SEMINAR NASIONAL TEKNOKA

Vol. 9, 2024
ISSN No. 2502-8782

Awareness Cybercrime Phishing Email Menggunakan *Secure Socket Layer* Sebagai *Interpretasi Information Security*

Kotim Subandi*, Dinar Munggaran Ahmad, Victor Ilyas Sugara, Adriana Sari Aryani, & Hermawan

Universitas Pakuan, Jl. Pakuan, Bogor, Jawa Barat, Indonesia.
Email: kotim.subandi@unpak.ac.id
Corresponding author: kotim.subandi@unpak.ac.id

Abstrak

Phishing email adalah teknik penipuan yang digunakan oleh pelaku kejahatan siber untuk memperoleh informasi sensitif melalui email yang tampak sah namun memiliki tujuan jahat Keamanan informasi menjadi salah satu aspek krusial dalam dunia digital yang semakin berkembang, terutama seiring dengan meningkatnya ancaman kejahatan siber, seperti phishing email.. Dalam konteks ini, penerapan Secure Socket Layer (SSL) menjadi salah satu solusi untuk meningkatkan kesadaran dan mitigasi risiko terhadap serangan phishing. SSL, yang merupakan protokol keamanan untuk enkripsi data, dapat membantu melindungi komunikasi digital dengan mengautentikasi server dan mengenkripsi data yang dikirimkan, sehingga mengurangi potensi penyalahgunaan data pribadi yang dikirim melalui email. Penelitian ini bertujuan untuk mengkaji peran SSL dalam memberikan perlindungan terhadap phishing email serta meningkatkan kesadaran pengguna mengenai pentingnya keamanan informasi dalam penggunaan teknologi digital. Melalui pendekatan interpretasi keamanan informasi, studi ini menyarankan bahwa SSL dapat berfungsi sebagai penghalang efektif dalam mengurangi risiko serangan phishing dan meningkatkan tingkat kepercayaan pengguna terhadap email yang diterima. Oleh sebab itu, maka penting bagi individu atau organisasi untuk memahami dan menerapkan prinsip-prinsip keamanan informasi seperti penggunaan SSL untuk menjaga integritas dan kerahasiaan data yang dipertukarkan secara daring.

***Kata Kunci**: Kejahatan Siber, Phishing Email, Keamanan Informasi, Enkripsi, Kesadaran Pengguna*

Abstract

Email phishing is a fraudulent technique used by cybercriminals to obtain sensitive information through emails that appear legitimate but have malicious purposes. Information security has become a crucial aspect in the increasingly developing digital world, especially along with the increasing threat of cybercrime, such as email phishing. In this context, implementing Secure Socket Layer (SSL) is one solution to increase awareness and mitigate risks against phishing attacks. SSL, which is a security protocol for data encryption, can help protect digital communications by authenticating servers and encrypting data sent, thereby reducing the potential for misuse of personal data sent via email. This research aims to examine the role of SSL in providing protection against email phishing and increasing user awareness regarding the importance of information security in the use of digital technology. Through an information security interpretation approach, this study suggests that SSL can serve as an effective barrier in reducing the risk of phishing attacks and increasing the level of user trust in the emails received. Therefore, it is important for individuals or organizations to understand and apply information security principles such as the use of SSL to maintain the integrity and confidentiality of data exchanged online.

***Keywords**: Cybercrime, Email Phishing, Secure Socket Layer (SSL), Information Security, Encryption, User Awareness*

Dipresentasikan pada Tanggal 30 November 2024

1. PENDAHULUAN

Tindak kejahatan dalam dunia maya akhir-kahir ini sangat mengkhawtirkan hal ini menjadikan kita harus semakin waspada. Bentuk kejahatan di jejaringan sosial banyak terjadi saat ini dari sekian serangan adalah email phising. Phising itu sendiri merupakan ancaman bagi pengguna internet ketika sedang berselancar. Jika kita dalam kondisi target phising, Banyak kerugian yang akan kita alamai jika tidak waspada terhadap tindak kejahatan didunia maya. Contohnya, tindak pencurian data atau bahkan ada penipuan yang bersifat materi. Tantangan yang muncul dalam Teknologi informasi terus berkembang secara pesat memberikan peluang bagi penyerang untuk mendapatkan akses ke berbagai alat dan perangkat lunak yang dapat digunakan untuk melakukan tindak serangan, seperti malware, exploit kits, dan layanan hacking yang dijual di pasar gelap.

