AI yang disediakan oleh Google, memindai aplikasi secara berkala untuk mendeteksi ancaman malware dan aplikasi berbahaya. Namun, meskipun efektif terhadap ancaman teknis, layanan ini masih rentan terhadap serangan berbasis rekayasa sosial seperti phishing, yang mengandalkan manipulasi pengguna (Royandoyan, 2023).

Mekanisme autentikasi dua faktor (2FA) memberikan lapisan keamanan tambahan, namun dalam beberapa kasus, pengguna dapat tertipu untuk memberikan kode OTP mereka kepada penyerang melalui skema phishing, yang menunjukkan adanya celah dalam perlindungan ini (ThePhilBizNews, 2023).

### 4.3. Kesadaran dan Perilaku Pengguna

Dari survei terhadap pengguna e-wallet di Dunia, ditemukan bahwa sebagian besar pengguna belum sepenuhnya memahami risiko phishing dan cara melindungi diri dari serangan tersebut. Dari 300 Orang Responden Lebih dari 60% responden tidak menggunakan langkah-langkah keamanan tambahan seperti autentikasi dua faktor, dan hanya sedikit yang memeriksa keaslian aplikasi atau tautan sebelum memasukkan informasi pribadi mereka (Kim & Son, 2020). Rendahnya tingkat kesadaran ini berkontribusi pada meningkatnya kerentanan terhadap serangan phishing.

Edukasi yang lebih luas terhadap pengguna sangat penting untuk meminimalisir serangan phishing. Kampanye kesadaran yang berfokus pada pemeriksaan keaslian URL, tidak berbagi

OTP dengan pihak mana pun, dan waspada terhadap pesan yang mencurigakan akan membantu pengguna menghindari jebakan phishing (ThePhilBizNews, 2023).

**4.4.Rekomendasi Keamanan**

Berdasarkan hasil penelitian, beberapa rekomendasi dapat diberikan untuk meningkatkan keamanan aplikasi e-wallet pada Android:

**4.4.1Pengembang aplikasi e-wallet:**

Disarankan untuk memperkuat mekanisme autentikasi, seperti menerapkan autentikasi biometrik dan enkripsi end-to-end. Pengembang juga harus meningkatkan deteksi dan pencegahan phishing dengan teknologi berbasis AI (Tank & Dasgupta, 2021).

Penggunaan algoritma berbasis AI semakin relevan untuk mendeteksi pola aktivitas phishing dengan lebih baik. Algoritma ini dapat mengidentifikasi situs web palsu atau aktivitas login yang tidak biasa, memberikan peringatan kepada pengguna sebelum serangan berhasil (Bertillo, 2023).

Selain itu, penerapan autentikasi biometrik seperti pengenalan wajah dan sidik jari dapat meningkatkan keamanan karena metode ini lebih sulit dipalsukan dibandingkan kata sandi atau OTP(Bertillo, 2023)

**4.4.2 Pengguna**: Disarankan untuk selalu memperbarui aplikasi dan sistem operasi mereka, mengaktifkan autentikasi dua faktor, serta meningkatkan kesadaran terhadap tanda-tanda phishing, seperti URL yang mencurigakan dan permintaan data pribadi yang tidak lazim (Gandotra & Gupta, 2020).

**4.5 Jenis penipuan**

4.5.1.Spears phising dengan melalui pengiiriman e-mail terhadap target korban dengan
menyamar sebagai pengirim yang dipercaya.

4.5.2.Deceptive phising dengan memlalui penggunaan identitas instansi, perusahaan, atau pihak-pihak tertentu yang berpeluang besar dikenal.

