E-journal Field of Economics, Business, and Entrepreneurship (EFEBE)

KEJAHATAN SIBER DAN PENIPUAN KOMPUTER: APA PENCEGAHAN YANG DAPAT DILAKUKAN?

Raisa Aqila Birlin[1], Lisa Oktaviani[2], Maninggor Esteria Silaban[3] , Aryan Danil Mirza BR[4]
[1234]Universitas Lampung
[1]raisaqila573@gmail.com, [2] lisaoktaviani06105@gmail.com, [3]estermaninggor@gmail.com, aryan.danil@feb.unila.ac.id [4]

Informasi Naskah

Update Naskah:
Dikumpulkan: 10 November 2025
Diterima: 12 November 2025
Terbit/Dicetak: 13 November 2025

Keywords:
Cybercrime, Computer Fraud, Cybersecurity, Data Security, Ransomware

Abstract

A The fast development of technology has brought both positive and negative effects, incluiding an increase in cybercrime like computer fraud. Cybercrime involves illegal actions through computer networks, such as data theft and online scams, whic harm individuals, organizations, and goverments. Data from e-MP Robinospal Bareskrim Polri (2022) shows that cybercrime cases are on the rise, with criminals becoming more skilled at exploiting systems. Computer fraud uses technology to gain illegal profits through methods like phising and ransomware. The losses from cybercrime are significant, affecting both finances and reputation. Therefore, preventive measures are important at all levels, from indivuduals to organizations. This article takes a qualitative approach, using a literature review to explore tge issue of cybercrime and computer fraud, along with strategies for prevention. Key actions include implementing security protocols, improving digital literacy, and encouraging collaboration among different parties to reduce the negative effects of cybercrime and protect information security.

A. PENDAHULUAN

Dewasa ini, perkembangan dunia dan masyarakat selalu diikuti dengan perkembangan teknologi yang berkembang pesat. Perkembangan teknologi membuat segala sesuatu berubah mulai dari pemerintahan, pasar ekonomi, perdagangan global, perjalanan dan komunikasi. Munculnya Internet membuat masyarakat menjadi lebih maju dan efisien (Butarbutar, 2023).

Perkembangan teknologi yang semakin canggih memberikan dampak positif dan negatif bagi setiap penggunannya. Teknologi yang semakin canggih terutama dalam penggunaan komputer membantu sebuah perusahaan dalam menjalankan operarasionalnya menjadi lebih eifisien, seperti pengurangan biaya dan meminimalisir terjadinya kesalahan yang dibuat manusia. Permasalahan yang sangat disayangkan terhadap penggunaan teknologi ini adalah masyarakat menggunakannya untuk hal-hal negatif yang merugikan orang lain. Tindakan ini muncul karena disebabkan oleh faktor-faktor seperti ekonomi, pergaulan yang tidak tepat, dan kesempatan. Faktor-faktor tersebut akhirnya membuat masyarakat melakukan tindakan tersebut dengan tujuan untuk memenuhi kebutuhan hidupnya (Pratama, 2017:124). Adapun tindakan negatif yang muncul dari teknologi, yaitu kejahatan siber dan

* *Corresponding Author*.
Raisa Aqila Birlin, e-mail : raisaqila573@gmail.com

DOI 10.23960/efebe.v3i1.315

penipuan komputer.

Kejahatan siber *(Cybercrime)* merujuk pada tindakan ilegal yang dilakukan melalui jaringan komputer, seperti pencurian data, penipuan online, dan serangan malware. Kejahatan siber menjadi ancaman yang berbahaya bagi setiap pengguna teknologi, pemerintah pun kesulitan dalam mengimbangi teknik kejahatan yang dilakukan pelaku dengan menggunakan komputer (Ketaren, 2016:35).

Menurut data dari e-MP Robinopsal Bareskrim Polri (2022) menjukkan bahwa jumlah kasus kejahatan siber meningkat secara signifikan dalam beberapa tahun terakhir, dengan ribuan laporan baru setiap harinya. Hal ini menunjukkan bahwa pelaku kejahatan semakin canggih dan menggunakan berbagai teknik untuk mengeksploitasi kelemahan sistem. Salah satu bentuk dari kejahatan siber ini yaitu penipuan komputer, bentuk penipuan yang memanfaatkan teknologi untuk merugikan orang lain, baik secara finansial maupun emosional, dengan atau tanpa memperhatikan keuntungan (Accounting Department, Bina Nusantara University, 2020).

