CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol. 11 No. 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

PHISHING SEBAGAI KEJAHATAN DUNIA MAYA: ANALISIS YURIDIS DAN UPAYA PENCEGAHANNYA

Alvita Apsari Azura[1], Monica[2], Ricky Banke[3]

[1,2,3]Program Studi Hukum, Fakultas Hukum Universitas Pelita Harapan Kampus Medan,
E-mail: 03051220019@student.uph.edu[1] , 03051220008@student.uph.edu[2],
ricky.banke@uph.edu[3]

Abstrak

Phishing merupakan salah satu bentuk kejahatan dunia maya (cyber crime) yang semakin marak terjadi akibat kemajuan teknologi informasi dan internet. Kejahatan ini tidak hanya menyasar sistem komputer, tetapi juga menargetkan data pribadi pengguna dengan berbagai metode penipuan, seperti email, SMS, hingga situs palsu yang menyerupai situs resmi. Motif dari kejahatan ini beragam, mulai dari pencurian data, keuntungan ekonomi, hingga penyalahgunaan identitas. Penelitian ini bertujuan untuk menganalisis aspek yuridis terhadap phishing di Indonesia serta mengevaluasi langkah-langkah preventif yang dapat dilakukan. Metode penelitian yang digunakan adalah pendekatan normatif dengan studi pustaka dari berbagai dokumen hukum dan literatur terkait. Hasil penelitian menunjukkan bahwa phishing dapat dikenai sanksi berdasarkan UU ITE, KUHP, dan beberapa undang-undang terkait lainnya seperti UU Telekomunikasi dan UU Hak Cipta. Selain itu, ditemukan bahwa dampak phishing terhadap korban mencakup kerugian finansial, kerusakan reputasi, dan trauma psikologis. Pencegahan yang dapat dilakukan meliputi edukasi digital, penggunaan autentikasi ganda (2FA), verifikasi sumber informasi, serta penerapan aplikasi keamanan. Diperlukan peningkatan kesadaran hukum dan literasi digital masyarakat untuk meminimalkan risiko menjadi korban phishing di era digital saat ini.

***Kata kunci**: Hukum siber, Kejahatan dunia maya, Phishing*

Abstract

Phishing is a form of cybercrime that has become increasingly prevalent due to the advancement of information technology and the internet. This crime does not only target computer systems but also aims at stealing users' personal data through various fraudulent methods such as emails, SMS, and fake websites that mimic official sites. The motives behind this crime vary, ranging from data theft and financial gain to identity misuse. This study aims to analyze the legal aspects of phishing in Indonesia and to evaluate preventive measures that can be taken. The research method used is a normative approach through literature review of various legal documents and related literature. The findings indicate that phishing can be subject to legal sanctions under the Electronic Information and Transactions Law (UU ITE), the Indonesian Criminal Code (KUHP), and several other relevant laws such as the Telecommunications Law and the Copyright Law. Furthermore, the impact of phishing on victims includes financial losses, reputational damage, and psychological trauma. Preventive measures that can be taken include digital education, the use of two-factor authentication (2FA), verification of information sources, and the implementation of security applications. Enhancing public legal awareness and digital literacy is essential to minimize the risk of becoming a phishing victim in today's digital era.

***Keywords**: Cyber crime, Cyber law, Phishing*

Article history
Received: April 2025
Reviewed: April 2025
Published: April 2025

Plagirism checker no 323
Doi : prefix doi :
10.8734/causa.v1i2.365
Copyright : author
Publish by : causa

CAUSA
ISSN 3031-0369

Jurnal Hukum dan Kewarganegaraan
Vol. 11 No. 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

PENDAHULUAN

Kemajuan teknologi di Indonesia telah mempengaruhi ke beberapa bidang salah satunya adalah penggunaan internet dan penggunaan media sosial. Penggunaan internet dan media sosial telah menjadi bagian dari hidup masyarakat. Internet dan media sosial membantu dari berbagai hal seperti meningkatkan komunikasi, akses informasi yang mudah didapatkan dan memperluas jaringan sosial. Lebih dari 170 juta pengguna *Facebook, Instagram, Twitter* dan lainnya yang menyebabkan Indonesia menjadi salah satu pengguna internet tertinggi di dunia, tetapi media sosial juga memiliki dampak negatif, salah satunya adalah faktor kurangnya literasi dalam media sosial. Banyak orang dalam masyarakat yang tidak memahami pemahaman tentang perlindungan diri di internet dan sering menjadi korban dalam jebakan pelaku kejahatan pelaku internet.

