JURNAL DIGITAL TEKNOLOGI INFORMASI
Vol. 06, No. 01, Meret 2023, pp. 29-34
E-ISSN 2714-9706 | P-ISSN 2686-4185
Terakreditas Sinta 5 oleh Dirjen Pendidikan Tinggi, Riset, dan Teknologi No. 164/E/KPT/2021

Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari

Purnamasari [a,1,*]; Tata Sutabri [a,2]
[a] Universitas Bina Darma, Jl. Jenderal Ahmad Yani No.3, 9/10 Ulu, Kecamatan Seberang Ulu I, Palembang dan Indonesia
[1] saribintizulfadli@gmail.com; [2] tata.sutabri@binadarma.ac.id
** Corresponding author*

Artikel Histori: Diterima 07/02/2023; Revisi 14/02/2023; Terbit 01/03/2023

Abstrak

Teknologi Jaringan Komputer dewasa ini berkembang hampir di seluruh belahan dunia. selain memberikan pengaruh positif perkembangan teknologi juga berdampak negatif. banyak oknum tidak bertanggung jawab yang memanfaatkan teknologi komputer untuk melakukan kejahatan. Kejahatan seperti ini dapat disebut dengan kejahatan dunia maya atau CybeCrime. Ada banyak jenis dan ragam kejahatan dunia maya, termasuk phishing. Phishing merupakan metode yang bertujuan untuk mendapatkan informasi seperti nama pengguna, kata sandi, dan informasi kartu kredit dengan berkamuflase sebagai perusahaan komunikasi elektronik terpercaya. Cara menghindari Kejahatan Phising yaitu melakukan Two Factor Authentication atau 2FA, Memastikan keamanan website yang dikunjungi dan email yang diterima, Menggunakan browser versi terbaru, Melakukan scan malware secara berskala, Memasang aplikasi pelindung Phising. Cara melawan dari serangan Phising yaitu PhishTank Site Checker, Google Safe Browsing, Web Of Trust, Verisign EV Green Bar, iTrustPage, Finjan Secure Browsing, FirePhish.

Kata Kunci: Cyber Crime, Kejahatan, Phising.

Pendahuluan

Teknologi jaringan komputer saat ini berkembang hampir di seluruh belahan dunia. Seiring dengan pesatnya perkembangan internet sebagai media penyedia informasi, muncullah dunia kedua yang bisa disebut ruang siber (cyber space). Berkat jaringan ini, segala macam informasi di dunia dapat diketahui 24 jam. Namun perkembangan teknologi informasi saat ini dipandang sebagai pedang bermata dua, karena selain berkontribusi terhadap peningkatan kemajuan, kesejahteraan dan peradaban manusia [1] [2].

Di sisi lain, teknologi informasi adalah sarana yang efektif untuk kegiatan ilegal. Banyak orang memanfaatkan internet untuk mencari keuntungan pribadi dengan menghalalkan segala cara, sekalipun merugikan orang lain. Kejahatan seperti ini bisa disebut cybercrime atau kejahatan dunia maya. Tindakan Cyber Crime perlu diperhatikan karena kejahatan ini sangat berbeda dengan kejahatan lainnya, biasanya Cyber contact antar pelaku dan korban kejahatan kriminalitas [3].

Ada banyak jenis dan ragam kejahatan dunia maya, termasuk phishing. Phishing merupakan metode mencoba mendapatkan informasi seperti nama pengguna, kata sandi, dan informasi kartu kredit dengan berpura-pura menjadi perusahaan komunikasi elektronik yang sah. Posting dari situs web terkenal, situs penjualan, pemroses pembayaran online, atau administrator TI sering kali digunakan untuk menarik perhatian yang tidak menaruh curiga. Informasi ini kemudian digunakan oleh penjahat untuk mengakses akun pengguna, menarik dana dari akun tersebut atau mentransfernya ke penjahat, atau melakukan pembelian online menggunakan kartu kredit orang lain. Berbagai cara digunakan untuk memenuhi keinginan penulis, yang paling umum adalah memikat seseorang dengan hadiah, membuat email dan situs website palsu yang terlihat seperti email asli dan situs web perbankan [4].

