Blantika : Multidisciplinary Jornal
Volume 2 Number 1, February, 2023
p- ISSN xxxx-xxxx e-ISSN 2985-4199

ANALISIS KEJHATAN CARDING PADA BNI 46

Zulkarnain[1], Tata Sutabri[2]
Fakultas Ilmu Komputer Pasca Sarjana, Universitas Bina Darma Palembang, Indonesia[12]
E-mail: zul1444h@gmail.com[1], tatasutabri@binadarma.ac.id[2]

INFO ARTIKEL
Diterima: 15 Februari 2023
Direvisi: 20 Februari 2023
Disetujui: 25 Februari 2023

ABSTRAK

Saat ini, hampir semua proses bisnis perusahaan kecil maupun besar tidak lepas dari peran sistem informasi, baik melalui jaringan kabel maupun nirkabel. Pengguna sistem informasi dan teknologi digital biasanya hanya memiliki pengetahuan dasar tentang cara kerja teknologi tersebut. Di sisi lain, sedikit yang tahu bagaimana melindungi sistem dan teknologi informasi, sehingga peretas memiliki banyak peluang untuk mengeksploitasi celah tersebut untuk kepentingan pribadi atau kelompok tertentu.
Perbankan (*e-banking*) dan perdagangan elektronik (*e-commerce*). Dengan berkembangnya kebutuhan akan alat pembayaran yang lebih efisien, mudah digunakan dan nyaman, masyarakat mulai menggunakan kartu kredit dan uang elektronik untuk bertransaksi. Jumlah nasabah yang menggunakan kartu kredit juga semakin meningkat setiap tahunnya. Dan banyak terjadi kejahatan *Carding* yang merupakan bagian dari *cybercrime* dalam transaksi perbankan dengan menggunakan layanan internet sebagai dasar transaksi pembayaran, khususnya sistem layanan perbankan online (*online banking*). *Card skimming* dilakukan oleh pelaku kejahatan (*carder*) secara ilegal memperoleh informasi kartu kredit dengan menggunakan teknologi informasi (*Internet*) menggunakan nomor kartu kredit orang lain untuk memesan barang secara online. Komunikasi awalnya dilakukan melalui e-mail untuk menanyakan tentang status barang dan untuk melakukan bisnis. Setelah menyelesaikan kontrak, pelaku memberikan nomor kartu kreditnya dan penjual mengirimkan barangnya. Tentu saja pemegang kartu kredit asli tidak tahu apa-apa tentang ini.

Kata Kunci: Kejahatan Carding; Perbankan; Carder; Internet; Kartu Kredit

ABSTRACT

Currently, almost all business processes of small and large companies are inseparable from the role of information systems, both via wired and wireless networks. Users of information systems and digital technology usually only have basic knowledge of how the technology works. On the other hand, few know how to protect information systems and technology, so hackers have many opportunities to exploit these loopholes for personal or certain group interests.

Banking (e-banking) and electronic commerce (e-commerce). With the growing need for payment instruments that are more efficient, easy to use and comfortable, people are starting to use credit cards and electronic money for transactions. The number of customers using credit cards is also increasing every year. And there are many Carding crimes which are part of cybercrime in banking transactions using internet services as the basis for payment transactions, especially online banking service systems (online banking). Card skimming is carried out by criminals (carders) illegally obtaining credit card information using information technology (Internet) using other people's credit card numbers to order goods online. Communication was initially done via e-mail to inquire about the status of goods and to conduct business. After completing the contract, the writer provides his credit card number and the seller ships the item. Of course the original credit card holder knows nothing about this.

