

Faktor Kunci Keberhasilan Dan Tantangan Dalam Edukasi Kesadaran *Phishing*

Syahlu Zuanna Tanjung¹, Muhammad Irwan Padli Nasution²

Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Sumatera Utara, Indonesia^{1,2}

Corresponding Author: syahluzuanna@gmail.com¹, irwannst@uinsu.ac.id²

Info Artikel

Submitted: 19 Januari 2026

Revised : 29 Februari 2026

Accepted: 15 Maret 2026

Published: 25 April 2026

Keywords: Service Recovery, Policy Implementation, Public Service, Technical Services, Customer Satisfaction

Kata Kunci: Service Recovery, Implementasi Kebijakan, Pelayanan Publik, Jasa Teknik, Kepuasan Pelanggan

Abstract

The rapid development of digital technology has made various activities easier, but it has also increased the risk of cybercrime, such as phishing. Phishing is a scam that exploits user negligence to obtain personal information by impersonating a trusted party.

On the other hand, several challenges arise, such as difficult-to-change user habits, overconfidence, and increasingly sophisticated phishing techniques that are difficult to recognize for users who are not familiar with social media.

Abstrak

Perkembangan teknologi digital semakin pesat memberi kemudahan dalam berbagai aktivitas, tetapi juga meningkatkan risiko kejahatan siber contohnya phishing. Phishing adalah sebuah penipuan yang memanfaatkan kelalaian pengguna untuk mengetahui informasi pribadi dengan cara menyamar menjadi pihak yang terpercaya. Sedangkan di sisi lain, ada beberapa tantangan, contohnya kebiasaan pengguna yang sulit diubah, tingkat kepercayaan diri yang berlebihan dan teknik phishing yang semakin berkembang dan sulit dikenal oleh pengguna yang tidak mengerti media sosial..



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).

Publisher: Lembaga Penerbit Penelitian Nusantara

Pendahuluan

Perkembangan teknologi digital saat ini membaawa berbagai perubahan ke dalam kehidupan sehari-hari, contohnya dalam bidang komunikasi dan akses informasi. Namun, di balik kemudahan ini muncul berbagai ancaman-ancaman kejahatan siber yang semakin beragam, salah satu adalah phishing. Phishing adalah sebuah bentuk penipuan yang menyamar sebagai pihak yang terpercaya untuk memperoleh informasi pribadi pengguna.

Dalam beberapa tahun terakhir ini kasus phishing terus meningkat seiring dengan tingginya aktivitas masyarakat di dunia digital. Hal ini justru menunjukkan bahwa masih banyak pengguna yang belum memiliki kesadaran dan pemahaman yang cukup tentang keamanan digital. Salah satu penyebab utama keberhasilan serangan phishing adalah faktor manusia, seperti kebiasaan terburu-buru dalam mengambil keputusan dan kurangnya ketelitian dalam memeriksa informasi.

Cara mengatasi permasalahan tersebut adalah dengan cara edukasi kesadaran phishing yang efektif. Edukasi bukan hanya berfokus pada pemberian pengetahuan, tetapi juga pada pembentukan perilaku pengguna agar lebih waspada. Metode pembelajaran yang efektif, seperti simulasi dan praktik langsung, dinilai lebih efektif dalam meningkatkan pemahaman pengguna di bandingkan dengan metode konvensional.

Namun, pelaksanaan edukasi kesadaran phishing masih menghadapi berbagai macam tantangan, seperti rendahnya minat pengguna, kebiasaan yang sulit diubah, serta perkembangan teknik phishing yang semakin canggih. Oleh karena itu, penting untuk mengkaji lebih dalam mengenai faktor keberhasilan dan tantangan dalam edukasi kesadaran phishing agar dapat meningkatkan efektivitasnya dimasa yang akan datang.

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian studi pustaka (*literature review*). Pendekatan ini dipilih karena penelitian berfokus pada pengkajian teori dan hasil penelitian sebelumnya yang berkaitan dengan edukasi kesadaran phishing.

Data yang digunakan dalam penelitian ini merupakan data sekunder, yaitu data yang diperoleh dari berbagai sumber seperti jurnal ilmiah, artikel, dan publikasi yang relevan dengan topik penelitian. Sumber-sumber tersebut dipilih berdasarkan kesesuaian dengan pembahasan mengenai faktor keberhasilan dan tantangan dalam edukasi kesadaran phishing.

