Jurnal Pendidikan dan Konseling
Volume 4 Nomor 5 Tahun 2022
E-ISSN: 2685-936X dan P-ISSN: 2685-9351
Universitas Pahlawan Tuanku Tambusai

Kejahatan *Phising* dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia

MOHD. Yusuf DM[1], Addermi[2], Jasmine Lim[3]
[1]Fakultas Hukum, Universitas Lancang Kuning
[2,3] Ilmu Hukum, Fakultas Hukum, Universitas Lancang Kuning
Email: adermi.sbci30@gmail.com

Abstrak

Cyber Crime merupakan kejahatan yang timbul karena dampak negatif pemanfaatan teknologi internet. *Cyber Crime* ini bukan hanya kejahatan terhadap komputer tetapi juga kejahatan terhadap sistem jaringan komputer dan pengguna. Pelaku *Cyber Crime* saat ini melakukan kejahatan tersebut bukan hanya karna mempraktikkan keahlian yang dimiliki tetapi juga karena motif lain seperti uang, dendam, politik, iseng, dan sebagainya. Salah satu bentuk kejahatan teknologi ialah kejahatan *phising* (pengelabuan) terhadap situs *online* seperti *website*. Metode pengumpulan data dilakukan dengan mengumpulkan dokumen dari jurnal, artikel, makalah, dan lain-lain. Oleh karena itu, hasil penelitian penulis diharapkan dapat memberikan kontribusi minimal bagi mereka yang ingin mendalami permasalahan *Cyber Law* di Indonesia. Latar belakang terjadinya kejahatan di dunia maya yaitu saling terhubungnya antara jaringan yang satu dengan yang lain sehingga memudahkan pelaku kejahatan untuk melakukan aksinya. Selain itu, tidak meratanya penyebaran teknologi menjadi salah satu factor terjadinya Cyber Crime.
Kata Kunci: *Cyber Crime, Cyber Law, Phising*.

Abstract

Cyber Crime is a crime that arises because of the negative impact of using internet technology. Cyber Crime is not only a crime against computers but also crimes against computer network systems and users. Cybercriminals are currently committing these crimes not only because of practicing their skills but also for other motives such as money, revenge, politics, fun, and so on. One form of technology crime is the crime of phishing (deception) against online sites such as websites. The method of data collection is done by collecting documents from journals, articles, papers, and others. Therefore, the results of the author's research are expected to provide a minimal contribution for those who want to explore the problems of Cyber Law in Indonesia. The background of the occurrence of crimes in cyberspace is the interconnectedness of networks with one another, making it easier for criminals to carry out their actions. In addition, the uneven distribution of technology is one of the factors for the occurrence of Cyber Crime.
Keywords: *Cyber Crime, Cyber Law, Phising*

PENDAHULUAN

Kemajuan ilmu pengetahuan dan teknologi telah memberikan dampak yang sangat positif bagi peradaban umat manusia. Salah satu fenomena abad modern yang sampai saat ini masih terus berkembang dengan pesat adalah internet. Pada mulanya jaringan internet hanya dapat digunakan oleh lingkungan pendidikan (perguruan tinggi) dan lembaga penelitian. Pesatnya perkembangan teknologi informasi dan komunikasi juga diiringi dengan meluasnya penyalahgunaan teknologi

informasi dan komunikasi, sehingga menjadi masalah yang sangat meresahkan yaitu terjadinya kejahatan yang dilakukan di dunia maya atau yang biasa dikenal dengan istilah "*Cyber Crime*".

Berbagai kejahatan telah terjadi di dunia maya ini, kasus-kasus tersebut tentu saja merugikan dan berdampak negatif, kejahatan dunia maya semacam ini tidak hanya mencakup Indonesia, tetapi juga mencakup seluruh dunia. Beberapa kejahatan yang terjadi disebabkan oleh maraknya penggunaan *e-mail, e-banking* dan *e-commerce* di Indonesia. Semakin banyaknya kasus *cybercrime* (khususnya di Indonesia) telah menarik perhatian pemerintah untuk segera memberlakukan undang-undang yang dapat digunakan untuk menjebak pelaku kejahatan di dunia maya. Pemerintah Indonesia sendiri telah memasukkan UU *Cyber crime* (UU Siber) ke dalam UU ITE Nomor 11 Tahun 2008, dan berharap dengan adanya UU ITE Nomor 11 Tahun 2008 dapat mengatasi, mengurangi, dan menghentikan pelaku kejahatan di dunia maya.