Keyword; Carding Crime; Banking; Carder; Internet; Credit Card

PENDAHULUAN

Cybercrime adalah bentuk kejahatan yang muncul melalui penggunaan teknologi internet (Abidin, 2017). Melalui Internet atau dunia maya aspek positif dari dunia maya ini tentunya mendorong perkembangan teknologi dunia, terutama segala kreativitas dan kegiatan lain dalam ilmu pengetahuan (Syauqi, 2016). Namun, efek negatif tidak dapat dihindari. Dengan berkembangnya teknologi internet, lahirlah kejahatan yang disebut kejahatan dunia maya atau *cybercrime*. Ada beberapa kasus kejahatan dunia maya di Indonesia, seperti pencemaran nama baik atau tindakan tidak pantas yang dibagikan di media sosial, pencurian kartu kredit, peretasan beberapa situs web, meneruskan informasi orang lain seperti email dan memanipulasi data dengan meletakkan perintah yang tidak diinginkan di komputer pengembang (Indarta et al., 2022). Serangan peretasan biasanya bertujuan untuk mendapatkan informasi spesifik tentang target (Putri, Aditya, Musthofa, & Widodo, 2022). Namun ada juga hacker yang tujuannya menghancurkan data atau sistem tertentu sedemikian rupa sehingga efeknya seperti kerusakan digital (Bernoza, Fadlan, & Nurkhotijah, 2020). Didalam peraturan tersebut juga menyebutkan bahwa

kasus kejahatan dunia maya terkait dengan pengumpulan data atau sistem elektronik. Pembobolan ATM yang kerap menimpa korban kejahatan dunia maya bisa dikatakan meretas data dan mencuri uang milik korban (Ibrahim, 2018).

Kasus pembobolan kartu kredit sejak Januari 2020 yang dialami seorang perempuan berinisial LHJ (54) warga Gajahan, Colomadu, Karanganyar, makin membuat korban menderita. Selain tidak menggunakan kartu kreditnya, LHJ kerap ditagih untuk membayar tunggakan kartu kredit BNI 46 baik melalui surat resmi, dihubungi via telepon, didatangi debt colector (DC) hingga disomasi oleh kuasa hukum Bank BNI 46 untuk melunasi semua kewajibannya.

Kasus ini bermula, saat LHJ menerima tagihan penggunaan kartu kredit melalui pesan email mencapai Rp 134 Juta. LHJ sendiri memiliki empat kartu kredit. LHJ menduga ada orang yang telah membobol keempat kartu kredit miliknya untuk membeli barang-barang di toko online. Dia mengaku, telah mengklarifikasi kejadian itu kepada pihak perbankan yang menerbitkan kartu kredit. Terkait transaksi kartu kredit miliknya, LHJ mengatakan, terdapat dua transaksi yang mengakibatkan kerugian hingga Rp 134 Juta, yakni pada 16 Januari 2020 dan 19 Januari 2020. Pada tanggal 16 Januari 2020 itu ada 24 transaksi dengan jumlah kerugian Rp 120,2 Juta dan berlanjut tanggal 19 Januari 2020 dengan nilai kerugian Rp 13,9 Juta. terus ditagih untuk membayar kewajibannya terhitung sejak Februari hingga Juli 2020. Total tagihan dari bank milik BUMN tersebut kepada LHJ pada bulan Juni totalnya Rp 20 Juta, Rp 24 Juta dan Rp 40 Juta (Widodo, Ichsan, & Sutabri, 2020).

Memerangi kejahatan dunia maya dalam kategori *hacker* membutuhkan keseriusan dari semua pihak yang terlibat, mengingat perkembangan teknologi informasi sebagai alat komunikasi budaya. Keberadaan undang-undang yang mengatur kejahatan dunia maya, khususnya dalam klasifikasi peretas, diperlukan, tetapi jika implementasinya tidak memiliki kapasitas dan keahlian di bidang ini dan masyarakat terus menjadi sasaran. Tata Sutabri mengemukakan Monitoring merupakan proses rutin dalam pemantauan serta pengumpulan data kemajuan suatu objek, baik dari segi proses, kualitas, dan hasil akhir. Sehingga dapat di memerangi para hecker dalam pembobolan carding atau tidak kejahatan melalui internet secara terus menerus (Sutabri, 2012).

Rumusan Masalah

Rumusan masalah dari pertanyaan "carding" ini adalah:

1. Apa itu carding?
2. Siapakah pelakunya?
3. Bagaimana pelaku melakukan carding?
4. Modus apa yang digunakan pelaku?
5. Bagaimana cara menangani carding?
6. Apa efek dari carding?
7. Hukum apa yang berlaku untuk carding?