Proses pengumpulan data dilakukan dengan cara menelusuri, membaca, dan memahami isi jurnal yang telah dipilih. Informasi yang dianggap penting kemudian dicatat dan dikelompokkan sesuai dengan kebutuhan pembahasan.

Selanjutnya, data yang telah dikumpulkan dianalisis menggunakan teknik analisis deskriptif, yaitu dengan menguraikan dan menjelaskan isi dari berbagai sumber secara sistematis. Analisis ini bertujuan untuk menemukan hubungan antara teori dan fakta yang ada, sehingga dapat diperoleh pemahaman yang lebih jelas mengenai faktor-faktor yang mempengaruhi keberhasilan serta tantangan dalam edukasi kesadaran phishing.

Hasil dan Pembahasan

Hasil

Berdasarkan hasil kajian dari beberapa sumber yang telah dianalisis, ditemukan bahwa tingkat kesadaran pengguna terhadap phishing masih tergolong rendah. Hal ini terlihat dari masih

banyaknya pengguna yang belum mampu membedakan antara pesan asli dan pesan palsu, terutama jika pesan tersebut terlihat meyakinkan atau berasal dari pihak yang dianggap terpercaya.

Menurut Kumaraguru et al. (2009), phishing tidak hanya mengandalkan kecanggihan teknologi, tetapi juga memanfaatkan faktor manusia, seperti kurangnya kewaspadaan dan kecenderungan pengguna untuk mempercayai informasi yang terlihat meyakinkan. Hal ini menyebabkan banyak pengguna yang menjadi korban meskipun telah memiliki pengetahuan dasar tentang keamanan digital.

Selain itu, diketahui bahwa pengetahuan tentang phishing tidak selalu berbanding lurus dengan kemampuan dalam menghindari serangan tersebut. Beberapa pengguna yang sudah memahami konsep phishing tetap berisiko menjadi korban karena tidak menerapkan pengetahuan tersebut dalam aktivitas sehari-hari.

Hasil lainnya menunjukkan bahwa perilaku pengguna dalam menggunakan teknologi juga berpengaruh terhadap tingkat kerentanan terhadap phishing. Pengguna yang cenderung terburu-buru dalam mengambil keputusan, seperti langsung mengklik tautan tanpa melakukan pengecekan, memiliki risiko yang lebih tinggi.

Dari sisi metode edukasi, pendekatan yang melibatkan interaksi langsung, seperti simulasi dan latihan praktik, menunjukkan hasil yang lebih baik dibandingkan metode pembelajaran yang hanya bersifat teori.

Tabel 1. Contoh Kasus Phishing

Kasus	Deskripsi	Analisis
Phishing melalui WhatsApp (mengatasnamakan Bank)	Seorang mahasiswa menerima pesan WhatsApp yang menyatakan bahwa akun banknya akan diblokir jika tidak segera melakukan verifikasi melalui link tertentu. Karena panik, pengguna langsung mengklik link tersebut tanpa mengecek keaslian.	Kasus ini menunjukkan adanya unsur urgensi yang membuat pengguna terburu-buru. Kurangnya kebiasaan memeriksa informasi juga menjadi penyebab utama pengguna tertipu.

FAKTOR KUNCI KEBERHASILAN DAN TANTANGAN DALAM EDUKASI KESADARAN PHISHING

Syahlu Zuanna Tanjung¹, Muhammad Irwan Padli Nasution²

Phishing melalui email promo	Seorang pengguna menerima email yang terlihat seperti dari platform belanja online dengan tawaran diskon besar. Pengguna langsung mengklik link dan memasukkan data akun tanpa mengecek kebenarannya.	Kasus ini memanfaatkan ketertarikan pengguna terhadap promo. Meskipun terlihat menarik, pengguna tetap harus waspada terhadap keaslian sumber.
Simulasi edukasi Phishing	Dalam sebuah pelatihan, peserta diberikan contoh email asli dan phishing untuk dibedakan. Setelah mengikuti simulasi, peserta menjadi lebih mampu mengenali ciri-ciri phishing.	Menunjukkan bahwa metode simulasi dan praktik langsung lebih efektif dibandingkan hanya teori dalam meningkatkan kesadaran pengguna.

