

Peluang Kejahatan Dalam Pemanfaatan *E-Business*

Muhammad Dimas Aldy¹, Rika Wulandari², Mesi Suharni Banurea³, Nurbaiti⁴

^{1,2,3,4} Universitas Islam Negeri Sumatera Utara

Email : mdimasaldy04@gmail.com¹, wldrrika@gmail.com², mesisuharni13@gmail.com³

Abstract. Opportunities for crime in the digital business world include various forms of threats, such as system hacking, theft of personal data, financial fraud, and other criminal acts that can harm companies and damage consumer trust. Digital business is a business activity that in its implementation utilizes technology as a medium, either when creating or in a series of marketing activities. In an effort to deal with opportunities for crime in the world of e-business, companies must prioritize information security, strict policy implementation, education and training for employees, as well as partnerships with security and government agencies. This research uses a qualitative literature study method by obtaining secondary data through published journal articles with the question "Are there many opportunities for crime in the utilization or use of e-business?". Based on this, it is clear that there are still many opportunities for crime in the digital business world and continue to occur, where the crimes that often occur are fraud, hacking, as well as cybercrime and cyberfraud.

Keywords: E-Business, Fraud, Hacking, Crime, and E-Commerce.

Abstrak. Peluang kejahatan dalam dunia bisnis digital mencakup berbagai bentuk ancaman, seperti peretasan sistem, pencurian data pribadi, penipuan keuangan, dan tindakan kriminal lainnya yang dapat merugikan perusahaan dan merusak kepercayaan konsumen. Bisnis digital ialah kegiatan usaha yang dalam pelaksanaannya memanfaatkan teknologi sebagai media, baik saat menciptakan ataupun serangkaian kegiatan pemasarannya. Dalam upaya menghadapi peluang kejahatan di dalam dunia e-business, perusahaan harus memprioritaskan keamanan informasi, implementasi kebijakan yang ketat, pendidikan dan pelatihan bagi karyawan, serta kemitraan dengan lembaga keamanan dan pemerintah. Dalam penelitian ini menggunakan metode kualitatif studi pustaka dengan pemerolehan data sekunder melalui artikel jurnal yang telah terbit dengan mengusung pertanyaan "Apakah peluang kejahatan dalam pemanfaatan atau penggunaan e-business begitu banyak?". Berangkat dari hal tersebut, terjawab bahwasanya peluang kejahatan dalam dunia bisnis digital masih banyak dan terus berlangsung di mana kejahatan yang sering terjadi ialah penipuan, peretasan, serta cybercrime dan cyberfraud.

Kata Kunci: E-Business, Penipuan, Hacking, Kejahatan, dan E-Commerce.

PENDAHULUAN

Dalam era digital yang serba terhubung, *e-business* atau bisnis elektronik telah menjadi landasan ekonomi global. Namun, dengan kemajuan teknologi juga muncul tantangan baru, termasuk peluang kejahatan yang mengancam keamanan dan integritas operasi *e-business*. Kejahatan siber telah menjadi ancaman serius bagi perusahaan dan konsumen di dunia *e-business*, mengingat semakin canggihnya metode yang digunakan oleh para pelaku kejahatan.

Peluang kejahatan dalam dunia *e-business* mencakup berbagai bentuk ancaman, seperti peretasan sistem, pencurian data pribadi, penipuan keuangan, dan tindakan kriminal lainnya yang dapat merugikan perusahaan dan merusak kepercayaan konsumen. Oleh karena itu, diperlukan strategi yang terencana dan efektif untuk mengatasi potensi kejahatan ini dan menjaga keamanan serta kepercayaan dalam ekosistem *e-business*.

