BAB II

TEKNIK PELAKU PRAKTIK PHISING DALAM *GAME ONLINE* TERHADAP *CYBER CRIME*

2.1 C*yber Crime* Dalam Bentuk Phising

Phising (password harvesting fishing) adalah tindakan penipuan yang menggunakan email palsu atau situs website palsu yang bertujuan untuk mengelabui pengguna sehingga pelaku bisa mendapatkan data pengguna tersebut.[28] Penipuan ini berupa sebuah email yang seolah-olah berasal dari sebuah perusahaan resmi, misalnya bank dengan tujuan untuk mendapatkan data-data pribadi seseorang, seperti kata sandi, nomor rekening, nomor kartu kredit, dan sebagainya**.**

Terjadinya phising dilakukan saat seseorang menyamar sebagai orang lain yang menggunakan situs web palsu, untuk mengelabui korban agar berbagi informasi pribadi. Tindakan phising biasa dilakukan dengan cara penyerang mengirimkan email yang seolah-olah berasal dari bank atau layanan web terpercaya yang biasa digunakan korban. Subjek email phising tersebut biasanya berisi "Harap perbarui informasi anda di bank!" Email tersebut akan berisi tautan phising yang seakan mengarahkan korban ke situs website resmi, yang mana sebenarnya akan mengarahkan korban ke situs web penipu. Pada website phising korban akan diminta untuk masuk dan tanpa sengaja mengungkapkan nomor rekening bank, nomor kartu kredit, sandi atau informasi sensitif lainnya kepada penipu.[29]

---

[28] Vyctoria, 2013, "Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding", (Yogyakarta:CV Andi Offset, h. 214.

[29] Min Li Chan dkk, (4 September 2022), "20 Topik Penting Seputar Peramban dan Dunia Web", dalam http://www.20thingsilearned.com/in-ID/malware/1.

Menurut IGN Mantra dosen peneliti cyber war dan security inspection menjelaskan bahwa phising adalah percobaan penipuan menggunakan surel (surat elektronik) yang bertujuan untuk mendapatkan username, kata sandi, token, dan informasi-informasi sensitif lainnya yang dikirim melalui surat elektronik. Email phising datang seolah-olah dari perusahaan atau organisasi di mana user adalah anggota atau member.[30]

Pelaku phising dikenal dengan sebutan phiser. Apabila seorang phiser mengirimkan email kepada seribu orang korban dengan dalih update informasi data konsumen maka dari keseluruhan angka tersebut, 5 % saja yang merespon maka phiser telah berhasil mendapatkan data dari 50 orang. Hal ini bisa terjadi karena phiser juga berdalih apabila tidak dilakukan perubahan data maka *user account* akan dihapus sehingga tidak bisa digunakan lagi. Pengguna yang menjadi korban yang tidak tahu modus penipuan ini tentu akan takut akun mereka dihapus oleh pihak bank sehingga tanpa pikir panjang langsung memberikan informasi rekening termasuk username dan kata sandinya. Pada kebanyakan kasus phising, teknik yang digunakan adalah perubahan data, termasuk di dalamnya kata sandi dan nomor kartu kredit[31]

Modus penipuan yang paling banyak ditemui saat ini adalah usaha phising melalui SMS pada telepon seluler, yang mana sudah banyak korban yang terkena penipuan phising dan harus kehilangan uangnya karena diminta untuk melakukan

[30] IGN Mantra, "Potensi Ancaman Keamanan Email Perusahaan", Info Komputer, h. 71.
[31] Vyctoria, 2013, "Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding", CV Andi Offset, Yogyakarta, h. 215.

transaksi ke rekening tertentu dengan berbagai alasan yang seolah-olah masuk akal sehingga menjebak korban.[32]

Tindakan phising biasanya memanfaatkan email, website palsu, software dan berbagai media lainnya untuk melakukan aksinya. Beberapa faktor yang menyebabkan aksi phising ini terus terjadi dan memakan banyak korban adalah sebagai berikut[33]

1. Kurangnya pengetahuan korban akan teknologi komputer membuat pelaku phising mudah mendapatkan informasi pribadi korbannya. pelaku phising akan memberikan email yang berisi pesan menakutkan, seperti ancaman hilangnya nama domain akan membuat korbannya segera melakukan apa yang diminta.
2. Ketidaksadaran pengguna yang masih awam terhadap tampilan palsu yang menyesatkan. Hal tersebut dilakukan dengan cara copy dan paste, maka sebuah website yang mirip dengan asli akan langsung tercipta. Pelaku phising akan membuat website yang tampak sangat bagus dan mirip dengan aslinya dengan berbagai komentar pengguna yang semuanya fiktif untuk meyakinkan calon korbannya.
3. Kurangnya keamanan terhadap pesan palsu. Sangat sering, pesan-pesan yang muncul tidak dibaca oleh pengguna. Pada umunya pesan phising terlihat terlalu teknis untuk pengguna awam sehingga korban akan selalu mengklik tombol “OK” untuk melanjutkan.

