Analisis Upaya Kejahatan Siber Terhadap Pencurian Data Digital Pengguna Internet dan Perangkat Seluler

Ilham Dio Bhakti[1]

[1] Program Studi Akuntansi, Universitas Pembangunan Nasional "Veteran" Jawa Timur

E-mail: 21013010092@student.upnjatim.ac.id[1]

Abstrak. Penelitian ini bertujuan untuk menganalisis upaya kejahatan siber, berfokus dalam pencurian data pengguna internet dan perangkat seluler dengan menggunakan metode penelitian *literature review*. *Fraud* atau kecurangan atau penipuan merupakan suatu tindakan yang digunakan oleh seseorang menimbulkan ketidakadilan atau kerugian bagi pihak lain. Dengan pertumbuhan penggunaan internet yang signifikan, semakin banyak orang yang memberikan informasi pribadi mereka secara *online*. Akibatnya, terdapat sejumlah besar informasi pribadi dan transaksi keuangan menjadi rentan terhadap penjahat dunia maya. Penipuan komputer memiliki pengertian kejahatan yang dilakukan oleh seseorang maupun sekelompok orang dengan cara menggunakan atau dengan sasaran komputer atau sistem komputer atau jaringan komputer. Penelitian ini diharapkan dapat memberikan gambaran pada pembaca tentang potensi kejahatan dan penipuan berbasis digital atau siber agar dapat memberikan suatu pemahaman sehingga dapat dicari dan diteliti kedepannya bagaimana cara menghindari dan menanggulanginya.
Kata kunci: keamanan siber; kecerdasan buatan; *machine learning*; deteksi ancaman; *ransomware*

Abstract. *This study aims to analyze the impact of Cybercrime, focusing on the theft of internet user data and mobile devices. Fraud or cheating or deception is an action used by someone to cause injustice or loss to other parties. With the significant growth in internet usage, more and more people are sharing their personal information online. As a result, large amounts of personal information and financial transactions become vulnerable to cybercriminals. Computer fraud has the meaning of a crime committed by a person or group of people by using or targeting a computer or computer system or computer network. It is hoped that this research can provide readers with an overview of the potential for digital or cyber-based crimes and fraud in order to provide an understanding so that further research can be sought and investigated on how to avoid and overcome them.*

Keywords: *Cybercrime, Digital Data Theft, Internet Users, Mobile Devices, Fraud, Digital Fraud, Cybersecurity, Computer Fraud, Cyber Crime, Data Protection.*

1. Pendahuluan

Di era digital yang mana teknologi dan informasi semakin berkembang pesat dan luas, telah muncul berbagai kejahatan siber atau dunia maya yang memanfaatkan perangkat digital dengan ilegal atau tidak bertanggung jawab. Tidak dapat dipungkiri, terkadang mereka menyerang informasi pribadi guna