Bahkan dapat mengubah model ekonomi dan model bisnis dalam dunia industri. Kejahatan phishing muncul seiringn dengan banyak kegiatan dalam internet serta beberapa alasan utama yang berkaitan dengan teknik penipuan sangat efektif karena lemahnya kesadaran mengenai sistem keamanan di jejaringan sosial. Biasanya kelemahan manusia *(Human Error)* bahwa user ini sering mengabaikan kewaspadaan atau bahkan tidak terlatih dalam mengenali tanda-tanda phishing. Sering kali penipu memanfaatkan kondisi pengguna dengan menciptakan rasa khawatir , takut , urgensi, sehingga tanpa disadari membuat korban memberikan informasi pribadi mereka. Mail phishing adalah bentuk serangan pada pengguna email dimana pelaku berusaha menipu target yang akan menjadi korban melalui email yang memilikia tujuan untuk mencuri informasi sensitif seperti kata sandi (password), nomor kartu kredit *(Credit Card)*, bahkan data pribadi seperti e-ktp. Email phishing sering kali diciptakan seolah-olah seperti email yang sah dari organisasi/perusahaan yang tepercaya, seperti bank, layanan online, bahkan perusahaan besar. Kegiatan email phishing, para pelaku biasanya menggunakan teknik seperti penipuan identitas email yang dikirim terlihat seperti dari sebuah organisasi yang resmi, sering kali dengan mencatumkam logo, format, serta menggunakan bahasa yang sangat menyakinkan. Tautan (link) palsu yang diterima user kedalam email, menyertakan tautan yang mengarahkan korban/target mengeklik ke situs web palsu yang yang dibuat tampak situs asli, biasanya target diminta memasukkan informasi pribadi mereka. *Attachment* dalam email juga dapat menyer-takan lampiran yang sudah disusupi malware, ketika lampiran tersebut dibuka, dapat menginstal malware bahkan virus di komputer pengguna. Email phishing sering kali menyertakan pesan yang mendesak serta memebrikan rasa takut kepada korban untuk segera mengambil tindakan, seperti mengonfirmasi informasi akun atau memperbarui detail penting. Peretasan email adalah tindakan kejahatan dari seseorang atau biasa disebut hacker berusaha untuk menda-patkan akses ke akun email orang lain yang menjadi target bahkan tanpa izin. Kondisi ini bisa terjadi melalui beberapa metode seperti phishing, serangan brute force, menggunakan perangkat-perangkat lunak (*software*) berbahaya, bahkan sering memanfaatkan lemahnya keamanan pada layanan email. Pelaku dapat menggunakan data yang korban untuk berbagai perbuatan tanpa bertanggung jawab, sebagai contoh penipuan serta penjualan data secara illegal. Phising adalah merupakan tindak keja-hatan yang sangat berbahaya bahkan dilakukan dengan cara menyerang berbagai sektor. Seperti sektor Financial, teknologi, retail, dan berbagai sector lainya.. Informasi yang diperoleh melalui phishing, seperti kata sandi, nomor kartu kredit, atau informasi pribadi lainnya, sangat berharga bagi para pelaku karena bisa dijual belikan atau digunakan untuk melakukan tidak penipuan seperti judi online ,pinjaman online. Melihat dari sisi urgensi email phishing sering kali menciptakan rasa ketakutan pada korban misalnya, ancaman akun akan diblokir yang menjadikan penerima segera melakukan dan bertindak cepat tanpa memikirkan dampak yang akan muncul. Dalam upaya mengatasi dan memberikan solusi terhadap tindakan phishing email, penulis menggunakan metode dan teknik untuk diterapkan baik oleh individu, organisasi, maupun perusahaan demi terciptaknya keamanan dan mencegah serangan phishing. Dengan menerapkan *Secure Socket Layer (SSL)* atau *Transport Layer Security (TLS)* untuk mengenkripsi

ISSN No. 2502-8782

komunikasi email antara server pengirim dan penerima. Dengan SSL/TLS, data yang ditransmisikan melalui email akan dienkripsi, membuatnya lebih sulit bagi pelaku phishing untuk mencuri informasi sensitif.

2. DASAR TEORI

2.1 *Cybercrime*

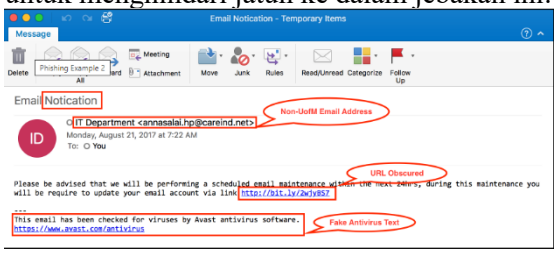
Cybercrime, atau kejahatan siber, merupakan bentuk kejahatan yang dilakukan dengan menggunakan teknologi komputer dan jaringan internet. Hal ini dapat mencakup berbagai jenis aktivitas ilegal, contohnya penipuan secara online, skema phishing dilakukukan penjahat dengan berusaha mendapatkan informasi pribadi seperti nomor kartu kredit melalui email atau situs web palsu. *Hacking* aksi tidak sah untuk mengakses sistem komputer atau jaringan, sering kali dengan niat untuk mencuri data atau merusak sistem. *Malware* merupakan *software* berbahaya seperti virus, trojan, atau ransomware yang diciptakan untuk merusak sistem dan mencuri informasi. Pencurian data identitas menggunakan informasi pribadi orang lain tanpa izin untuk melakukan tidak penipuan, seperti membuat akun atau mengakses layanan keuangan *(mobile banking)*.

Gambar 1. Serangan Ransomware

Penyebaran konten secara ilegal seperti pornografi yang ditujukan kepada anak-anak, bahkan konten kekerasan yang ekstrem, atau materi terlarang lainnya. Serangan *Denial of Service* (DoS) dengan cara mengirimkan lalu lintas secara berlebih ke server untuk membuat layanan online terganggu. Tindak kejatahan siber biasannya menargetkan individu, perusahaan, atau bahkan infrastruktur kritis negara. Dalam upaya melawan tindak kejahatan siber, sangat penting untuk selalu memiliki sistem keamanan yang baik, seperti penggunaan kata sandi yang kuat, perangkat lunak antivirus terbaru, dan kesadaran akan praktik keamanan online.