Cybercrime dimulai dengan aktivitas peretasan selama lebih dari satu abad. Pada tahun 1870-an, beberapa remaja menghancurkan sistem telepon negara yang baru lahir dengan mengubah otoritas.

Pada awal 1960-an, fasilitas universitas dengan komputer mainframe besar, seperti Lab Kecerdasan Buatan MIT, menjadi tempat berkumpulnya para peretas. Awalnya, istilah "peretas" memiliki konotasi yang baik untuk seorang ahli komputer yang dapat membuat program yang melampaui apa yang dirancang untuk itu [4].

Pada awal 1970-an, John Draper melakukan panggilan telepon jarak jauh gratis dengan meniupkan nada panggil yang benar ke dalam telepon, yang menginstruksikan sistem telepon untuk membuka saluran. Draper memandang peluit sebagai hadiah gratis di kotak sereal anak. Draper mendapat julukan "Captain

https://doi.org/10.32502/digital.v6i1.5620

P-ISSN : 2686-4185
E-ISSN : 2714-9706

Crunch" setelah berulang kali ditangkap karena merusak telepon pada tahun 1970. Gerakan sosial Yippie meluncurkan majalah YIPL/TAP (Youth International Party Line/Technical Assistance Program) untuk membantu peretas telepon atau "phreaks" untuk mendapatkan waktu luang yang lama panggilan jarak jauh.

Dua anggota Homebrew Computer Club di California mulai membuat "Blue Boxes", alat yang digunakan untuk meretas sistem telepon. Para anggota menggunakan pegangan "Berkeley Blue" (Steve Jobs) dan "Oak Toebark" (Steve Wozniak) dan kemudian mendirikan Apple Computer.

Pada awal 1980-an, penulis William Gibson menciptakan istilah "Cyberspace" dalam sebuah novel fiksi ilmiah berjudul Neuromancer. Dalam salah satu penangkapan peretas pertama, FBI menggerebek Markas Besar 414 di Milwaukee dan anggotanya menghancurkan 60 komputer dari Memorial Sloan-Kettering Cancer Center ke Los Alamos National Laboratory. Comprehensive Crime Contmrol Act memberikan yurisdiksi Secret Service atas penipuan kartu kredit dan komputer. Ada dua jenis kelompok peretas: Legion of Doom di Amerika Serikat dan Chaos Computer Club di Jerman.

Pada akhir 1980-an, Undang-Undang Penipuan dan Penyalahgunaan Komputer memberikan lebih banyak kekuasaan kepada otoritas federal. Tim Tanggap Darurat Komputer dibentuk oleh Badan Pertahanan Amerika Serikat yang berbasis di Universitas Carnegie Mellon di Pittsburgh, tujuan tim tersebut adalah untuk menyelidiki volume serangan pada jaringan komputer.

Kevin Mitnick, seorang peretas veteran selama 25 tahun, diam-diam memantau email karyawan keamanan di MCI dan Peralatan Digital. Kevin Mitnick dijatuhi hukuman satu tahun penjara setelah mengaku bersalah merusak komputer dan mencuri perangkat lunak.

Pada bulan Oktober 2008, sebuah virus baru bernama Conficker (juga disebut Downup, Downandup dan Kido) muncul dan diklasifikasikan sebagai virus jenis worm. Conficker menyerang Windows dan paling sering ditemukan di Windows XP. Microsoft merilis patch untuk menghentikan worm pada 15 Oktober 2008. Heinz Heise memperkirakan bahwa Conficker menginfeksi 2,5 juta PC pada 15 Januari 2009. The Guardian memperkirakan bahwa 3,5 juta PC telah terinfeksi. Pada 16 Januari 2009, worm telah menginfeksi sekitar 9 juta PC, menjadikannya salah satu infeksi dengan pertumbuhan tercepat dalam waktu singkat [4] [5].