menimbulkan kerusakan pada identitas pribadi. Bahkan tidak sedikit data pribadi tersebut dijual maupun diperjual belikan, yang tentunya dapat merugikan pemilik data pribadi tersebut. Penjahat-penjahat siber atau dunia maya juga telah melakukan adaptasi dan pengembangan dari metode-metode yang mereka gunakan untuk mencuri informasi, namun serangan dengan menggunakan rekayasa sosial masih menjadi pendekatan yang sering mereka pilih. Umumnya, kejahatan siber atau kejahatan dunia maya merupakan kejahatan yang menggunakan perangkat teknologi komputer dengan basis pada kecanggihan teknologi dan jaringan internet (Laksana & Mulyani, 2023) . Di Indonesia, peningkatan jumlah pengguna internet mencapai 196,71 juta orang pada tahun 2019, yang setara dengan 73,7% dari total populasi. Namun, peningkatan ini juga diiringi dengan meningkatnya insiden penyalahgunaan data pribadi, seperti kebocoran data yang mengakibatkan kerugian finansial dan ancaman terhadap privasi individu (Delphia & K. Harjono Maykada, 2021). Serangan siber seperti *phishing*, *malware*, dan *ransomware* semakin canggih dengan memanfaatkan rekayasa sosial serta celah keamanan dalam sistem teknologi. *Phishing* sering digunakan untuk menipu korban agar memberikan informasi sensitif melalui email atau situs palsu yang menyerupai platform resmi, sementara *malware* dapat menyusup ke perangkat untuk mencuri data atau mengendalikan sistem tanpa sepengetahuan pengguna. *Ransomware*, yang mengenkripsi data korban dan menuntut tebusan, menjadi ancaman besar bagi perusahaan dan institusi pemerintah, mengganggu operasional serta berpotensi membocorkan informasi rahasia jika tuntutan tidak dipenuhi. Dampak serangan ini tidak hanya terbatas pada kerugian finansial, tetapi juga merusak reputasi organisasi dan menurunkan tingkat kepercayaan publik terhadap keamanan data mereka. Diperlukan langkah-langkah mitigasi yang komprehensif, seperti peningkatan kesadaran keamanan siber, penerapan sistem pertahanan berlapis, serta kebijakan proteksi data yang ketat untuk mengurangi risiko serangan (BPPTIK, 2023) .

Penelitian yang dilakukan Van Nguyen (2022) menemukan bahwa Vietnam berpotensi menjadi basis operasi bagi penjahat domestik dan asing dalam melancarkan penipuan komputer lintas negara. Penipuan ini mencakup dua jenis utama: penipuan data kartu bank dan penipuan melalui telepon. Teknologi memungkinkan para pelaku menipu korban secara transnasional tanpa interaksi langsung. Sebagai studi pertama di Vietnam yang mengkaji topik ini, penelitian ini memberikan kontribusi penting dalam pemahaman tentang penipuan komputer, khususnya di Asia, dan menjadi dasar bagi investigasi lebih lanjut terkait kejahatan siber semacam ini. Penelitian yang dilakukan oleh Nguyen & Luong (2021) menganalisis struktur jaringan kejahatan siber dalam penipuan komputer transnasional di Vietnam. Dengan menggunakan analisis jaringan sosial, studi ini menemukan bahwa modus utama kejahatan melibatkan penipuan kartu bank dan telepon. Hasilnya menunjukkan bahwa jaringan kejahatan ini beroperasi dalam berbagai struktur, seperti *swarm networks* dan *distributed networks*. Studi ini juga menyoroti bahwa organisasi kejahatan siber lebih kompleks dari yang diasumsikan sebelumnya. Penelitian ini memberikan wawasan baru tentang pola kejahatan siber di Asia. Kesadaran masyarakat terhadap pentingnya perlindungan data pribadi masih tergolong rendah. Banyak pengguna yang kurang memahami risiko yang ada dan sering kali lalai dalam menjaga keamanan informasi mereka. Oleh karena itu, edukasi dan peningkatan literasi digital menjadi krusial dalam upaya pencegahan kejahatan siber (Arief et al., 2024) . Tujuan dari penelitian ini adalah untuk meneliti tentang upaya kejahatan siber dalam pencurian data pengguna internet dan perangkat seluler. Penelitian ini diharapkan dapat memberikan gambaran pada pembaca tentang potensi kejahatan dan penipuan berbasis digital atau siber agar dapat memberikan suatu pemahaman sehingga dapat dicari dan diteliti kedepannya bagaimana cara menghindari dan menanggulanginya.

2. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah *literature review*. *Literature review* merupakan sebuah metode yang sistematis, eksplisit dan reprodusibel untuk melakukan identifikasi, evaluasi dan sintesis terhadap karya-karya hasil penelitian dan hasil pemikiran yang sudah dihasilkan oleh para peneliti dan praktisi. Dalam mencapai tujuan penelitian, langkah pertama yang dilakukan

adalah mencari dan menentukan artikel-artikel yang dapat dijadikan sumber informasi dan pembahasan. Artikel-artikel tersebut dapat ditemukan di *database* jurnal. Kemudian dari hasil pencarian artikel-artikel yang telah dilakukan, ditentukan sejumlah lima artikel yang paling relevan untuk diidentifikasi dan dianalisis dalam penelitian ini.