[32] Richardus Eko Indrajit, 2014*, Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, Graha Ilmu, Jakarta, Hal. 116.

[33] S’to, Certified Ethical Hacker 400% Illegal, (t.tp.: Jasakom, 2011), h. 146.

> Kebiasaan semacam ini akan membawa keuntungan tersendiri untuk pelaku phising sehingga mereka bisa memalsukan website dan mendapatkan informasi berharga yang dimasukkan oleh korbannya.

2.2 *Cyber Crime* Dalam Bentuk Phising Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Atas Perubahan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik

Indonesia memiliki undang-undang cyber pertama yang disusun oleh kementrian komunikasi dan informatika dan disetujui oleh Dewan Perwakilan Rakyat pada 25 Maret 2008 yakni Undang-undang Nomor 11 Tahun 2008 yang mengalami perubahan menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. Dengan diberlakukannya undang-undang ini, maka berbagai jenis tindakan kriminal di dunia maya dapat dikenakan sanksi secara perdata maupun pidana[34]

Kriminalisasi cybercrime dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik terdiri dari rumusan tindak pidana dan rumusan sanksi pidana. Adapun mengenai kata-kata hukuman, perbuatan-perbuatan pokok pada dasarnya sesuai dengan ketentuan KUHP dan terbatas pada dunia maya. Sedangkan dalam hal sanksi pidana pada dasarnya terdapat pemberatan sanksi dibanding KUHP, selain itu juga diatur mengenai kejahatan korporasi.[35]

---

[34] Richardus Eko Indrajit, 2014, *Konsep dan Strategi Keamanan Informasi di Dunia Cyber*, Graha Ilmu, Jakarta, h. 14.

[35] Budi Suhariyanto, 2019, "Cybercrime- Urgensi Pengaturan Dan Celah Hukumnya" Rajawali Pers, Jakarta, h. 181.

Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik terdapat Pasal yang menyimpan ancaman sanksi pidana bagi pelanggarnya, yakni mulai dari Pasal 27 sampai dengan Pasal 37. Hal-hal yang dikenakan dengan sanksi pidana antara lain adalah

1. Perbuatan mendistribusikan, mentransmisikan, dan/atau membuat dapat diakses informasi elektronik dan/atau dokumen elektronik yang memiliki muatan:

    a. Melanggar kesusilaan;
    b. Perjudian;
    c. Pemerasan dan/atau pengancaman (ditujukan untuk umum);

2. Perbuatan menyebarkan:

    a. Berita bohong dan menyesatkan sehingga merugikan konsumen dalam transaksi elektronik;
    b. Rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan SARA;

3. Perbuatan mengirim pesan ancaman kekerasan dan/atau menakutnakuti pribadi tertentu;
4. Perbuatan sengaja dan tanpa hak mengakses komputer dan/atau sistem elektronik pihak lain;

5. Perbuatan sengaja dan tanpa hak mengintersepsi atau menyadap informasi elektronik dan/atau dokumen elektronik milik orang lain;
6. Perbuatan sengaja dan tanpa hak mengubah, menambah, mengurangi, merusak, menghilangkan, memindahkan, atau menyembunyikan informasi elektronik dan/atau dokumen elektronik milik orang lain;
7. Perbuatan sengaja dan tanpa hak mengganggu sistem elektronik, sehingga sistem tersebut tidak dapat bekerja sebagaimana mestinya;
8. Perbuatan sengaja dan tanpa hak memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki perangkat keras atau perangkat lunak komputer yang dirancang khusus untuk memfasilitasi perbuatanperbuatan pidana yang telah disebutkan di atas; dan
9. Perbuatan sengaja dan tanpa hak memanipulasi informasi elektronik dan/atau dokumen elektronik agar dinilai seolah-olah otentik.