Meskipun dampak dari kejahatan siber dapat merugikan, langkah pencegahan yang dapat dilakukan oleh individu, masyarakat, organisasi dan pemerintahan adalah dengan cara memahami skema kejahatan dunia maya dan mencari tahu apa yang menjadi objek sasaran mereka untuk melancarkan aksinya, sehingga dari penjagaan dan pengawasan yang ketat terhadap objek yang digunakan pelaku dalam melancarkan aksinya, pencurian data dan kejahatan internet lainnya dapat diminimalisir (Cybersecurity and Infrastructure Security Agency, 2018).

B. TINJAUAN PUSTAKA

Kejahatan Siber

Kejahatan siber merupakan tindakan kriminal yang dilakukan melalui jaringan komputer atau internet, dengan sasaran berupa sistem informasi, data, atau jaringan itu sendiri (Yar, 2006). Selain itu, kejahatan siber dapat dibagi menjadi dua bagian yaitu arti luas dan sempit. Dalam arti luas, kejahatan siber adalah kejahatan yang melibatkan komputer atau jaringan komputer, serta tindakan yang menggunakan komputer untuk melakukan penipuan. Sedangkan dalam arti sempit, kejahatan siber hanya mencakup tindakan kriminal yang terjadi di dalam sistem komputer itu sendiri. Sementara itu, Ransbotham et al. (2019) mendefiniskan kejahatan siber sebagai tindakan yang sangat dipengaruhi oleh perilaku manusia. Penekanan pada aspek manusia ini menunjukkan bahwa kejahatan siber tidak hanya berkaitan dengan sistem dan data, tetapi juga dengan cara orang berinteraksi dengan teknologi.

Selanjutnya, kejahatan siber didefinisikan pula sebagai suatu fenomena yang semakin terorganisir, di mana pelaku membentuk jaringan kriminal yang rumit. Ini menunjukkan bahwa kejahatan siber tidak hanya melibatkan orang perorangan, tetapi juga melibatkan elemen organisasi dan strategi yang lebih kompleks (Sharma, 2020). Adapun McGuire dan Dowling (2013) menjelaskan bahwa kejahatan siber melibatkan berbagai tindakan kriminal yang dilakukan melalui teknologi informasi dan komunikasi, terutama di internet. Kejahatan ini berdampak pada individu, organisasi, dan masyarakat secara keseluruhan, sehingga penting untuk menerapkan pendekatan yang menyeluruh dalam menghadapinya. Undang-Undang Nomor 11 Tahun 2008 mendefiniskan kejahatan siber sebagai tindakan ilegal yang dilakukan melalui media elektronik, yang mencakup penyebaran informasi palsu, penipuan elektronik, pelanggaran privasi, dan akses ilegal ke sistem komputer. Tindakan ini dianggap melanggar hukum, sehingga melalui undang-undang ini, pemerintah berupaya melindungi pengguna internet dan menjaga keamanan informasi di dunia digital.

Penipuan Komputer

Penipuan komputer merupakan salah satu jenis kejahatan siber yang semakin marak terjadi di era digital saat ini. Kejahatan ini memanfaatkan teknologi informasi untuk meraih keuntungan secara ilegal, baik itu dalam bentuk uang, data pribadi, maupun sumber daya lainnya. Penipuan komputer adalah tindakan ilegal yang dilakukan dengan menggunakan komputer sebagai alat maupun sebagai objek, dengan tujuan untuk merugikan orang lain, baik dengan memperoleh keuntungan ataupun tidak

(Accounting Department, Bina Nusantara University, 2020). Andi Hamzah (1987) mengemukakan bahwa penipuan komputer yaitu segala bentuk aktivitas ilegal yang melibatkan penggunaan komputer untuk tujuan kriminal. Sekecil apapun dampak atau kerugian yang diakibatkan oleh penggunaan komputer secara ilegal dianggap sebagai kejahatan.