Tabel 1. Artikel *Literature Review*

No.	Penulis	Judul Artikel	Tahun	Jurnal
1.	Trong Van Nguyen	*The modus operandi of transnational computer fraud: a crime script analysis in Vietnam*	2022	*Jurnal of Trends in Organized Crime*
2.	Trong Nguyen dan Hai Thanh Luong	*The structure of cybercrime networks: transnational computer fraud in Vietnam*	2021	*Journal of Crime and Justice*
3.	Randi Jiang	*Exploring Employees Computer Fraud Behaviors using the Fraud Triangle Theory*	2022	*Journal of the Association for Information Systems*
4.	Tom Davison	*Cyberthreats are going mobile and it's time to take action*	2021	*Journal of Computer Fraud & Security*
5.	Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz Khan	*Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*	2021	*Journal Frontiers in Computer Science*

3. Hasil dan Pembahasan

3.1. Aspek Jumlah Artikel

Berdasarkan tahun terbit, ada 3 artikel yang dipublikasikan pada tahun 2021, dan 2 artikel terbit pada tahun 2022. Berdasarkan sumber artikel, terdapat masing-masing 1 artikel dari *Jurnal of Trends in Organized Crime, Journal of Crime and Justice, Journal of the Association for Information Systems, Journal of Computer Fraud & Security, Journal Frontiers in Computer Science*

3.2. Aspek Tema Pembahasan Artikel

Adapun terkait tema pembahasan Analisis Dampak Kejahatan Siber Dalam Pencurian Data Pengguna Internet dan Perangkat Seluler, ada 5 artikel terpilih yang membahas tema penipuan komputer secara spesifik.

Penelitian yang dilakukan oleh Davison (2021) mengamati pada era pandemi Covid-19 yang menyerang Sebagian besar negara di dunia telah mengakibatkan dampak amat besar dalam berbagai aspek terutama pada aspek teknologi yaitu meningkatnya penggunaan perangkat seluler dan internet yang tidak diikuti dengan upaya proteksi data pengguna yang maksimal sehingga memunculkan berbagai peluang aksi kejahatan. Peneliti dalam hal ini meneliti, mengidentifikasi, dan menganalisis berbagai tujuan dan motivasi penjahat dalam melakukan tindakan kejahatan dan bagaimana saja bentuk atau upaya-upaya aksi kejahatan siber dalam mengeksploitasi perangkat seluler serta bagaimana upaya pencegahan yang dapat dilakukan.

Penelitian yang dilakukan oleh Alkhalil et al. (2021) menyelidiki tentang serangan *phishing* pada pengguna internet. Peneliti telah mengklasifikasikan serangan *phishing* menurut mekanisme *phishing* mendasar dan tindakan pencegahan yang mengabaikan pentingnya siklus hidup *phishing* ujung ke ujung. Penelitian ini mengusulkan anatomi rinci baru *phishing* yang melibatkan fase serangan, tipe penyerang, kerentanan, ancaman, target, media serangan, dan teknik menyerang. Selain itu, anatomi yang diusulkan akan membantu pembaca memahami proses siklus hidup serangan *phishing* yang pada gilirannya akan meningkatkan kesadaran akan serangan *phishing* ini dan teknik yang digunakan; juga, ini membantu dalam mengembangkan sistem anti-*phishing* holistik.

Penelitian yang dilakukan oleh Nguyen & Luong (2021) meneliti tentang dampak penipuan *online* terhadap pendapatan *e-commerce*. Penelitian menyebutkan negara Amerika Utara, Amerika Latin, Timur Tengah dan Afrika, Asia Pasifik, dan Eropa masing-masing kehilangan 1,3% hingga 1,9% dari pendapatan tahunan mereka karena penipuan *online* dan diperkirakan Amerika Utara, Amerika Latin, Timur Tengah dan Afrika, Asia Pasifik, dan Eropa masing-masing mendapatkan tambahan pendapatan keuangan negara meningkat alasannya karena perkembangan teknologi berpengaruh pada bahan pokok, maupun kenaikan saham dan pendapatan negara yang lain.

