JHP 17 (Jurnal Hasil Penelitian) E-ISSN : 2502-8308
Januari 2020, Vol. 5, No. 2 P-ISSN : 2579-7980
http://jurnal.untag-sby.ac.id/index.php/jhp17

TINDAK PIDANA *CYBERCRIME* BAGI PELAKU PEMALSUAN DATA PADA SITUS *E-COMMERCE (PHISING)*

Budi Suharto, Arnold Bagas Kurniawan
Fakultas Hukum Universitas 17 Agustus 1945 Surabaya

Abstrak

Masyarakat umum biasanya sering menyebut dengan phising. Istilah phishing berasal dari Bahasa inggris yaitu *fishing* (memancing). Phishing yaitu suatu bentuk penipuan yang dilakukan dengan cara memalsukan data untuk mengelabui korban, tujuan dari phising yaitu agar mendapatkan informasi terhadap korban dari kata sandi sampai dengan kartu kredit, dengan cara menyamar menjadi orang atau bisnis yang terpercaya dalam suatu komunikasi elektronik resmi seperti surat elektronik atau pesan instan. Maka dari itu hal ini dinamakan memancing yang berarti memancing informasi keuangan dan kata sandi pengguna.

Latar Belakang

Pada saat ini teknologi informasi dan komunikasi (TIK) terutama internet berkembang dengan sangat pesat. Hampir semua aspek dalam kehidupan memanfaatkan penggunaan terknologi informasi dan komunikasi dalam menjalankan aktifitasnya. Dimulai dari bidang kesehatan, ekonomi, pendidikan, pemerintahan, agama, perbankan, hingga pekerjaan rumah tangga dapat lebih mudah dengan menggunakan TIK.

Berbagai manfaat dari TIK ini dapat kita gunakan sebagai contoh dalam pendidikan dengan adanya web dari universitas memudahkan mahasiswa dan dosen untuk memperoleh informasi dari web tersebut. Dan memudahkan dosen untuk mengajar dengan upload materi atau modul yang ditujukan untuk mahasiswa, agar mahasiswa tidak lagi mencatat tetapi mendownload apa yang sudah diupload dosen tersebut.(Michael, 2019)

Akan tetapi dibalik semua kemudahan itu terkadang ada beberapa pihak yang menyalahgunakan penggunaan TIK khususnya internet. Mereka melakukan kejahatan-kejahatan dalam dunia maya (cybercrime) untuk kepentingan pribadi. Misal masuk kesitus lembaga untuk mencuri, merusak atau memanipulasi data.

Kejahatan-kejahatan dunia maya (*cybercrime*) banyak jenis dan beragam namun pada dasarnya semuanya itu sama yaitu melakukan tindakan kejahatan pada dunia maya terutama internet untuk kepentingan pribadi maupun golongan tertentu.(Raissa et al., 2018)

Maksud Dan Tujuan

Maksud penulisan ini adalah :

1. Untuk lebih memahami dan mengetahui tentang kejahatan dunia maya (*cybercrime*) terutama dengan metode phising dan hukuman beserta Undang-Undang yang diberikan
2. Untuk lebih memahami dan mengetahui tentang bahaya dari *cybercrime* dengan metode phising dan semoga kita dapat mencegah dan menghindari phising agar tidak menimpa kita.

Sedangkan tujuan penulisan ini adalah sebagai salah satu tugas untuk memenuhi nilai mata kuliah Tindak Pidana Khusus.

Pembahasan

Pengertian *Cybercrime*

Kejahatan dunia maya (Inggris: *cybercrime*) merupakan istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk ke dalam kejahatan dunia maya antara lain yaitu penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit/carding, confidence fraud, penipuan identitas, pornografi anak, dll. Pada dasarnya cybercrime meliputi tindak pidana yang berkenaan dengan sistem informasi baik system informasi itu sendiri juga sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya.

Jenis-Jenis *Cybercrime*

Cybercrime menjadi beberapa jenis yaitu :

1. *Unauthorized Acces to Computer System and Service*

   Yaitu sebuah perbuatan kejahatan yang dilakukan dengan cara memasuki / menyusup kedalam suatu sistem jaringan komputer secara tidak sah,tanpa izin, atau tanpa sepengetahuan dari pemilik system jaringan yang di masuki Contoh : Hacking

2. *Illegal Content*

   Yaitu sebuah perbuatan kejahatan dengan memasukkan data atau informasi ke internet tentang sesuatu hal yang tidak benar, tidak etis dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Contoh : Pornografi , pencemaran nama baik.