2.2 *Phising*

Di dunia maya merujuk pada praktik penipuan di mana penyerang berusaha untuk memperoleh informasi sensitif dari calaon korban, seperti kata sandi (password), nomor kartu kredit *(Credit Card)* , atau data pribadi lainnya, dengan cara yang menipu.Taktik yang digunakan penipu dengan sering menggunakan email, pesan teks, atau media sosial untuk mengirimkan tautan atau lampiran berbahaya. Pelaku biasanya berpura-pura menjadi organisasi atau individu yangsangat tepercaya. Bahkan phishing memanfaatkan teknik psikologis, seperti menciptakan rasa urgensi atau ketakutan, untuk mendorong calon korban agar segera mengambil tindakan tanpa berpikir panjang dan mencari informasi dengan detail. Seperti, email yang mengklaim akun akan ditutup jika tidak segera diverifikasi. Dampak yang muncul ketika Jika berhasil, phishing dapat mengakibatkan pencurian identitas, kehilangan uang, dan kerugian bagi individu dan organisasi. Ini juga dapat merusak reputasi perusahaan dan menurunkan kepercayaan pelanggan. Sangat dianjurkan bagi pengguna internet untuk selalu tetap waspada dan mengetahui tanda-tanda phishing untuk menghindari jatuh ke dalam jebakan ini.



Gambar 2. Phishing Email

2.3 Variasi Phising

Agar lebih mengenal tindakan phising, berikut jenis phising yang paling banyak ditemui ketika berselancar di dunia maya:

2.3.1 Email Phising

Merupakan metode penipuan di mana pelaku penyerangan dengan cara mengirimkan email seolah-olah seperti dari sumber tepercaya untuk mencuri informasi yang bersifat pribadi, misalnya kata sandi atau nomor kartu kredit. Setelah penyerang mendapatkan informasi tersebut, mereka dapat menggunakannya untuk mencuri identitas, mengakses akun, atau melakukan transaksi

ISSN No. 2502-8782

yang merugikan. Penyerang membuat email yang menyerupai email resmi sperti perusahaan, bank, atau layanan lainnya. Mereka sering menggunakan logo dari suatu perusahaan terkenal kemudian menggunakan bahasa yang sangat meyakinkan. Dalam email tersebut , biasanya juga terdapat tautan yang mengarah ke situs web palsu yang dirancang untuk meniru situs asli. Ketika korban mengklik tautan tersebut, mereka dibawa ke situs yang tampak asli. Sebagai upaya untuk melindungi diri, selalu memeriksa alamat email pengirim, tidak mengklik tautan sembarangan, dan selalu memverifikasi permintaan informasi yang bersifat sensitif atau pribadi.

2.3.2 *Angler* Phising

Pelaku biasanya emanfaatkan media sosial sebagai sarana untuk menipu pengguna. Pelaku juga sering kali berpura-pura sebagai pemberi layanan bagi pelanggan atau mengatas namakan akun resmi untuk mencuri informasi dari korban. Jenis phishing yang menargetkan pengguna di media sosial. Serangan ini sering terjadi di platform seperti Twitter, Facebook, atau Instagram, di mana penyerang menyamar sebagai akun layanan pelanggan atau perwakilan resmi dari perusahaan. Dengan data yang telah dikumpulkan, penyerang bisa mengakses akun pengguna, melakukan transaksi, atau menye-barkan lebih banyak serangan kepada kontak korban.

2.3.3 *Quishing (QR Code Phising)*

Pemakaian kode QR yang sedang trend saat ini dengan cara mengarahkan korban ke berse-lancaran menuju situs phishing dan unduhan berupa malware.Penyerang membuat kode QR yang dirancang untuk mengarahkan pengguna ke situs phishing. Situs ini sering kali meniru halaman login atau situs resmi dari lembaga yang terpercaya, seperti bank atau portal kerja. Dalam beberapa kasus, kode QR juga dapat menyebarkan malware ke perangkat korban setelah dipindai. Hal ini memungkinkan penyerang untuk mengakses data yang lebih luas atau mengendalikan perangkat korban.

2.3.4 *Pharming*

Teknik ini gunakan untuk manipulasi DNS yang akan mengarahkan pengguna menuju situs palsu walaupun korban ini sudah berada alamat web yang benar.arget utama serangan pharming adalah pengguna internet umum yang melakukan aktivitas seperti perbankan online, belanja, atau akses ke situs layanan berbasis login. Serangan ini bertujuan untuk mencuri data sensitif, seperti kredensial login, informasi kartu kredit, atau detail pribadi lainnya.enyerang sering menargetkan pengguna perbankan online dengan mengarahkan mereka ke situs web palsu yang menyerupai situs bank asli. Pengguna yang terhubung ke jaringan publik atau tidak aman (seperti Wi-Fi publik) lebih rentan terhadap serangan pharming, karena penyerang dapat lebih mudah melakukan redirect atau DNS poisoning di jaringan tersebut.