Penelitian yang dilakukan oleh Van Nguyen (2022) meneliti tentang modus operasi penipuan komputer transnasional dengan menggunakan analisis naskah kejahatan yang terjadi di Vietnam. Peneliti memprediksi Vietnam akan menjelma menjadi basis operasi bagi penjahat-penjahat domestik maupun internasional dalam menjalankan praktik kejahatan dan penipuan komputer transnasional. Alasan yang mendasari pernyataan tersebut adalah hasil penggabungan data dari profil kriminal dan wawancara mendalam dengan penyelidik yang berwenang dalam hal ini yaitu polisi *cyber*. Jenis penipuan dan kejahatan tersebut mencakup mulai penggunaan Sebagian elemen teknologi hingga seluruh faktor teknologi. Peran dari pelaku kejahatan tersebut baik domestik dan internasional diklasifikasikan dalam dua jenis penipuan komputer transnasional yaitu penipuan data kartu bank dan penipuan telepon.

Penelitian yang dilakukan oleh Jiang (2022) mengeksplorasi sejauh mana persepsi karyawan tentang peluang, rasionalisasi, dan tekanan kerja yang berkontribusi pada kemungkinan mereka melakukan penipuan komputer (yaitu, disengaja, jahat, atau saat termotivasi melalui keuntungan kepentingan diri sendiri) dan dengan menggunakan teori segitiga penipuan secara empiris dapat mengemukakan betapa pentingnya pemantauan tekanan kerja untuk mencegah karyawan melakukan kegiatan penipuan komputer.

3.3. Aspek Metodologi yang Digunakan

Masing-masing dari kelima artikel ini menggunakan metodologi yang beragam, artikel pertama menggunakan metodologi kualitatif (Alkhalil et al., 2021), artikel kedua menggunakan *mixed method approach* (metode campuran) (Nguyen & Luong, 2021), artikel ketiga menggunakan metodologi *literature review* (Davison, 2021), artikel keempat menggunakan metodologi analisis kualitatif (Nguyen & Luong, 2021), dan artikel kelima metodologi empiris yang dilakukan dengan mengumpulkan data survei dari 213 karyawan yang berasal dari berbagai industri yang menggunakan komputer dengan tanggung jawab keuangan dalam organisasi mereka di A.S (Jiang, 2022).

3.4. Aspek Temuan Penting Pada Artikel

Penggunaan internet dan perangkat seluler di era globalisasi semakin meningkat drastis. Dengan adanya peningkatan tersebut, terdapat sebagian orang yang menyalahgunakannya untuk hal yang merugikan serta tidak bertanggungjawab. Hal ini tentunya menjadi suatu ancaman langsung pengguna internet dan perangkat seluler. (Alkhalil et al., 2021; Davison, 2021; Jiang, 2022; Nguyen & Luong, 2021; Van Nguyen, 2022). Jumlah dan intensitas dari serangan siber akan meningkat selaras dengan meningkatnya ketergantungan terhadap perangkat seluler. Perangkat seluler bisa membuka peluang keuntungan finansial yang luas tetapi juga bisa membuka ruang pencurian data tanpa batas (Davison, 2021). Kejahatan di dunia maya saat ini tidak perlu lagi dilakukan dengan pendekatan fisik seperti melakukan

