

## KESADARAN KORBAN CYBER CRIME DALAM KASUS PHISING

**Vania Trisnawati \*<sup>1</sup>**

Fakultas Psikologi, Universitas Bhayangkara Jakarta Raya, Indonesia  
[202110515259@mhs.ubharajaya.ac.id](mailto:202110515259@mhs.ubharajaya.ac.id)

**Edy Soesanto**

Fakultas Psikologi, Universitas Bhayangkara Jakarta Raya, Indonesia  
[edy.soesanto@dsn.ubharajaya.ac.id](mailto:edy.soesanto@dsn.ubharajaya.ac.id)

**Sandra Mutiara Tirta**

Fakultas Psikologi, Universitas Bhayangkara Jakarta Raya, Indonesia  
[202110515255@mhs.ubharajaya.ac.id](mailto:202110515255@mhs.ubharajaya.ac.id)

**Thalia Amelinda Setiawan**

Fakultas Psikologi, Universitas Bhayangkara Jakarta Raya, Indonesia  
[202110515278@mhs.ubharajaya.ac.id](mailto:202110515278@mhs.ubharajaya.ac.id)

### **Abstract**

*Phishing is a form of cyber crime that impersonates a website with the aim of stealing someone's personal identity data. The aim of this research is to find out individual awareness of cyber crime in cases of phishing. The method used to search for data information regarding this phishing case is by using literature studies. The results of data information found from various journals show that this phishing case is very dangerous for individuals who have a low level of awareness and do not have knowledge about cyber security in using social media.*

**Keywords:** Cyber Crime, Cyber Security, Phishing

### **Abstrak**

Phising merupakan suatu bentuk tindakan kejahatan *cyber crime* yang menyamar sebagai situs web dengan tujuan mencuri identitas data pribadi seseorang. Tujuan dalam penelitian ini adalah mencari tahu kesadaran individu dalam *cyber crime* dalam kasus yang terjadi pada phising. Metode yang di pakai dalam mencari informasi data mengenai kasus phising ini dengan menggunakan studi literatur. Hasil informasi data yang ditemukan dari berbagai jurnal bahwa kasus phising ini sangat berbahaya bagi individu yang memiliki tingkat kesadaran yang rendah dan tidak memiliki pengetahuan tentang adanya keamanan cyber dalam menggunakan sosial media.

**Kata Kunci:** Cyber Crime, Cyber Security, Phising

---

<sup>1</sup> Korespondensi Penulis.

## **PENDAHULUAN**

*Phising* yang sedang marak terjadi merupakan suatu bentuk kejahatan sebagai tindakan yang menyamar dengan situs web yang bertujuan untuk mencuri identitas pribadi seperti nama pengguna, kata sandi dan lain sebagainya melalui jaringan internet atau computer. Cara kerja *phishing* itu sendiri adalah pelaku dari *phishing* tersebut biasanya mengirimkan email atau pesan dari sumber yang valid seperti bank, undangan pernikahan dan lain-lain, agar korban mendapatkan masalah dan memperbaiki nya dengan membuka situs web tersebut tetapi sebenarnya situs web tersebut memiliki informasi palsu yang tujuan nya untuk mencuri data pribadi korban (Vadila & Pratama, 2021).

Dari kasus *phising* termasuk kedalam cyber untuk mereka mencari uang dengan mudah, tetapi juga tidak hanya dari uang saja, namun hanya ingin mengetahui kegiatan si korban atau si pemilik akun. Selain itu kita sebagai individu harus bisa memanfaatkan nya sebaik mungkin dengan menciptakan alat pendeteksi atau aplikasi untuk mencegahnya dari kasus *phising* (Wahyu Hidayat M et al., 2023). Maka sangat penting kesadaran manusia terhadap penggunaan media sosial tentang kerahasiaan *password* masih terlalu rendah, individu tersebut harus memiliki keamanan data pribadi ganda dalam sebuah perangkat dan mengenali perbedaan jenis situs web yang palsu dan tidak palsu untuk melindungi diri dari kasus *phising* tersebut (Ramadhan et al., 2022).