Menurut Gregory (dalam Dista, 2005 : 186) *Cyber crime* adalah suatu bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung ke internet, dan mengeksploitasi komputer lain yang terhubung dengan internet juga. Adanya lubang-lubang keamanan pada sistem operasi menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan para *hacker, cracker* dan *script kiddies* untuk menyusup ke dalam komputer tersebut. Sedangkan Menurut Tavani (dalam Fajri, 2008) definisi *Cyber crime*, yaitu "kejahatan di mana tindakan kriminal hanya bisa dilakukan dengan menggunakan teknologi *cyber* dan terjadi di dunia *cyber*".[1]

Kejahatan tersebut dibedakan menjadi dua kategori yakni *Cybercrime* dalam pengertian sempit dan dalam pengertian luas. *Cybercrime* dalam pengertian sempit merupakan kejahatan terhadap sistem komputer, sedangkan *Cybercrime* dalam pengertian luas mencakup kejahatan terhadap sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer.[2] Dari beberapa pengertian di atas, dapat disimpulkan bahwa *Cyber Crime* merupakan perbuatan melawan hukum yang dilakukan dengan menggunakan jaringan komputer atau internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi untuk memperoleh keuntungan dengan merugikan pihak lain.

Sumber-sumber ancaman siber dapat berasal dari berbagai sumber, seperti intelijen asing (*foreign intelligence service*), kekecewaan (*disaffected employees*), investigasi jurnalis (*investigative journalist*), organisasi ekstremis (*extremist organization*), aktivitas para *hacker* (*hacktivist*), dan kelompok kejahatan terorganisir (*organized crime groups*).[3] *Hacker* adalah seseorang atau sekelompok orang yang memberikan sumbangan yang bermanfaat terhadap dunia jaringan internet, sistem operasi, serta memberikan bantuan untuk dunia internet dan komputer. Pekerjaan *hacker* juga dapat dikategorikan sebagai seseorang yang mencari kelemahan dari suatu sistem dan memberikan ide untuk menutup celah atau kelemahan yang terdapat dalam sistem tersebut. Sedangkan *Cracker* adalah sebutan untuk seseorang yang mencari kelemahan sistem serta memasukinya guna kepentingan dirinya sendiri (pribadi). Tindakan yang dilakukan oleh *cracker* seperti pencurian data, penggantian atau manipulasi data, penghapusan data serta lain sebagainya.[4]

Phising merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang dibutuhkan oleh sang penjebak. *Phishing* termasuk dalam kejahatan cyber crime, dimana sekarang ini marak terjadi tindak kriminal melalui jaringan komputer. Seiring perkembangan zaman, tindak kriminal juga semakin merebak di seluruh dunia. Sehingga ancaman yang banyak terjadi saat ini juga melalui komputer. Bagi *hacker* cara ini merupakan cari paling mudah untuk di jadikan serangan. Meskipun di anggap mudah dan sepele tapi tetap saja ada pengguna yang masuk ke perangkap sang *hacker*.[5] *Phising* yaitu aktivitas seseorang untuk mendapatkan informasi rahasia pengguna dengan cara menggunakan email dan situs web palsu yang tampilannya menyerupai tampilan asli atau resmi web sebenarnya. Informasi yang didapat atau

dicari oleh *phiser* adalah berupa password akun atau nomor kartu kredit korban. Penjebak (*phisher*) menggunakan email, *banner* atau *pop-up window* untuk menjebak user agar mengarahkan ke situs web palsu (*fake webpage*), di mana pengguna diminta untuk memberikan informasi pribadinya. Di sinilah *phiser* memanfaatkan kecerobohan dan ke tidak telitian pengguna dalam web palsu tersebut untuk mendapatkan informasi.[6]

METODE

Metode yang digunakan penulis adalah metode penelitian normatif dengan model deskriptif yang mengeksplorasi berbagai aspek peraturan perundang-undangan terkait *cyber crime*. Metode pengumpulan data dilakukan dengan mengumpulkan dokumen (baik dokumen tertulis maupun dokumen elektronik) dari jurnal, artikel, makalah, dan lain-lain. Data-data yang terkumpul kemudian dibandingkan dan diseleksi untuk ditampilkan dalam penulisan ini. Oleh karena itu, hasil penelitian penulis diharapkan dapat memberikan kontribusi minimal bagi mereka yang ingin mendalami permasalahan *cyber law* di Indonesia.