Secara umum, kita melihat hukum merupakan seluruh aturan tingkah laku yang tertulis maupun yang tidak tertulis yang mengatur tata tertib yang harus ditaati oleh Masyarakat berdasarkan keyakinan dan kekuasaan hukum. Hukum pada dasarnya harus mengikuti perkembangan zaman, agar dapat menindak atau menjangkau suatu perbuatan melawan hukum atau kejahatan. 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*”.Salah satu bentuk kejahatan *cyber* adalah *phishing*. *Phishing* merupakan sebuah bentuk kejahatan di dunia maya yang bertujuan untuk mencuri informasi dan data pribadi milik individu dengan menggunakan berbagai metode, seperti *email*, telepon, pesan teks, atau tautan yang tampaknya sah. Para pelaku *phishing* biasanya menyamar sebagai organisasi atau pihak yang terpercaya, seperti bank, penyedia layanan, atau bahkan teman dekat korban, untuk menipu mereka agar memberikan informasi sensitif. Tujuan utama dari tindakan ini adalah untuk memperoleh data pribadi yang dapat disalahgunakan.

Analogi dari serangan *phishing* dapat disamakan dengan "memancing" individu yang menjadi target oleh penyerang, yang dikenal sebagai phisher, melalui situs web palsu yang menyerupai dengan persis situs-situs terkenal dan resmi di dunia maya. Meskipun halaman-halaman ini memperlihatkan antarmuka pengguna yang mirip, situs *phishing* memiliki *Uniform Resource Locator* (URL) yang berbeda dari situs yang sah. Dengan meningkatnya aktivitas online, ancaman *phishing* menjadi semakin serius. *Phishing* merupakan bentuk ancaman yang berusaha mengakses informasi seperti login, identitas, kata sandi, dan detail kartu kredit. Metode phishing ini dapat mengambil informasi pribadi pengguna yang seharusnya tetap

rahasia, sehingga dapat jatuh ke tangan orang lain dan disalahgunakan. Apabila informasi kartu kredit berhasil diambil, maka dapat digunakan untuk bertransaksi sesuai dengan keinginan pelaku.

Secara lebih rinci, kata "*scam*" yang sering digunakan dalam konteks ini merujuk pada penipuan yang dilakukan dengan cara yang tidak lazim atau tidak standar, dan berasal dari istilah "memancing" atau "menggali." Dalam hal ini, para penipu atau scammers akan "merayu" korban mereka dengan berbagai trik atau janji palsu untuk mendapatkan data sensitif. Data yang dimaksud bisa berupa informasi yang sangat penting dan pribadi, seperti kata sandi akun, nomor kartu kredit, alamat email, serta kode OTP (*One-Time Password*) yang biasa digunakan untuk autentikasi di berbagai transaksi online. Data yang berhasil dicuri oleh pelaku *phishing* ini bisa dimanfaatkan untuk berbagai kejahatan, seperti pencurian identitas, pemerasan, atau bahkan penipuan finansial. Oleh karena itu, sangat penting untuk selalu berhati-hati dan waspada ketika melakukan transaksi di dunia maya, terutama dalam transaksi online yang melibatkan situs web perbankan atau platform yang menyimpan informasi pribadi. Sebaiknya, pastikan bahwa situs atau layanan yang digunakan adalah resmi dan terpercaya, serta selalu periksa kembali setiap pesan atau permintaan yang mencurigakan.