Definisi Cyber Crime

Kata “cyber“ berasal dari “cyberneticcs” yaitu bidang ilmu yang menggabungkan robotika, matematika, elektronika dan psikologi. Didirikan oleh Nobert Wiener pada tahun 1948. Cybercrime (Cyber Cybercrime adalah istilah yang merujuk pada tindakan kriminal dengan menggunakan komputer atau jaringan komputer sebagai alat, target, atau TKP, baik yang menyerang ruang publik di Internet maupun ruang pribadi.

Sejarah Phising

Phising telah mengganggu dunia maya selama lebih dari 2 dekade, dimulai pada tahun 1995 dengan America Online (AOL) (James, 2006). Istilah phishing adalah variasi dari istilah memancing di mana tindakan phishing menyerupai penangkapan ikan dengan cara berikut: penyerang “memancing” korban menggunakan “umpan” dan “memancing” untuk informasi pribadi atau rahasia korban (James , 2006; McFedries, 2006; Khonji et al., 2013; Purkait, 2012). Studi komprehensif tentang definisi phishing dilakukan oleh Lastdrager (2014) di mana dia mengidentifikasi definisi phishing yang disepakati: “Phishing adalah tindakan penipuan yang dapat diskalakan di mana peniruan identitas digunakan untuk mendapatkan informasi dari target”.

Penyerang menggunakan berbagai saluran untuk menipu korban secara langsung dengan scam atau mengirimkan muatan melalui cara tidak langsung dengan tujuan untuk mendapatkan informasi pribadi atau rahasia dari korban (Ollmann, 2004).

Serangan phishing telah berkembang selama bertahun-tahun secara global dengan peningkatan sebesar 65% menjadi 1.220.523 pada tahun 2016 dibandingkan dengan tahun sebelumnya (APWG, 2017). APWG melaporkan peningkatan 5.753% dari serangan phishing rata-rata per bulan selama periode 12 tahun, dari 2004 hingga 2016. Pada 2015, lebih dari setengah miliar catatan pribadi dicuri, meningkat dibandingkan tahun sebelumnya (Symantec, 2016). Lab Kaspersky melaporkan bahwa phishing di sektor keuangan mencapai rekor tertinggi sepanjang masa pada tahun 2016 (Kaspersky, 2017). Antara periode Oktober 2013 hingga Februari 2016, FBI menerima laporan penipuan email bisnis dengan total kerugian sebesar $2,3 miliar (McCabe, 2016). Kerugian ini hanya melalui penipuan email bisnis saja dan tidak termasuk kerugian melalui penipuan phishing lainnya. Karena masalah phishing ini serius, menarik untuk mengetahui secara detail vektor serangan phishing saat ini. Informasi ini akan sangat berharga dalam pengembangan teknik anti-phishing serta untuk menciptakan kesadaran publik.

Dalam makalah ini, kami menyajikan survei terperinci tentang teknik phishing dan cara kerjanya. Keterkaitan antara media phishing, vektor atau saluran yang digunakan dan pendekatan teknis yang diterapkan dalam pelaksanaan operasi phishing dibahas. Interlink tersebut adalah (i) interlink antara media

phishing dan vektor dan (ii) interlink antara vektor dan pendekatan teknis. Tautan pertama menunjukkan elemen dalam media yang dieksploitasi dan digunakan dalam serangan phishing [7] [8].

Definisi Phising

Kata "phishing" yang muncul pada tahun 1996, banyak orang yang percaya bahwa kata tersebut berasal dari kata alternatif “memancing” serta “memancing Informasi" [9]. Phising juga dikenal dengan istilah “Brand Spoofing” atau “Carding” adalah variasi dari “memancing”, idenya adalah umpan dibuang dengan harapan sebagian besar akan mengabaikan umpan tersebut dan ada juga beberapa akan tergoda untuk menggigit umpan tersebut [10]. Menurut Felten et al (1997) spoofing sebagai “teknik yang digunakan untuk mendapatkan akses tidak sah ke komputer atau informasi, dimana penyerang berurusan dengan pengguna dengan berpura-pura menjadi terpecaya” [7].