2.3.5 *Clone* Phising

Metode ini dengan cara mengkloning email yang pernah diterima korban dan mengganti tautan di dalamnya agar bisa mengarahkan korban berselancar ke situs berbahaya.Clone phishing sering kali berisi pesan yang mendesak atau meminta user segera mengambil tindakan, seperti mengonfirmasi akun atau mengubah kata sandi. Bank dan organisasi resmi biasanya tidak akan meminta data sensitif melalui email.Clone phishing sering kali mencantumkan lampiran yang tampak sah, seperti dokumen atau PDF. Pastikan untuk tidak mengunduh atau membuka lampiran dari email yang mencurigakan.

2.3.6 Tabnabbing

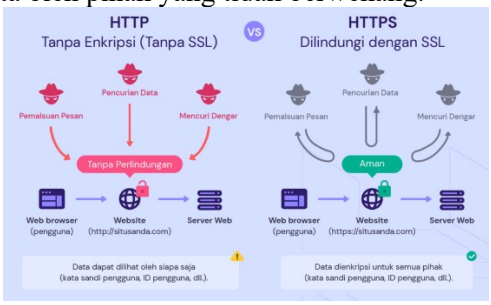
Cara ini gunakan pelaku mengubah isi tab yang tidak aktif di browser pengguna dengan menu login yang tidak resmi atau palsu agar pengguna memasukkan kredensialnya. Serangan ini memanfaatkan kecenderungan pengguna yang sering membuka banyak tab dalam sesi browsing. Ketika pengguna meninggalkan satu tab dalam keadaan terbuka dan beralih ke tab lain, penyerang dapat memanfaatkan waktu ini untuk mengubah tampilan tab yang tidak aktif menjadi halaman login palsu, seperti halaman login email atau akun bank.abnabbing umumnya bekerja dengan memuat skrip jahat di tab yang tidak aktif. Ketika pengguna kembali ke tab tersebut, mereka melihat halaman login palsu dan memasukkan kredensial mereka tanpa menyadari bahwa ini adalah halaman palsu.

2.4 *Secure Socket Layer*

Secure Socket Layer (SSL) yaitu protokol keamanan yang digunakan untuk mengenkripsi

ISSN No. 2502-8782

komunikasi antara pengguna dan server melalui internet. Yang bertujuan melindungi data yang dikirimkan dari situs menuju ke situs web dari pihak ketiga yang tidak memiliki kewenaangan yang sah. Berikut adalah beberapa poin penting dalam SSL. Enkripsi data SSL akan mengenkripsi data yang dikirimkan melalui browser pengguna dan server, sehingga informasi data login, informasi kartu kredit, dan data pribadi tidak dapat dibaca oleh pihak ketiga yang mungkin mencoba mengaksesnya. Autentikasi memastikan bahwa data dikirimkan ke server yang benar dan bukan ke server palsu. Ini membantu mencegah serangan seperti man-in-the-middle di mana biasannya penyerang mampu memanipulasi bahkan mencuri data. Integritas data memastikan bahwa data yang dikirim dan diterima tidak diubah selama transmisi. Ini membantu mencegah manipulasi data oleh pihak yang tidak berwenang.



Gambar 3. *Secure Socket Layer (SSL) Work*

Indikator saat SSL sedang aktif, URL di browser biasanya dimulai dengan "https://" dan bahkan akan mucul ikon berupa gembok pada alamat web tersebut, hal ini menjadi tanda bahwa komunikasi antara browser dan server dienkripsi. SSL telah berkembang dengan berbagi versi yang lebih canggih dan bahkan aman yang dikenal sebagai *Transport Layer Security (TLS)*. TLS merupakan penerus SSL dan lebih umum digunakan karena memberikan peningkatan keamanan dibandingkan dengan SSL. Namun, istilah "SSL" masih sering digunakan secara umum untuk merujuk pada kedua protokol tersebut.

2.5 *Information Security*

Data Mining atau Penambangan Data Interpretasi dari sebuat *Information Security* (Keamanan Informasi) merujuk pada praktik dan prinsip yang dirancang dalam upaya melindungi semua informasi dari berbagai ancaman yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan data. Kerahasiaan *(Confidentiality)* menjaga informasi agar hanya dapat diakses oleh pihak yang berwenangHal ini berarti melindungi data agar tidak jatuh ke tangan pihak yang tidak berhak atau tidak memiliki kewenangan. .

Seperti menggunakan enkripsi untuk melindungi data pribadi dan bisnis. Integritas *(Integrity)* memastikan bahwa informasi tidak dimodifikasi dan dimanipulasi secara tidak sah selama proses penyimpanan atau transmisi. Ini bertujuan untuk menjaga akurasi dan konsistensi data. Contoh praktik integritas termasuk penggunaan checksum digital signature. Ketersediaan *(Availability)* memastikan bahwa informasi dan sistem yang menyimpannya tersedia dan dapat diakses oleh pengguna yang berwenang kapan pun diperlukan. Ini melibatkan pengelolaan sumber daya sistem untuk menghindari downtime dan serangan seperti *Denial of Service (DoS)* yang dapat mengganggu akses ke data. Autentikasi *(Authentication)* proses untuk memastikan bahwa individu atau sistem yang meminta akses adalah siapa yang mereka yang sah. Hal ini sering dilakukan melalui kata sandi, biometrik, atau metode otentikasi multi-faktor.