METODE PENELITIAN

Model penelitian deskriptif diartikan sebagai prosedur penyelesaian, suatu masalah yang dikaji dengan menggambarkan objek penelitian, seperti individu, lembaga, masyarakat, dan lain-lain, berdasarkan fakta-fakta yang dapat diamati atau pada masa kini (Nawawi, 2012, p. 63). Bogdan & Taylor dalam Moleong mengemukakan hal yang sama, mendefinisikan metode kualitatif sebagai prosedur penelitian yang menghasilkan data deskriptif berupa bahasa lisan dan tulisan orang serta perilaku yang dapat diamati. Oleh karena itu, dalam penelitian ini, penulis menggunakan metode kualitatif deskriptif yaitu penelitian secara detail dan analisis terhadap dokumen atau literatur yang berkaitan dengan kasus yang terjadi (Moleong, 2017).

HASIL DAN PEMBAHASAN

Analisis Kejahatan Carding Dengan Menggunakan Internet

Pencurian kartu kredit melalui internet di Indonesia baru-baru ini menjadi lebih canggih dan kejahatan yang dilakukan adalah pencurian nomor kartu kredit, kerentanan dunia kejahatan dunia maya saat ini dan kerugian melebihi dunia nyata ketika perampokan bank mencapai puncaknya. Mereka bisa mencuri uang puluhan atau ratusan juta rupiah serta pencurian online dengan cepat merampok jutaan bahkan miliaran dolar dalam waktu singkat. Di dunia kriminal modern, di mana banyak peretas terlibat secara langsung atau tidak langsung, pencurian tidak hanya tentang mencuri barang dan material fisik, tetapi juga mengekstraksi data berdasarkan fakta secara ilegal. Berbagai masalah baru terjadi di dunia maya. Ini berat di tingkat internasional dan sangat rumit mencari otoritas hukum untuk menanganinya. Dalam tindak pidana pencurian kartu kredit (perampokan ATM/pencurian melalui internet). Tata Sutabri mengemukakan jenis transaksi sudah beragam, baik menggunakan Kartu Debit, Kartu Kredit yang memanfaatkan jaringan ATM atau Debit Acces Transaction di Chasier (Sutabri, 2019). Sehingga para aparat penegak hukum dan pegawainya harus segera mengungkap kasus perampokan ATM/pencurian kartu kredit, jika tidak maka keresahan sosial dapat menyebar dan berdampak pada organisasi. Kecuali pihak berwenang dapat segera mendeteksi kasus pencurian/penipuan kartu kredit yang telah terjadi, sementara manajemen bank tidak dapat meyakinkan publik tentang sistem keamanan dana nasabah, industri perbankan domestik akan terus berlanjut.

Seiring maraknya pencurian data kartu kredit menggunakan internet, oknum-oknum yang tidak bertanggung jawab menggunakan beberapa cara seperti:

a) Jika kartu kredit dicuri, maka cara yang digunakan dimulai dengan mencuri kartu kredit tersebut atau mendapatkan informasi rekening, termasuk nomor rekening kartu kredit atau informasi lain yang diperlukan oleh penerima kartu kredit (merchant) dalam bertransaksi;
b) Pencurian identitas dapat dilakukan dengan menanam *parasit spyware* (pencurian identitas) dan nomor kartu kredit dapat melacak jika ada Pemegang kartu kredit menggunakan kartu kredit mereka untuk berbelanja online;

c) Penjual (pedagang) menyalin kuitansi penjualan barang yang dibeli oleh pelanggan untuk digunakan dalam kejahatan berikutnya;
d) Melakukan *skimming*, di mana informasi pribadi diperoleh melalui *skimming*, maka *skimming* adalah metode berteknologi tinggi (*hi-tech method*) di mana pencuri memperoleh informasi pribadi tentang pemegang kartu kredit atau nomor rekening bank, pelaku penjelajahan menggunakan perangkat elektronik untuk mengumpulkan informasi tersebut untuk menerima. *Skimmer* yang digunakan sebagai *skimmer* berukuran sangat kecil dan mudah disembunyikan sehingga tidak sulit bagi seorang skimmer untuk membaca informasi kartu kredit tanpa sepengetahuan kartu kredit tersebut.

Apa itu Carding ?