Phising mengacu pada kejahatan diamana mengambil kata sandi milik orang lain. Phishing adalah salah satu bentuk Kejahatan. Phishing adalah bentuk phishing untuk memperoleh informasi contohnya kata sandi, nomor kartu kredit, dan lain-lain untuk mengelabui calon korban agar mengunduh file palsu yang terinfeksi atau terdapat virus dengan berkamuflase menjadi orang atau badan usaha tepercaya dalam intelijen komunikasi elektronik formal berupa email atau pesan singkat lainnya [9].

Perilaku ini bisa kapan saja terjadi di setiap saat. Di seluruh dunia, penipuan pada Januari 2005 adalah 42% lebih tinggi dari bulan sebelumnya. Kelompok Kerja (APWG) mengatakan dalam laporan bulanannya bahwa 12.845 email baru dan unik serta 2.560 situs palsu yang diperguanakan sebagai alat phishing. Seiring dengan peningkatan tersebut, tingkat serangan juga meningkat. Artinya, situs palsu dihosting di suatu sistem komputer yang tidak memiliki keamanan standar untuk menghindari deteksi [11].

Penggunaan komunikasi dimulai dari situs web sosial yang populer di mata publik, memproses transaksi pembayaran online atau di mana pengguna biasanya menggunakan situs tersebut untuk tujuan administratif, seperti situs perpesanan, situs jejaring publik, dan sebagainya.

Jenis phishing lainnya adalah pengiriman email resmi dan instant messenger, biasanya kepada pengguna situs yang sah dan situs perusahaan terkenal, dengan logo perusahaan, kop surat email resmi, bahkan stempel dan tanda tangan manajer perusahaan.

Tujuan dari phising ini ada beberapa cara yaitu:

a) Menangkap hanya akun pengguna dan kata sandi, bertujuan untuk mengeksploitasi data pengguna dan administrator.
b) Membagikan penawaran berupa penanaman modal palsu, yang bertujuan untuk menipu.
c) Membagikan informasi yang salah kepada calon korban yang bertujuan untuk membuat alasan buruk bagi perusahaan lain (kampanye hitam). Cara ini bisa dikatakan sebagai teknik sosial yang jarang digunakan oleh para seorang peretas namun sangat efektif untuk menimbulkan kesan negatif pada perusahaan pesaing [7].

Metode Penelitian

Pada penelitian ini menggunakan metode kualitatif penelitian kepustakaan (literature review). Metode ini digunakan untuk mengkaji sumber data dari studi, laporan dan dokumen, termasuk jurnal ilmiah, artikel dan publikasi lain yang terkait dengan topik penelitian. Penulis menggunakan beberapa sumber dalam penelitian ini, seperti buku dan artikel jurnal yang berkaitan dengan topik penelitian.

Hasil dan Pembahasan

Ciri-ciri Phising

a) Tautan tidak sama dengan halaman situs
   Phishing dapat dikirim melalui berbagai media. Jika Anda melihat link yang tidak sesuai dengan halaman website resminya, bisa dipastikan link tersebut adalah phising.
b) Tidak memiliki HTTPS
   HTTPS berfungsi untuk meningkatkan keamanan situs. Oleh karena itu hacker umumnya tidak menggunakan HTTPS.
c) Kirim melalui email atau nomor ponsel pribadi
   Ciri-ciri phishing juga bisa diketahui dengan menghubungi pengirimnya. Jika pengirim pesan menggunakan email atau nomor handphone pribadi, bisa dipastikan bahwa pesan tersebut adalah phising.

Kejahatan phising terdiri atas beberapa jenis yang wajib kamu ketahui, di antaranya:

a) Email Phising, Jenis phising ini akan menggunakan email - email palsu untuk mengelabui korbannya dengan email yang dikirim secara acak kepada calon korban. Pelaku akan membuat email dengan format menyerupai email asli dan resmi sehingga korban bisa percaya.