2. *Data Forgery*

   Yaitu sebuah perbuatan Kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet Contoh : Phising

Pengertian *Phising*

Phising ysaitu suatu tindakan untuk memperoleh informasi pribadi seperti User ID, PIN, nomor rekening bank, nomor kartu kredit Anda secara tidak sah. Informasi ini kemudian akan dimanfaatkan oleh pihak penipu untuk mengakses rekening, melakukan suatu penipuan kartu kredit atau memandu nasabah agar melakukan perbuatan transfer ke rekening tertentu dengan iming-iming sebuah hadiah[1]. Aksi ini semakin marak terjadi. Tercatat secara global, jumlah penipuan bermodus phising selama Januari 2005 bertambah samapai denagan 42% dari bulan sebelumnya. Anti-Phishing Working Group (APWG) dalam laporan bulanannya, mencatat bahwa ada 12.845 e-mail baru dan unik serta 2.560 situs palsu yang digunakan sebagai sarana phishing.

Selain terjadi peningkatan kuantitas, kualitas serangan pun juga mengalami kenaikan. Artinya, situs-situs palsu itu ditempatkan pada server yang tidak menggunakan protokol standar sehingga terhindar dari pendeteksian

Teknik umum yang sering digunakan oleh penipu yaitu dengan cara:

Penggunaan alamat e-mail palsu dan grafik agar menyesatkan Nasabah sehingga Nasabah terpancing untuk menerima keabsahan e-mail atau web sites. Supaya terlihat meyakinkan, pelaku juga sering memanfaatkan logo dan merk dagang milik lembaga resmi, seperti; bank atau penerbit kartu kredit. Pemalsuan ini dilakukan supaya memancing korban untuk memberikan data pribadi, seperti; password, PIN dan nomor kartu kredit

Membuat situs palsu yang sama persis dengan situs resmi.atau . pelaku phishing mengirimkan e-mail yang berisikan link ke situs palsu tersebut.

Membuat hyperlink ke web-site palsu atau menyediakan form isian yang ditempelkan pada e-mail yang dikirim.

Berikut 10 tips untuk mencegah serangan phising:

1. Untuk situs sosial seperti Facebook, buat bookmark untuk halaman login atau mengetik URL www.facebook.com secara langsung di browser address bar.
2. Jangan mengklik link pada pesan email.
3. Hanya mengetik data rahasia pada website yang aman.
4. Mengecek akun bank Anda secara regular dan melaporkan apapun yang mencurigakan kepada bank Anda.
5. Kenali tanda giveaway yang ada dalam email phising:
    - Jika hal itu tidak ditujukan secara personal kepada anda.
    - Jika anda bukan satu-satunya penerima email.
6. -Jika terdapat suatu kesalahan ejaan, tata bahasa atau sintaks yang buruk atau kekakuan lainnya dalam penggunaan bahasa. Biasanya ini dilakukan penyebar phising untuk mencegah filtering.
7. Menginstall software untuk kemanan internet dan tetap mengupdate antivirus.
8. Menginstall patch keamanan.
9. Waspada terhadap email dan pesan instan yang tidak diminta.
10. Berhati-hati ketika login yang meminta hak Administrator. Cermati alamat URL-nya yang ada di address bar.
11. 10.Back up data anda.

CONTOH KASUS *PHISING*

1.Phising,pada E-Banking BCA

Pada tahun 2001, internet banking diributkan oleh kasus pembobolan internet banking milik bank BCA, Kasus ini dilakukan oleh seorang mantan mahasiswa ITB Bandung dan merupakan suatu karyawan media online (satunet.com) yang bernama Steven Haryanto. Anehnya Steven ini bukan Insinyur Elektro ataupun Informatika, akan tetapi Insinyur Kimia. Ide ini timbul ketika Steven pernah salah melakukan suatu pengetikkan alamat website. Kemudian dia membeli domain-domain internet dengan harga sekitar US$20 yang menggunakan nama dengan kemungkinan orang-orang salah mengetikkan dan tampilan yang sama persis dengan situs internet banking BCA.

Kemudian dia membeli domain-domain internet dengan harga sekitar US$20 yang menggunakan nama dengan kemungkinan orang-orang salah mengetikkan dan tampilan yang sama persis dengan situs internet banking BCA, http://www.klikbca.com , seperti:

wwwklikbca.com

kilkbca.com

clikbca.com

klickbca.com

klikbac.com

Orang tidak akan menyadari bahwa dirinya telah menggunakan situs aspal tersebut dikarenakan tampilan yang disajikan serupa dengan situs aslinya.(Afifah, 2018) Hacker ini mampu mendapatkan User ID dan password dari suatu pengguna yang memasuki situs aspal tersebut, namun hacker tersebut tidak bermaksud melakukan suatu tindakan criminal seperti mencuri dana nasabah, hal ini murni dilakukan atas suatu keingintahuannya mengenai seberapa banyak orang yang tidak sadar menggunakan situs klikbca.com, Sekaligus menguji tingkat keamanan dari situs milik BCA tersebut.