Otorisasi *(Authorization)* menentukan tingkat akses yang diizinkan bagi individu atau sistem setelah autentikasi. Ini memastikan bahwa pengguna hanya dapat mengakses informasi atau melakukan tindakan yang sesuai dengan hak akses yang mereka miliki. Akuntabilitas (Accountability) merekam dan melacak tindakan yang dilakukan pada sistem dan data untuk memastikan bahwa semua aktivitas dapat ditelusuri kembali kepada pengguna atau entitas tertentu. Ini melibatkan penggunaan log dan audit trails.

Gambar 4. Aspek Keamanan Informasi

Pengelolaan *Risiko (Risk Management)* mengidentifikasi, mengevaluasi, dan mengelola risiko yang dapat mengancam

ISSN No. 2502-8782

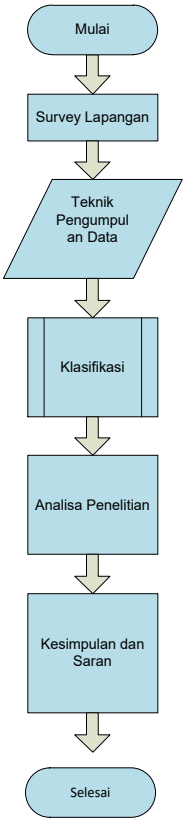
keamanan informasi. Ini termasuk menilai potensi ancaman dan kerentanan, serta menerapkan kontrol untuk mengurangi risiko tersebut. Keamanan informasi mencakup berbagai kebijakan, prosedur, dan teknologi yang dirancang untuk melindungi data dari ancaman yang mungkin timbul dari serangan siber, kecelakaan, atau kesalahan manusia. Praktik keamanan informasi sangat penting untuk menjaga kepercayaan dan melindungi aset informasi dalam lingkungan digital yang semakin kompleks.

3. METODOLOGI

Dalam peniltian ini akan disampaikan langkah-langkah yang akan dilakukan oleh penelitian . berikut ini langkah seperti mengumpulkan data, *preprocessing* data, pembuatan model klasifikasi hingga skenario uji coba yang akan dilaksanakan dalam penelitian ini.

3.1 Gambaran Umum Penelitian

Metodologi dalam penelitian ini digambarkan dalam diagram seperti dibawah ini.



Gambar 5. Tahapan Penelitian

3.2 Teknik Pengumpulan Data

Metode ini digunakan untuk mengumpulkan seluruh informasi yang diperlukan dalam melakukan penelitian serta analisa. Alat bantu dalam mengumpulkan data melalui serangkaian pertanyaan tertulis yang dijawab oleh responden. Setelah itu dilakukan pengamatan kemudian mencatat perilaku atau kejadian secara langsung di lapangan tanpa intervensi. Data yang didapat seperti laporan, artikel, atau catatan historis akan di dokumetsikan untuk tidak lanjut. Di bawah ini adalah contoh studi kasus ciri-ciri phising email yang berhasil didapatkan seperti *Password Experation, Mailbox Full*, *Password* Bocor.

3.3 Klasifikasi

Metode klasifikasi dalam mendeteksi email phising dengan memeriksa struktur URL untuk menemukan sebuah pola dana kata kunci yang sering dipakai oleh pelaku phishing. Untuk memasikan beberapa kriteria dalam membantu mengidentifikasi kemudian mengelompokkan email yang di anggap mencurigakan.

3.4 *Klasifikasi Email Phishing*

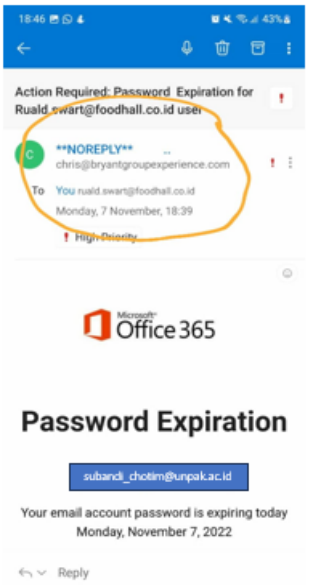
Gambar 6. Model Klasifikasi

4. HASIL DAN PEMBAHASAN

4.1 Analisa Peneliti

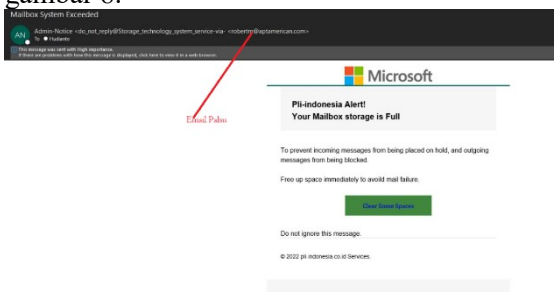
Penelitian melakukan analisa pada user yang sering menerima email yang tidak dikenal. Berikut merupakan beberapa kejadian yang dialami ketika user beraktifikas menggunakan email. Adanya pemberitahuan lewat email mengenai perubahan password kemudian akan meminta password lama dan password baru, tujuan web tersebut bukan untuk mengganti password, tetapi lebih kearah memperoleh password milik user tersebut seprti terlihat pada gambar 7.