P-ISSN : 2686-4185
E-ISSN : 2714-9706

b) Web Phising, biasanya menggunakan media website palsu untuk menjerat calon korban. Di mana, pelaku akan membuat email dengan nama domain yang seolah-olah resmi atau juga disebut dengan domain spoofing.
c) Spear Phising, merupakan bentuk lain dari email phising dengan pelaku yang sudah memiliki data pribadi korban berupa nama dan alamat, nantinya akan berusaha mendapatkan informasi pribadi lanjutan dari korban.
d) Whaling, merupakan kejahatan phising dengan menargetkan orang-orang dalam kewenangan besar seperti manajer personalia, penanggung jawab suatu kegiatan, bahkan pemilik bisnis. Data korban dengan kewenangan besar tentunya akan menarik korban seperti perekrutan karyawan palsu [4].

Meski kasus phising sudah sering terjadi, tapi terkadang masih ada yang menjadi korbannya. Biasanya para korban dapat terkena tindak penipuan tersebut, karena lima penyebab ini.

a) Mudah percaya
Alasan pertama adalah korban mudah mempercayai sesuatu. Ini pertanda sangat buruk karena pelaku mengincar korban yang percaya penipuan mereka. Orang tepercaya akan memberikan informasi pribadi secara gratis. Praktik ini akan memudahkan pelaku dalam melakukan aktivitasnya.
b) Ceroboh dalam mengecek sesuatu
Salah satu contoh kejahatan yang sering terjadi adalah mengirim email, telepon atau SMS atas nama bank karena korban mudah ditipu. Ini sangat berbahaya jika korban ceroboh dengan fakta.
Jika korban memberikan data pribadinya secara bebas, kecil kemungkinan akan berdampak. Dalam hal ini, akses ke rekening bank korban akan mudah dilakukan.
c) Tergiur dengan penawaran
Penawaran tentang hadiah atau kupon biasanya terjadi melalui telepon, SMS atau email. Hal ini membuat banyak korban mudah tertipu oleh hal semacam ini.
Para korban seringkali begitu mudah tergoda oleh hadiah-hadiah ini sehingga mereka rela memberikan informasi pribadi. Dalam hal ini, phishing tidak dapat dihindari lagi.
d) Membuat password yang sangat lemah
Kejahatan phishing sering dilakukan melalui media sosial, salah satunya menyebarkan informasi bohong. Pasalnya, korban biasanya menggunakan opsi password yang lemah sehingga mudah ditebak. Jadi diperlukan kombinasi mulai dari huruf kecil, huruf besar, simbol dan angka yang kuat harus digunakan untuk memilih kata sandi. Dengan begitu, peretas tidak akan dapat memperoleh akses mudah ke akun media sosial korban.
e) Mengakses link website secara sembarangan
Phiser akan mengirim link website melalui pesan langsung, email, atau bahkan SMS. Calon korban harus mengetahui situs yang dikirimkannya.
Tidak cukup memasukkan situs web yang terlihat mencurigakan. Pasalnya, link web tersebut justru mengandung virus atau berpotensi menyerang akses media sosial.

Operasi phising dilakukan untuk menipu korban oleh phiser. Phisher akan melakukannya untuk menangkap korban. Phishing adalah tindakan untuk memperoleh informasi rahasia pengguna dengan menggunakan email palsu dan situs web yang berkamuflase sebagai situs web asli atau resmi. Informasi yang diperoleh atau diminta oleh phisher termasuk kata sandi akun atau nomor kartu kredit. Penipu menggunakan email, spanduk, atau pop-up untuk memikat pengguna ke situs web palsu di mana pengguna diminta untuk memberikan informasi pribadi. Disinilah para phisher memanfaatkan kelalaian dan kecerobohan website palsu untuk mendapatkan informasi.