Carding adalah kejahatan di mana teknologi informasi digunakan untuk bertransaksi pada kartu kredit orang lain dengan cara yang dapat menyebabkan kerugian materil dan non-materiil pada seseorang. Carder adalah istilah yang digunakan untuk menunjukkan pelaku kejahatan carding. Menurut IFFC (*Internet Fraud Complaint Center*, unit FBI), skimming adalah "Penggunaan yang tidak sah dari kartu kredit atau kartu debet fraudlently memperoleh uang atau properti di mana kredit atau nomor kartu debet dapat dicuri dari situs web yang tidak aman atau dapat diperoleh dalam pencurian identitas scheme." Adapun jenis tindakan dalam kejahatan Carding :

1. Wiretapping
   Wiretapping adalah jenis carding di mana transaksi kartu kredit disadap melalui jaringan komunikasi. Pelaku penyadapan dapat memperoleh banyak informasi pribadi sehingga menimbulkan kerugian yang besar bagi korban.
2. Counterfeiting
   Counterfeiting adalah jenis kartu dimana kartu kredit dipalsukan sehingga terlihat sangat mirip dengan aslinya. Peralatan dan pengetahuan khusus mendukung penipuan kartu kredit.
3. Phishing
   Phishing adalah jenis kartu yang berbentuk phishing melalui website. Penjahat mencuri informasi kartu kredit melalui situs web yang dapat menipu korban untuk mengisi atau mengirimkan informasi pribadi mereka.
4. Misuse of Card Data
   Misuse of Card Data adalah carding berupa penyalahgunaan kartu kredit yang tidak diketahui oleh pemilik aslinya. Umumnya para penjahat mewaspadai kartu kredit ini, mulai dari denominasi kecil.

A. Siapakah Pelaku Carding

Pelaku kejahatan carding tidak melakukan dengan sendiri tetapi pelaku ini melibatkan beberapa pihak dalam melaksakan kejahatan carding tersebut antara lain :

1. Carder
   Carder pelaku dari carding, carder menggunakan email, spanduk atau pop-up untuk memikat pengguna Internet ke situs web palsu di mana pengguna Internet diminta untuk memberikan informasi pribadi. Teknik umum yang

sering digunakan oleh penerbit kartu untuk pencurian termasuk membuat situs web atau email palsu, juga dikenal sebagai phishing, yang dirancang untuk mendapatkan informasi pelanggan seperti nomor rekening, nomor identifikasi pribadi (PIN), atau kata sandi. Penjahat kemudian, setelah menerima informasi pelanggan, memasang PIN atau kata sandi untuk menarik uang dari pelanggan. Target pengguna kartu adalah pengguna layanan online banking atau website periklanan, jejaring sosial, toko online dan sejenisnya yang ceroboh dan tidak teliti saat melakukan pembelian online melalui website online.

2. Netter
   Netter adalah orang yang gemar membuka internet/dunia maya untuk mencari informasi sebanyak-banyak mungkin dalam hal ini adalah penerima email yang dikirimkan oleh carder.
3. Cracker
   Cracker adalah istilah untuk orang yang mencari kerentanan dalam suatu sistem dan menanamkannya untuk keuntungan pribadi dan mencari keuntungan dari sistem yang tertanam tersebut seperti pencurian data, penghapusan, penipuan.
4. Bank
   Bank adalah badan hukum yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk pinjaman dan/atau bentuk lain untuk meningkatkan taraf hidup masyarakat pada umumnya. Bank juga merupakan pihak yang menerbitkan kartu kredit/debit dan menyelenggarakan transaksi online, pembelian online, layanan perbankan online dan lain-lain.

B. Kapan Peristiwa Carding Terjadi

Seperti bentuk kejahatan lainnya, kejahatan kartu ini biasanya secara rahasia menargetkan informasi pribadi korban. Hacker atau peretas dapat memperoleh detail dan nomor kartu korban secara ilegal. Nomor kartu kredit telah dicuri dari halaman atau situs web yang tidak aman.