peretasan secara langsung terhadap perangkat seluler korban tetapi dapat menggunakan teknologi yang dapat dioperasikan dari jarak jauh melalui internet dan komunikasi nirkabel. Jaringan operasi kejahatan dunia maya dilihat dari tingkat penggunaan teknologi yang digunakan, yaitu mulai jaringan berteknologi tinggi hingga berteknologi rendah (Van Nguyen, 2022). Kejahatan dunia maya terus meningkat di negara berkembang akibat lemahnya regulasi dan infrastruktur digital. Laporan dari Utama (2024) menunjukkan bahwa serangan *ransomware* semakin sering menargetkan lembaga pemerintahan dan bisnis di wilayah ini. Selain itu, CNN Indonesia (2024) mencatat bahwa jaringan penipuan siber global menghasilkan hingga US$3 triliun per tahun, terutama di Asia Tenggara. Di Indonesia, kasus serangan siber meningkat dengan target yang semakin beragam. Peningkatan ini menegaskan perlunya kerja sama internasional dan penguatan kebijakan keamanan

Akan tetapi, bentuk serangan bukan hanya dilakukan secara jarak jauh, beberapa penjahat siber bisa saja berusaha menyusupi perangkat secara langsung atau fisik. Penjahat dapat *menginstal malware* ke perangkat digital yang dapat diakses oleh mereka secara langsung atau fisik. Penjahat yang mempunyai sumber pendanaan yang cukup baik bisa memanfaatkan *malware* untuk mengeksploitasi perangkat melalui sistem operasi, hal tersebut memberikan kendali atas perangkat tanpa campur tangan dari korban. Hal ini dapat disebut 'serangan tanpa klik' dikarenakan korban hanya perlu mendapat pesan teks, atau email supaya *malware* bisa dioperasikan atau diaktifkan. Metode serangan fisik menggunakan *malware* ini adalah salah satu metode serangan paling mutakhir, sekaligus merupakan metode paling mahal. Metode serangan paling populer lain adalah *phishing* seluler (Davison, 2021).

Serangan *phishing* menjadi salah satu ancaman utama bagi individu dan organisasi hingga saat ini. Seperti yang disorot dalam artikel, ini terutama didorong oleh keterlibatan manusia dalam siklus *phishing*. Sering kali *phisher* mengeksploitasi kerentanan manusia selain mendukung kondisi teknologi (yaitu, kerentanan teknis). Telah diidentifikasi bahwa usia, jenis kelamin, kecanduan internet, stres pengguna, dan banyak atribut lainnya mempengaruhi kerentanan terhadap *phishing* di antara orang-orang (Alkhalil et al., 2021).

Ketika seseorang mendapat tingkat tekanan kerja yang tinggi mereka akan berpotensi mengalami stres, sehingga mereka akan cenderung melakukan penipuan komputer. Perilaku ini dapat dicegah dengan melakukan pemantauan beban kerja yang ditugaskan kepada karyawan dan ekspektasi kinerja untuk mencegah perilaku yang tidak diinginkan ini dan tidak ditemukan dampak yang signifikan pada variabel kontrol (jenis kelamin, pendidikan, keterampilan komputer, dan pemantauan), hal ini menunjukkan bahwa perilaku penipuan komputer didasari oleh faktor-faktor yang berakar pada model teoretis yang disajikan daripada pemantauan komputer dan oleh karena itu, perusahaan harus memahami betapa pentingnya memantau tekanan kerja untuk mencegah karyawan melakukan perilaku penipuan komputer dan menggunakan teknik keamanan yang berbeda untuk menghilangkan perilaku penipuan komputer. Singkatnya, ketika merancang kebijakan keamanan informasi organisasi, perilaku penipuan komputer harus dipertimbangkan secara terpisah dari perilaku kepatuhan keamanan lainnya (Jiang, 2022).

