MODUS KEJAHATAN CYBER DI E-COMMERCE: STRATEGI, ANCAMAN, DAN CARA MENGHINDARINYA

Yustin Nur Faizah[1], Eklamsia Sakti[2], Moh. Toyyib[3]

[1]Akuntansi, [1]Politeknik NSC Surabaya
[1]faizah.yustin@gmail.com

ABSTRAK

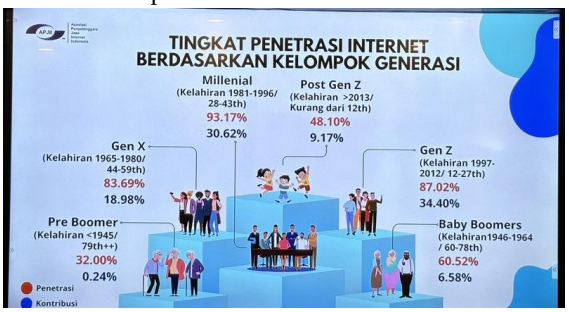
Penelitian ini bertujuan untuk mengungkap modus operandi kejahatan siber (cybercrime) yang terjadi melalui e-commerce. Penelitian ini menggunakan pendekatan kualitatif dengan metodologi fenomenologi untuk memahami berbagai pola perilaku kejahatan dalam transaksi daring. Data diperoleh melalui wawancara dengan pihak-pihak terkait.Hasil penelitian menunjukkan bahwa transaksi online memberikan manfaat bagi penjual dalam memperluas pasar dan membantu konsumen memenuhi kebutuhannya dengan lebih mudah. Namun, berbagai modus kejahatan juga ditemukan dalam ekosistem e-commerce. Beberapa di antaranya meliputi pembuatan akun kloningan untuk memanfaatkan cashback dan poin reward, peretasan akun pengguna, pencurian data kartu kredit saat transaksi, serta pencemaran nama baik produk pesaing dengan tujuan meminta ganti rugi. Kasus-kasus dengan nilai kerugian kecil sering kali tidak dilaporkan ke ranah hukum karena biaya litigasi yang tinggi dibandingkan dengan jumlah kerugian yang dialami.

Kata kunci: *Cybercrime, E-commerce*, Penipuan digital

PENDAHULUAN

Indonesia, dengan populasi sekitar 250 juta jiwa, berada pada posisi yang sangat strategis dalam intensitas transaksi bisnis, baik domestik maupun internasional. Di era globalisasi yang identik dengan kemajuan pesat teknologi dan informasi, fenomena ini meluas ke seluruh penjuru dunia, tanpa memandang status negara maju atau berkembang, termasuk Indonesia. Globalisasi sendiri adalah proses integrasi yang membawa negara-negara ke dalam ruang lingkup dunia secara lebih terbuka dan saling terhubung (Irawan et al., 2020).

Pesatnya perkembangan teknologi informasi telah membawa perubahan signifikan dalam kehidupan manusia, menjadikannya lebih mudah berkat kecanggihan serta efisiensi kinerjanya. Awalnya, teknologi informasi hanya digunakan oleh kalangan tertentu, namun kini hampir seluruh lapisan masyarakat, termasuk instansi pemerintah dan swasta, telah memanfaatkannya. Berikut adalah data pengguna internet di Indonesia pada tahun 2024.



Gambar 1 : Pengguna Internet di Indonesia
Source : Asosiasi Penyelenggara Jasa Internet Indonesia (APJII, 2024)

Instansi swasta atau badan usaha semakin mengandalkan teknologi informasi untuk mengelola berbagai jenis data dan menjalankan transaksi penjualan secara online (e-commerce). Namun, di balik manfaatnya, teknologi informasi juga memiliki dampak negatif yang dapat merugikan banyak pihak. Hal ini disebabkan oleh belum jelasnya regulasi yang mengatur penggunaannya, sehingga membuka peluang bagi kejahatan di dunia telematika (cybercrime)(Leukfeldt et al., 2017).