C. Modus Apa Yang Digunakan Pelaku?

Penipu biasanya melalui beberapa langkah-langkah modus untuk melakukan kejahatan:

1. Dapatkan nomor kartu kredit, yang bisa dilakukan dengan beberapa cara antara lain: *Phishing* (pembuatan website palsu, seperti dalam kasus klik.bca), *hacking*, *sniffing*, *keylogging*, *worm*, *chat* dengan rayuan dan pengungkapan nomor kartu kredit secara tidak sadar secara sukarela, pertukaran informasi antara pemegang kartu, mengunjungi website yang khusus menyediakan kredit nomor kartu adalah kartu dan lainnya yang pada dasarnya mendapatkan nomor kartu kredit.
2. Kunjungi situs online yang banyak digunakan seperti *eBay*, *Amazon* dan kemudian produsen kartu akan menguji nomor yang diperlukan untuk mengetahui apakah kartu tersebut masih valid atau batasnya cukup.
3. Beli barang secara online seolah-olah pemegang kartu adalah pemilik asli kartu tersebut.

4. Memberikan alamat tujuan atau pengiriman, karena kita tahu bahwa Indonesia memiliki tingkat penetrasi internet masih terendah seperti di tabel berikut :

Top 25 Countries, Ranked by Internet Users, 2013-2018
millions

	2013	2014	2015	2016	2017	2018
1. China*	620.7	643.6	669.8	700.1	736.2	777.0
2. US**	246.0	252.9	259.3	264.9	269.7	274.1
3. India	167.2	215.6	252.3	283.8	313.8	346.3
4. Brazil	99.2	107.7	113.7	119.8	123.3	125.9
5. Japan	100.0	102.1	103.6	104.5	105.0	105.4
6. Indonesia	72.8	83.7	93.4	102.8	112.6	123.0
7. Russia	77.5	82.9	87.3	91.4	94.3	96.6
8. Germany	59.5	61.6	62.2	62.5	62.7	62.7
9. Mexico	53.1	59.4	65.1	70.7	75.7	80.4
10. Nigeria	51.8	57.7	63.2	69.1	76.2	84.3
11. UK**	48.8	50.1	51.3	52.4	53.4	54.3
12. France	48.8	49.7	50.5	51.2	51.9	52.5
13. Philippines	42.3	48.0	53.7	59.1	64.5	69.3
14. Turkey	36.6	41.0	44.7	47.7	50.7	53.5
15. Vietnam	36.6	40.5	44.4	48.2	52.1	55.8
16. South Korea	40.1	40.4	40.6	40.7	40.9	41.0
17. Egypt	34.1	36.0	38.3	40.9	43.9	47.4
18. Italy	34.5	35.8	36.2	37.2	37.5	37.7
19. Spain	30.5	31.6	32.3	33.0	33.5	33.9
20. Canada	27.7	28.3	28.8	29.4	29.9	30.4
21. Argentina	25.0	27.1	29.0	29.8	30.5	31.1
22. Colombia	24.2	26.5	28.6	29.4	30.5	31.3
23. Thailand	22.7	24.3	26.0	27.6	29.1	30.6
24. Poland	22.6	22.9	23.3	23.7	24.0	24.3
25. South Africa	20.1	22.7	25.0	27.2	29.2	30.9
Worldwide* **	**2,692.9**	**2,892.7**	**3,072.6**	**3,246.3**	**3,419.9**	**3,600.2**

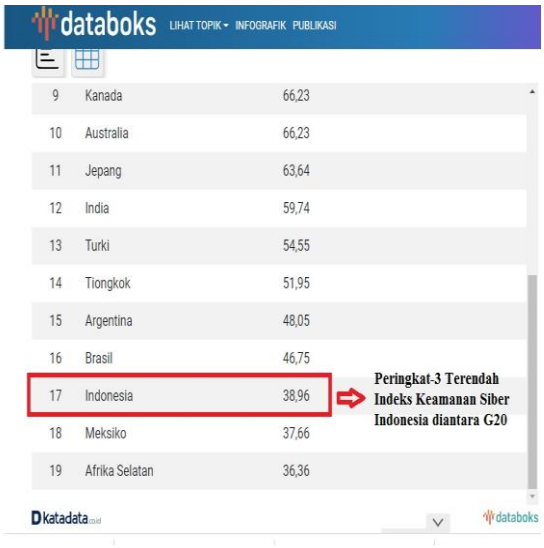
*Note: individuals of any age who use the internet from any location via any device at least once per month; *excludes Hong Kong; **forecast from Aug 2014; ***includes countries not listed*
Source: eMarketer, Nov 2014
181948 www.eMarketer.com