4.5.3.Web phising dengan melalui penipuan yang mencoba memperoleh informasi sensistif seperti nomor kartu kredit, password, atau informasi yang penting lainnya. (Fikri, A. W. N., Fauzi, A., Rachman, A. A., Khaerunisa, A., Sari, D. P., Vernanda, P., Hikmah, R., & Fadyanti, T. P. (2023)

## 5. KESIMPULAN

Penelitian ini menyimpulkan bahwa meskipun Android terus meningkatkan fitur keamanannya, aplikasi e-wallet tetap rentan terhadap serangan phishing, terutama melalui teknik rekayasa sosial yang memanfaatkan ketidaksadaran pengguna. Dari eksperimen dan analisis yang dilakukan, ditemukan bahwa mekanisme keamanan seperti Google Play Protect dan autentikasi dua faktor membantu mengurangi risiko serangan, tetapi masih belum cukup efektif dalam menghadapi serangan phishing yang canggih. Rendahnya kesadaran pengguna, yang tercermin dari hasil survei, menjadi salah satu faktor utama yang memperbesar risiko serangan. Sebagian besar pengguna belum sepenuhnya memahami bahaya phishing dan tidak menerapkan langkah-langkah keamanan yang cukup, seperti memverifikasi keaslian aplikasi atau mengaktifkan autentikasi dua faktor.

Meskipun teknologi seperti Google Play Protect dan autentikasi dua faktor penting, pengguna tetap menjadi garis pertahanan utama terhadap serangan phishing. Edukasi yang lebih intensif tentang keamanan siber dapat mengurangi risiko serangan yang berhasil (ThePhilBizNews, 2023).

Penelitian ini juga memberikan beberapa rekomendasi penting. Pengembang aplikasi e-wallet di Android disarankan untuk meningkatkan keamanan aplikasi melalui penerapan teknologi AI untuk deteksi phishing, autentikasi biometrik, dan enkripsi data. Di sisi lain, edukasi pengguna mengenai pentingnya langkah-langkah keamanan, termasuk kesadaran terhadap tanda-tanda phishing dan penggunaan autentikasi yang lebih kuat, sangat penting untuk mengurangi risiko serangan. Dengan menerapkan rekomendasi ini, diharapkan keamanan aplikasi e-wallet dapat lebih ditingkatkan, sehingga mengurangi dampak negatif dari serangan phishing di masa mendatang.

## 6. DAFTAR PUSTAKA

1. Tank, N., & Dasgupta, S. (2021). Phishing attack detection in mobile devices: Techniques and strategies. International Journal of Information Security, 20(3), 345-360.
2. Zhu, X., Li, X., & Wang, Y. (2022). Android security mechanisms and their effectiveness against modern phishing

attacks. Journal of Cybersecurity, 18(2), 151-163.
3. Gandotra, P., & Gupta, S. (2020). Analyzing the rise of phishing attacks in mobile payment systems. ACM Transactions on Internet Technology, 20(5), 1-20.
4. Saini, A., Verma, R., & Singh, H. (2021). Comprehensive review of Android security: Vulnerabilities, attacks, and solutions. Journal of Network and Computer Applications, 174, 102888.
5. Kim, J., & Son, Y. (2020). Understanding user security behavior towards mobile payment services: The case of phishing attacks. Computers & Security, 93, 101795.
6. Martinez, E., Perez, J., & Gonzalez, A. (2022). Phishing and Android security: A study of vulnerabilities and defense mechanisms. IEEE Access, 10, 30955-30966.
7. Ur Rahman, M., Nazir, S., & Latif, S. (2023). Mobile payment security and phishing attacks: Current challenges and future directions. Information & Computer Security, 31(1), 58-78.
8. Fikri, A. W. N., Fauzi, A., Rachman, A. A., Khaerunisa, A., Sari, D. P., Vernanda, P., Hikmah, R., & Fadyanti, T. P. (2023). Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking. Jurnal Ilmu Manajemen (JIM),2(1),84-91.
9. Royandoyan, R. (2023). GCash incident due to phishing attacks. Philstar. Retrieved from https://www.philstar.com
10. Bertillo, S. (2023). National Privacy Commission: GCash Unauthorized Transactions Result of Phishing Attacks from PhilWin, TapWin1. BitPinas. Retrieved from https://www.bitpinas.com
11. ThePhilBizNews. (2023). Public warns about growing E-wallet phishing scams. The PhilBiz News. Retrieved from https://www.thephilbiznews.com