Pendekatan yang dipergunakan adalah pendekatan perundang-undangan dan pendekatan konseptual. Penulis mengkaji Undang-Undang mengenai *cyber law* sedangkan Bahan Hukum yang dipergunakan adalah bahan hukum primer dan bahan hukum sekunder. Bahan hukum primer adalah bahan hukum yang berasal peraturan perundang-undangan yang berkaitan dengan penulisan ini. Adapun bahan hukum sekunder adalah bahan hukum yang berasal dari jurnal ataupun karya tulis ilmiah yang berkaitan dengan penelitian ini.

HASIL DAN PEMBAHASAN

Sumber Ancaman-ancaman *Phising*

Untuk mengetahui sumber-sumber ancaman *phising* kami telah melakukan *survey* literatur *phising* dengan membaca beberapa jurnal. Berikut adalah garis besar dari beberapa sumber ancaman *phising* berdasarkan *survey* yang telah kami lakukan:

1. Email Berdasarkan *survey* yang telah dilakukan pada tahun 2014 ada lebih dari 120.000 serangan *phising* yang berpuncak pada miliaran transmisi email.[7] 65% dari serangan *phising* mulai dengan mengunjungi link yang diterima dalam sebuah email. Pada Maret 2016, 229.265 laporan email phising diterima oleh Kelompok Kerja *Anti-Phising* dari konsumen.[8] 18,3% penduduk Australia menjadi korban dari *phising* melalui email.[8]
2. *Website Phising* pada *website* meliputi iklan dan sosial media (Facebook, Twitter, Instagram). Berdasarkan *survey* yang telah dilakukan Facebook memperkirakan 8,7% dari akun yang berjumlah 83.090.000 bukan milik pengguna yang sebenarnya dan perkiraan sekitar 1,5% (14.320.000) adalah akun yang secara tidak sengaja menyebarkan isi berbahaya tanpa diketahui oleh pengguna, seperti pesan spam dan *link* yang mencurigakan.[9] Sebagian besar serangan *phising* dilakukan melalui web server yang sudah di *hack* dan 73% situs telah menjadi korban.[10] Pada Maret 2016 123.555 situs *phising* terdeteksi oleh Kelompok Kerja *Anti-Phising*.[8] 15,7% penduduk Australia menjadi korban *phising* melalui situs belanja online dan 6,9% melalui sosial media.[8]
3. Malware Phising yang dilakukan melalui penyebaran *malware* salah satunya adalah *malware* Koobface yang telah membuat 81% pengguna menjadi korbannya.[9]

Cara Kerja Phising

Berikut merupakan cara kerja *phising* berdasarkan sumber-sumber ancaman *phising* yang telah kami survey dari beberapa jurnal:

1. Email Serangan ini di mulai dengan mengirimkan email yang terlihat dari sebuah organisasi yang kenal dengan korban. Kemudian email tersebut akan meminta mereka untuk memperbarui informasi mereka dengan mengikuti *link* URL yang terdapat dalam email tersebut.[7] Pada dasarnya, *phising* menggabungkan rekayasa sosial dan vektor serangan kompleks untuk menciptakan ilusi atau penipuan di mata penerima email.[8] Penyerang akan mengirimkan jutaan email ke jutaan pengguna dan ribuan dari mereka setidaknya akan jatuh pada rekayasa tersebut.[11] Pastinya serangan-serangan tersebut menggunakan email palsu untuk menipu pengguna untuk menipu pengguna agar mau membocorkan data pribadi.[12]
2. *Website* Pada situs web mereka akan diminta untuk memasukkan informasi rahasia pribadi, seperti *password* dan nomor rekening bank yang pada akhirnya akan digunakan untuk pencurian identitas.[7] *Phiser* juga menggunakan *tool* untuk mencuri kode sumber laman web yang sah dan menggantinya dengan web palsu.[6] Selain itu, *phiser* menciptakan *embedding link* untuk mendapatkan informasi sensitif milik korban.[9]
3. *Malware* Cara penyerangan dengan berpura-pura meminta karyawan untuk *download* suatu *file* yang di kirim oleh *phiser* sebagai *penetralisir malware* di komputer nantinya.[8]

Cara Mencegah Phising

Berikut adalah hasil *survey* kami mengenai cara pencegahan atau antisipasi terhadap serangan *phising* melalui *website* dari beberapa literatur:

1. Medeteksi dengan *toolsdetect*

   Sekarang ini internet sudah dianggap sebagai makanan sehari-hari, bahkan ada beberapa orang yang beranggapan tanpa internet mereka tidak bisa hidup. Ada banyak hal yang bisa kita lakukan dengan internet, mulai dari mencari informasi, berbagi informasi, dsb. Namun, pasti kita pernah menjumpai situs-situs yang muncul tanpa kita inginkan dan mengandung informasi berhadiah yang menggiurkan. Tentu saja hal tersebut akan menarik kita untuk mengisinya dengan data penting tanpa tau bahwa itu hanyalah situs *phising*. Untuk mencegah hal tersebut kita dapat menggunakan *toolsdetect* yang mana dapat membedakan mana situs yang asli dan palsu (*phising*).
2. Menggunakan add ons web browser anti tabnabbing

   Setiap tahunnya para *phisher* melancarkan aksi-aksinya dengan membuat serangan-serangan baru. Dan salah satu serangan baru tersebut yaitu bernama tabnabbing. Serangan *phising* tersebut dapat menyerang pada web. Dimana cara penyerangannya ketika pengguna membuka banyak tab, *phising* tersebut akan terbuka di sela-sela tab yang lain. Saat pengguna lengah, maka tab tersebut akan di buka dan serangan di mulai. Tab palsu itu di samarkan menjadi salah satu tab yang di buka oleh pengguna dan tab asli yang sebelumnya lenyap. Untuk itulah serangan ini di anggap serangan yang pintar karena tidak lagi menggunakan link yang di klik dulu agar pengguna masuk perangkap *phisher*.
3. Menggunakan mekanisme *pre-filter*

   Pencegahan *phising* juga dapat di lakukan dengan penggunaan *anti-phishing pre-filter* ini. Di dalam *pre-filter* terdapat tiga bagian pencegahan yakni *Site Identifier, Login Form Finder*, dan *Webpage Feature Generator*. Ketiganya tersebut melakukan pencegahan secara berurutan. *Site Identifier* digunakan untuk mengurangi jumlah perhitungan situs yang tidak perlu dan hanya mendeteksi halaman yang sah.
4. Self-efficacy

   Untuk mencegah terjadinya *phising* tidak hanya membutuhkan suatu aplikasi atau *software* anti-phishing melainkan juga membutuhkan *self-efficacy. Self-efficacy* adalah keyakinan individu dalam mengambil tindakan pengamanan[4]. Dengan memiliki sikap tersebut dapat menunjukkan

kepercayaan individu dalam pemecahan masalah dan penyelesaian tugas sesuai kemampuan mereka sendiri.

Dalam Upaya Menangani kasus-kasus yang terjadi khususnya yang berkaitan dengan *Cyber crime*, diperlukan Penegakan Hukum di Indonesia mengenai *Cyber Crime*, antara lain:

1. Undang-Undang Nomor 11 Tahun 2008 Tentang Internet & Transaksi Elektronik (ITE)

   Sejak tanggal 21 April 2008, bangsa Indonesia memasuki babak baru dalam pengaturan penggunaan teknologi dan informasi dan transaksi elektronik, yaitu adanya pengesahan rancangan Undang-undang tentang informasi dan transaksi elektronik yang kemudian di Undangkan menjadi Undang-Undang Negara Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (selanjutnya disingkat UU-ITE) tersebut mutlak diperlukan bagi Negara Indonesia, karena saat ini Indonesia merupakan salah satu negara yang menggunakan dan memanfaatkan teknologi informasi secara luas dan efisien, dan secara faktual belum banyak memiliki ketentuan hukum, terutama dari aspek hukum pidana. Cakupan materi UU-ITE secara umum antara lain berisi tentang Informasi dan dokumen elektronik, pengiriman dan penerimaan surat elektronik, tanda tangan elektronik, sertifikat elektronik, penyelenggaraan sistem elektronik.
2. Kitab Undang-undang Hukum Pidana
   a. Pasal 362 KUHP yang dikenakan untuk kasus *carding*.
   b. Pasal 378 KUHP dapat dikenakan untuk penipuan.
   c. Pasal 335 KUHP dapat dikenakan untuk kasus pengancaman dan pemerasan yang dilakukan melalui *e-mail* yang dikirimkan oleh pelaku untuk memaksa korban melakukan sesuatu sesuai dengan apa yang diinginkannya.
   d. Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media Internet.
   e. Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara Online di Internet dengan penyelenggara dari Indonesia
   f. Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi.
   g. Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang.
   h. Pasal 406 KUHP dapat dikenakan pada kasus *deface* atau *hacking* yang membuat sistem milik orang lain.
3. Undang - Undang Nomor 28 Tahun 2014 tentang Hak Cipta
4. Undang - Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.
5. Undang - Undang Nomor 32 Tahun 32 Tahun 2002 tentang Penyiaran