Strategi yang efektif harus mencakup pendekatan yang holistik, meliputi penerapan teknologi keamanan terbaru, pengembangan kebijakan yang kuat, pendidikan karyawan, dan kerjasama erat dengan pihak-pihak terkait seperti penegak hukum dan lembaga keamanan siber. Dalam upaya menghadapi peluang kejahatan di dalam dunia *e-business*, perusahaan harus memprioritaskan keamanan informasi, implementasi kebijakan yang ketat, pendidikan dan pelatihan bagi karyawan, serta kemitraan dengan lembaga keamanan dan pemerintah. Selain itu, inovasi teknologi dan pemantauan terus-menerus terhadap tren keamanan siber juga menjadi kunci dalam menjaga daya saing dan integritas *e-business*. Dengan menerapkan strategi yang tepat, perusahaan *e-business* dapat memitigasi risiko kejahatan siber, melindungi aset mereka, dan menjaga integritas dan kepercayaan konsumen. Dalam tulisan ini, akan dibahas berbagai strategi yang dapat membantu perusahaan *e-business* mengatasi peluang kejahatan dan membangun fondasi yang kokoh untuk kelangsungan bisnis yang aman dan berkelanjutan dalam dunia *e-business* yang terus berkembang.

TINJAUAN TEORITIS

Teori Kesempatan (*Opportunity Theory*)

Teori ini memandang bahwa kejahatan terjadi ketika terdapat adanya peluang yang memungkinkan seseorang untuk melakukan tindakan kriminal. Dalam konteks *e-business*, peluang kejahatan muncul karena kerentanan dalam sistem, kurangnya perlindungan keamanan, serta celah teknis yang dimanfaatkan oleh pelaku kejahatan.

Teori Teknologi Sosial (*Social Technology Theory*)

Teori ini menyoroti interaksi antara teknologi, individu, dan masyarakat. Dalam pemanfaatan *e-business*, teknologi menjadi alat yang mempengaruhi perilaku sosial, termasuk perilaku kriminal. Hal ini bisa terjadi karena teknologi membentuk norma baru, memungkinkan keberadaan komunitas kejahatan online, atau mengubah dinamika interaksi sosial yang bisa dimanfaatkan untuk tujuan kejahatan.

Teori Penegakan Hukum Elektronik (*Electronic Law Enforcement Theory*)

Teori ini menekankan pentingnya penegakan hukum dalam lingkungan online. Dalam konteks *e-business*, keberadaan undang-undang dan penegakan hukum yang efektif diperlukan untuk mencegah dan menindak tindak kriminal di ruang digital. Upaya penegakan hukum yang tanggap terhadap kejahatan online dapat menjadi salah satu cara untuk memitigasi peluang kejahatan dalam *e-business*.

Teori Perilaku Kriminal (*Criminal Behavior Theory*)

Teori ini mencakup motivasi individu dalam melakukan tindakan kriminal. Dalam *e-business*, faktor-faktor seperti keuntungan finansial, kecenderungan terhadap risiko, dan ketidaktahuan atau ketidaksadaran terhadap hukum dan etika dapat mendorong seseorang untuk melakukan kejahatan dalam lingkungan digital.

Teori Kesesuaian (*Suitability Theory*)

Teori ini menekankan pada sejauh mana individu atau kelompok merasa tindakan kriminal sesuai dengan nilai-nilai, norma, dan kemampuan mereka. Dalam konteks *e-business*, perkembangan teknologi mungkin mengubah pandangan individu terhadap apa yang dianggap dapat diterima atau sesuai dalam ruang digital, yang bisa mempengaruhi perilaku kriminal.

Teori Ketidaksetaraan Dan Keadilan (*Inequality and Justice Theory*)

Menyoroti dampak ketidaksetaraan ekonomi dan keadilan terhadap perilaku kriminal. Dalam pemanfaatan *e-business*, akses terbatas atau kesenjangan digital bisa menjadi pemicu tindakan kriminal karena ketidakadilan dalam akses dan kesempatan.

Teori Keamanan Informasi (*Information Security Theory*)

Fokus pada upaya untuk melindungi informasi dari akses yang tidak sah. Dalam *e-business*, kekurangan keamanan informasi atau perlindungan data dapat membuka peluang bagi peretasan, pencurian data, atau serangan siber. Masing-masing teori tersebut memberikan pemahaman yang berbeda terkait dengan peluang kejahatan dalam pemanfaatan *e-business*. Kombinasi dari perspektif-perspektif ini dapat membantu dalam memahami, menganalisis, dan merancang strategi pencegahan yang lebih efektif terhadap kejahatan dalam lingkup *e-business*.