Internet User Penetration in Asia-Pacific, by Country, 2017-2022
% of population

	2017	2018	2019	2020	2022	2022
South Korea	89.8%	90.2%	90.3%	90.4%	90.4%	90.4%
Hong Kong	83.8%	84.6%	85.3%	85.9%	86.3%	86.7%
Taiwan	82.7%	83.9%	85.0%	85.9%	86.5%	86.9%
Japan	82.3%	82.8%	83.3%	83.7%	84.1%	84.5%
New Zealand	82.3%	82.8%	83.3%	83.5%	83.6%	83.6%
Australia	82.0%	82.5%	83.0%	83.2%	83.3%	83.4%
Singapore	80.9%	81.4%	81.9%	82.2%	82.3%	82.4%
Malaysia	69.9%	71.4%	72.7%	73.7%	74.5%	75.1%
Thailand	56.5%	59.7%	61.9%	63.4%	64.5%	65.3%
China*	56.0%	58.8%	61.5%	64.1%	66.2%	68.2%
Vietnam	52.6%	55.0%	57.4%	59.4%	60.8%	62.0%
Philippines	52.0%	53.5%	55.0%	56.2%	57.3%	58.1%
Indonesia	38.7%	42.3%	45.9%	48.6%	51.0%	53.0%
India	30.3%	33.2%	35.8%	38.3%	40.9%	43.5%
Other	36.7%	38.9%	40.9%	42.9%	44.5%	46.1%
Asia-Pacific	**45.5%**	**48.1%**	**50.5%**	**52.7%**	**54.7%**	**56.6%**

*Note: individuals of any age who use the internet from any location via any device at least once per month; *excludes Hong Kong*
Source: eMarketer, Oct 2018
243189 www.eMarketer.com

Tahun 2018 indonesia menduduki peringkat ke-6 dunia, ke-13 (McNair, 2018). di Asia dan Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20 sebagai Sumber terklasifikasi untuk carding kriminal (Annur, 2022).



https://databoks.katadata.co.id/datapublish/2022/09/13/indeks-keamanan-siber-indonesia-peringkat-ke-3-terendah-di-antara-negara-g20

Hingga akhirnya Indonesia di-*blacklist* oleh banyak website sebagai negara tujuan pengiriman. Carder dari Indonesia yang tersebar di Yogyakarta, Bali,

Banding, dan Jakarta, oleh karena itu kebanyakan menggunakan alamat di Singapura atau Malaysia sebagai alamat perantara, sementara mereka sudah memiliki mitra di negara-negara tersebut.

5. Pengambilan barang oleh carder.

Bagaimana Cara Menangani Carding ?

Ada 2 cara yang dapat dilakukan untuk menangani kejahatan carding baik secara *Off-line* maupun *On-line*. Adapun penanganan secara *Off-line* dengan langkah-langkah sebagai berikut :

1. Anda harus memastikan bahwa kartu kredit Anda disimpan di tempat yang aman.
2. Jika kartu kredit dan KTP Anda hilang, segera laporkan ke pihak berwajib dan pihak bank dan segera tutup.
3. Jangan berharap disetujui karena orang lain menggunakannya (baik toko fisik maupun online).
4. Pastikan jika Anda membuat fotokopi kartu kredit dan KTP Anda, agen layanan (yang meminta salinan kartu kredit Anda) atau salinan agen dan CCV tidak akan disimpan. Tutupi 3 digit terakhir CVV dengan kertas putih sebelum menyalin kartu kredit Anda. Hal ini untuk mencegah pihak ketiga menyalahgunakan kartu kredit kami. Perlakukan keamanan CVV Anda sama seperti Anda memperlakukan PIN atau kata sandi.
5. Jangan dengan mudah atau sembarangan menyuruh orang lain untuk menyalin kartu kredit dan KTP.
6. Hati-hati tempat kita berbelanja, pastikan tempat belanja / counter / gerai / toko / hotel benar-benar kredibel.