## **METODE PENELITIAN**

### **Desain Penelitian**

Penelitian ini menggunakan metode studi literatur dengan memperoleh data yang dapat membaca, mencatat dan mengelola laporan bahan penelitian terdahulu. Penelitian studi literatur ini merupakan sumber sekunder yang memiliki arti bahwa peneliti memperoleh data angka dari pandangan seseorang yang membuat penelitian tersebut dengan mengandung prasangka, aliran pemikiran atau teori-teori yang ada pada penelitian tersebut. Studi literatur ini dapat melakukan pencarian data penelitian melalui sumber atau bukti yang terpercaya yaitu dengan research paper dari setiap jurnal, buku yang telah dipilih kriteria nya melalui pembacaan abstrak terlebih dahulu, mencatat point-point penting dalam permasalahan penelitian tersebut, lalu dibuat nyalaporan hasil studi literatur ini dalam bentuk narrative synthesis yang dilengkapi dengan kesimpulan penelitian yang telah dilakukan (Radiansyah et al., 2016).

### **Analisis Data**

Setelah data keseluruhan sudah didapatkan dari penelitian yang menggunakan metode studi literatur terkait *phising* dan kesadaran masyarakat Indonesia, selanjutnya penulis menganalisa data untuk memperoleh suatu kesimpulan yang hasil benar dan tepat

dalam menganalisa data tersebut digunakan teknik analisis isi. Analisis isi (*Content Analysis*) adalah penelitian yang membahas secara mendalam terhadap suatu isi informasi tertulis maupun tercetak yang ada di media massa. Analisis ini digunakan untuk mengambil data dengan menganalisa dalam bentuk komunikasi, surat kabar, berita maupun radio serta iklan yang didapatkan dari semua bahan dokumentasi lainnya, sehingga dapat dikaitkan pada sebuah pembahasan untuk memudahkan penulis menganalisa suatu kebenaran melalui pendapat para ahli yang sebagai acuan penelitian.

## **HASIL DAN PEMBAHASAN**

### **Analisa**

Kejahatan cyber memiliki beberapa faktor penyebab yaitu faktor motivasi finansial, perbanyak keuntungan, kurangnya pengetahuan pada perkembangan zaman khususnya sistem teknologi, kurangnya kesadaran dan kelemahan dalam infrastruktur keamanan teknologi pada media sosial. Hal tersebut didukung karena terdapat upaya-upaya yang harus dicegah khususnya pada penegakan hukum dari kejahatan cyber dalam kasus phishing (Mahira Dewantoro & Dian Alan Setiawan S.H., M.H., 2023).

Upaya masyarakat di Indonesia termasuk di daerah Bekasi dapat dilihat bahwa masyarakat sudah memiliki kesadaran atau knowledge berupa kebiasaan perilaku atau behavior yang baik terhadap keamanan siber seperti dengan pengetahuan yang dimiliki oleh masyarakat cukup bagus dengan tindakan tidak menyebarkan informasi atau data pribadi sehingga kebiasaan perilaku ini dapat memunculkan kebiasaan selektif dan hati-hati ketika menerima dokumen soft file atau link. Kebiasaan perilaku atau behavior pengguna yaitu hal-hal yang dapat dilakukan oleh pengguna. Keamanan informasi sangatlah penting untuk mendukung individu dapat meningkatkan pengetahuan dengan kesadaran, sehingga dapat mengikuti berbagai kegiatan seperti pelatihan, webinar, training atau sharing knowledge (Arie Budi Suprio & Najib, 2022).

Suatu pengaruh atau dampak yang akan terjadi apabila kita tetap menjaga kesadaran kita terhadap kemajuan teknologi yang semakin pesat dapat mempermudah kita. Ada beberapa pengetahuan-pengetahuan dasar tentang pentingnya menjaga keamanan informasi dan warga Bekasi sendiri menggunakan attitude atau sikap dalam menjaga keamanan informasi. Dapat diambil kesimpulan dari penelitian sebelumnya ancaman keamanan siber bukanlah tantangan yang tidak dapat diatasi tetapi dapat diterapkan dari berbagai strategi dan tindakan untuk melindungi data dan sistem dengan kombinasi pendekatan teknis, kebijakan keamanan yang kuat, pelatihan kesadaran pengguna, dan kerja sama antara pihak-pihak yang terlibat, keamanan siber dapat ditingkatkan secara signifikan.