4. Kesimpulan

Dalam penelitian ini, digunakan 5 artikel yang menjadi bahan kajian. Kelima artikel ini diteliti dan berfokus pada penipuan komputer. Fokus teliti dari kelima artikel tersebut adalah menjabarkan hasil berupa kemajuan dan perkembangan teknologi dan informasi yang memiliki dampak signifikan terhadap kejahatan dan penipuan berbasis digital. Metodologi penelitian dari kelima artikel ini sangatlah beragam namun terdapat 2 artikel yang menggunakan metodologi yang sama yaitu (Alkhalil et al., 2021; Van Nguyen, 2022) yang sama-sama menggunakan metodologi pendekatan kualitatif, di samping kedua artikel tersebut, artikel lainnya menggunakan metodologi metode campuran Nguyen & Luong (2021), metodologi *literature review* Davison (2021), dan metodologi empiris Jiang (2022) . Kesimpulan dari sisi temuan penting Keterbatasan pada penelitian artikel ini adalah pembahasan artikel ini terbatas pada 5 artikel saja. Sehingga data penelitian yang telah ditemukan terbatas serta tidak meluas dikarenakan

keterbatasan tersebut. Maka pada penelitian selanjutnya, diharapkan peneliti mampu mengembangkan jumlah artikel yang menjadi bahan penelitian dan menghasilkan hasil pembahasan yang jauh lebih akurat. Artikel penelitian yang diteliti oleh penulis masih belum dapat menjabarkan secara keseluruhan terkait dengan bagaimana kemajuan teknologi dan informasi dapat memiliki dampak yang signifikan terhadap tingginya aksi kejahatan dan penipuan berbasis digital. Saran yang dapat diberikan oleh penulis dalam penelitian selanjutnya dari penelitian yang telah dilakukan yaitu agar penelitian berikutnya lebih memperhatikan modus-modus operasi penjahat di dunia maya yang memanfaatkan penggunaan data digital secara ilegal.

5. Daftar Pustaka

[1] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Science*, *3*, 563060.

[2] Arief, M. H., Fitri, K. A., & Sakti, E. M. S. (2024). Analisis Kesadaran Cyber Crime Di Kalangan Masyarakat Menengah Kebawah. *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, *25*(2), 24–39.

[3] BPPTIK. (2023, May 15). *Jenis-Jenis Serangan Siber di Era Digital*. Bpptik.Kominfo.Go.Id. https://bpptik.kominfo.go.id/Publikasi/detail/jenis-jenis-serangan-siber-di-era-digital?utm_source

[4] CNN Indonesia. (2024, March 29). *Interpol: Darurat Perdagangan Orang, Mafia di ASEAN Raup Rp47.586 T* . Cnnindonesia.Com. https://www.cnnindonesia.com/internasional/20240329095145-106-1080363/interpol-darurat-perdagangan-orang-mafia-di-asean-raup-rp47586-t

[5] Davison, T. (2021). Cyberthreats are going mobile and it's time to take action. *Computer Fraud & Security*, *2021*(3), 18–19.

[6] Delphia, R., & K. Harjono Maykada. (2021). *PERSEPSI MASYARAKAT ATAS PELINDUNGAN DATA PRIBADI*. https://aptika.kominfo.go.id/wp-content/uploads/2021/12/Persepsi-Masyarakat-terhadap-Pelindungan-Data-Pribadi.pdf?utm_source

[7] Jiang, R. (2022). Exploring employees' computer fraud behaviors using the fraud triangle theory. *Pacific Asia Journal of the Association for Information Systems*, *14*(4), 4.

[8] Laksana, T. G., & Mulyani, S. (2023). FAKTOR–FAKTOR MENDASAR KEJAHATAN SIBER TERHADAP KEMANUSIAAN: Key Determinants Of Cybercrimes Targeting The Human Population. *Jurnal Hukum PRIORIS*, *11*(2), 136–160.

[9] Nguyen, T., & Luong, H. T. (2021). The structure of cybercrime networks: transnational computer fraud in Vietnam. *Journal of Crime and Justice*, *44*(4), 419–440.

[10] Utama, L. (2024, December 24). *Indonesia Harus Hati-hati dengan Metaverse* . Viva News & Insights. https://www.viva.co.id/digital/digilife/1435029-indonesia-harus-hati-hati-dengan-metaverse

[11] Van Nguyen, T. (2022). The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. *Trends in Organized Crime*, *25*(2), 226–247.