Serangan *Phishing* di Indonesia juga menjadi masalah yang cukup sering terjadi. Meskipun serangan *phishing* sering dikaitkan dengan negara-negara maju, kenyataannya serangan ini juga terjadi di negara-negara berkembang seperti Indonesia. Berdasarkan informasi yang diperoleh dari Indonesia *Anti-Phishing Data Exchange* (IDADX), jumlah pengaduan mengenai serangan *phishing* di Indonesia menunjukkan peningkatan yang cukup signifikan. Pada tahun 2023, IDADX mencatat adanya 26.675 laporan serangan *phishing* yang diterima, angka yang cukup besar dan menunjukkan betapa seriusnya ancaman ini di Indonesia. Dari laporan yang diterima, serangan *phishing* paling banyak terjadi pada bulan Februari dengan total aduan sebanyak 15.050 kasus. Angka ini jauh lebih tinggi dibandingkan dengan bulan Januari yang hanya mencatatkan sekitar 7.665 kasus dan bulan Maret yang tercatat 3.960 kasus. Meskipun jumlah laporan bervariasi setiap bulannya, tren peningkatan kasus *phishing* pada kuartal pertama tahun 2023 menunjukkan adanya potensi ancaman yang terus berkembang.

IDADX dalam analisis lebih lanjut juga mengidentifikasi beberapa *Second Level Domain* (SLD) yang paling sering menjadi target serangan *phishing* selama periode tersebut. Beberapa domain yang paling banyak diserang adalah id, biz.id, dan my.id. Domain-domain ini menjadi sasaran utama karena banyak digunakan oleh individu dan organisasi di Indonesia, sehingga menjadikannya target yang menguntungkan bagi para pelaku *phishing*. Data ini memberikan gambaran jelas tentang seberapa meluas serangan *phishing* di Indonesia dan pentingnya upaya untuk meningkatkan kesadaran dan perlindungan terhadap ancaman siber ini (Databoks.com, 2023).

METODE

Metode yang digunakan adalah metode penelitian normatif yang bertujuan untuk mengeksplorasi berbagai aspek terkait peraturan perundang-undangan dalam bidang cyber crime. Metode yang digunakan dalam pengumpulan data adalah dengan mengumpulkan berbagai dokumen, baik yang berbentuk tertulis maupun elektronik, seperti jurnal, artikel, makalah, dan sumber lainnya. Data yang terkumpul kemudian dianalisis, dibandingkan, dan diseleksi untuk disajikan dalam penulisan ini. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi, setidaknya bagi mereka yang berminat untuk lebih mendalami permasalahan cyber law yang berkembang di Indonesia.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol. 11 No. 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

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

Phishing merupakan bentuk kejahatan siber yang melibatkan penipuan untuk mendapatkan data sensitif. Pelaku biasanya mengirimkan email atau pesan yang tampak resmi, meminta korban untuk memberikan informasi pribadi. Adapun aspek hukum yang mengatur tentang *phishingI* di Indonesia:

1. Undang-Undang Nomor 1 Tahun 2024 Tentang Internet & Transaksi Elektronik (ITE) Sejak Undang-Undang Nomor 1 Tahun 2024 ini memiliki cakupan materi yang luas, yang mencakup berbagai hal terkait dengan dunia informasi dan teknologi digital. Secara umum, UU-ITE mencakup pengaturan mengenai informasi dan dokumen elektronik, mekanisme pengiriman dan penerimaan surat elektronik, penggunaan tanda tangan elektronik, pengaturan sertifikat elektronik, hingga pengelolaan dan penyelenggaraan sistem elektronik. UU ini juga mengatur hal-hal terkait dengan keabsahan hukum dari berbagai transaksi yang dilakukan secara elektronik, serta menjamin perlindungan terhadap data dan informasi yang bersifat pribadi dan sensitif di dunia maya.
   Dengan adanya UU-ITE ini, diharapkan dapat tercipta sebuah kerangka hukum yang jelas dalam mengatur segala bentuk transaksi elektronik, sekaligus memberi perlindungan bagi para pengguna teknologi informasi, baik itu individu, perusahaan, maupun negara. Selain itu, UU ini juga dimaksudkan untuk menanggulangi berbagai bentuk kejahatan yang dapat terjadi di dunia maya, seperti penipuan, penyebaran konten ilegal, serta penyalahgunaan teknologi informasi untuk tujuan yang merugikan pihak lain.
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 No 28 Tahun 2014 tentang Hak Cipta.
4. Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi
5. Undang-Undang No 32 Tahun 2002 tentang Penyiaran

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol. 11 No. 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Phishing sendiri memiliki banyak jenis dan teknik berbeda yang dilakukan oleh pelaku seperti:

1. Smishing
   Smishing adalah jenis *phishing* yang dilakukan melalui pesan teks (SMS), dan ini menjadi salah satu bentuk penipuan yang paling sering kita temui. Istilah "smishing" berasal dari gabungan kata "SMS" dan "*phishing*." Penipuan ini cukup mudah dilakukan, karena para pelaku hanya perlu mengirimkan pesan ke sejumlah nomor telepon. Pesan tersebut sering kali berisi tautan atau informasi palsu yang dirancang untuk memancing korban memberikan data pribadi atau sensitif, seperti kata sandi atau nomor rekening. Karena pesan teks sering dianggap lebih terpercaya, banyak orang yang terperdaya dan akhirnya membagikan informasi tanpa berpikir panjang.
2. Blind Phishing
   Jenis penipuan kedua yang paling umum adalah *blind phishing*, di mana penipu mengirimkan email atau pesan massal. Ciri utama dari blind phishing adalah pelaku tidak menyebutkan nama penerima tertentu, karena pesan tersebut dikirimkan kepada banyak orang sekaligus. Biasanya, pesan tersebut berisi informasi palsu atau tautan yang bertujuan untuk menipu korban agar memberikan data pribadi atau sensitif. Karena pesan ini bersifat umum dan tidak ditargetkan pada individu tertentu, para penipu berharap ada orang yang terperdaya dan memberikan informasi berharga mereka.
3. Deceptive Phishing
   Deceptive Phishing adalah jenis penipuan yang dilakukan dengan mengirimkan email yang berpura-pura berasal dari organisasi resmi, yang meminta korban untuk melakukan aktivitas tertentu, seperti memverifikasi informasi akun, memberikan nama pengguna dan kata sandi, mengubah kata sandi, atau melakukan transaksi pembayaran. Informasi yang diperoleh melalui metode ini digunakan oleh peretas untuk mengakses akun korban tanpa sepengetahuan mereka, dan kemudian digunakan untuk keuntungan pribadi.
   Ada dua cara umum yang digunakan oleh penipu dalam deceptive phishing. Pertama, pelaku menyamar sebagai perwakilan dari organisasi resmi dan meminta data pribadi korban, seperti informasi login atau data sensitif lainnya. Kedua, penipu berpura-pura menjadi lembaga resmi dan memberikan tautan berbahaya yang dapat mengekspos korban pada ancaman keamanan.
4. Web Phishing
   Web phishing adalah jenis penipuan di mana pelaku menyalin atau membuat tiruan situs web asli untuk menipu dan menarik pengguna. Situs phishing ini biasanya meminta korban untuk memasukkan informasi sensitif, seperti nama pengguna, kata sandi, atau data pribadi lainnya, ke dalam kolom yang disediakan. Setelah informasi dimasukkan, data tersebut akan langsung dikirimkan kepada penipu. Setelah itu, korban biasanya akan dialihkan ke halaman web asli tanpa menyadari bahwa mereka telah menjadi korban phishing dan data mereka telah dicuri oleh pelaku.
5. Phishing PDF
   Jenis phishing terbaru ini sering terjadi melalui pesan *WhatsApp* yang mengirimkan file PDF sebagai umpan. Penipuan ini mencoba menipu korban dengan mengirimkan file yang tampaknya sah, namun sebenarnya berisi program aplikasi jahat. Ketika file tersebut dibuka, program berbahaya ini dapat menyebabkan pencurian data pribadi korban. Metode ini menjadi semakin populer karena banyak orang cenderung mempercayai file yang dikirim melalui pesan pribadi seperti WhatsApp, sehingga rentan terhadap ancaman ini.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol. 11 No. 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