Cybercrime merupakan suatu kejahatan tindak pidana yang sulit terdeteksi. Tidak seperti kebanyakan kejahatan konvensional, korban kejahatan pada umumnya tidak menyadari bahwa mereka adalah korban. Pada dasarnya korban mengetahui bahwa ia adalah korban akan tetapi korban percaya bahwa hukum saat ini tidak dapat menahan pelaku. Selain itu pengetahuan penegak hukum tentang perkembangan teknologi tidak dapat menentukan perkembangan yang diperkirakan. Oleh sebab itu, korban biasanya tidak akan mengajukan laporan, serta

korban juga menganggap pembuktian telah terjadi kejahatan di depan pengadilan sangatlah sulit.[36]

2.3 Analisis Kasus Cyber Crime Dalam Bentuk Phising Di Indonesia

Kasus cybercrime dalam bentuk phising dilakukan dengan cara menyabotase fasilitas internet. Hal tersebut dilakukan dengan cara membuat beberapa nama situs pelesetan yang mirip situs aslinya. Adapun nama situs pelesetan yang dibuat peretas yaitu kilkgame.com, wwwklikgamea.com, clikgamecom, klickgame.com dan klikgame.com.

Oleh sebab itu apabila nasabah yang menggunakan fasilitas Internet gamer online salah dalam mengetik nama situs resminya (klikgameonline.com) seperti lima nama situs pelesetan tersebut, maka nasabah atau korban akan dibawa pada situs palsu buatan peretas tadi, selanjutnya korban akan tertarik pada hadiah yang ditawarkan oleh penipu, sementara itu data pribadi milik gamer akan terekam di situs palsu tersebut.[37]

Tindakan dari pelaku phising tersebut tidak bertujuan untuk menarik keuntungan, tetapi hanya untuk menguji kemampuannya dan mengukur berapa banyak pengguna internet yang akan terjebak ke situs buatannya. Pada konteks sistem hukum pidana tindakan pelaku phising sudah dapat dimasukkan sebagai tindak pidana oleh sebab itu pelaku dapat dipidana.

---

[36] Niniek Suparni, 2009, "Cyberspace Problematika & Antisipasi Pengaturannya", Sinar Grafika, Jakarta, h. 122.

[37] Majalah Tempo, (24 Juni 2001), "Rubrik Teknologi Informasi", dikutip dari Dikdik M. Arief.

Kasus cybercrime dalam bentuk phising yang terbaru adalah pencurian yang dilakukan oleh seorang hacker yang berasal dari Ukraina, hacker tersebut berhasil mengambil uang senilai 130 miliar rupiah dari 300 rekening nasabah bank di Indonesia. Peretas asal ukraina tersebut melakukan tindakan kejahatannya dengan cara memanipulasi website internet banking, sehingga pengguna aplikasi yang login pada website internet banking palsu ini dapat terekam identitas prinadinya. Transaksi yang dilakukan oleh nasabah tidak sesuai dengan yang diinginkan oleh nasabah, melainkan diarahkan kepada rekening orang lain yang telah bekerja sama dengan peretas, karena peretas berasal dari luar negeri sehingga tidak dapat membuka rekening Indonesia[38]

Beberapa penyebab utama terjadinya *cyber crime* di Indonesia antara lain akses di dalam internet yang tidak terbatas, pengguna internet yang ceroboh, kurangnya pengetahuan terhadap *cyber crime* itu sendiri, serta tingkat keamanan dan resiko yang rendah sehingga implementasinya cukup mudah. Dapat dikatakan bahwa masyarakat Indonesia masih kekurangan wawasan terhadap bahaya *cyber crime* yang memudahkan pelaku untuk mengakses atau merusak sistem computer.

Untuk mengatasi masalah kejahatan di dalam internet, setiap negara dapat menerapkan hukum positifnya sendiri. Hal ini didasarkan bahwa teori yurisdiksi negara dapat dikembangkan lebih lanjut untuk menangkap pelaku *cyber crime* mengingat ruang cyber dipandang sebagai bentuk perluasan lingkungan hidup manusia, sehingga Indonesia berhak mengadili tindak pidana yang dilakukan di

[38] Idr, (14 April 2015),"Hacker Sedot Rp 130 Miliar dari Rekening 300 Nasabah", Jawa Pos, h. 1.

dalam atau di luar Negara Indonesia apabila dianggap merugikan keamanan dan kepentingan Negara.[39]

Dalam merumuskan tindak pidana phising atau *cyber crime*, di Indonesia terdapat dasar hukum sebagai acuan untuk menetapkan tindak pidana phising yang sebagaimana diatur dalam UU ITE dijelaskan pada Pasal 27 sampai Pasal 37 dan KUHP yang terdapat pada Pasal 378, Pasal 263 dan Pasal 362 KUHP. Pada Pasal 378 KUHP tentang penipuan yang berbunyi :

"Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang dikenakan karena penipuan dengan pidana paling lama empat tahun."

