JOURNAL OF KNOWLEDGE AND COLLABORATION
Journal website: https://ojs.arbain.co.id/index.php/jkc/index
ISSN: 3047-5147

Research Article

Modus Operandi Phisher dalam Kejahatan Phishing (Studi Kasus Ditreskrimsus Polda Riau)

Helma Oktaviana[1], Kasmanto Rinaldi[2]
Universitas Islam Riau[1,2]
Email: Helmaokotavianaaa@gmail.com, Kasmanto_kriminologiriau@soc.uir.ac.id

Abstrak

Perkembangan teknologi yang terjadi saat ini semakin mengalami peningkatan yang pesat. Seiring pesatnya perkembangan teknologi tidak menutup kemungkinan untuk tindak kejahatan juga mengikuti perkembangan tersebut. Fakta bahwa zaman serba teknologi juga memiliki kejahatan dalam internet atau dunia maya yang sering kali disebut cybercrime, salah satunya kejahatan Phishing. Dalam konteks kejahatan phishing, modus operandi atau cara kerja pelaku menjadi kunci untuk memahami bagaimana serangan ini dilakukan dan bagaimana mereka terus beradaptasi dengan perkembangan teknologi serta perilaku pengguna. Penelitian ini bertujuan untuk mengungkap modus operandi yang digunakan oleh pelaku phisher dalam melancarkan aksinya, Penelitian ini menggunakan pendekatan kualitatif dengan teknik pengumpulan data melalui wawancara mendalam terhadap pihak kepolisian, pelaku kejahatan phishing yang sedang menjalani pidana di Lapas Pekanbaru, serta perwakilan dari Otoritas Jasa Keuangan (OJK). Hasil penelitian menunjukkan bahwa modus operandi phisher melibatkan beberapa tahapan: perencanaan, pelaksanaan, dan upaya penyamaran atau penghilangan jejak. Teori aktivitas rutin digunakan sebagai landasan untuk menganalisis pola tindakan kejahatan ini. Temuan menunjukkan bahwa kejahatan phishing berhasil terjadi karena adanya pelaku termotivasi, target yang layak (korban yang memiliki literasi digital rendah), dan lemahnya pengawasan. Penelitian ini memberikan kontribusi penting dalam memahami dinamika kejahatan siber serta implikasinya terhadap kebijakan penanggulangan.

Kata Kunci : Phishing, Modus Operandi, Aktivitas Rutin, Kejahatan Siber.

PENDAHULUAN

Phishing *(password harvesting fishing)* merupakan tindakan penipuan yang dilakukan oleh pelaku dengan tujuan untuk memperoleh informasi pribadi yang bersifat sensitive, seperti data login, nomor kartu kredit, atau informasi finansial lainnya. Dengan cara berpura pura menjadi entitas yang sah. Phiser (sebutan bagi pelaku phishing) berupaya menipu untuk mendapatkan informasi sensitif, seperti username, password dan rincian kartu kredit yang disalahgunakan para phisher dalam tindakan pencurian identitas. Dalam konteks kejahatan phishing, modus

operandi atau cara kerja pelaku menjadi kunci untuk memahami bagaimana serangan ini dilakukan dan bagaimana mereka terus beradaptasi dengan perkembangan teknologi serta perilaku pengguna. Modus operandi phishing biasanya menggunakan halaman website palsu (fake webpage) atau surel palsu untuk mengelabui dan mencuri data-data pribadi pengguna. Setelah korban atau target memberikan informasi yang diminta, phisher akan dapat mengambil alih akun, melakukan transaksi keuangan, mencuri uang, mengajukan pinjaman utang ataupun tindakan lain yang mengakibatkan pemilik identitas mengalami kerugian finansial. Phisher dalam hal ini menguasai mengenai sistem komputer dan juga sangat ahli dalam mencari celah-celah keamanan dalam sebuah sistem komputer, dapat dikatakan mereka memiliki penguasaan dalam komputer lebih daripada orang pada umumnya.

Penelitian terdahulu menyimpulkan tentang temuan menunjukan tren peningkatan kasus Phishing terutamaa terkait UU ITE, dengan pelaku yang semakin canggih dalam menipu dan mencuri informasi pribadi melalui email, situs web palsu, dan pesan teks berbahaya. Mayoritas kasus terjadi secara online melalui media sosial seperti email, facebook, dan Instagram, meningkatkan risiko pencurian data karena banyak korban tidak memahami tanda tanda modus phising.