Cybercrime adalah tindakan melanggar hukum yang dilakukan dengan memanfaatkan teknologi komputer dan internet untuk merugikan individu, organisasi, atau sistem digital (www.lintasberita.com). Cybercrime adalah kejahatan yang dilakukan dengan memanfaatkan teknologi dan jaringan internet di dunia maya(Douglas, T., & Loader, 2000; Tarjo, 2022).

Terkait dengan cybercrime, Tarjo, (2022) mengklasifikasikan cybercrime menjadi dua jenis, yaitu **computer fraud** dan **computer crime**. Beberapa faktor yang menyebabkan terjadinya cybercrime antara lain: akses internet yang tidak terbatas(Oreku & Mtenzi, 2017), kelalaian pengguna dalam menjaga keamanan data(Iqbal et al., 2020), kemudahan dalam melakukan kejahatan dengan risiko yang relatif kecil(Roderic, 2006), serta tidak memerlukan peralatan canggih untuk menjalankannya(Broadhurst, 2006). Para pelaku cybercrime umumnya adalah individu yang cerdas, memiliki rasa ingin tahu yang tinggi, serta fanatik terhadap teknologi komputer. Kejahatan ini semakin marak akibat lemahnya sistem keamanan jaringan serta kurangnya pengawasan dari masyarakat dan penegak hukum(Ibrahim, 2016).

Bentuk-bentuk penyerangan atau kejahatan komputer terhadap suatu sistem dapat bervariasi. Salah satunya adalah **interupsi**(Carlo & Obergfaell, 2024), yaitu gangguan yang menyebabkan sistem tidak dapat beroperasi sebagaimana mestinya. Selain itu, terdapat **intersepsi**, di mana pihak yang tidak berwenang berhasil mengakses aset atau informasi secara ilegal(Omolara Patricia Olaiya et al., 2024). Selain itu, **modifikasi** juga menjadi ancaman, di mana data atau informasi dalam sistem diubah tanpa izin, yang dapat menyebabkan kerusakan atau penyalahgunaan informasi(Marri et al., 2024). Terakhir, ada **pabrikasi**, yaitu tindakan penyisipan objek palsu ke dalam sistem oleh pihak yang tidak berwenang, yang dapat digunakan untuk menipu atau menciptakan informasi yang menyesatkan(Rather et

al., 2025).

Beberapa bentuk lain dari kecurangan komputer meliputi pemalsuan nilai evidentiary data, alterasi (pengubahan) data, sabotase komputer, pengungkapan rahasia perdagangan dan industri, serta akuisisi data secara illegal (Boczko, 2024). Tindakan-tindakan ini dapat merugikan individu maupun organisasi, terutama dalam aspek keamanan informasi dan bisnis. Selain itu, intensi untuk melakukan cybercrime memiliki pengaruh positif terhadap meningkatnya kejahatan siber. Semakin tinggi niat atau motivasi seseorang untuk melakukan kejahatan di dunia maya, semakin besar kemungkinan terjadinya tindakan cybercrime, terutama jika tidak ada sistem pengamanan yang memadai atau penegakan hukum yang efektif (Kassa et al., 2024).

Survei yang dilakukan oleh Kaspersky Lab dan B2B International mengungkapkan bahwa Indonesia termasuk salah satu negara dengan tingkat kejahatan siber yang tinggi, di mana 26 persen konsumennya menjadi target serangan online. Selain itu, survei ini juga menemukan bahwa 48 persen konsumen pernah menjadi sasaran aksi penipuan yang dirancang untuk mencuri informasi sensitif dan data keuangan guna melakukan tindak kriminal. Pada prinsipnya, penipuan online memiliki kesamaan dengan penipuan konvensional. Perbedaannya terletak pada sarana yang digunakan dalam menjalankan aksinya. Jika penipuan konvensional dilakukan secara langsung, penipuan online memanfaatkan sistem elektronik, seperti komputer, internet, dan perangkat telekomunikasi, untuk menipu korban dan memperoleh keuntungan secara illegal (Tarjo, 2022) . Berbagai modus penipuan melalui media online terus berkembang, dengan para pelaku semakin cermat dan terorganisir dalam menjalankan aksinya. Hal ini terlihat dari maraknya pembuatan situs jual beli palsu serta transaksi yang dilakukan menggunakan akun fiktif, yang bertujuan untuk menipu dan merugikan korban.