Dibawah ini adalah beberapa bahaya yang ditimbulkan oleh virus phising:

a) Pemalsuan Link
Teknik phising menggunakan pemalsuan link agar terlihat seperti alamat organisasi yang sebenarnya. URL yang salah kata atau penggunaan subdomain adalah trik umum digunakan oleh phisher.
b) Filter Penghindaran
Phisher mengambil gambar (bukan teks) untuk mengelabui calon korban agar membocorkan informasi pribadi. inilah sebabnya mengapa Gmail atau Yahoo akan menonaktifkan gambar yang gagal [7].

Cara untuk menghindari kejahatan phising seperti berikut:

a) Melakukan Two Factor Authentication atau 2FA
Two Factor Authentication adalah langkah yang dapat ditempuh untuk melindungi akun. Dalam sistem ini, pemilik akun akan melakukan 2 step verifikasi untuk memastikan data-data yang ada di akun terjaga dengan aman. Selanjutnya setiap kali mengakses akun pengguna perlu memasukkan kode verifikasi terlebih dahulu.

b) Memastikan Keamanan Website yang Dikunjungi dan Email yang Diterima
Kejahatan phising umumnya dilakukan melalui web atau email sehingga cara ampuh untuk menghindari kejahatan ini yaitu dengan memastikan keamanan website yang dijelajahi serta email yang diterima. Selain itu, kamu bisa menghindarinya dengan tidak mengklik link sembarangan. Untuk mengecek keamanan email kamu bisa melakukan verifikasi kepada contact person yang biasanya ada di footer email. Kamu bisa mencari tahu terlebih dulu alamat resmi email seperti mencari alamat email resmi perusahaan. Untuk mengecek keamanan website sebaiknya kamu mengakses web yang menggunakan SSL, apalagi untuk melakukan pembayaran online.
c) Menggunakan Browser Versi Terbaru
Melakukan update pada browser bisa menjadi cara aman untuk menghindari kejahatan phising. Umumnya browser akan melakukan pembaharuan untuk memastikan keamanan setiap pengguna ketika berselancar di browser sehingga versi terbaru tentu memiliki keamanan yang lebih baik.
d) Melakukan Scan Malware Secara Berkala
Kejahatan phising dapat dilakukan melalui malware tanpa disadari bekerja untuk mengambil informasi pribadi dari perangkat yang kamu gunakan. Malware ini biasanya diunduh tanpa disadari sehingga kamu perlu membersihkannya di perangkat secara berkala.
e) Memasang Aplikasi Pelindung Phising
Saat ini sudah banyak penyedia aplikasi yang bisa melindungi kamu dari kejahatan phising. Pasang aplikasi dengan jaminan keamanan terbaik di perangkat yang digunakan. Kamu bisa mengunduh aplikasi keamanan phising di AppStore.

Cara paling populer untuk melawan dari serangan phising adalah dengan cara melacak situs di luar web yang dianggap sebagai situs phising. Dibawah ini adalah beberapa ekstensi browser yang dapat digunakan untuk melawan serangan phising.