Maka dari itu unsur-unsur yang terdapat dalam Pasal 378 KUHP dapat dikatakan sebagai salah satu acuan dalam menjatuhi pidana phising itu sendiri.

2.4 Praktik Phising Dalam *Game Online* Termasuk *Cyber Crime*

Game online menghubungkan kita dengan orang – orang di seluruh dunia, tetapi juga memaparkan kita terhadap resiko keamanan *cyber* seperti serangan phising, virus, dan pencurian identitas. Resiko ini dapat menyebabkan kerugian yang mempengaruhi kita secara individu atau organisasi dan bisnis yang terhubung dengan kita. Dalam game online serangan phising ini bertujuan untuk mendapatkan

[39] Ayu Putriyanti, 2009, "Yurisdiksi di Internet/Cyberspace", 9 *Media Hukum*. h. 15.

akses ke akun game milik korban yang di manfaatkan untuk mencuri barang berharga game, karakter dalam game, uang virtual, item virtual, dan inventaris lainnya. Terkadang, serangan ini mengambil alih dan menjual akun korban di pasar gelap. Dalam beberapa kasus, pelaku phising menggunakan informasi keuangan korban lebih jauh untuk melakukan pembelian dari akun korban tanpa sepengetahuan atau izin dari korban.

Phising merupakan suatu bentuk kejahatan dunia maya yang menggunakan email, telepon atau pesan teks yang menyamar sebagai badan resmi yang bertujuan untuk mengambil identitas pribadi korban. Misalnya pada perusahaan keamanan Kaspersky telah menemukan adanya 260 halaman phishing yang menawarkan kesempatan untuk memenangkan item baru game PUBG. Hal ini biasanya dilakukan dengan memanfaatkan *moment* tertentu contoh pada game PUBG, setiap 2 bulan sekali akan ada pergantian *season*. Dalam season baru PUBG, akan ada sesuatu yang baru seperti *item*, *skin*, tema, dan *update* lainnya. Tencent selaku developer game PUBG selalu memberikan hadiah seperti *battle point* dan *item* secara cuma – Cuma. Hal ini yang dimanfaatkan oleh para pelaku phising untuk mendapatkan keuntungan.

Cara kerja pelaku phising adalah dengan membagikan link yang seolah – olah resmi dari platform game tersebut melalui profil media sosial seperti Twitter atau Facebook untuk mendapatkan hadiah (Gambar .1). Ketika para korban tergiur, otomatis mereka akan *click* link tersebut dan di wajibkan mengisi *username* dan *password* akun platform game. Setelah pengguna mengisi, akan muncul notifikasi bahwa proses *entry* gagal pengguna diminta untuk memberikan informasi tambahan

seperti nama lengkap, email pribadi, nomor telepon, dan informasi tambahan lainnya. Akibatnya pelaku phising tidak hanya mendapatkan akun game korban saja, tetapi juga detail pribadi lainnya. Hal ini bertujuan untuk mendapatkan keuntungan dengan cara menjual akun game milik korban.[40]

Cara menanggulangi hal tersebut adalah :

1. Jangan tergiur untuk bergabung dalam undian apapun selain dari situs web game resmi.
2. Periksa informasi melalui sumber resmi. Apabila aktivitas terkait benar-benar ada, para pengembang game kemungkinan tidak akan merahasiakannya.
3. Menggunakan solusi keamanan yang dapat dipercaya yang tidak akan membiarkan anda mengunjungi halaman phising.

[40] Franedya, R. https://www.cnbcindonesia.com/tech/20201125105029-37-204456/peringatan-gamer-pubg-beredar-phising-berbahaya-pencuri-akun diakses pada 26 November 2022.