Adapun penanganan secara On-line dengan langkah-langkah sebagai berikut :

1. Berbelanja di website aman (situs belanja online), jangan asal beli, tapi pengelolaannya tidak jelas, atau mungkin baru pertama kali tahu, sehingga kredibilitasnya masih diragukan.
2. Pastikan operator situs transaksi online menggunakan SSL (Secure Sockets Layer) bertanda HTTPS pada login transaksi online yang Anda gunakan untuk berbelanja.
3. Hati-hati menyimpan file scan kartu kredit, termasuk di *flashdisk* (*memory stick*) dan di email Anda.
4. Jangan pernah melakukan transaksi secara online menggunakan wifi publik karena besar kemungkinan ID name dan Password dan nomor kartu kredit bisa di bobol karena tingkat keamanan yang masih minim.

Apa Efek Dari Carding?

Dampak dari kejahatan carding tersebut adalah :

1. Kehilangan uang secara misterius
2. Pemerasan carder dan pengosongan kartu kredit
3. Kecemasan masyarakat saat menggunakan kartu kredit untuk bertransaksi.
4. Hilangnya kepercayaan masyarakat terhadap jasa keuangan di negeri ini
5. Merugikan banyak orang lain dari pengguna kartu kredit.

Hukum apa yang berlaku untuk carding?

Saat ini Indonesia belum memiliki undang-undang khusus/hukum siber yang mengatur tentang kejahatan dunia maya, meskipun undang-undang ini telah berlaku sejak tahun 2000, namun pemerintah belum meratifikasinya untuk menangani kasus-kasus yang muncul, terutama yang terkait dengan kejahatan dunia maya. Dalam proses pemetaan perkara, penyidik (khususnya Kepolisian Negara) membuat analogi atau persamaan dan kemiripan dengan pasal-pasal hukum pidana yang dapat diatur dalam KUHP *Cybercrime*.

Di Indonesia, carding digolongkan sebagai tindak pidana pencurian, dimana definisi hukum pencurian dan unsur-unsurnya dirumuskan dalam Pasal 362 KUHP (Moeljatno, 2021), yaitu:

> *"Barang siapa mengambil suatu benda yang seluruhnya atau sebagian milik orang lain, dengan maksud untuk dimiliki secara melawan hukum, diancam karena pencurian, dengan pidana penjara paling lama 5 tahun atau denda paling banyak sembilan ratus rupiah".*

Kemudian, setelah lahirnya undang-undang ITE, kasus kartu khususnya dapat dijerat Pasal 31 1 dan 2, yang mengatur tentang peretasan.

- Pasal 31 ayat 1*: "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronika dan atau dokumen elektronik dalam suatu komputer dan atau sistem elektronik secara tertentu milik orang lain".*
- Pasal 31 ayat 2: *"Setiap orang dengan sengaja atau tanpa hak atau melawan hukum melakukan intersepsi atau transmisi elktronik dan atau dokumen elektronik yang tidak bersifat publik dari, ke dan di dalam suatu komputer dan atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan perubahan, penghilangan dan atau penghentian informasi elektronik dan atau dokumen elektronik yang ditransmisikan."*

KESIMPULAN

Peretas dam penjahat dunia maya telah ada sejak lama. *Cybercrime* ada karena efek negatif dari perkembangan teknologi. Saat ini orang terhubung ke internet hampir setiap menit. Jika kita tidak hati-hati saat menggunakannya, kita bisa menjadi korban kejahatan dunia maya. Carding adalah jenis kejahatan dunia maya yang melibatkan peretasan informasi kartu kredit untuk digunakan oleh seseorang yang bukan pemegang kartu kredit. Sifat pemetaan kejahatan adalah non-kekerasan dan kekacauan yang mereka ciptakan tidak segera terlihat, namun dampak yang ditimbulkannya bisa sangat besar. Carding merupakan salah satu jenis kejahatan internet (*cybercrime*) yang sangat sulit untuk diberantas. Oleh karena itu, kita harus lebih waspada dan selektif dalam transaksi kartu kredit/debit, karena kita tidak dapat menjamin keamanan sistem perusahaan ternama. Bisa jadi ada faktor x yang bisa membuka lubang keamanannya. Menurut Tata Sutabri dalam (Saeppu, Mary, & Mulyono, 2019) sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian yang mendukung fungsi operasi organisasi yang bersifat manajerial dengan dengan kegiatan strategi dari suatu organisasi untuk dapat menyediakan kepada pihak luar tertentu dengan laporan-laporan yang diperlukan. Pemegang kartu kredit harus

memahami dengan hati-hati dalam penggunaannya baik bertransaksi secara offline atau online dan dampak kerugian yang ditanggung.