Kemudian, Marshall B. Romney dan Paul John Steinbart (2015) mendefinisikan penipuan komputer sebagai tindakan yang menggunakan komputer untuk mendapatkan data atau informasi secara ilegal, memanipulasi sistem, atau mencuri aset melalui teknologi informasi. Penipuan ini bisa terjadi dengan berbagai cara, seperti mengubah data secara tidak sah, mencuri informasi sensitif, serta mengakses sistem komputer perusahaan tanpa izin. Penipuan komputer ini merupakan salah satu bentuk fraud dalam sistem informasi akuntansi, di mana manipulasi data melalui komputer dapat menyebabkan kerugian finansial bagi organisasi atau individu yang terkena dampaknya.

Undang-Undang Nomor 19 Tahun 2016 mendefinisikan penipuan komputer sebagai tindakan yang dengan sengaja menggunakan informasi elektronik untuk menipu dan merugikan orang lain. Ini termasuk akses yang tidak sah, pengubahan data, atau penyebaran informasi palsu. Hal ini diatur dalam Pasal 27 ayat (3) dan Pasal 28, yang melarang tindakan yang dapat merugikan orang lain melalui teknologi informasi.

C. METODE PENELITIAN

Penyusunan artikel ini menggunakan metode penelitian kualitatif melalui pendekatan studi literatur. Metode ini dipilih karena mendukung analisis mendalam terhadap aspek kejahatan siber dan penipuan komputer, serta pemahaman mengenai strategi pencegahannya. Moleong (2017) menjelaskan bahwa penelitian kualitatif bertujuan untuk memahami fenomena sosial secara mendalam dengan menggali makna di balik data, sehingga menghasilkan wawasan yang lebih kaya dan mendalam. Studi literatur dilakukan dengan mengumpulkan dan menganalisis berbagai sumber yang relevan, mencakup jurnal ilmiah, artikel, buku, dan laporan keamanan siber.

D. HASIL DAN PEMBAHASAN

Jenis-Jenis Kejahatan Siber

Kejahatan siber meliputi berbagai tindakan ilegal yang memanfaatkan teknologi informasi dan internet untuk mendapatkan keuntungan secara tidak sah atau merugikan orang lain. Jenis kejahatan siber terus berkembang seiring dengan kemajuan teknologi (Wall, D.S., 2007). Jenis-jenis kejahatan siber berikut ini sering menyebabkan kerugian besar bagi individu maupun organisasi.

Salah satu jenis kejahatan siber adalah penipuan komputer. Penipuan komputer merupakan salah satu bentuk kejahatan siber yang memanfaatkan teknologi untuk melakukan tindakan ilegal, seperti manipulasi data dan peretasan sistem. Brenner (2010) menjelaskan bahwa praktik ini sering kali sulit dideteksi karena kompleksitas teknik yang digunakan oleh pelaku, yang membuat mereka merugikan pihak lain dengan memperoleh keuntungan secara tidak sah.

Jenis penipuan komputer selanjutnya adalah *phising*. *Phising* merupakan metode penipuan yang mengandalkan teknik manipulasi sosial untuk mendapatkan informasi pribadi, misalnya kata sandi, nomor kartu kredit, dan data identitas lainnya. Gulo et al. (2020) menyebutkan bahwa *phising* adalah salah satu kejahatan elektronik dalam bentuk penipuan. Dimana proses phising ini bermaksud untuk menangkap informasi yang sangat sensitif.

Selain penipuan komputer dan phising, *ransomware* juga termasuk ke dalam jenis kejahatan siber. *Ransomware* adalah jenis malware yang mengenkripsi file atau data penting miik korban, ini menyebabkan file atau data penting itu tidak bisa diakses. Kharraz et al. (2015) menekankan bahwa *ransomware* terus berkembang menjadi lebih canggih dan sering kali menargetkan organisasi besar serta individu yang memiliki data berharga untuk mendapatkan tebusan dengan jumlah besar.

Selain itu, pencurian identitas juga menjadi salah satu bentuk kejahatan siber. Pencurian identitas terjadi ketika informasi pribadi seseorang dicuri dan digunakan untuk melakukan tindakan kriminal. Pencurian identitas telah berkorelasi dengan penyalahgunaan komputer, kejahatan komputer, dan

kejahatan terkait komputer karena internet memvasilitasi mereka, itu disebut pencurian identitas online. Misalnya adalah kasus peretas yang mencuri informasi pribadi seseorang melalui pelanggaran data online (Artiningsih dan Sasmita, 2016).