Berdasarkan pemaparan di atas, penelitian ini mengangkat modus perilaku *cybercrime* yang dilakukan oleh pembeli dan penjual dalam transaksi e-commerce. Penelitian ini berbeda dari penelitian sebelumnya karena fokusnya terletak pada perilaku pelaku dalam menjalankan modus kejahatan di platform e-commerce.

Penelitian ini memberikan beberapa kontribusi penting. Pertama, penelitian ini menghadirkan konsep baru dalam ilmu pengetahuan, khususnya di bidang teknologi investigatif, untuk memahami perilaku *cybercrime* dalam *e-commerce*. Kedua, penelitian ini memberikan contoh nyata berbagai modus kejahatan dalam e-commerce serta keterkaitannya dengan kebijakan hukum, khususnya Undang-Undang No. 19 Tahun 2016 yang mengatur tentang Informasi dan Transaksi Elektronik (ITE).

METODE PENELITIAN

Penelitian ini menggunakan paradigma interpretif dengan pendekatan kualitatif. Melalui pendekatan ini, diharapkan hasil penelitian dapat menghasilkan simpulan yang mendalam dan bernilai, sehingga memberikan informasi yang berkualitas serta relevan. Untuk mencapai tujuan penelitian dan menggali pengalaman serta pemahaman subyek dalam situasi dan kondisi yang mereka alami, peneliti menggunakan metode fenomenologi. Pendekatan ini memungkinkan eksplorasi mendalam terhadap makna pengalaman subyek secara langsung.

Informan dalam penelitian ini adalah individu yang terlibat langsung dalam aktivitas pembelian dan penjualan di e-commerce. Mereka dipilih karena memiliki pengalaman nyata dalam berinteraksi dalam transaksi jual beli melalui platform e-commerce. Untuk menjaga kerahasiaan dan menghormati permintaan mereka, nama informan disamarkan.

No	Nama (disamarkan)	Gender	Usia
1	Dissa	Wanita	25 Tahun
2	Venny	Wanita	17 Tahun
3	Anton	Pria	30 Tahun
4	Rizky	Pria	

Tabel 1 : Data Informan
Source : Data diolah peneliti

Metode pengumpulan data dalam penelitian ini menggunakan teknik wawancara tidak terstruktur. Wawancara dilakukan secara langsung dengan mendatangi restoran X dan mewawancarai tiga informan kunci. Selain itu, komunikasi melalui telepon dan SMS juga digunakan apabila diperlukan untuk memperoleh informasi tambahan atau klarifikasi dalam situasi yang mendesak.

HASIL & PEMBAHASAN

Pengguna Jasa E-Commerce Dalam Transaksi Jual beli

Teknologi informasi dan komunikasi, khususnya internet, kini semakin dimanfaatkan dalam dunia bisnis. Transaksi bisnis telah beralih ke ranah digital, yang dikenal sebagai e-commerce. Kehadiran internet mempermudah proses jual beli dengan memungkinkan pelaku usaha membuka toko daring, sehingga memberikan kemudahan bagi konsumen dalam mengakses produk serta bagi penjual dalam menjangkau pasar yang lebih luas(Vučković et al., 2018).

Kegiatan usaha e-commerce membuka peluang besar bagi para pemuda untuk mengembangkan bisnis mereka, bahkan dengan modal yang terbatas. Berbagai platform digital seperti Bukalapak, Tokopedia, Shopee, Lazada, dan OLX telah menjadi pionir dalam memasarkan produk secara online, mendorong semakin banyak pelaku usaha untuk beralih ke dunia digital. Seperti yang diungkapkan oleh Mbak Veny:

> "*jual beli lewat internet itu lebih enak dan simple tidak harus membuka lapak dan harus punya stand atau toko. Jualanpun bisa dirumah sambal santai-santai, paling nanti kalau beli barang kita butuh ngambil saja*"