SIMPULAN

Berdasarkan pembahasan di atas dapat disimpulkan bahwa *Cyber Crime* merupakan kejahatan yang timbul karena dampak negatif pemanfaatan teknologi internet. *Cyber Crime* ini bukan hanya kejahatan terhadap komputer tetapi juga kejahatan terhadap sistem jaringan komputer dan pengguna. Pelaku *Cyber Crime* saat ini melakukan kejahatan tersebut bukan hanya karna mempraktikkan keahlian yang dimiliki tetapi juga karena motif lain seperti uang, dendam, politik, iseng, dan sebagainya. Cyber Crime dilakukan oleh orang-orang yang memiliki kemampuan tinggi terhadap komputer dan jaringannya. Oleh karena itu, dalam penanggulangannya dibutuhkan pengaturan hukum yang berkaitan dengan pemanfaatan teknologi tersebut, selain itu juga diperlukan adanya kerja sama dengan lembaga khusus untuk memberikan informasi tentang *Cyber Crime*, melakukan sosialisasi secara intensif kepada masyarakat, serta melakukan riset-riset khusus dalam penanggulangan *Cyber Crime*.

DAFTAR PUSTAKA

D. A. Arifah, "KASUS CYBERCRIME DI INDONESIA Indonesia's Cybercrime Case," *J. Bisnis dan Ekon.*, vol. 18, no. 2, pp. 185–195, 2011.

H. S. Sumarwani, "Tinjauan Yuridis Pemidanaan Cybercrime Dalam Perpektif Hukum Pidana Positif," *J. Pembaharuan Huk.*, vol. 1, no. 3, pp. 287–296, 2014, [Online]. Available: http://jurnal.unissula.ac.id/index.php/PH/article/view/1489

I. Rahmawati, "the Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense," *J. Pertahanan Bela Negara*, vol. 7, no. 2, pp. 51–66, 2017, doi: 10.33172/jpbh.v7i2.193.

A. Antoni, "Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online," *Nurani J. Kaji. Syari'ah dan Masy.*, vol. 17, no. 2, pp. 261–274, 2018, doi: 10.19109/nurani.v17i2.1192.

Mia Haryati Wibowo dan Nur Fatimah, "Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime," *JOEICT(jurnal Educ. Inf. Commun. Technol.*, vol. 1, pp. 1–5, 2017, [Online]. Available: http://jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/view/69

D. Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber," *J. Ilm. Saintikom, Univ. Sumatera Utara, Medan*, vol. 1978–6603, pp. 209–216, 2014.

N. Abdelhamid, "Multi-label rules for phishing classification," *Appl. Comput. Informatics*, vol. 11, no. 1, pp. 29–46, 2015, doi: 10.1016/j.aci.2014.07.002.

M. Junger, L. Montoya, and F.-J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," *Comput. Human Behav.*, vol. 66, pp. 75–87, 2017, doi: https://doi.org/10.1016/j.chb.2016.09.012.

K. S. Adewole, N. B. Anuar, A. Kamsin, K. D. Varathan, and S. A. Razak, "Malicious accounts: Dark of the social networks," *J. Netw. Comput. Appl.*, vol. 79, pp. 41–67, 2017, doi: https://doi.org/10.1016/j.jnca.2016.11.030.

M. Moghimi and A. Y. Varjani, "New rule-based phishing detection method," *Expert Syst. Appl.*, vol. 53, pp. 231–242, 2016, doi: https://doi.org/10.1016/j.eswa.2016.01.028.

R. S. Rao and S. T. Ali, "PhishShield: A Desktop Application to Detect Phishing Webpages through Heuristic Approach," *Procedia Comput. Sci.*, vol. 54, pp. 147–156, 2015, doi: 10.1016/j.procs.2015.06.017.

N. M. Shekokar, C. Shah, M. Mahajan, and S. Rachh, "An ideal approach for detection and prevention of phishing attacks," *Procedia Comput. Sci.*, vol. 49, no. 1, pp. 82–91, 2015, doi: 10.1016/j.procs.2015.04.230.