METODE PENELITIAN

Guna mengetahui banyaknya peluang kejahatan dalam pemanfaatan atau penggunaan bisnis secara digital, peneliti bermaksud menggunakan metode kualitatif studi pustaka dengan pemerolehan data sekunder melalui artikel jurnal yang telah terbit dan ditulis oleh beberapa peneliti lainnya sebelum ini.

Metode penelitian kualitatif adalah pendekatan atau penelusuran untuk mengeksplorasi dan memahami suatu gejala sentral yang memperlakukan partisipan benar-benar sebagai subjek dan bukan objek. Dengan artian, partisipan berhak mengutarakan pendapat atau pikirannya tanpa batasan. Adapun penelitian kualitatif studi pustaka merupakan penelitian

yang menggunakan sumber data berupa buku, penelitian, dan dokumen-dokumen terpercaya yang dapat dipertanggungjawabkan serta sesuai dengan kebutuhan penelitian.

Data sekunder juga merupakan bagian dari penelitian ini, di mana maksud dari data sekunder ialah data yang diperoleh dari sumber-sumber yang sudah ada sebelumnya. Data sekunder bisa berupa hasil survei, laporan, publikasi ilmiah, data historis, dokumen perusahaan, dokumen pemerintah, situs web, buku, dan sebagainya yang digunakan sebagai pelengkap kebutuhan data penelitian atau untuk mendapatkan pemahaman yang lebih dalam tentang suatu topik.

HASIL PENELITIAN

Dalam hal ini, peneliti menggunakan 10 artikel jurnal terdahulu sebagai rujukan bahan penelitian untuk menjawab pertanyaan “Apakah peluang kejahatan dalam pemanfaatan atau penggunaan *e-business* begitu banyak?” dengan pemerolehan sebagai berikut.

1. Pada artikel “*Era Fintech: Peluang Dan Tantangan Bagi Ekonomi Syariah*” oleh Rokhmat Subagiyo yang terbit pada Desember 2019 di Jurnal Ekonomi Islam, kejahatan dalam dunia perbankan (dalam hal ini bank digital) yang sering dijumpai adalah pencurian identitas atau phising oleh pengguna untuk mengambil data-data perusahaan tanpa izin, penipuan berkedok bisnis *online*, dan sebagainya.
2. Pada artikel “*Pajak E-Commerce, Pemecahan dan Solusinya*” oleh Ajat Sudrajat yang terbit pada September 2020 di Jurnal Pajak Vokasi dinyatakan bahwa keberadaan *e-commerce* (dalam hal ini bisnis digital) saat ini begitu rentan dari masalah kejahatan pembobolan, *hacking*, atau *cracking* dengan mengubah atau mengganti data tertentu dengan data palsu.
3. *Cybercrime* (kejahatan pada jaringan internet) yang tentunya memengaruhi bisnis digital yang dinyatakan pada artikel “*Cyber Crime Awareness: Internet Knowledge dan E-Commerce Use pada UMKM di Kabupaten Bantul Yogyakarta*” oleh Tri Siwi Nugrahani, Faizal Ardiyanto, dan Sulkhanul Umam pada September 2019 ialah berupa penyebaran virus dan software yang bersifat merusak, peretasan, dan serangan *distributed denial of service*.
4. Adapun dalam hal uang elektronik, artikel “*Tantangan dan Peluang Kebijakan Non-Tunai: Sebuah Studi Literatur*” oleh Izzani Ulfi menunjukkan bahwa risiko keamanan yang potensial ialah penggandaan alat, duplikasi pada perangkat lunak/data, pencurian, penyalahgunaan transaksi hingga risiko malfungsi atau data yang hilang.