Pernyataan di atas menggambarkan bahwa bisnis berbasis internet memberikan dampak positif bagi dunia usaha. Jika sebelumnya menjalankan usaha memerlukan modal besar, kini pemasaran dapat dilakukan secara lebih efektif melalui platform digital. Penjual cukup menampilkan produknya melalui internet, baik melalui aplikasi maupun situs seperti WhatsApp, Facebook, dan lainnya. Dengan jangkauan pasar yang luas, produk pun

lebih cepat terjual. Konsumen hanya perlu memilih barang yang diinginkan dan melakukan pemesanan langsung kepada pemilik lapak. Hal ini sejalan dengan pernyataan Dissa:

> "*saya lebih senang jualan lewat internet karena barang lebih cepat terjual dan pangsa pasar dalam memasarkan mampu menjangkau pasar yang luas baik dalam kota atau luar kota hingga beda pulau*"

Pangsa pasar yang luas membuka peluang besar bagi peningkatan penjualan produk, tidak hanya di dalam kota tetapi juga hingga ke luar daerah. Selain itu, tren belanja online semakin diminati, terutama di kalangan anak muda. Kebiasaan berbelanja secara digital telah berkembang pesat, bahkan hampir semua kebutuhan, baik primer maupun sekunder, kini dapat dipenuhi melalui transaksi online. Seperti yang disampaikan oleh saudara Anton:

> "*keseringan saya itu saat ada di kota membeli kebutuhan atau produk itu lewat online sampai kebiasaan saya sekarang di rumah. Saya tetap membeli kebutuhan biasanya lewat onlie karena ada cashback dan poin yang bisa ditukarkan lagi*"

Transaksi online kini telah menjadi kebiasaan yang meluas, tidak hanya di kalangan pemuda tetapi juga di seluruh elemen masyarakat, mulai dari anak-anak hingga orang dewasa. Kebiasaan ini berkontribusi pada pertumbuhan ekonomi serta mempermudah pelaku usaha dalam mengembangkan bisnisnya secara strategis. Kemudahan fasilitas layanan pembelian online memberikan dampak positif dengan meningkatkan minat konsumen untuk berbelanja. Bagi pengusaha yang membutuhkan barang dalam jumlah besar, pemesanan secara online juga menawarkan keuntungan tambahan, seperti memperoleh poin atau diskon yang signifikan. Seperti yang diungkapkan oleh Kak Risky:

> "*saya biasanya beli barang berupa vocher lewat online dalam jumlah banyak. Biasanya saya dapat ovo point yang nantinya bisa ditukarkan barang lagi tidak usah pakai uang. Kalau dapat cashback kas biasanya ditransfer*"

Pemberian cashback dalam bentuk poin memberikan nilai tambah bagi konsumen, sekaligus menjadi strategi efektif untuk meningkatkan loyalitas pelanggan. Insentif ini mendorong konsumen untuk berbelanja lebih banyak dan lebih sering. Selain itu, transaksi jual beli online telah menjadi faktor strategis dalam pertumbuhan bisnis, dengan minat masyarakat yang terus meningkat. Penggunaan e-commerce dan platform digital dalam dunia usaha terus mengalami peningkatan setiap tahunnya. Tren ini tercermin dalam pertumbuhan grafik permintaan pasar yang terus naik secara signifikan dalam lima tahun terakhir.

Jual beli melalui e-commerce lebih efektif dan efisien, baik dari segi finansial, tenaga kerja, maupun operasional, karena tidak memerlukan gudang besar seperti di toko ritel konvensional. Penyimpanan barang dapat dilakukan di rumah, sehingga lebih praktis dibandingkan dengan membangun fasilitas penyimpanan seperti di Matahari atau Hypermart. Dalam hal pengiriman, berbagai jasa ekspedisi dapat digunakan selama barang sampai ke tujuan dengan aman dan tanpa kerusakan. Jika terjadi kerusakan akibat kelalaian penjual, umumnya barang akan diganti sesuai kebijakan yang berlaku. Namun, jika kesalahan berasal dari konsumen, maka penggantian tidak menjadi tanggung jawab penjual. Ketentuan dan kebijakan dalam transaksi jual beli online biasanya sudah tercantum dengan jelas dan dapat dipercaya, sehingga memberikan rasa aman bagi pembeli maupun penjual.