Penelitian ini bertujuan untuk menganalisis dan memahami berbagai modus operandi yang digunakan oleh phisher dalam menjalankan kejahatan phishing. Dengan memahami modus yang digunakan oleh phisher, diharapkan dapat ditemukan langkah-langkah preventif yang efektif untuk melindungi individu dan organisasi dari Kejahatan phishing.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode studi kasus menggunakan pendekatan kualitatif deskriptif. Pendekatan ini dipilih untuk mendapatkan pemahaman mendalam mengenai bagaimana modus operandi phisher dalam kejahatan phishing dengan memahami modus yang digunakan oleh phisher, diharapkan dapat ditemukan langkah-langkah preventif yang efektif untuk melindungi individu dan organisasi dari Kejahatan phishing. Langkah awal dalam pelaksanaan studi kasus ini adalah pemilihan subjek penelitian yang terdiri dari penyidik Ditreskrimsus, narapidana pelaku phishing, dan pihak OJK. Teknik pengumpulan data dilakukan melalui wawancara mendalam, observasi, dan dokumentasi. Analisis data dilakukan secara tematik, dimulai dari reduksi data, penyajian data, hingga penarikan kesimpulan. Validitas data diperoleh melalui triangulasi sumber.

HASIL DAN PENELITIAN

Berdasarkan hasil penelitian ini menunjukan bahwa Modus Operandi Phisher dalam kejahatan phishing dilakukan secara terstruktur dan memanfaatkan kemajuan teknologi informasi. Berdasarkan wawancara dengan Iptu Irwan Samson dan Panit 3 Unit 1 Subdit V, Hendri Joni, diketahui bahwa modus operandi phisher tidak hanya terbatas pada satu bentuk melainkan bersifat dinamis dan berkembang sesuai dengan kemajuan teknologi dan kelemahan korban. Para pelaku secara aktif memanfaatkan situs palsu (fake website) yang menyerupai situs resmi, memanfaatkan media sosial seperti Facebook, aplikasi jual beli online, dompet digital), serta manipulasi psikologis untuk menjerat korban.

Berdasarkan wawancara dengan Rizki, seorang narapidana pelaku kejahatan ITE di Lapas Kelas IIA Pekanbaru, mengungkapkan bahwa modus operandi dilakukan secara individual namun dengan strategi teknis yang kompleks. Rizki mengaku menggunakan teknik manipulasi psikologis tanpa ancaman eksplisit, serta

memanfaatkan alat seperti IP transmitter untuk menyembunyikan lokasi. Ia menyebutkan bahwa 90% informasi yang dibutuhkannya diperoleh dari media sosial, dan salah satu kunci keberhasilan aksinya adalah kelalaian korban dalam menjaga informasi pribadi. Modus lain yang digunakan adalah pembuatan situs web palsu dengan kemiripan hampir sempurna dari situs asli, teknik eksploitasi melalui email, dan penguasaan perangkat lunak seperti ScriptWaiter dan Trojan Backdoor.

Berdasarkan wawancara kepada bapak Bio Fawwaz Prakoso dari OJK, modus phishing yang sedang tren saat ini adalah fake BTS (Base Transceiver Station), yakni pengiriman pesan SMS yang tampak seperti berasal dari institusi resmi, lengkap dengan tautan ke situs palsu. Modus ini tergolong sulit dideteksi karena memanfaatkan teknologi penguat sinyal yang canggih.

Berdasarkan hasil wawancara dapat disimpulkan penelitian menunjukkan bahwa modus operandi pelaku phishing dapat dirinci dalam tiga tahap:

- Perencanaan: Pelaku menentukan target yang dianggap mudah tertipu, menyusun pesan bohong (biasanya berupa undangan wawancara kerja, promo hadiah, dll), dan mempersiapkan perangkat teknologi seperti laptop, SIM card palsu, dan software pendukung.
- Pelaksanaan: Pelaku mengirimkan pesan atau link palsu melalui email, WhatsApp, atau media sosial. Setelah korban mengisi data pribadi, pelaku menggunakan informasi tersebut untuk mengakses akun perbankan korban.
- Penyamaran dan Penghilangan Jejak: Pelaku biasanya memalsukan identitas, menggunakan rekening penampungan atas nama orang lain, dan memanfaatkan jaringan VPN atau perangkat orang lain untuk menghindari pelacakan.