5. Pada artikel “*Perkembangan dan Transformasi Teknologi Digital*” oleh Muhamad Danuri pada September 2019, kejahatan yang diisukan beredar dalam pemanfaatan bisnis digital ialah pemanfaatan dan pengarahannya serangan ke *database* sebagai pilihan utama untuk menguasai semua akses seseorang.
6. Pada artikel “*Industri E-Commerce dalam Menciptakan Pasar yang Kompetitif Berdasarkan Hukum Persaingan Usaha*” oleh Melisa Setiawan Hotana, kejahatan pada suatu bisnis digital yang diisukan ialah penipuan, yang mana tidak hanya dilakukan oleh penjual melainkan juga pembeli yang bisa dilakukan dengan penipuan transaksi/pembayaran.
7. Pada artikel “*Kajian Etika Bisnis dalam Praktik Bisnis Online di Indonesia Melalui Studi Kasus dari Perspektif Penjual, Pembeli, dan Penyedia Layanan Online Marketplace*” oleh Anggi Triantoro menyampaikan adanya tiga isu kejahatan, di antaranya:
 - a. Seorang penjual melakukan duplikasi terhadap suatu akun Instagram dan bermaksud menipu dengan cara mengaku sebagai penjual yang sesungguhnya dengan menggunakan akun Instagram yang telah diduplikasi. Dari kejahatan ini, ada pembeli yang tertipu karena sudah mengirimkan uang ke pelaku tanpa menyadari bahwa toko *online* tersebut adalah palsu, begitupun dengan penjual asli yang dirugikan karena kehilangan kepercayaan *customer* dan kehilangan pelanggan.
 - b. Seorang pembeli yang menipu dengan membeli barang dan pembayaran dilakukan hanya dengan mengirimkan bukti transfer yang *notabene* palsu dan mengaku bahwa telah mengirimkan uang sesuai dengan nominal yang tertera pada bukti transfer tersebut.
 - c. Kejahatan terjadi pada acara yang dimanfaatkan oleh beberapa oknum dengan mendesain sistem agar hanya “mereka” saja yang bisa dengan mudah masuk ke dalam acara dan mempersulit akses pembeli lain untuk berpartisipasi. Dalam hal ini, seolah-olah konsumen hanya mengetahui bahwa acara sulit diakses karena *traffic* pengunjung yang sangat padat padahal hanya oknum tertentu saja yang bisa mengaksesnya.
8. Pada artikel “*Pemakaian E-Commerce untuk Usaha Kecil dan Menengah Guna Meningkatkan Daya Saing*” oleh Julisar dan Eka Miranda disampaikan bahwa kejahatan yang hampir menjadi tren dalam bisnis digital ialah pengeksposan data pribadi, pemalsuan identitas, pemalsuan data, serta penyadapan data di dunia maya, baik itu data pribadi maupun perusahaan.

9. Dalam artikel “*Analisis Kendala Pemanfaatan E-Commerce dalam Pengembangan Produktivitas Usaha Perbelanjaan*” oleh Munaldi dan Tias Tia Mutiara dinyatakan bahwa UNCTAD memberikan laporan di mana sebuah survei pada 2013 silam menginformasikan bahwa sebagian besar pengguna internet takut melakukan transaksi *online* baik dalam bisnis digital ataupun tidak karena khawatir adanya penipuan.
10. Adapun dalam artikel “*Pengaruh Media Sosial Facebook terhadap Perkembangan E-Commerce di Indonesia*” oleh Sarif Hidayat pada November 2017 di Jurnal Simetris dinyatakan bahwa *e-commerce* dan bisnis digital mengalami hambatan berupa kejahatan siber seperti *hacker*, *carding*, *cracker* dan *cyberfraud* dalam pemanfaatan atau penggunaannya.

PEMBAHASAN

Dari hasil yang diperoleh dan tertera di atas, dapat diketahui bahwa masih banyak kejahatan yang terjadi dalam dunia bisnis yang dilakukan secara digital ini. Bisnis digital ialah kegiatan usaha yang dalam pelaksanaannya memanfaatkan teknologi sebagai media, baik saat menciptakan ataupun serangkaian kegiatan pemasarannya. Bisnis digital meliputi penyediaan barang dan jasa atau jual-beli yang dilakukan secara *online*. Di mana, antara penjual dan pembeli bisa terhubung hanya dengan melewati jaringan tanpa usaha yang lebih untuk hadir ke toko secara langsung.