Kerugian akibat Kejahatan Siber

Kejahatatan siber telah menjadi ancaman serius di era digital, membawa berbagai kerugian yang signifikan, baik dalam aspek keamanan data, finansial, maupun reputasi. Dampak negatif dari serangan siber meliputi kerugian yang dirasakan oleh individu, organisasi, bahkan sampai negara. Kerugiannya semakin meningkat beriringan dengan semakin luasnya penggunaan teknologi digital (Symantec, 2020). Salah satu target utama dalam kejahatan siber adalah data pribadi. Data pribadi yang dicuri dalam serangan siber dapat digunakan untuk berbagai aktivitas kriminal, mencakup pencurian identitas, penipuan, dan lain sebagainya. Nurdiani (2020) mendefinisikan pencurian data pribadi sebagai tindakan yang dilakukan dengan sengaja dan tanpa hak untuk mengakses komputer atau sistem elektronik milik orang lain. Tujuannya adalah untuk memperoleh informasi elektronik atau dokumen elektronik dengan cara melanggar keamanan sistem.

Di Indonesia, kasus pencurian data pribadi telah meningkat seiring dengan perkembangan teknologi digital. Semuel Abrijani Pangerapan (2020) mencatat bahwa perlindungan data pribadi di Indonesia masih lemah, sehingga kebocoran data sering kali terjadi dan menyebabkan kerugian besar bagi masyarakat. Hal ini diperburuk dengan rendahnya kesadaran masyarakat mengenai pentingnya melindungi data pribadi mereka.

Selain dampak pada data pribadi, kerugian finansial merupakan salah satu bentuk kerugian yang paling sering dirasakan oleh korban kejahatan siber. Serangan seperti *phising* dan *ransomware* memberi peluang penyerang untuk mencuri uang secara langsung ataupun meminta tebusan yang besar. Di indonesia, Otoritas Jasa Keuangan (OJK) mencatat bahwa pada tahun 2021 kerugian yang diakibatkan oleh kejahatan siber di sektor perbankan mencapai lebih dari Rp246,5 miliar, menunjukkan bahwa dampak ekonomi kejahatan siber semakin nyata dan merugikan berbagai sektor.

Kejahatan siber tidak hanya menyebabkan kerugian pada data pribadi dan finansial, tetapi juga menimbulkan dampak negatif lainnya, seperti kehilangan reputasi, gangguan operasional, dan penurunan kepercayaan masyarakat terhadap teknologi. Misalnya, ketika suatu perusahaan menjadi korban serangan siber, terlebih dalam kasus kebocoran data pribadi, maka reputasi perusahaan tersebut dapat menurun drastis. Harvard Business Review (2020) mencatat bahwa sekitar 65% konsumen mengaku kehilangan kepercayaan terhadap perusahaan yang mengalami penyalah gunaan data, dan banyak dari mereka yang memilih untuk berhenti menggunakan layanan dari perusahaan tersebut. Kehilangan ini dapat menyebabkan penurunan penjualan dan hilangnya pelanggan.

Di era digital saat ini, reputasi menjadi aset penting yang sangat sulit dipulihkan ketika sudah tercemar, terutama dalam industri yang berbasis kepercayaan, seperti perbankan, *e-commerce*, dan layanan kesehatan. Kejahatan siber di Indonesia, telah menjadi masalah yang signifikan bagi pemerintah dan berbagai sektor lainnya. Budi Rahardjo (2023) mencatat bahwa serangan siber terhadap institusi sering kali mengakibatkan kerugian finansial dan gangguan pada layanan penting bagi masyarakat. Sebagai contoh, serangan *ransomware* yang menargetkan layanan publik dapat menghentikan operasional penting, seperti layanan kesehatan dan transportasi. Oleh sebab itu, pemerintah dan sektor bisnis harus bekerja sama untuk meningkatkan sistem keamanan siber demi melindungi infrastruktur penting negara.

Langkah Pencegahan dan Solusi

Pencegahan kejahatan siber menjadi isu yang sangat penting di era digital saat ini, karena serangan siber semakin sering terjadi dan dampaknya semakin merugikan. Langkah pencegahan kejahatan siber harus dimulai dari tingkat individu, organisasi dan pemerintah. Parulian (2021) menjelaskan bahwa salah satu cara yang efektif untuk mengurangi risiko serangan siber adalah dengan menerapkan protokol keamanan yang ketat, seperti penggunaan *firewall* dan enskripsi data. Upaya ini dapat mencegah peretas

mengakses data sensitif dan mengurangi risiko kebocoran informasi.