ISSN No. 2502-8782



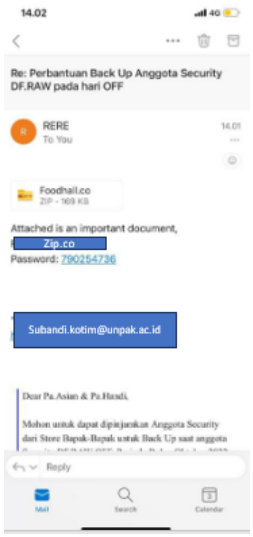
Gambar 7. *Mail Phishing Password Expiration*

Laporan berikutnya adalah email informasi tentang mailbox, pengirim ini memanipulasi penerima agar mengungkapkan informasi sensitif atau mengklik tautan yang mengarah ke situs web berbahaya terlihat pada gambar 8.



Gambar 8. *Mail Phishing Mailbox Full*

Analisa dan emuan penelitian berikutya password email yang bocor real email dari Rere emailnya nyambung dari email sebelumnya. Jika diperhatikan ada kejanggalan di email ini s, yaitu pengirim meminta penerima email membuka attachment dengan menggunakan password yang tertera di body email ini masuk di kategori karakteristik kontens seperti gambar 9.



Gambar 9. *Password* Bocor

Dengan adanya permasalahan tersebut, maka penulis mengidentifikasi serta mengaanlisa kemudian mendalami tentang skema yang digunakan oleh para *cybercrime* dalam melakukan tindakan *phising*. Untuk menghidari dari berbagai ancaman *phishing* peneliti mencoba menerapkan *Secure Socket Layer* (SSL) dan memberikan kebijakan bagi user sebagai upaya terciptanya *interprestasi information security*.

Media sosial seperti Email, Facebook, Instagram, dan Twitter memiliki miliaran pengguna aktif. hal ini berati memberikan kesempatan yang besaR bagi pelaku peretas untuk menjangkau dan memanipulasi banyak calon korban potensial dengan satu serangan. Banyak akun media sosial, terutama yang memiliki banyak pengikut atau terhubung ke toko online, dapat dijadikan sumber keuntungan finansial jika berhasil diretas. Selain itu, akun yang diretas bisa dijual kembali di pasar gelap atau digunakan untuk penipuan finansial. Di media sosial, peretas dapat membuat akun palsu yang menyerupai akun resmi atau akun orang terdekat korban. Dengan teknik seperti *cloning* atau *impersonation*, mereka dapat meyakinkan pengguna untuk berbagi informasi pribadi atau mengklik tautan yang berbahaya.

Media sosial juga digunakan untuk menyebarkan *malware* atau *ransomware*. Tautan berbahaya yang dikamuflase sebagai video, artikel menarik, atau promosi bisa disebarkan dengan mudah dan memiliki

ISSN No. 2502-8782

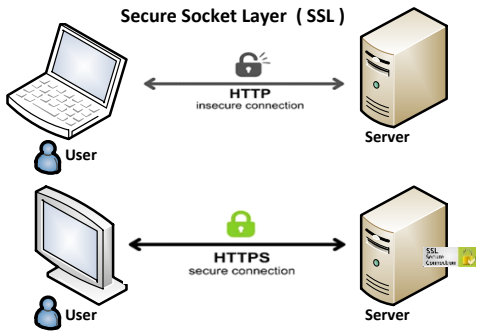
tingkat interaksi yang tinggi di media sosial. Banyak pengguna membagikan informasi pribadi di profil mereka, seperti tanggal lahir, alamat email, nomor telepon, dan bahkan lokasi. Data ini dapat dimanfaatkan untuk serangan yang lebih personal, seperti phishing dan spear phishing, atau digunakan untuk mencuri identitas seseorang.

4.2 Solusi Mengatasi Phishing

Dalam hal ini peneliti memberikan proteksi pada situs web dengan sertifikat SSL/TLS akan memiliki URL yang dimulai dengan "https://" yang menunjukkan bahwa koneksi aman. Pengguna sebaiknya hanya memasukkan informasi sensitif di situs dengan koneksi aman. DNS yang aman dan email yang memiliki proteksi seperti DMARC, SPF, dan DKIM dapat membantu organisasi mencegah email palsu mengklaim berasal dari domain mereka sendiri, yang merupakan taktik umum dalam phishing.

Email akan dilengkapi proteksi *SSL (Secure Sockets Layer)* atau *TLS (Transport Layer Security)* agar email lebih aman daripada email yang tidak memiliki proteksi tersebut. Karena SSL/TLS membantu mengamankan data yang dikirim melalui email dengan cara mengenkripsi koneksi antara server email dan klien (pengguna) atau antara dua server email. Dengan enkripsi ini, data yang dikirim menjadi sulit diakses atau dibaca oleh pihak ketiga yang tidak berwenang, termasuk peretas yang mencoba menyadap data di jaringan.

SSL/TLS hanya melindungi data saat sedang dikirimkan (data in transit), yaitu selama email dikirim dari pengirim ke penerima. Begitu email sampai di server penerima atau diakses oleh pengguna, enkripsi ini tidak berlaku lagi. Proteksi SSL/TLS pada email memang meningkatkan keamanan dan melindungi data selama proses pengiriman, tetapi bukan jaminan keamanan penuh. Pengguna tetap perlu berhati-hati dengan email yang diterima, terutama terhadap serangan phishing, memastikan server yang digunakan aman, dan menghindari jaringan yang tidak aman atau publik untuk mengakses email seperti terlihat pada gambar di bawah.