4. Gunakan situs web resmi untuk pembelian apapun yang terkait dengan game, jangan klik tautan yang mengarahkan ke situs web pihak ketiga.
5. Jangan tanggapi email atau permintaan pesan langsung yang meminta informasi perbankan, keuangan, atau data pribadi, meskipun terlihat seperti email resmi.
6. Jangan membagikan informasi pribadi, data identitas, atau informasi akun secara online.
7. Gunakan kata sandi yang kuat untuk login game dan menggantinya secara berkala.

2.5 Metode Dan Teknik Serangan Phising

Banyak cara yang dilakukan pelaku phising untuk mendapatkan korban dan hal ini biasanya terus berkembang sesuai dengan perkembangan yang ada di dalam dunia internet. Berikut beberapa cara yang populer digunakan adalah:

1. Email / SPAM

   Media yang paling favorit digunakan untuk mencari korban adalah email. Pelaku phising mengggunakan Email untuk penipuan dikarenakan murah dan mudah untuk digunakan. Pelaku phising dapat mengirimkan jutaan email setiap harinya tanpa perlu mengeluarkan biaya yang cukup besar. Selain itu pelaku phising juga suka menggunakan server-server bajakan untuk melakukan aksinya. Penggunaan email dalam tindakan phising dilakukan karena sangat mudah memalsukan email. Pelaku bisa mengubah *"From"* menjadi apa

saja karena memang tidak ada verifikasi di dalam email. Pelaku bisa membuat email dengan mengambil format dari email resmi agar lebih meyakinkan dan mengubah bagian-bagian yang diperlukan saja.

2. Web-baseddelivery

Selain menggunakan email pelaku phising juga memanfaatkan website dalam melakukan aksinya. Pelaku biasanya membuat website yang mirip dengan website-website terkenal untuk mengelabui korbannya. Membuat website yang mirip dengan website perusahaan besar sangatlah mudah untuk dilakukan karena pelaku hanya perlu membuat tampilan yang sama, tanpa perlu memperhatikan fungsi atau fasilitas yang sama karena tujuannya adalah agar korban memasukkan username dan password di dalamnya kemudian korban akan dibawa ke situs asli agar tidak curiga. Pelaku phising yang kreatif bahkan memanfaatkan banner dan media iklan resmi untuk mengelabui korbannya. Korban yang merasa mengklik iklan dari website resmi akan mengira website yang dikunjungi pantas untuk dipercaya, padahal hal ini tidak berhubungan sama sekali. Misalnya, anda melihat sebuah iklan di situs kompas yang tepercaya, tentunya anda tidak akan mengira website yang anda kunjungi mempunyai maksud buruk. Atas dasar kepercayaan semacam ini, pelaku phising tidak akan ragu-ragu memanfaatkan website-website ternama untuk melakukan aksinya.

3. IRC / Instant Messaging

Media chatting banyak digunakan oleh pelaku phising untuk mengirimkan alamat-alamat yang menjebak kepada korbannya. Biasanya pelaku mengirimkan tautan ini secara acak namun ada juga yang melakukan pendekatan terlebih dahulu sebelum mengirimkan informasi situs palsu ini.

4. Trojan

Pelaku phising, tak jarang melakukan tindakan menipu korbannya untuk menginstall trojan dan memanfaatkan trojan tersebut untuk mengelabui korbannya. Trojan sendiri memungkinkan pengontrolan secara penuh komputer korban sehingga korban bisa dialihkan ke situs yang telah disediakan jebakan.

Adapun menurut Vyctoria mengenai metode yang digunakan dalam phising adalah sebagai berikut[41]

1. Pelaku phising akan menggunakan alamat email palsu untuk menyesatkan nasabah sehingga nasabah terpancing menerima keabsahan email atau situs web. Untuk meyakinkan korban, pelaku phising akan menggunakan serta memanfaatkan logo atau merek dagang milik lembaga resmi, seperti bank atau penerbit kartu kredit. Pemalsuan ini dilakukan untuk memancing korban menyerahkan data pribadi (password, PIN, dan nomor kartu kredit).

[41] Vyctori, 2013, "Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding", CV Andi Offset, Yogyakarta, h. 122.