Meskipun kasus phishing sudah sering terjadi, nyatanya masih ada saja orang yang menjadi korban. Biasanya, ada beberapa alasan mengapa seseorang bisa terjebak dalam penipuan semacam ini. Berikut adalah lima faktor utama yang sering menyebabkan korban phishing:

a. Kemudahan untuk Percaya
   Alasan pertama adalah korban yang terlalu mudah mempercayai sesuatu yang mereka terima, baik itu melalui email, pesan teks, atau telepon. Kepercayaan yang berlebihan ini menjadi celah bagi para pelaku untuk menjalankan aksinya. Orang yang mudah percaya cenderung memberikan informasi pribadi mereka tanpa curiga, yang sangat menguntungkan bagi penipu. Dengan cara ini, pelaku dapat lebih leluasa dalam menjalankan penipuan mereka.
b. Kelalaian dalam Memeriksa Informasi
   Salah satu bentuk penipuan yang umum terjadi adalah pengiriman email, telepon, atau SMS yang berpura-pura datang dari bank atau institusi terpercaya. Banyak korban yang terjebak karena mereka tidak berhati-hati dalam memeriksa kebenaran informasi yang diterima. Ketika korban tanpa sadar memberikan data pribadi mereka, hal ini dapat menyebabkan kerugian yang signifikan, termasuk akses tak sah ke rekening bank mereka.
c. Tergoda oleh Penawaran Menggiurkan
   Penawaran hadiah, kupon, atau diskon besar yang datang melalui telepon, SMS, atau email sering kali menjadi daya tarik bagi banyak orang. Penipu memanfaatkan kesempatan ini dengan menawarkan sesuatu yang tampaknya menguntungkan, yang akhirnya membuat korban merasa tertarik untuk memberikan informasi pribadi mereka. Keinginan untuk mendapatkan hadiah atau keuntungan cepat membuat korban tidak waspada, sehingga terjebak dalam penipuan phishing.
d. Penggunaan Kata Sandi yang Lemah
   Phishing sering kali menyasar akun media sosial atau email korban, dengan cara menyebarkan informasi palsu atau mencuri data login. Salah satu alasan mengapa banyak orang mudah menjadi korban adalah karena mereka menggunakan kata sandi yang lemah dan mudah ditebak. Oleh karena itu, penting untuk menggunakan kombinasi karakter yang kuat, seperti huruf kecil, huruf besar, angka, dan simbol, saat membuat password. Dengan cara ini, akun-akun tersebut akan lebih aman dan sulit diakses oleh peretas.
e. Membuka Link yang Tidak Dikenal
   Seringkali, pelaku phishing mengirimkan link yang tampak mengarah ke situs web tertentu melalui email, SMS, atau pesan langsung. Namun, banyak korban yang tanpa pikir panjang mengklik link tersebut tanpa memeriksa keaslian situs yang dimaksud. Link yang mencurigakan ini biasanya mengarah ke situs berbahaya yang dapat menginstal virus atau malware, yang memungkinkan peretas mengakses data pribadi dan akun media sosial korban.

Kerugian yang Ditimbulkan Bagi Korban *Phishing*

Berdasarkan berbagai laporan dari lembaga internasional dan nasional, banyak rekomendasi yang diberikan untuk mencegah atau mengurangi dampak dari serangan *phishing*. Rekomendasi tersebut mencakup beberapa aspek penting, seperti penguatan undang-undang yang relevan, penyuluhan dan edukasi yang lebih intensif bagi para pengguna internet, peningkatan kesadaran masyarakat tentang bahaya phishing, serta penerapan langkah-langkah keamanan teknis yang lebih canggih dan terjamin. Dalam konteks ini, kesadaran tentang *phishing* semakin penting, baik dalam lingkup pribadi maupun profesional. Serangan phishing

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol. 11 No. 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

tidak hanya mengancam individu, tetapi juga organisasi dan perusahaan yang berpotensi menjadi sasaran empuk bagi para pelaku kejahatan siber. Dampak yang dialami oleh korban juga berpengaruh diantaranya adalah :

Kerugian secara finansial. Korban serangan phishing dapat mengalami kerugian finansial secara langsung apabila mereka memberikan informasi terkait rekening bank atau kartu kredit kepada penipu. Dengan informasi tersebut, para penipu bisa menguras saldo atau melakukan transaksi ilegal yang merugikan korban. Selain kerugian langsung, korban juga berisiko kehilangan uang secara tidak langsung jika data pribadi mereka dijual kepada pihak ketiga yang kemudian dapat memanfaatkannya untuk kejahatan lain, seperti pencurian identitas atau pemerasan. Menurut Federal Trade Commission (FTC) Amerika Serikat, kerugian akibat penipuan online melalui media sosial mencapai 11 triliun rupiah pada tahun 2021. Laporan lain dari FBI menyebutkan bahwa pada tahun 2020, phishing menjadi jenis kejahatan siber yang paling banyak dilaporkan di Amerika Serikat, dengan total kerugian yang mencapai lebih dari 4,2 miliar USD. Selain itu, laporan dari Proofpoint, sebuah perusahaan keamanan siber global, mengungkapkan bahwa pada kuartal pertama tahun 2021, serangan phishing yang ditujukan kepada sektor kesehatan, keuangan, dan ritel mengalami peningkatan sebesar 25%.