Gambar 10. Diagram SSL

Konfigurasi *Secure Socket Layer (SSL)* yang handal melibatkan beberapa langkah dan praktik terbaik untuk memastikan keamanan komunikasi data yang dilakukan melalui email ini benar-benar terjaman keamnanannya. Meskipun SSL telah banyak digantikan oleh *TLS (Transport Layer Security),* istilah SSL masih sering digunakan sampai saat ini. Gunakan sertifikat yang valid dan dikeluarkan oleh *Certificate Authority (CA)* yang tepercaya. Sebagai pengaturan keamanan tambahan ktifkan HSTS untuk memastikan browser selalu menggunakan HTTPS. Untuk keamanan jika menggunakan email, imple-mentasikan MTA-STS untuk memastikan penggunaan TLS dalam pengiriman email.

Berikut ini konfigurasi SSL/TLS untuk server web menggunakan Nginx dan Apache. Konfigurasi ini mencakup pengaturan dasar untuk mengaktifkan SSL/TLS menggunakan sertifikat yang valid.

```
server {
    listen 443 ssl;
    server_name example.com www.unpak.ac.id;
    ssl_certificate /path/to/your/certificate.crt; # Sertifikat SSL
    ssl_certificate_key /path/to/your/private.key; # Kunci pribadi

    # Pengaturan SSL/TLS
    ssl_protocols TLSv1.2 TLSv1.3; # Hanya gunakan versi terbaru
    ssl_ciphers 'ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256'; # Cipher suites yang aman
    ssl_prefer_server_ciphers on; # Prioritaskan cipher server

    # HSTS
    add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
    location / {
        # Pengaturan lokasi
        try_files $uri $uri/ =404;
    }
}
```

Gambar 11. Konfigurasi SSL dengan Nginx

```
<VirtualHost *:443>
    ServerName example.com
    ServerAlias www.unpak.ac.id

    SSLEngine on
    SSLCertificateFile /path/to/your/certificate.crt # Sertifikat SSL
    SSLCertificateKeyFile /path/to/your/private.key # Kunci pribadi
    SSLCertificateChainFile /path/to/your/chainfile.pem # Rantai sertifikat (jika diperlukan)

    # Pengaturan SSL/TLS
    SSLProtocol -all +TLSv1.2 +TLSv1.3 # Hanya gunakan versi terbaru
    SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256 # Cipher suites yang aman
    SSLHonorCipherOrder on # Prioritaskan cipher server

    # HSTS
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

    DocumentRoot /var/www/html
    <Directory /var/www/html>
        AllowOverride All
    </Directory>
</VirtualHost>
```

Gambar 12. Konfigurasi SSL dengan Apache

.

4.3 Interpretasi Keamanan Dengan SSL

Berfokus pada penyediaan lapisan perlindungan untuk data yang ditransmisikan antara klien (seperti browser) dan server. SSL mengenkripsi seluruh data yang akan dikirimkan, sehingga informasi sensitif seperti kata sandi, nomor kartu kredit, dan data pribadi tidak dapat dibaca oleh pihak ketiga yang mungkin mencegat komunikasi. Enkripsi ini memastikan bahwa hanya penerima yang berhak dan sah yang dapat mendekripsi dan mengakses informasi.

Dengan menggunakan sertifikat digital, SSL membantu memverifikasi identitas server. Ketika pengguna terhubung ke situs web yang menggunakan SSL, mereka dapat memastikan bahwa mereka terhubung ke server yang benar dan bukan ke server palsu. Ini melindungi pengguna dari serangan seperti man-in-the-middle. SSL memastikan bahwa data yang dikirimkan tidak dapat dimodifikasi atau dicuri tanpa terdeteksi selama proses transmisi. Jika data diubah, koneksi akan terputus, dan pengguna akan diberitahu.

SSL membantu melindungi data dari berbagai serangan, termasuk mencegah pihak ketiga mendengarkan komunikasi, melindungi dari penyerang yang mencoba memposisikan diri di antara klien dan server., menghindari serangan di mana data yang ditangkap digunakan kembali oleh penyerang.

4.4 Edukasi Keamanan Informasi

Salah satu cara untuk melindungi informasi dari berbagia ancaman, risiko, dan serangan yang dapat merusak, kerahasiaan, integritas dan ketersediaan atau biasa disebut dengan *CIA (Confidential , Integrity Availability)* . Dengan Tujuan untuk meningkatkan kesadaran dan keterampilan tiap individu/user bahkan organisasi dalam menjaga keamanan data dan sistem informasi berharga. Dalam memahami berbagai jenis ancaman, seperti *malware, phishing, ransomware*, dan serangan siber lainnya.

Pemberian pelatihan dan edukasi mengenai prinsip-prinsip dasar seperti penggunaan kata sandi(password) yang kuat seperti huruf kapital,angka,symbol ,minimal karakter yang digunakan, kemudian melakukan update software secara berkala, dan pengelolaan akses yang tepat, memahami dan menerapkan kebijakan serta prosedur keamanan yang ada di organisasi atau perusahaan sebagai upaya untuk melindungi data sensitif, termasuk enkripsi, backup data, dan pengelolaan hak akses.Prosedur ini diterapkan untuk menangani dan merespons insiden keamanan apabila ada pelanggaran atau serangan kedalam system informasi yang dimiliki.