2. Membuat situs web palsu yang sama persis dengan situs web resmi. Bisa juga pelaku phising mengirimkan email yang berisi tautan ke situs web palsu tersebut.
3. Membuat hyperlink ke situs web palsu atau menyediakan formulir isian yang ditempelkan pada email yang dikirim. Serangan phising mengikuti perkembangan teknologi, oleh sebab itu di dalam dunia underground (kumpulan para hacker yang jahat), terdapat pasar gelap yang menjual berbagai program untuk melakukan aksi phising ini. Aksi phising juga sangat erat hubungannya dengan teknik hacking karena pelaku phising banyak memanfaatkan kelemahan-kelemahan yang ada untuk mengelabui korban.[42]

Adapun teknik serangan phising adalah sebagai berikut:

1. Man in the middle

   Dengan teknik ini peretas akan menempatkan dirinya diantara korban dan website resmi. Kemudian peretas akan menerima informasi data pribadi dari korbannya yang dapat dimodifikasi sesuai kebutuhan. Serangan man in the middle ini dapat terjadi dijaringan local maupun jaringan global.

2. URL Obfuscation

   URL (Uniform Resource Locator atau alamat web yang diketik dalam browser untuk membuka suatu website) Obfuscation adalah

[42] S'to, 2011, Certified Ethical Hacker 400% Illegal, Jasakom, h. 148.

Teknik penyamaran alamat URL agar tidak menimbulkan kecurigaan dari pengguna. Adapun macam-macamnya adalah sebagai berikut:

Rangkaian yang menyesatkan akan memanfaatkan rangkaian yang tampak asli seperti adanya kata-kata "Microsoft" atau kata-kata yang umum dikenal pada umumnya. Untuk memalsukan website "Microsoft" pelaku phising akan membuat direktori yang menggunakan kata "Microsoft" misalnya seperti http://XX.com/Microsoft.com /freelogin.php kemudian pelaku phising akan membuat halaman jebakan untuk mendapatkan username dan password atau informasi berharga lainnya.[43] Pelaku phising akan menggunakan tanda "@". Tanda keong (@) sebenarnya digunakan untuk website yang membutuhkan autentikasi di mana tanda sebelum tanda @ menunjukkan username, sedangkan setelahnya menunjukkan domain. Contoh sederhana pada email sto@jasakom.com. Nama yang mirip yang pernah menimpa situs klikbca.com ini akan membuat nama yang semirip mungkin dan memanfaatkan kelemahan pengguna yang suka salah ketik atau salah ingat. Sebagai contoh pada kasus klikbca.com, peretas bisa membuat website kilikbca.com, klickbca.com dan lain sebagainya.

Alamat palsu yang digunakan juga dibuat dengan tampilan yang sama persis dengan situs aslinya. Memanfaatkan nama yang mirip tidak

[43] Ibid, Hal. 149.

harus selalu memanfaatkan kesalahan ketikan, peretas juga bisa membuat nama domain yang tampak asli.

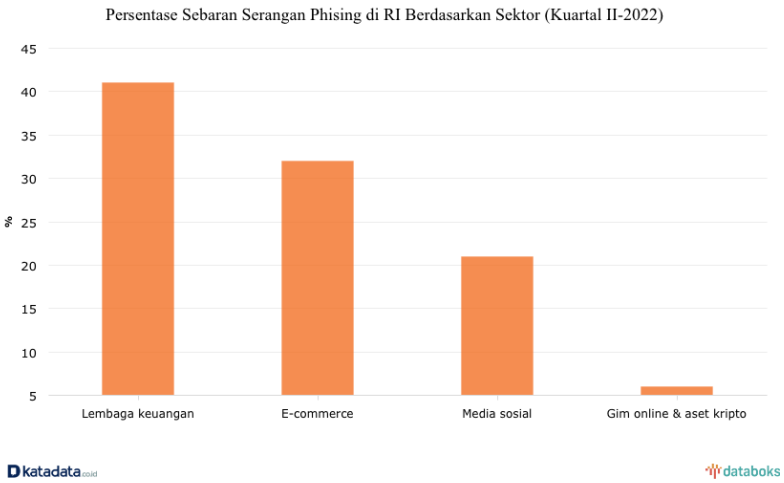
2.6 Analisis Lembaga Dan Media Yang Digunakan Oleh Pelaku Phising