Steven Haryanto dapat disebut sebagai hacker, karena dia telah mengganggu suatu system milik orang lain, yang dilindungi privasinya. Sehingga tindakan Steven ini disebut sebagai hacking.(Michael, 2018) Steven dapat digolongkan dalam tipe hacker sebagai gabungan white-hat hacker dan black-hat hacker, dimana Steven hanya mencoba mengetahui seberapa besar tingkat keamanan yang dimiliki oleh situs internet banking Bank BCA. Disebut white-hat hacker karena dia tidak mencuri dana nasabah, tetapi hanya mendapatkan User ID dan password milik nasabah yang masuk dalam situs internet banking palsu. Namun tindakan yang dilakukan oleh Steven, juga termasuk black-hat hacker karena membuat situs palsu dengan diam-diam mengambil data milik pihak lain. perbuatan yang dilakukan Steven antara lain scans, sniffer, dan password crackers.

Karena perkara ini kasus pembobolan internet banking milik bank BCA, sebab dia telah mengganggu suatu system milik orang lain, yang dilindungi privasinya dan pemalsuan situs internet bangking palsu. Maka perkara ini bisa dikategorikan sebagai perkara perdata. Melakukan kasus pembobolan bank serta telah mengganggu suatu system milik orang lain, dan mengambil data dari pihak orang lain yang dilindungi privasinya artinya mengganggu privasi orang lain dan dengan diam-diam mendapatkan User ID dan password milik nasabah yang masuk dalam situs internet banking palsu.

Hukuman dan Undang-Undang Yang Diberikan Kepada Pelaku Phising

Undang-Undang Nomor 11 Tahun 2008 Tentang Internet dan Transaksi Elektronik (ITE)

1. Pasal 27 UU ITE Tahun 2008
2. Pasal 28 UU ITE Tahun 2008
3. Pasal 29 UU ITE Tahun 2008
4. Pasal 30 UU ITE Tahun 2008
5. Pasal 33 UU ITE Tahun 2008
6. Pasal 34 UU ITE Tahun 2008
7. Pasal 35 UU ITE Tahun 2008

Kitab Undang-Undang Hukum Pidana

1. Pasal 362 KUHP yang dikenakan untuk kasus *carding*
2. Pasal 378 KUHP dapat dikenakan untuk penipuan
3. 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 yang diinginkannya
4. Pasal 311 KUHP dapat dikenakan untuk kasus pencemaran nama baik dengan menggunakan media internet
5. Pasal 303 KUHP dapat dikenakan untuk menjerat permainan judi yang dilakukan secara online di Internet dengan penyelenggara dari Indonesia
6. Pasal 282 KUHP dapat dikenakan untuk penyebaran pornografi
7. Pasal 282 dan 311 KUHP dapat dikenakan untuk kasus penyebaran foto atau film pribadi seseorang
8. Pasal 406 KUHP dapat dikenakan pada kasus deface atau hacking yang membuat system milik orang lain.

Penutup

Kesimpulan

Dari hasil penulisan diatas kami dapat mengambil kesimpulan sebagai berikut :

1. *Cybercrime* kejahatan dunia maya atau internet yang sangat merugikan bagi pihak yang menggunakan internet
2. *Cybercrime* adalah kejahatan yang dapat merusak atau mengambil data-data rahasia penting
3. *Phising* adalah tindakan memperoleh informasi pribadi sperti User ID, PIN, nomor rekening bank, nomor kartu kredit Anda secara tidak sah
4. Kejahatan *phising* ini lebih ditujukan untuk pemalsuan juga pencurian data-data maupun dokumen-dokumen penting baik di instansi pemerintahan maupun perusahaan swasta
5. Kejahatan *phising* berpengearuh terhadap resiko kemanan Negara yang dapat merugikan masyarakat dan Negara

Daftar Pustaka

Afifah, W. (2018). *eksistensi perlindungan hukum*. *14*.

Hadi, S. (2018). HUKUM POSITIF DAN THE LIVING LAW (Eksistensi dan Keberlakuannya dalam Masyarakat). *DiH: Jurnal Ilmu Hukum*. https://doi.org/10.30996/dih.v0i0.1588

Michael, T. (2018). LAW ENFORCEMENT THROUGH 'LUDRUK' AND CULTURAL ADVANCEMENT. *Asia Pacific Fraud Journal*. https://doi.org/10.21532/apfj.001.18.03.01.15

Michael, T. (2019). PERMASALAHAN HUKUM DALAM PERATURAN WALIKOTA SURABAYA NOMOR 21 TAHUN 2018 TENTANG TATA CARA PENYELENGGARAAN REKLAME. *DiH Jurnal Ilmu Hukum Volume 15 Nomor 1 Februari 2019 – Juli 2019*, *15*(1), 79–86.

Raissa, A., Sukendar, A. Y. S., & Michael, T. (2018). MENUMBUHKEMBANGKAN SIKAP KRITIS DAN TOLERANSI SISWA MELALUI PENINGKATAN PENGETAHUAN SISWA TENTANG ILMU NEGARA. *JMM (Jurnal Masyarakat Mandiri)*. https://doi.org/10.31764/jmm.v0i0.1337