Bisnis digital sendiri memiliki beragam jenis, seperti *online shop* atau *e-commerce* (toko elektronik), mengonversi barang fisik menjadi digital seperti *e-book*, jurnal, ataupun penyedia jasa secara daring lainnya. Bisnis digital juga memiliki kelebihan dan kekurangan apabila digunakan, di antaranya sebagai berikut:

A. Kelebihan

1. Kebutuhan modal yang dibutuhkan kecil karena tidak terpakai untuk memproduksi barang, menyewa tempat operasional, dan lain sebagainya.
2. Jangkauan pasar lebih luas dan berpotensi mendapatkan banyak pelanggan tanpa adanya batasan wilayah hingga ke luar negeri.
3. Dapat terus beroperasi selama 24 jam yang memungkinkan konsumen mengunjungi dan membeli produk lewat digital tanpa dibatasi waktu.
4. Promosi lebih tertata dan terukur karena bisa dilakukan melalui media sosial.
5. Mudah terhubung dengan pelanggan yang memungkinkan meningkatkan penjualan dengan pengembangan bisnis berdasarkan umpan balik dari pelanggan.

6. Banyak pilihan platform untuk mulai berbisnis, di mana diketahui bahwa bisnis digital bisa dilakukan di mana saja dan melalui apa saja,

B. Kekurangan Bisnis Digital

1. Terdapat kendala teknis pada platform seperti *website* yang *down* atau tidak bisa diakses.
2. Persaingan bisnis berlaku secara ketat karena siapa saja bisa memulai bisnis digital, bahkan tanpa modal sedikitpun.
3. Dalam pelaksanaannya mengharuskan penjual siap sedia untuk menanggapi keluhan dan pertanyaan pelanggan secepat mungkin.
4. Pengiriman atau kedatangan produk bisa terlambat.

Pertanyaan “Apakah peluang kejahatan dalam pemanfaatan atau penggunaan *e-business* begitu banyak?” terjawab dengan banyaknya tindakan penipuan, pencurian data, pemalsuan identitas, dan lain sebagainya yang merugikan, baik bagi penjual ataupun pembeli.

Dalam penemuan kasus pertama yang dikutip dari artikel jurnal “*Era Fintech: Peluang Dan Tantangan Bagi Ekonomi Syariah*” oleh Rokhmat Subagiyo yang terbit pada Desember 2019 di Jurnal Ekonomi Islam, kejahatan yang ditemukan ialah pencurian identitas atau phising dalam sebuah toko elektronik. Di mana, phising adalah pencurian data penting yang dimiliki orang lain, seperti nama lengkap, alamat tempat tinggal, dan nomor telepon untuk membobol akun nasabah yang ditanggungjawab oleh pengguna (*user*). Selain itu, pada penemuan kedua di artikel “*Pajak E-Commerce, Pemecahan dan Solusinya*” oleh Ajat Sudrajat yang terbit pada September 2020 di Jurnal Pajak Vokasi, dinyatakan bahwa tindak kejahatan pada bisnis digital bisa berupa hacking dan cracking pada sebuah data. Di mana, perilaku *hacking* yang biasa mengganggu kenyamanan dan keamanan suatu individu atau perusahaan yang sempat mempersulit penanganan hukum dan pajak karena penggantian data tertentu yang dimaksud dengan data palsu. Hal ini juga harus mendapat perhatian lebih dari pemerintah selaku penyelenggara birokrasi bagi segala tindak kejahatan di Internet.

Kemudian, penemuan lainnya menyatakan bahwa kejahatan bisnis digital lainnya ialah penyebaran virus dan *software* yang bersifat merusak sistem hingga pemberlakuan peretasan. Pertumbuhan teknologi informasi yang bagaikan pisau—memiliki dua sisi tajam ini memang mempermudah pengguna untuk menyelesaikan pekerjaan, tetapi hal ini telah membuat sistem menjadi rentan terhadap serangan atau kejahatan seperti fraud, hacking, pornografi, perdagangan anak, perdagangan hak intelektual, pencurian identitas, pelanggaran privasi, dan

sebagainya. Berdasarkan pendapat yang dikemukakan Furnell & Dowling, terdapat dua kategori umum tentang kejahatan dunia maya yaitu:

1. **Cyber-dependent Crimes** berupa serangan-serangan kejahatan internet yang diterima melalui komputer, jaringan komputer, dan bentuk lain dari teknologi informasi dan komunikasi. Sebagai contoh tindakan ini adalah penyebaran virus dan software yang bersifat merusak, peretasan, dan serangan *distributed denial of service*.
2. **Cyber-enabled Crimes** digolongkan kepada kejahatan tradisional tetapi sudah memasuki skala yang meningkat yakni dapat dijangkau dengan komputer, jaringan komputer, atau teknologi informasi, dan komunikasi lainnya. Akan tetapi, kejahatan yang dimaksud dilakukan tanpa menggunakan teknologi informasi dan komunikasi seperti fraud (phishing dan scams), pencurian, dan pelecehan seksual terhadap anak.