Pembahasan

Hasil penelitian menunjukkan bahwa faktor manusia menjadi penyebab utama keberhasilan serangan phishing. Banyak pengguna yang terbiasa mengambil keputusan dengan cepat tanpa memeriksa informasi secara teliti. Hal ini membuat mereka lebih mudah tertipu oleh pesan yang terlihat meyakinkan.

Selain itu, metode edukasi juga sangat berpengaruh. Pendekatan interaktif seperti simulasi memberikan pengalaman langsung kepada pengguna, sehingga mereka lebih mudah memahami dan mengingat ciri-ciri phishing.

Namun, terdapat beberapa tantangan dalam edukasi phishing, seperti kebiasaan pengguna yang sulit diubah, rasa percaya diri yang berlebihan, serta teknik phishing yang semakin canggih.

Hasil penelitian menunjukkan bahwa kesadaran pengguna terhadap phishing masih tergolong rendah. Banyak pengguna yang belum mampu membedakan antara pesan asli dan pesan palsu. Hal ini disebabkan oleh kurangnya pengetahuan serta kebiasaan pengguna yang tidak teliti dalam memeriksa informasi.

Selain itu, perilaku pengguna yang cenderung terburu-buru juga menjadi faktor utama yang meningkatkan risiko phishing. Pengguna sering kali langsung mengklik tautan tanpa melakukan verifikasi terlebih dahulu. Hal ini menunjukkan bahwa pengetahuan saja tidak cukup, tetapi perlu diimbangi dengan perubahan perilaku.

Dari sisi edukasi, metode pembelajaran yang interaktif seperti simulasi phishing terbukti lebih efektif dibandingkan metode konvensional. Pengguna yang mendapatkan pelatihan berbasis praktik cenderung lebih mampu mengenali ancaman phishing.

Namun, terdapat beberapa tantangan dalam meningkatkan kesadaran phishing, seperti rendahnya minat pengguna untuk mempelajari keamanan digital serta perkembangan teknik phishing yang semakin canggih. Hal ini membuat edukasi harus terus diperbarui agar tetap relevan dengan kondisi saat ini.

SIMPULAN

Berdasarkan pembahasan yang telah dilakukan, dapat disimpulkan bahwa phishing merupakan salah satu bentuk kejahatan siber yang memanfaatkan kelalaian pengguna untuk memperoleh informasi pribadi. Tingginya aktivitas digital membuat risiko phishing semakin meningkat, terutama bagi pengguna yang kurang memiliki kesadaran terhadap keamanan digital.

Kebhasilan edukasi kesadaran phishing dipengaruhi oleh beberapa faktor, seperti metode pembelajaran yang digunakan, relevansi materi dengan kehidupan sehari-hari, serta kemampuan edukasi dalam mengubah perilaku pengguna. Pendekatan yang bersifat interaktif, seperti simulasi dan praktik langsung, terbukti lebih efektif dalam membantu pengguna memahami dan mengenali phishing dibandingkan hanya teori.

Di sisi lain, terdapat berbagai tantangan dalam pelaksanaan edukasi kesadaran phishing, seperti kebiasaan pengguna yang sulit diubah, kurangnya perhatian terhadap keamanan digital, serta teknik phishing yang semakin canggih. Faktor manusia menjadi penyebab utama keberhasilan serangan phishing, sehingga edukasi tidak hanya harus meningkatkan pengetahuan, tetapi juga membentuk kebiasaan pengguna agar lebih berhati-hati.

Dengan demikian, edukasi kesadaran phishing perlu dilakukan secara berkelanjutan dengan metode yang lebih menarik dan mudah dipahami, agar dapat meningkatkan kewaspadaan pengguna dalam menghadapi ancaman di dunia digital.

DAFTAR PUSTAKA

- Canfield, C. I., Fischhoff, B., & Davis, A. (2024). Fishing for phishy messages: How users perceive phishing attacks. *Humanities and Social Sciences Communications*, 11(1), 1–12.
<https://doi.org/10.1057/s41599-024-04083-1>
- Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 581–590.
<https://doi.org/10.1145/1124772.1124832>
- Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2009). School of phish: A real-world evaluation of anti-phishing training. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 905–914.
<https://doi.org/10.1145/1518701.1519052>
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373–382.
<https://doi.org/10.1145/1753326.1753687>