Kerusakan reputasi. Korban serangan phishing tidak hanya berisiko kehilangan uang, tetapi juga dapat mengalami kerusakan reputasi yang signifikan. Jika data pribadi mereka digunakan untuk melakukan aktivitas yang merugikan atau melanggar hukum, dampaknya bisa sangat merusak. Sebagai contoh, para pelaku phishing dapat memanfaatkan akun email atau media sosial korban untuk mengirimkan spam, malware, atau konten yang tidak pantas kepada orang lain. Tindakan semacam ini dapat merusak citra dan kepercayaan terhadap korban, terlebih jika mereka adalah seorang pelaku bisnis atau pejabat publik yang memiliki reputasi penting. Phishing terbukti dapat menyebabkan kerusakan reputasi yang besar, baik bagi individu maupun institusi yang menjadi targetnya. Informasi yang dicuri dapat digunakan untuk berbagai tujuan kejahatan, seperti penipuan, pencurian identitas, atau penyalahgunaan akun. Semua ini dapat menciptakan dampak jangka panjang bagi korban, yang harus menghadapi konsekuensi dari kerusakan citra dan reputasi yang ditimbulkan oleh tindakan para penipu.

Stres dan trauma. Korban serangan phishing sering kali mengalami stres dan trauma akibat pengalaman yang sangat meresahkan dan tidak menyenangkan. Rasa takut, marah, bersalah, malu, dan depresi adalah beberapa perasaan yang umum dialami oleh korban setelah menjadi sasaran penipuan. Mereka juga bisa merasa tidak aman dan terus-menerus khawatir tentang data dan privasi pribadi mereka yang telah terekspos di dunia maya. Dampak psikologis ini dapat mempengaruhi kesehatan mental dan fisik korban dalam jangka panjang. Beberapa dampak psikologis yang mungkin timbul akibat serangan phishing antara lain:

1. Stres. Korban phishing dapat merasa stres karena khawatir data pribadi mereka akan disalahgunakan oleh pelaku. Stres juga dapat muncul karena adanya tekanan dari pihak-pihak yang terlibat, seperti bank, perusahaan, atau instansi pemerintah yang harus menangani kasus pencurian data tersebut.
2. Trauma. Serangan phishing bisa meninggalkan trauma yang mendalam, yang membuat korban merasa takut atau ragu untuk menggunakan layanan online di masa depan. Ketakutan ini bisa menghalangi mereka untuk berbelanja online, melakukan transaksi digital, atau bahkan berkomunikasi melalui platform online.
3. Depresi. Korban phishing juga bisa jatuh ke dalam depresi akibat perasaan bersalah, malu, atau rendah diri setelah menjadi sasaran penipuan online. Selain itu, depresi juga bisa disebabkan oleh kerugian finansial yang besar yang dialami korban, atau hilangnya kepercayaan dari orang-orang di sekitar mereka yang mungkin meragukan integritas mereka setelah kejadian tersebut.

CAUSA
ISSN 3031-0369
Jurnal Hukum dan Kewarganegaraan
Vol. 11 No. 9 Tahun 2025
Prefix doi.org/10.3783/causa.v2i9.2461

4. Kecemasan. Kecemasan menjadi dampak psikologis lainnya yang sering dialami korban phishing. Mereka merasa cemas karena tidak tahu bagaimana cara mengatasi masalah yang ditimbulkan oleh pencurian data tersebut. Selain itu, mereka juga khawatir akan menjadi sasaran serangan phishing lagi di masa depan, yang semakin memperburuk rasa tidak aman mereka dalam menggunakan teknologi dan layanan digital.

Dampak-dampak psikologis ini menunjukkan betapa pentingnya untuk meningkatkan kesadaran dan perlindungan terhadap serangan phishing, agar korban dapat memitigasi dampak negatif tersebut.