Analisis Berdasarkan Teori Aktivitas Rutin

Teori aktivitas rutin menjelaskan bahwa kejahatan terjadi karena pertemuan antara pelaku yang termotivasi, target yang layak, dan tidak adanya penjaga. Dalam konteks phishing:

- Pelaku termotivasi: Pelaku merupakan individu dengan pengetahuan teknologi yang memadai dan motif ekonomi yang memampuni
- Target yang layak: Korban biasanya kurang memiliki literasi digital dan mudah percaya pada pesan palsu, dan mudah diiming imingi keuntungan.
- Tidak adanya penjaga: Minimnya sistem keamanan serta pengawasan dari institusi finansial maupun pribadi korban mempermudah pelaku menjalankan aksinya.

KESIMPULAN

Modus operandi pelaku phishing menunjukkan pola tindakan yang sistematis dan memanfaatkan kelemahan literasi digital masyarakat. Kejahatan ini didorong oleh motif ekonomi dan difasilitasi oleh kemajuan teknologi. Berdasarkan teori aktivitas rutin, kejahatan phishing dapat ditekan jika terdapat penguatan pengawasan, peningkatan kesadaran digital masyarakat, serta peran aktif institusi keuangan dalam memberikan edukasi dan perlindungan. Kejahatan ini tidak hanya menyebabkan kerugian finansial tetapi juga merusak integritas identitas korban. Pencegahan yang efektif memerlukan pendekatan multidimensi, baik dari sisi penegakan hukum, penguatan teknologi pengamanan, serta peningkatan edukasi masyarakat.

Bibliograpi

Radiansyah, I., Rusdjan, C., & Priyadi, Y. (2016). Analisis Ancaman Phishing Dalam Layanan Online Banking. *Journal of Innovation in Business and Economics*, *7*(1), 1-14.

LAURENTINA, M. D. (2022). Modus Operandi Tindak Pidana Phishing Dan Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Phishing Di Surabaya (Studi Putusan Pengadilan).

Permana, F. A., & Jamaludin, A. (2023). Personal Data Vulnerability in the Digital Era: Study of Modus Operandi and Mechanisms to Prevent Phishing Crimes. *Jurnal Al-Hakim: Jurnal Ilmiah Mahasiswa, Studi Syariah, Hukum dan Filantropi*, 201-216.

Kurniawan, M. R., & Pujiyono, P. (2018). Modus Operandi Korupsi Pengadaan Barang dan Jasa Pemerintah oleh PNS. *Law Reform*, *14*(1), 115-131.

Wiranata, G. A., Ucuk, Y., & Sidarta, D. D. (2024). PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA PHISHING. *COURT REVIEW: Jurnal Penelitian Hukum (e-ISSN: 2776-1916)*, *4*(02), 13-25.

Saputra, D., & Marpaung, Z. A. (2023). ANALISIS YURIDIS PENANGGULANGAN PENYALAHGUNAAN DATA PRIBADI DALAM BENTUK PHISING YANG DILAKUKAN OLEH PAID VERIFIED ACCOUNT DI MEDIA SOSIAL MENURUT UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI. *UNES Law Review*, 5(4), 4764-4775.

Warsiti, T., & Markoni, M. (2023). Perlindungan Hukum Terhadap Korban Kejahatan Cyber Crime Berbentuk Phising Dalam Transaksi Perdagangan Internasional. *Jurnal Multidisiplin Indonesia*, *2*(6), 1109-1125.

Yustitiana, R. (2021). Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phishing Transaksi Elektronik Sebagai Bagian dari Upaya Penegakan Hukum di Indonesia Dikaitkan Dengan Teori Efektivitas Hukum. *Jurnal Hukum Visio Justisia*, *1*(1), 98-126.

Pranata, E. J., & Ependi, L. (2023). Phising Terhadap Website Bank BCA. *The Journal Implementation of Data Science*, *1*(1).

Ramadhanti, A. N., Tias, T. A., Lestari, E. D., & Hosnah, A. U. (2024). Cara Operasi Kejahatan Phising di Ranah Siber yang Diatur Oleh Hukum Positif Indonesia. *Jurnal Pendidikan Tambusai*, *8*(1), 1299-1305.

Putri, R. N. S. (2022). Analisa Pola–Pola Sosialisasi Pencegahan Modus Social Engineering Oleh Bank Melalui Media Website Dan Media Sosial Twitter.

Tomara, K. J., & NASIONAL, K. P. (2011). Kajian Yuridis Pertanggungjawaban Pidana Penyedia Jasa Internet dan Pemilik Domain Situs Phising. *Skripsi, Fakultas Hukum Universitas Brawijaya*.

Purwandari, M. D. (2024). *Analisis Peran Polda Daerah Istimewa Yogyakarta dalam Pengungkapan Kasus Phishing* (Doctoral dissertation, Universitas Islam Indonesia).