Pada kasus lain, kejahatan yang berpotensi berlaku pada bisnis digital ialah pada uang elektronik, dalam hal ini disebut juga dengan *potential security risk* berupa penggandaan alat, duplikasi pada perangkat lunak/data, pencurian, penyalahgunaan transaksi, hingga risiko malfungsi atau data yang hilang. Pada posisi ini, langkah-langkah keamanan bertujuan untuk memastikan ketiadaan ancaman kejahatan serta memberikan peringatan pada pengguna apabila ada indikasi penyalahgunaan. Adapula contoh kejahatan pada bisnis digital lain, penipuan misalnya. Salah satu kejahatan ini biasa terjadi pada proses transaksi pembelian secara daring melalui internet. Perlu diketahui bahwa penipuan tidak hanya bisa dilakukan oleh pelaku usaha, tetapi seorang konsumen pun juga dapat melakukan penipuan. Pada kasus ini menyebut seorang konsumen yang melakukan transfer sejumlah uang dan meminta produk dikirim. Namun, pelaku usaha yang tidak teliti tersebut langsung mengirimkan produk pada konsumen tanpa menerima pembayaran.

Kita ambil contoh lain dari penipuan, kali ini dilakukan oleh penjual. Di mana, sang penjual melakukan duplikasi produk terhadap akun Instagram yang merupakan usaha penjual lain. Ia bermaksud menipu dengan mengaku-ngaku sebagai penjual asli dengan menggunakan akun Instagram yang telah diduplikasi (memiliki kemiripan). Hingga pada akhirnya ada pembeli yang tertipu karena sempat mengirimkan uang ke sang penipu tanpa menyadari bahwa toko tersebut adalah palsu. Dalam kasus ini, yang dirugikan tidak hanya pembeli, melainkan penjual asli yang nama baiknya harus tercoreng dan berkemungkinan mengalami penurunan penjualan karena para pembeli yang mengira toko miliknya adalah penipu.

Berbagai contoh kasus di atas dianggap sebagai fraud (kejahatan) dalam pemanfaatan *e-business* atau bisnis digital. Pengeksposan data pribadi, pemalsuan identitas, pemalsuan data, penyadapan data, peretasan, serta penipuan di masa sekarang ini mengalami peningkatan secara

terus-menerus. Tingginya angka kejahatan di Indonesia didukung oleh data tahun 2012, di mana terdapat 39 juta serangan siber di Indonesia dan hampir seperempat computer terkena serangan *malware* hinggamenempati urutan ke-14 untuk kejahatan dunia maya.

Untuk mengatasi beberapa permasalahan di atas, dibutuhkan solusi yang mumpuni agar kejahatan-kejahatan terhadap bisnis digital setidaknya berkurang dalam merugikan penjual ataupun masyarakat. Terdapat beberapa cara yang dapat ditawarkan sebagai berikut.

1. Melindungi seluruh perangkat digital dengan memasang proteksi terhadap seluruh perangkat digital yang digunakan oleh perusahaan dengan menggunakan aplikasi atau software yang memiliki fitur antivirus seperti firewall, antispysware, antimalware, dan sejenisnya.
2. Memasang *Secure Socket Layer* (SSL) pada website perusahaan. SSL merupakan pengaman pertukaran data yang terjadi antara pengguna dengan website perusahaan melalui jaringan internet yang ditandai dengan “HTTPS” di bagian awal alamat domainnya.
3. Menerapkan autentifikasi dua faktor (2FA) untuk akses ke *website* guna mencegah seseorang mendapatkan akses secara ilegal. Jadi, ketika seorang berusaha melakukan *hacking*, mereka harus melewati pertahanan autentifikasi berikutnya untuk mengonfirmasi apakah yang masuk tersebut benar memiliki akses atau tidak.
4. Melakukan pencadangan data untuk melindungi dan memudahkan pemulihan data yang hilang atau dicuri apabila terkena serangan digital.
5. Selalu memperbarui keamanan perangkat lunak menutup celah keamanan dari peretasan yang terdapat pada perangkat.
6. Tidak lupa mengedukasi pengguna yang diamanahkan dari perusahaan agar selalu berhati-hati sebelum melakukan tindakan yang dapat merugikan perusahaan, seperti mengklik email spam yang berasal dari sumber yang tidak jelas, dan berbagai hal lainnya.
7. Tidak menggunakan software bajakan yang biasanya ditanami banyak malware (virus) yang akan menimbulkan masalah pada perangkat.