Jika sudah terjadi hal buruk seperti masuk ke dalam perangkap sebagai korban kasus phishing, namun di Indonesia sudah ada hukum yang mengatur keamanan digital dengan sebagai sanksi atau hukuman yang dijatuhkan kepada pelaku kejahatan cyber berupa phishing didasarkan pada penafsiran pasal 378 KUHP, dan penerapan hukum pidana tidak dapat didasarkan pada proses komunikasi secara lisan, tentu saja jika menyangkut kejahatan di media sosial perlu adanya pendekatan yang lebih baik berdasarkan UU ITE yang menggabungkan hukuman dasar seperti penjara atau denda, serta menggunakan angka pidana maksimal yaitu panjang kalimat atau jumlah kalimat setelah angka tertinggi (Phising et al., 2009).

Keamanan terhadap korban kejahatan cyber berupa phishing dalam UU ITE yang mengatur tentang penyelesaian kasus pelakunya dengan memberikan sanksi berupa pidana atau denda, sedangkan undang-undang yang khusus memberikan perlindungan terhadap korban kejahatan yaitu Undang-Undang Perlindungan Sanksi dan Korban yang mengatur bahwa korban kejahatan yang dilakukan oleh pelaku dapat memperoleh perlindungan berupa kompensasi atas permohonan yang diajukan kepada korban, pengadilan diasumsikan bahwa mempertimbangkan beberapa syarat untuk menyetujui atau menolak permohonan LPSK.

## **KESIMPULAN**

Teknologi zaman sekarang sudah semakin maju sehingga mempermudah kita dalam berbagai hal. Tapi di samping itu banyak hal yang menggunakan kesempatan tersebut untuk melakukan tindak kejahatan di media sosial atau internet, yang di sebut *cyber crime*. Salah satu kasus *cyber crime* adalah *phising*, dimana *phising* merupakan sebuah tindakan yang dilakukan pada pelaku yang bisa mengelabui atau memancing seseorang agar memasukkan data pribadi pada website *phising* yang telah memalsukan nama dalam bentuk website resmi yang hampir sama dengan website yang aslinya. Sehingga mengharuskan kita lebih berhati-hati pada penggunaan internet terutama media sosial yang mengharuskan mengisi data pribadi.

## **Saran**

### **Untuk Masyarakat**

Meningkatkan kesadaran keamanan siber dengan meningkatkan kesadaran keamanan dengan mengikuti berbagai kegiatan seperti pelatihan atau berbagai informasi, keamanan siber, kami berharap untuk menyaring informasi yang kami terima dan lebih berhati-hati saat memasukkan informasi pribadi kedalam layanan seluler. Masyarakat juga harus memiliki keterampilan teknis terkini untuk mengakses data dan menggunakan sistem keamanan.

## Untuk Pemerintah

Pemerintah harus memperkuat administrasi publik terkait pengembangan keamanan siber dengan membatasi penggunaan layanan yang servernya berlokasi diluar negeri dan mewajibkan penggunaan sistem yang aman, kurangnya legalitas yang memadai dalam menangani serangan di dunia siber, tata kelola kelembagaan keamanan siber ditingkat nasional masih bersifat parsial dan terfragmentasi, serta kurangnya koordinasi formal dalam mengatasi permasalahan keamanan siber. Industri kita masih lemah dalam bidang manufaktur dan pengembangan peralatan IT, sebab kuatnya tatanan kelembagaan dan organisasi keamanan siber suatu negara merupakan salah satu prasyarat terselenggaranya keamanan siber. Pengelolaan keamanan siber harus sangat terintegrasi dan melibatkan berbagai institusi terkait tentang intelijen, penegak hukum, pertahanan dan keamanan serta kementerian pertahanan dan TNI, serta pemerintah sebagai regulator yang dalam hal ini diwakili oleh Kominfo dan ISSIRTI dan Badan Kripto Nasional.

## Peran Mahasiswa

Mahasiswa dapat membuat penelitian terkait keamanan siber dan juga sosialisasi melalui media sosial.