Modus Cybercrime Dalam Transaksi *E-Commerce*

Perkembangan bisnis melalui platform online atau internet memberikan dampak positif bagi masyarakat. Transaksi jual beli secara daring memberikan manfaat bagi kedua belah pihak, baik konsumen maupun penjual. Masyarakat semakin dimudahkan dengan adanya e-commerce, yang memungkinkan akses ke pasar yang lebih luas, baik di dalam maupun luar kota. Namun, kemajuan ini juga membuka peluang bagi individu yang memiliki niat buruk untuk melakukan kecurangan atau penipuan melalui media online. Berbagai modus dan trik sering digunakan oleh oknum tidak bertanggung jawab demi keuntungan pribadi, sehingga menimbulkan risiko bagi para pengguna e-commerce.

> "*saya kan sering belanja melalui online dan pernah dapat cashback ke "S". Tetapi,saya hampir kena tipu karena ada yang mengaku mau mengirimkan cashback hadiah. Dia meminta alamat email dan password, nomor rekening, password masuk ke aplikasi "S" untuk memproses cashback tersebut dan akhirnya saya kasihkan. Ketika saya tahu kalau dia mengubah password maka saya cepat-cepat menghentikan tindakannya dan akhirnya selamat akun saya*".

Ungkapan di atas menjelaskan bahwa pelaku berupaya meretas akun dan menggunakannya untuk berbelanja online dengan akun milik saudara Anton. Tindakan ini dapat berdampak pada peralihan kepemilikan akun, memungkinkan pelaku untuk secara leluasa memanfaatkan akun Anton dalam menjalankan aksinya. Seperti yang disampaikan oleh Clough, (2015), pencurian identitas perlu ditangani secara khusus dan komprehensif, termasuk dalam ketentuan hukumnya. Selain itu, pelaku juga berusaha meminta nomor rekening korban dengan tujuan menguras seluruh isinya. Namun, beruntungnya, saldo di bank saat itu sudah kosong, sehingga pelaku tidak dapat melancarkan aksinya.

Saudara Anton kemudian memblokir nomor rekeningnya untuk mencegah pelaku meretas kembali saat saldo bank terisi lagi. Kasus serupa juga dialami oleh Mbak Dissa, yang mengalami peretasan rekening bank—tepatnya kartu kreditnya—ketika hendak membayar

produk yang dibelinya. Beliau mengungkapkan kejadian ini sebagai berikut:

> "*saya pesan barang kemudian saya ingin membayar pakai kartu kredit, pada saat saya membayar pakai kartu kredit ada oknum yang tahu nomor rekening saya dan meretasnya sehingga saya kehilangan uang 3jt*".

Peretasan kartu kredit saat berbelanja online semakin marak di masyarakat. Seperti yang disampaikan oleh Tarjo (2021), penipuan kartu kredit menyebabkan kerugian miliaran dolar setiap tahun bagi konsumen dan industri keuangan. Studi ini menggunakan data nyata dari transaksi kartu kredit internasional untuk mengagregasi transaksi dan memperkirakan model penipuan.Pelaku kejahatan siber terus mengembangkan trik dan modus yang semakin canggih, sering kali lebih cepat dibandingkan upaya pengamanan yang dilakukan oleh lembaga keuangan maupun bisnis online. Oleh karena itu, para pelaku bisnis online berupaya meningkatkan sistem keamanan secara ekstra guna melindungi konsumen dari ancaman kejahatan dunia maya, seperti peretasan akun.

Kasus yang dialami Saudara Anton berkaitan dengan peretasan akun miliknya. Berbeda dengan pengalaman Kak Risky, yang justru memanfaatkan pembuatan banyak akun untuk mendapatkan lebih banyak cashback poin demi keuntungan pribadi.Ia sengaja membuat beberapa akun berbeda untuk membeli berbagai kebutuhan, terutama voucher yang kemudian dijual kembali. Jika hanya menggunakan satu akun, poin yang diperoleh akan terbatas, sedangkan akun lama dan akun baru memiliki efek yang berbeda dalam perolehan cashback. Seperti yang diungkapkan oleh Kak Risky berikut ini:

> "*saya membuat akun sebanyak 9, satu hp satu akun sehingga tidak ketahuan bahwa akun itu akun kloningan*."