DAFTAR PUSTAKA

Abidin, Dodo Zaenal. (2017). Kejahatan dalam Teknologi Informasi dan Komunikasi. *Jurnal Processor*, *10*(2), 509–516.

Annur, Cindy Mutia. (2022). Indeks Keamanan Siber Indonesia Peringkat ke-3 Terendah di Antara Negara G20. Retrieved from Databooks website: https://databoks.katadata.co.id/datapublish/2022/09/13/indeks-keamanan-siber-indonesia-peringkat-ke-3-terendah-di-antara-negara-g20

Bernoza, Aulia, Fadlan, Fadlan, & Nurkhotijah, Siti. (2020). Analisis Yudiris Tindak Pidana Penipuan Berbasis Jual Beli Online di Kota Batam (Studi Penelitian Polresta Barelang). *Zona Hukum: Jurnal Hukum*, *14*(3), 1–11.

Ibrahim, Dicky Malik. (2018). *Tanggung Jawab Bank Terhadap Nasabah Yang Menjadi Korban Kejahatan Informasi dan TRANSAKSI Elektronik Dalam Layanan Aplikasi Mandiri Online (Studi Kasus di PT Bank Mandiri Kantor Cabang Area Yogyakarta)*.

Indarta, Yose, Ranuharja, Fadhli, Ashari, Ilham Firman, Sihotang, Jay Idoan, Simarmata, Janner, Harmayani, Harmayani, Algifari, M. Habib, Muslihi, Muhammad Takdir, Mahmudi, A. Aviv, & Fatkhudin, Aslam. (2022). *Keamanan Siber: Tantangan di Era Revolusi Industri 4.0*. Yayasan Kita Menulis.

McNair, Corey. (2018). *Global Digital Users Update 2018 Affordable Prices Drive Smartphone Adoption in Developing Markets*.

Moeljatno, S. H. (2021). *KUHP (Kitab undang-undang hukum pidana)*. Bumi Aksara.

Moleong, Lexy J. (2017). Metode penelitian kualitatif, Bandung: PT. *Remaja Rosda Karya*.

Nawawi, Hadari. (2012). Metode Penelitian Bidang Sosial.(cetakan ke-13). *Gajah Mada University Press, Yogyakarta, Hal*, *176*.

Putri, Amelia Widya Octa Kuncoro, Aditya, Abdul Razzaq Matthew, Musthofa, Desta Lesmana, & Widodo, Pujo. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, *6*(1), 35–46.

Saeppu, Julianus, Mary, Thomson, & Mulyono, Heri. (2019). Sistem Informasi Pemesanan Tiket Kapal Mentawai Fast Kota Padang Berbasis Web. *Jurnal Edik Informatika Penelitian Bidang Komputer Sains Dan Pendidikan Informatika*, *6*(1), 13–19.

Sutabri, Tata. (2012). *Analisis sistem informasi*. Penerbit Andi.

Sutabri, Tata. (2019). *Komputer dan masyarakat*.

Syauqi, Ahmad Thariq. (2016). Startup sebagai Digitalisasi Ekonomi dan Dampaknya bagi Ekonomi Kreatif di Indonesia. *Department of Electrical Engineering and Information Technology*, *3*(2), 1–4.

Widodo, Yohanes Bowo, Ichsan, Ade Muhammad, & Sutabri, Tata. (2020). Perancangan Sistem Smart Home Dengan Konsep Internet Of Things Hybrid

Berbasis Protokol Message Queuing Telemetry Transport. *Jurnal Teknologi Informatika Dan Komputer*, *124*.