Upaya Pencegahan Agar Tidak Menjadi Korban *Phishing*

Beberapa Upaya pencegahan agar tidak menjadi korban *phishing* antara lain adalah:

1. Melakukan *Two Factor Authentication*.
Two Factor Authentication (2FA) adalah metode keamanan yang penting untuk melindungi akun online dengan menambahkan langkah verifikasi ganda sebelum akses. Cara kerja 2FA:
   a. Langkah Pertama: pengguna memasukkan nama pengguna dan *password*
   b. Langkah Kedua: Pengguna menerima kode verifikasi (OTP) melalui SMS atau aplikasi autentikasi, yang harus dimasukkan untuk menyelesaikan proses login
2. Memastikan Keamanan Website 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.

3. 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.
4. 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.
5. Memasang Aplikasi Pelindung *Phishing*
   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 seperti Avast, Kaspersky dan lainnya.

KESIMPULAN

Perkembangan teknologi dan penggunaan media sosial yang pesat di Indonesia membawa manfaat besar, namun juga meningkatkan risiko kejahatan siber, terutama phishing. Phishing adalah penipuan digital yang bertujuan mencuri data pribadi melalui berbagai metode seperti email palsu, SMS, atau situs tiruan.

Meskipun Indonesia telah memiliki landasan hukum seperti UU ITE, KUHP, dan undang-undang lainnya untuk menindak pelaku phishing, kasusnya terus meningkat. Kurangnya literasi digital dan kesadaran akan keamanan siber menjadi faktor utama masyarakat mudah terjebak.

Phishing menimbulkan dampak serius, seperti kerugian finansial, kerusakan reputasi, dan gangguan psikologis. Oleh karena itu, pencegahan harus dilakukan melalui edukasi digital, penggunaan 2FA, keamanan perangkat, serta kebiasaan online yang lebih waspada.

Kerja sama antara pemerintah, masyarakat, dan sektor swasta sangat dibutuhkan untuk menciptakan ekosistem digital yang lebih aman dan tangguh terhadap ancaman siber.

DAFTAR PUSTAKA

CTI Content Writer (2021) Mengenal Phishing: Pengertian dan Cara Mengatasinya. Mengenal Phishing: Pengertian dan Cara Mengatasinya

Devie Rahmawati, Milla Viendyasari, Giri Lumakto, Rienzy Kholifatur, Wiratri Anindhita, Rizki Ameliah, Syavia Bachna, Aisyah Adienda, Waspada! Kejahatan Phishing Attack! https://repositorypenerbitlitnus.co.id/id/eprint/248/1/WASPADA%20KEJAHATAN%20PHISHING%20ATTACK!.pdf

Erizka Permatasari (2021) Jerat Hukum Pelaku Phishing dan Modusnya. file:///C:/Users/Hp/Downloads/20.+M+Arif+Bagus+Dewanto_Penipuan+Penambah+Followers+Instagram+Analisis+Serangan+Phising+dan+Dampaknya+pada+Keamanan+Data.pdf

MOHD. Yusuf DM1, Addermi2, Jasmine Lim, Kejahatan Phishing dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia. putrihana99,+8018-8023.pdf

Muhammad Arif Bagus Dewanto, Muhammad Fathurrahman, Danar Restu Firdaus, Aep Setiawan Penipuan Penambah Followers Instagram: Analisis Serangan Phishing dan Dampaknya pada Keamanan Data, 1, file:///C:/Users/Hp/Downloads/20.+M+Arif+Bagus+Dewanto_Penipuan+Penambah+Followers+Instagram+Analisis+Serangan+Phising+dan+Dampaknya+pada+Keamanan+Data.pdf

Purnamasari, Tata Sutabri, Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari. 5620-15835-1-PB.pdf

Universitas Bakrie, Kenalan dengan 5 Jenis Phishing yang Patut Diwaspadai. https://bakrie.ac.id/articles/599-kenalan-dengan-5-jenis-jenis-phising-yang-patut-diwaspadai.html

Yazid Haikal Lokapala, Fuad Januar Nurfauzi, Yeni Widowaty, Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia. 19853-Article Text-83555-1-10-20240611.pdf