Pembuatan beberapa akun berbeda terbukti cukup efektif dalam mengumpulkan poin. Modus atau trik ini masih ampuh hingga saat ini untuk menghindari deteksi dan melancarkan aksinya. Salah satu strategi yang digunakan adalah "satu HP, satu akun," karena umumnya dianggap bahwa pemilik perangkat juga merupakan pemilik akun. Celah ini dimanfaatkan untuk berbelanja dalam skala besar menggunakan berbagai akun, sehingga dapat memperoleh cashback poin yang lebih banyak. Selain itu, perbedaan antara akun lama dan akun baru juga berpengaruh signifikan terhadap jumlah poin yang diberikan. Seperti yang disampaikan oleh Kak Risky berikut ini:

> "*akun lama dan akun baru pastinya berbeda dalam pemberian cashback point. Akun lama lebih besar cashbacknya dibandingkan dengan akun baru. Kalau saya gabungkan akun semuanya kira-kira saya memperoleh cashbackpoint sekitar 10jtan*"

Pernyataan ini cukup mengejutkan dan mungkin menggoda sebagian orang untuk mencoba cara serupa dalam berbelanja online. Strategi "satu HP, satu akun" tampaknya masih efektif untuk mengelabui sistem, meskipun pengamanan aplikasi dan kebijakan cashback kini mulai diperketat oleh penyedia layanan.Tak menutup kemungkinan bahwa di masa depan akan muncul metode yang lebih canggih dan semakin sulit dideteksi. Oleh karena itu, sistem keamanan berlapis dan metode pencegahan harus terus dioptimalkan, mengingat kejahatan dunia maya terus berkembang dengan trik dan modus yang semakin beragam.

Perilaku kejahatan dunia maya yang dilakukan dengan berbagai trik dan modus merupakan cerminan dari individu itu sendiri. Tindakan ini menunjukkan adanya moral hazard, di mana seseorang berusaha menguntungkan dirinya sendiri dengan cara yang merugikan pihak lain.Perilaku semacam ini bertentangan dengan etika dan dapat dikategorikan sebagai tindak pidana. Jika konsumen atau penjual mengalami kerugian, mereka berhak mengajukan gugatan dan melaporkan kasus tersebut kepada pihak berwenang untuk diproses lebih lanjut. Dalam dunia bisnis, kejahatan siber umumnya akan ditindak secara hukum apabila kerugian yang ditimbulkan cukup besar dan ada pihak yang dirugikan secara signifikan.

KESIMPULAN

Perkembangan teknologi informasi di era globalisasi semakin pesat, terutama di era milenial. Di Indonesia, jumlah pengguna internet telah mencapai 171.176.716 orang, yang tentu memberikan dampak besar pada berbagai sektor. Salah satu sektor yang paling diuntungkan adalah dunia bisnis, khususnya perdagangan online atau yang lebih dikenal sebagai e-commerce.

Berdasarkan pembahasan di atas, dapat disimpulkan beberapa hal. Pertama, transaksi online memberikan keuntungan bagi penjual dengan memperluas jangkauan pasar, memungkinkan mereka memasarkan produk ke audiens yang lebih luas. Selain itu, e-commerce juga memudahkan konsumen dalam memenuhi kebutuhan mereka dengan lebih praktis dan efisien. Kedua, modus dan trik kejahatan yang dilakukan oleh pelaku sangat beragam. Beberapa di antaranya adalah membuat akun kloningan untuk memperoleh cashback poin dalam jumlah besar, meretas akun pengguna lain, membobol kartu kredit saat proses pembayaran, serta mencatut nama produk orang lain untuk kemudian memberikan ulasan negatif dengan tujuan meminta ganti rugi setengah dari harga pembelian.Ketiga, kasus-kasus dengan nilai kerugian kecil cenderung jarang dilaporkan ke ranah hukum. Hal ini disebabkan oleh pertimbangan biaya litigasi dan proses hukum yang sering kali tidak sebanding dengan nilai kerugian yang dialami.