Pada era modern saat ini, orang-orang tidak dapat dipisahkan dari sebuah gadget dan internet, apalagi media untuk mengakses ke dalam situs ataupun sosial media sangat mudah dijangkau. Maka dari itu setiap orang pasti memiliki salah satu akun media sosial seperti Facebook, Twitter, Instagram, Snapchat dan lain-lain, selain itu sosial media juga digunakan sebagai sarana berbisnis contohnya *online shop.* Hal ini yang dimanfaatkan oleh penjahat *cybe*r untuk mencari keuntungan dengan melancarkan aksinya melalui social media dengan cara phising. Banyak pengguna media sosial tidak memikirkan ancaman semacam itu. Mereka menganggap hal itu sebagai hal kecil dan tidak perlu dibesar – besarkan. Salah satu serangan penjahat cyber adalah memasang tautan palsu di akun media sosial dengan ajakan atau iklan yang sederhana dan menarik.[44]

Menurut laporan Direktorat Tindak Pidana Cyber Bareskim Polri, terdapat 5.579 kasus phising yang terjadi di Indonesia pada kuartal II tahun 2022. Jumlah kasus phising ini meningkat sebesar 41,52% dari bulan sebelumnya. Pada kuartal I tahun 2022 terdapat 3.942 kasus. Berdasarkan data tercatat kasus phising paling banyak menargetkan lembaga keuangan dengan presentase mencapai 41%.

[44] Mia Haryati Wibowo dan Nur Fatimah, 2017*, "Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime"*, JOEICT, Volume 1, No.1, h. 2

Selanjutnya, sebanyak 32% kasus phising menyerang *e-commerce*. Lalu sebanyak 21% kasus phising menargetkan media sosial. Sementara itu, hanya ada 6% kasus phising yang menargetkan pencurian data pada game online dan akun *cryptocurrentcy* (Gambar .2).[45]



Banyaknya laporan phising juga dipengaruhi oleh rendahnya tingkat kesadaran masyarakat. Sebagai negara berkembang, Indonesia masih tertinggal dalam mengikuti perkembangan teknologi informasi. Hal ini disebabkan strategi pengembangan teknologi yang tidak tepat karena mengabaikan riset sains dan teknologi. Alih teknologi dari negara industri maju tidak diikuti dengan kemampuan dalam penguasaan hal itu sendiri sehingga Indonesia menjadi negara yang tidak memiliki basis teknologi.[46] Selain itu, pelaku phising saat ini mungkin menggunakan lebih dari satu domain, sehingga menghasilkan lebih banyak laporan. Phising adalah kejahatan dunia maya dimana pelaku menyamar sebagai entitas

[45] Cindy Mutia Annur, https://databoks.katadata.co.id/datapublish/2022/08/23/ada-5-ribu-serangan-phising-terjadi-di-ri-pada-kuartal-ii-2022-ini-lembaga-yang-paling-banyak-diincar Diakses pada 28 November 2022.

[46] Nur Khalimatus Sa'diyah, 2012, "*Modus Operandi Tindak Pidana Cracker Menurut Undang-Undang Informasi Dan Trnsaksi Elektronik".* PERSPEKTIF, Volume 17, No.2, h. 80.

yang sah melalui email, nomor telepon, atau website untuk mengelabuhi orang agar memberikan informasi sensitive, seperti informasi pribadi, informasi kartu kredit dan perbankan, serta kata sandi. Informasi ini kemudian digunakan untuk mendapatkan akses ke akun penting yang dapat menyebabkan pencurian identitas dan kerugian finansial.

Salah satu contoh phising pada website yang mencakup iklan dan media sosial, salah satunya yaitu Facebook. Pelaku phising menggunakan halaman jebakan yang menyerupai web asli seperti tulisan www.facebook.com diubah menjadi www.faceb0k.com untuk mendapatkan username dan password atau informasi berharga lainnya (Gambar .3).

Berdasarkan survey oleh Facebook memperkirakan 8,7% dari akun yang berjumlah 83.090.000 akun adalah milik pengguna non-nyata, dan sekitar 1,5%

(14.320.0000) adalah akun yang secara tidak sengaja membagikan isi berbahaya seperti pesan spam dan link yang mencurigakan tanpa sepengetahuan pengguna. Sebagian besar serangan phising menggunakan server web yang diretas, dengan 73% situs web menjadi korbannya. Pada bulan Maret 2016 Gugus Tugas Anti-Phising mendeteksi 123.555 situs web phising. Sebanyak 15,7% warga Australia menjadi korban phising melalui situs belanja online dan 6,9% melalui media sosial.[47]

[47] Mia Haryati Wibowo dan Nur Fatimah, 2017, "*Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime"*, JOEICT, Volume. 1, No.1, h. 3.