Di samping itu, edukasi dan kesadaran pengguna terhadap ancaman siber juga merupakan hal yang penting. Banyak serangan siber terjadi karena kurangnya pemahaman pengguna tentang keamanan digital. Meningkatkan literasi digital dan memberikan pelatihan secara rutin tentang cara mengenali serangan siber benar-benar penting. Hal ini didukung oleh penelitian Aji (2019) yang menyebutkan bahwa peningkatan kapabilitas teknis dan kesadaran masyarakat adalah salah satu langkah fundamental untuk memperkuat pertahanan siber nasional.

Kerjasama antar pihak, baik pengguna, pemerintah, dan sektor swasta juga menjadi kunci dalam mencegah kejahatan siber. Parulian (2021) berpendapat bahwa koordinasi lintas sektor dan pembagian tanggung jawab antara penyedia layanan dan pengguna sangat penting untuk menciptakan ekosistem keamanan digital yang tangguh. Jadi, langkah-langkah pencegahan tidak hanya terbatas pada teknologi, tetapi melibatkan kebijakan dan perilaku yang mendukung keamanan siber secara menyeluruh juga.

Selanjutnya, Marshall B. Romney dan Paul Jhon Steinbart (2015) menyebutkan bahwa pencegahan terhadap kejahatan siber dan penipuan komputer dapat dilakukan dengan mengembangkan serangkaian kebijakan antipenipuan komprehensif yang dengan jelas menentukan ekspektasi untuk perilaku yang jujur dan etis, serta menjelaskan konsekuensi dari tindangan yang tidak jujur atau curang.

E. SIMPULAN DAN SARAN

Berdasarkan analisis yang penulis lakukan, dapat disimpulkan bahwa perkembangan teknologi yang cepat membawa banyak perubahan, termasuk risiko yang lebih besar dari kejahatan siber dan penipuan komputer. Tindakan ilegal ini tidak hanya merugikan individu dan perusahaan secara finansial, tetapi juga mengancam reputasi dan keamanan data mereka. Dengan semakin canggihnya cara yang digunakan oleh pelaku kejahatan siber, penting untuk mengambil langkah-langkah pencegahan yang efektif agar informasi dan aset penting dapat terlindungi.

Memahami jenis-jenis kejahatan siber, seperti pishing dan ransomware, adalah langkah awal yang penting. Upaya untuk meningkatkan pemahaman masyarakat tentang keamanan digital dan ancaman yang ada harus dilakukan secara terus-menerus. Selain itu, kerja sama antara individu, organisasi, dan pemerintah sangat penting untuk menciptakan lingkungan yang aman. Dengan menerapkan langkah-langkah keamanan yang ketat dan kebijakan anti-penipuan, diharapkan dampak negatif dari kejahatan siber dapat dikurangi, sehingga dunia digital bisa menjadi lebih aman untuk semua.

Dampak dari Kejahatan Siber dan Penipuan Komputer

Kejahatan siber dan penipuan komputer memiliki dampak besar bagi individu, organisasi, dam masyarakat secara umum. Kerugian finansial yang ditimbulkan bisa sangat besar, mengganggu jalannya bisnis, dan merusak reputasi. Selain itu, serangan siber dapat menimbulkan rasa tidak aman di kalangan pengguna teknologi, sehingga mengurangi kepercayaan terhadap layanan digital dan inovasi yang baru.

Keterbatasan penulisan

Tulisan ini mungkin memiliki keterbatasan dalam mendalami setiap jenis kejahatan siber dan dampaknya. Beberapa aspek, seperti motivasi pelaku atau detail cara pencegahan, mungkin belum dibahas secara mendalam. Selain itu, data yang digunakan mungkin terbatas pada sumber tertentu, sehingga tidak mencakup seluruh konteks global tentang masalah ini.

Peluang di Masa Depan

Di masa depan, penulisan tentang kejahatan siber dapat diperluas lagi dengan menambahkan lebih banyak penelitian mengenai teknologi terbaru dan dampaknya terhadap keamanan. Ada peluang untuk berkolaborasi antar bidang, seperti perilaku manusia dan ilmu komputer, yang dapat memberikan pemahaman baru. Selain itu, dengan meningkatnya kesadaran akan pentingnya keamanan siber, tulisan ini bisa menjadi dasar untuk program edukasi dan kebijakan yang lebih baik dalam mengatasi kejahatan siber.