## DAFTAR PUSTAKA

- Akraman, R., & Priyadi, Y. (2018). *Pengukuran Kesadaran Keamanan Informasi dan Privasi Pada Pengguna Smartphone Android di Indonesia*. 02, 1–8.
- Alif, M. S., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan di Kalangan Pengguna E-Wallet di Indonesia. *Jurnal Informasi*, 2(1), 1–7.
- Arie Budi Suprio, Y., & Najib, M. (2022). Analisa Dampak Kesadaran Keamanan Informasi Pengguna Aplikasi Whatsapp Terhadap Penyebaran Link Web Phising. *Seminar Nasional Corisindo*, 318–322.
- Djanggih, H., & Qamar, N. (2018). Penerapan Teori-Teori Kriminologi dalam Penanggulangan Kejahatan Siber (Cyber Crime). *Pandecta: Research Law Journal*, 13(1), 10–23. <https://doi.org/10.15294/pandecta.v13i1.14020>
- Eka, P. I. (2023). DASAR PERTIMBANGAN HAKIM DALAM MEMUTUS PERKARA TINDAK PIDANA PHISING YANG DILAKUKAN MELALUI MEDIA SOSIAL (Studi Kasus Putusan ... 1(Juni), 1–10. <http://scholar.unand.ac.id/204939/>
- Fitriani, Y., & Pakpahan, R. (2020). Analisa Penyalahgunaan Media Sosial untuk Penyebaran Cybercrime di Dunia Maya atau Cyberspace. *Cakrawala : Jurnal Humaniora*, 20(1), 2579–3314. <http://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala>
- Gulo, A. S., Lasmadi, S., & Nawawi, K. (2021). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal of Criminal Law*, 1(2), 68–81. <https://doi.org/10.22437/pampas.v1i2.9574>
- Hafid, M., Firjatullah, F. Z., Pamungkaz, B. W., Magister, S., Hukum, I., Wijaya, U., & Surabaya, K. (2023). *Tantangan Menghadapi Kejahatan Cyber dalam Kehidupan*

- Bermasyarakat dan Bernegara*. 7, 9548–9556.
- Mahira Dewantoro, N., & Dian Alan Setiawan S.H., M.H. (2023). Penegakan Hukum Kejahatan Siber Berbasis Phising dalam Bentuk Application Package Kit (APK) Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *Bandung Conference Series: Law Studies*, 3(2), 892–900. <https://doi.org/10.29313/bcsls.v3i2.7247>
- Naive Bayes Metode, C. D., Kesehatan, K., Karyawan, M., & Tempat, D. (2023). *Metode C4.5 Dan Naive Bayes Untuk Klasifikasi Kesehatan Mental Karyawan Di Tempat Kerja*. 11(2).
- Phising, B., Indonesia, D. I., Malunsenge, O. L. M., & Rorie, R. E. (2009). 1 2 3 4.
- Radiansyah, I., Rusdjan, C., & Priyadi, Y. (2016). Setelah keseluruhan data terkumpul menggunakan metode studi literatur maka langkah selanjutnya penulis akan menganalisa data tersebut untuk ditarik suatu kesimpulan. Untuk memperoleh hasil yang benar dan tepat dalam menganalisa data, penulis menggunakan t. *Journal of Innovation in Business and Economics*, 7(1), 1. <https://doi.org/10.22219/jibe.vol7.no1.1-14>
- Ramadhan, A., Alhafidh, M. A., & Firmansyah, M. D. (2022). Penyebaran Link Phising Kuota Kemendikbud Terhadap Kesadaran Informasi Pribadi Di Kalangan Mahasiswa UNINUS. *Kampret Journal*, 1(1), 11–15. <https://doi.org/10.35335/kampret.v1i1.9>
- Susanto, E., Antira, Lady, Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber Di Era Digital. *Journal of Business And Entrepreneurship*, 11(1), 23. <https://doi.org/10.46273/job.e.v1i1.365>
- Syah, R. (2023). Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber. *Jurnal Impresi Indonesia*, 2(9), 864–870. <https://doi.org/10.58344/jii.v2i9.3594>
- Vadila, N., & Pratama, A. R. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman Phishing. *Automata*, 2(2), 1–4.
- Wahyu Hidayat M, Hartini Ramli, Ikhrum, P. M. B., Sidrayanti, Ridhawi, A. R., Mukhtar, N. A., & Renaldy Junedy. (2023). Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar. *Vokatek : Jurnal Pengabdian Masyarakat*, 1(1), 28–33. <https://doi.org/10.61255/vokatekjp.m.v1i1.29>
- Wibowo, M. H., & Fatimah, N. (2017). Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime. *JOEICT(Jurnal of Education and Information Communication Technology)*, 1(1), 1–5. <https://www.jurnal.stkipppgritlungagung.ac.id/index.php/joeict/article/view/69>
- Zhuhadar, L., Thrasher, E., Marklin, S., & de Pablos, P. O. (2017). The next wave of innovation—Review of smart cities intelligent operation systems. *Computers in Human Behavior*, 66, 273–281. <https://doi.org/10.1016/j.chb.2016.09.030>