KESIMPULAN

Bisnis digital ialah kegiatan usaha yang dalam pelaksanaannya memanfaatkan teknologi sebagai media, baik saat menciptakan ataupun serangkaian kegiatan pemasarannya. Dalam upaya menghadapi peluang kejahatan di dalam dunia *e-business*, perusahaan harus

memprioritaskan keamanan informasi, implementasi kebijakan yang ketat, pendidikan dan pelatihan bagi karyawan, serta kemitraan dengan lembaga keamanan dan pemerintah. Dalam penelitian ini, pertanyaan “Apakah peluang kejahatan dalam pemanfaatan atau penggunaan *e-business* begitu banyak?” terjawab bahwasanya peluang kejahatan dalam dunia bisnis digital masih banyak dan terus berlangsung. Dalam hal ini, kejahatan yang sering terjadi ialah penipuan, peretasan, serta *cybercrime* dan *cyberfraud*. Untuk mencegah hal tersebut, dapat dilakukan beberapa hal pencegahan seperti memasang proteksi terhadap seluruh perangkat digital perusahaan, memasang *Secure Socket Layer* (SSL) pada *website* perusahaan, menerapkan autentifikasi dua faktor, melakukan pencadangan data secara berkala, rutin memperbarui keamanan perangkat lunak, mengedukasi pengguna agar selalu berhati-hai, serta tidak menggunakan *software* bajakan yang biasanya ditanami banyak virus.

DAFTAR PUSTAKA

- Subagiyo, Rokhmat. “Era Fintech: Peluang Dan Tantangan Bagi Ekonomi Syariah”. *Jurnal Ekonomi Islam*: Vol. 7 No. 2 (2019).
- Sudrajat, Ajat. “Pajak E-Commerce, Pemecahan dan Solusinya”. *Jurnal Pajak Vokasi*: Vol. 2 No. 1 (2020).
- Nugrahani, Tri Siwi, Faizal Ardiyanto, dkk. “Cyber Crime Awareness: Internet Knowledge dan E-Commerce Use pada UMKM di Kabupaten Bantul Yogyakarta”. *Manajemen Dewantara*: Vol. 3 No.2 (2019).
- Ulfi, Izzani. “Tantangan dan Peluang Kebijakan Non-Tunai: Sebuah Studi Literatur” *Jurnal Ilmiah Ekonomi Bisnis*: Vol. 25 No. 1 (2020).
- Danuri, Muhamad. “Perkembangan dan Transformasi Teknologi Digital”. *INFOKAM*: Nomor II Th. XV (2019).
- Hotana, Melisa Setiawan. “Industri E-Commerce dalam Menciptakan Pasar yang Kompetitif Berdasarkan Hukum Persaingan Usaha”. *Volume 1 No. 1* (2018).
- Triantoro, Anggi.. “Kajian Etika Bisnis dalam Praktik Bisnis Online di Indonesia Melalui Studi Kasus dari Perspektif Penjual, Pembeli, dan Penyedia Layanan Online Marketplace” *Institut Pertanian Bogor*: 2018.
- Julisar dan Eka Miranda. “Pemakaian E-Commerce untuk Usaha Kecil dan Menengah Guna Meningkatkan Daya Saing” *ComTech*: Vol.4 No. 2 (2013).
- Munaldi dan Tyas Tia Mutiara. “Analisis Kendala Pemanfaatan E-Commerce dalam Pengembangan Produktivitas Usaha Perbelanjaan” *Jurnal MANEKIN*: Vol. 1 No. 2 (2022).
- Hidayat, Sarif. “Pengaruh Media Sosial Facebook terhadap Perkembangan E-Commerce di Indonesia”. *Jurnal SIMETRIS*, Vol. 8 No. 2 (2017).