a) PhishTank SiteChecker
SiteChecker menutup semua situs phising menurut data dari komunikasi PhishTank. Halaman pemblokiran ditampilkan saat mengunjungi situs web yang diidentifikasi PhishTank sebagai situs web phising.
b) Google Safe Browsing
Google Safe Browsing menampilkan peringatan saat situs web mencoba mengekstrak informasi pribadi atau informasi akun. dengan menggabungkan algoritme yang rumit dengan informasi di situs web palsu dari berbagai teknologi, Google Safe Browsing dapat dengan mudah mendeteksi saat mengunjungi situs web pemancing yang mencoba menyamar sebagai situs web asli.
c) Web of Trust
Web of Trust mengidentifikasi situs dengan menunjukkan kelebihan situs di browser dengan mengetahui kelebihan sebuah website, diinginkan akan lebih mudah meninggalkan situs phising. reputasi situs didasarkan pada testimonial dari komunikasi Web of Trust.
d) Verisign EV Green Bar
Ekstensi ini menambahkan validari sertifikat ke browser. Saat mengakses situs “secure”, maka address bar akan berwarna hijau dan menunjukkan pemegang sertifikat dan otomatis. Ekstensi ini berguna untuk mendeteksi situs web palsu.
e) iTrustPage
iTrustPage menangkal pengguna web mengisi formulir di situs web palsu. Saat mengawasii situs web yang memiliki halaman formulir. iTrustPage akan menghitung nilai dari TrustScore pada halam formulir tersebut untuk melihat apakah situs web tersebut dapat dipercaya atau tidak.
f) Finjan Secure Browsing
Finjan Secure Browsing memeriksa tautan dalam hasil pencarian dan memperingatkan terhadap tautan yang mungkin merupakan tautan phising. Finjan akan mencoba membaca kode ancaman dan skrip ancaman. Setelah itu akan ditandai hijau untuk tautan aman dan merah untuk tautan tidak aman.
g) FirePhish
FirePhish akan menampilakan peringatan pada saat mengawasi situs yang dianggap dengan situs phising atau terdapat kode dan skrip yang mencurigakan [7].

Simpulan

Kejahatan dunia maya (CyberCrime) merupakan tindakan yang berupa kriminal dimana jaringan komputer atau komputer menjadi alat, sasaran atau lokasi utnuk kejahatan. Baik menyerang fasilitas publik maupun milik pribadi. Phising adalah memancing untuk mengumpulkan kata sandi atau password. Phishing adalah bentuk phishing untuk memperoleh informasi contohnya kata sandi, nomor kartu kredit dan yang serupa untuk mengelabui orang agar mendownload dokumen palsu yang mengandung virus dengan

P-ISSN : 2686-4185
E-ISSN : 2714-9706

menyamar sebagai orang atau badan usaha terpecaya dalam komunikasi elektronik resmi, misalnya email atau lainnya yang berupa pesan singkat. Phiser mengeksploitasi kelemahan keamanan untuk menemukan rahasia yang digunakan untuk semua kejahatan.

Daftar Pustaka

[1] T. Sutabri, Pengantar Teknologi Informasi, 1 ed. Yogyakarta: Andi Offset, 2014.
[2] T. Sutabri, Analisis Sistem Informasi, 1 ed. Yogyakarta: Andi Offset, 2012.
[3] T. Sutabri, KOMPUTER Dan MASYARAKAT, 1 ed. Yogyakarta: Andi Offset, 2013.
[4] Z. Alkhalil, C. Hewage, L. Nawaf, dan I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” Front. Comput. Sci., vol. 3, hlm. 563060, Mar 2021, doi: 10.3389/fcomp.2021.563060.
[5] J. J. H. St, J. S. Sh, dan A. N. Sh, “Mengenal Dan Mengantisipasi Kegiatan Cybercrime Pada Aktifitas Online Sehari-Hari Dalam Pendidikan, Pemerintahan Dan Industri Dan Aspek Hukum Yang Berlaku,” 2014.
[6] E. Ketaren, “Cybercrime, Cyber Space, Dan Cyber Law,” no. 2, 2016.
[7] T. Penyusun, “‘Cyber Crime Dengan Metode Phising’”.
[8] K. L. Chiew, K. S. C. Yong, dan C. L. Tan, “A survey of phishing attacks: Their types, vectors and technical approaches,” Expert Syst. Appl., vol. 106, hlm. 1–20, Sep 2018, doi: 10.1016/j.eswa.2018.03.050.
[9] F. E. Purwiantono, “Model Klasifikasi Untuk Deteksi Situs Phising Di Indonesia,” 2017.
[10] V. K. Gandhi, “An Overview Study on Cyber crimes in Internet,” vol. 2, 2012.
[11] A. S. Gulo, S. Lasmadi, dan K. Nawawi, “Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik,” PAMPAS J. Crim. Law, vol. 1, no. 2, hlm. 68–81, Apr 2021, doi: 10.22437/pampas.v1i2.9574.