DAFTAR PUSTAKA

Moleong, L.J. (2017). *Metodologi penelitian kualitatif* (3rd ed.). Remaja Rosdakarya.

Arief, B. (2006). Keamanan informasi dan cyber crime. Jakarta: Salemba Empat.

Yar, M. (2006) *Cybercrime and Society*, London: Sage

Sharma, S. (2020). Understanding Organized Cybercrime: The Emerging Threats. *Journal of Cybersecurity*, 5(2), 45-59.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*, 1-35.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2008). Jakarta: Sekretariat Negara.

Caseba, F. L., & Dewayanto, T. (2024). PENERAPAN ARTIFICIAL INTELLIGENCE, BIG DATA, DAN BLOCKCHAIN DALAM FINTECH PAYMENT TERHADAP RISIKO PENIPUAN KOMPUTER (COMPUTER FRAUD RISK): A SYSTEMATIC LITERATURE REVIEW. *Diponegoro Journal of Accounting*, *13*(3).

Kunz, M., & Wilson, P. (2004). Computer crime and computer fraud. *Report Submitted to the Montgomery County Criminal Justice Coordinating Commission*. Accounting Department, Bina Nusantara University.(2020). Computer Fraud (Part 1). Diakses pada 9 Oktober 2024 dari https://accounting.binus.ac.id/2020/05/21/computer-fraud-part-1/

Andi Hamzah. 1987. Aspek-Aspek Pidana di Bidang Komputer. Jakarta: Sinar Grafika.

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik. (2016). Lembaran Negara Republik Indonesia Tahun 2016, Nomor 251.

Kompas.(2021). *Serangan Siber, Perbankan Rugi Ratusan Miliar*. Diakses pada 10 Oktober 2024 dari https://kompas100.kompas.id/berita-ekonomi/serangan-siber-perbankan-rugi-ratusan-miliar/

Nurdiani, I. P. (2020). Pencurian Identitas Digital Sebagai Bentuk Cyber Related Crime. *Jurnal Kriminologi Indonesia*, 16(2).

Symantec. (2020). *Internet Security Threat Report*.

Pusiknas Bareskrim Polri.(2023). Kejahatan Siber di Indonesia Naik Berkali-kali Lipat. Pusiknas Bareskrim Polri. https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

Cybersecurity and Infrastucture Security Agency. 2018. CISA Cybersecurity Awareness Program. CISA. https://www.cisa.gov/resources-tools/programs/cisa-cybersecurity-awareness-program

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Pearson Education.

Otoritas Jasa Keuangan. (2021). Tantangan dan mitigasi kejahatan serta peningkatan keamanan siber di industri jasa keuangan.

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi). *Jurnal Politica Dinamika Masalah Politik Dalam Negeri* Dan Hubungan Internasional, 13(2).

Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Studi Tentang Ancaman dan Solusi Serangan Siber di Indonesia. *Telecommunications, Networks, Electronics, and Computer Technologies (TELNECCT), 1*(2).

Saputra Gulo, A., Lasmadi, S., & Nabawi, K. (2020). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal Of Criminal,* 1(2).

Artiningsih, A. (2016). Data Breaches and Identity Theft: A Case Study of US Retailers and Baking. *Jurnal Universitas Paramadina, 13.*

Harvard Business Review. (2020). How Data Breaches Affect Concumer Trust: AGlobal Study. Harvard Business Review Analytics Services. Dari https://www.hbr.org

Pangerapan, S. A. (2020). *Perlindungan Data Pribadi di Indonesia: Tantangan dan Solusi.* Kementerian Komunikasi dan Informatika Republik Indonesia.

Rahardjo, B. (2023). *Ransomware dan Tantangan Keamanan Siber di Indonesia.* Seminar Nasional Keamanan Siber Indonesia.

Brenner, S. W. (2010). *Cybercrime: criminal threats from cyberspace.* Bloomsburry Publishing USA.

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2015). Cutting the gordian knot: A look under the hood of ransomware attacks. In Detection of Instrusions an Malware, and Vulnerability Assessment: 12th International Conference, DIMVA 2015, Milan, *Italy, July 9-10, 2015, Proceedings 12* (pp.3-24). Springer International Publishing.