Penelitian ini mengungkap bahwa modus dan trik dalam kejahatan dunia maya melalui e-commerce semakin berkembang dan kreatif. Banyak pelaku yang menjalankan aksinya dengan cara yang terorganisir dan tampak elegan, sehingga sulit terdeteksi.Sebagai saran untuk penelitian selanjutnya, disarankan untuk merancang konsep

pencegahan dini yang lebih efektif dalam mengatasi kejahatan siber di ranah e-commerce. Selain itu, penelitian mendatang juga dapat memperkaya perspektif dengan menambah informan dari berbagai pihak, seperti aparat penegak hukum, akademisi di bidang hukum dan bisnis, serta kejaksaan, guna mendapatkan pemahaman yang lebih komprehensif mengenai aspek hukum dalam kejahatan dunia maya.

DAFTAR REFERENSI

Boczko, T. (2024). Risk Exposure, Fraud, Cyber Terrorism, and Computer Crime. In *Information Systems in Accounting and Finance* (pp. 425–476). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-48586-2_12

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime Policing. *An International Journal of Police Strategies and Management*, *2*(29), 408–433.

Carlo, A., & Obergfaell, K. (2024). Cyber attacks on critical infrastructures and satellite communications. *International Journal of Critical Infrastructure Protection*, *46*, 100701. https://doi.org/10.1016/j.ijcip.2024.100701

Clough, J. (2015). Towards a common identity? The harmonisation of identity theft laws. *Journal of Financial Crime*, *22*(4), 492–512. https://doi.org/10.1108/JFC-11-2014-0056

Douglas, T., & Loader, B. D. (2000). *Cybercrime: Security and surveillance in the information age*.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Iqbal, F., Debbabi, M., & Fung, B. C. M. (2020). *Cybersecurity And Cybercrime Investigation* (pp. 1–21). https://doi.org/10.1007/978-3-030-61675-5_1

Irawan, A. W., Yusufianto, A., Agustina, D., & Dean, R. (2020). *Laporan Survei Internet Apjii 2019-2020 (Q2)*. *2020*, 15.

Kassa, Y. W., James, J. I., & Belay, E. G. (2024). Cybercrime Intention Recognition: A Systematic Literature Review. *Information*, *15*(5), 263. https://doi.org/10.3390/info15050263

Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research*, *23*(3), 287–300. https://doi.org/10.1007/s10610-016-9332-z

Marri, R., Varanasi, S., Chaitanya, S. V. K., & Marri, S. K. (2024). Strengthening GIS Security: Anonymization and Differential Privacy for Safeguarding Sensitive Geospatial Data. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *4*(1), 338–361. https://doi.org/10.60087/jaigs.v4i1.264

Omolara Patricia Olaiya, Temitayo Oluwadamilola Adesoga, Adefisayo Ojo, Oluwabusola Dorcas Olagunju, Olajumoke Oluwagbemisola Ajayi, & Yusuf Olalekan Adebayo. (2024). Cybersecurity strategies in fintech: safeguarding financial data and assets. *GSC Advanced Research and Reviews*, *20*(1), 050–056. https://doi.org/10.30574/gscarr.2024.20.1.0241

Oreku, G. S., & Mtenzi, F. J. (2017). *Cybercrime: Concerns, Challenges and Opportunities* (pp. 129–153). https://doi.org/10.1007/978-3-319-44257-0_6

Rather, A. H., Haq, I. U., & Walia, N. K. (2025). Privacy and security in the metaverse. In *Leveraging Metaverse and Analytics of Things (AoT) in Medical Systems* (pp. 189–207). Elsevier. https://doi.org/10.1016/B978-0-443-24049-2.00002-9

Roderic, G. et al. (2006). *Cyber-crime: The Challenge in Asia*.

Tarjo, S. E. , et al. (2022). *Akuntansi Forensik dalam Referensi Analisis Transaksi Fraud Keuangan.* Jakad Media Publishing.

Vučković, Z., Vukmirović, D., Milenković, M. J., Ristić, S., & Prljić, K. (2018). Analyzing of e-commerce user behavior to detect identity theft. *Physica A: Statistical Mechanics and Its Applications*, *511*, 331–335. https://doi.org/10.1016/j.physa.2018.07.059