Cyber dan teknologi terus berkembang, edukasi.pelatihan harus bersifat berkelanjutan agar pengetahuan dan pemahaman juga up-to-date dengan tren berkembang atau terbaru.Memahami dan mematuhi peraturan dan standar yang relevan, seperti GDPR, HIPAA, atau ISO 27001 ini sangat penting, tergantung pada industri ,perusahaan serta lokasi.

Untuk mencapai suatu kemanan informasi yang kuat penuliskan menerpakan Memfilter spam dan konfigurasi perangkat untuk pendeteksi phishing di email secara otomatis mendeteksi dan memblokir email yang mencurigakan, pengguna juga harus rutin memeriksa dan memperbarui pengaturan filter yang digunakan. Menggunakan perangkat lunak untuk menganalisis lalu lintas email dan mendeteksi anomali yang menunjukkan potensi serangan phishing, seperti pola pengiriman yang tidak biasa atau volume email yang tinggi dalam waktu singkat. Menerapkan metode otentikasi dua faktor (2FA) untuk akun email dan layanan penting lainnya. 2FA mengharuskan pengguna untuk memasukkan informasi tambahan selain kata sandi (misalnya, kode yang dikirimkan melalui SMS atau aplikasi autentikasi) sebelum bisa mengakses akun.

5. SIMPULAN

Kesadaran terhadap ancaman kejahatan siber, khususnya serangan phishing email, merupakan hal yang sangat penting dalam upaya menjaga keamanan informasi. Phishing email sering kali menjadi metode yang digunakan oleh penjahat siber untuk menipu korban dan memperoleh data sensitif, seperti kata sandi, informasi pribadi, atau data keuangan.

Dalam konteks ini, *Secure Socket Layer (SSL)* dan protokol keamanan terkait seperti *Transport Layer Security (TLS)* memainkan peran yang sangat vital sebagai alat untuk meningkatkan keamanan komunikasi dan melindungi data dari potensi serangan. Melalui

ISSN No. 2502-8782

penggunaan SSL/TLS, transmisi data melalui email dapat dienkripsi, yang tidak hanya memastikan bahwa data yang dikirimkan tetap aman, tetapi juga mengurangi kemungkinan pencurian informasi sensitif. SSL/TLS membantu dalam verifikasi identitas pengirim, yang mengurangi risiko penipuan dalam bentuk phishing.

Oleh karena itu, SSL dapat dianggap sebagai salah satu komponen penting dalam membangun sistem keamanan informasi yang efektif dan terpercaya. Selain itu, penerapan teknik-teknik lain seperti autentikasi email MFA, filter spam dan phishing, serta edukasi pengguna juga memiliki peran yang tidak kalah penting dalam menanggulangi ancaman phishing. Dengan meningkatkan kesadaran pengguna terhadap tanda-tanda phishing dan pentingnya perlindungan data, risiko serangan dapat diminimalkan. Secara keseluruhan, pendekatan yang komprehensif dan penggunaan teknologi seperti SSL dalam mengamankan komunikasi email, dikombinasikan dengan kebijakan yang ketat dan edukasi yang berkelanjutan, akan secara signifikan mengurangi dampak dari serangan phishing email dan meningkatkan ketahanan sistem keamanan informasi pada tingkat individu maupun organisasi.

Hapus email phishing dari kotak masuk dan dari folder sampah atau arsip jika ada. Ini dapat mengurangi risiko jika tidak sengaja terpapar kembali, segera rubah kata sandi (password) akun yang mungkin terkena dampak. Gunakan kata sandi (password) yang kuat dan unik untuk setiap akun email.

DAFTAR REFERENSI

[1] SADIQ, A., ANWAR, M., BUTT, R. A., MASUD,F., SHAHZAD, M. K., NASEEM, S., & YOUNAS, M. (2021). A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. Human Behavior and Emerging Technologies, 3(5), 854–864. https://doi.org/10.1002/hbe2.301

[2] KOTO, I. (2021). IJRS: International JournalReglement & Society Cyber CrimeAccording to… Cyber Crime According tothe ITE Law. August, 103–110. http://jurnal.bundamediagrup.co.id/index.php/ijrs

[4] MISHRA, A., & FANCY. (2021). Efficient Detection of Phising Hyperlinks using Machineearning. International Journal on Cybernetics & Informatics, 10(2), 23–33. https://doi.org/10.5121/ijci.2021.100204

[5] IRAWAN, D. (2020). Mencuri Informasi PentingDengan Mengambil Alih Akun Facebook Dengan Metode Phising. JIKI (Jurnal LlmuKomputer & Lnformatika), 1(1), 43–46 https://doi.org/10.24127/jiki.v1i1.671

[6] MUSLIM, N., SENJAYA, O., HUKUM, F., & KARAWANG, U. S. (2022).Pertanggung jawaban Hukum PlatformMedia Sosial Terhadap Korban PhisingMelalui Mass Tagging. 9(2), 955–963

[8] MOORTHY, R. S., & PABITHA, P. (2020). OptimalDetection of Phising Attack using SCA based K-NN. Procedia Computer Science,171(2019), 1716 1725.

[6] RAMADHAN, A., ALHAFIDH, M. A., &FIRMANSYAH, M. D. (2022). Penyebaran Link Phising Kuota Kemendikbud TerhadapMahasiswa UNINUS. Kampret Journal,1(1), 11–15.https://doi.org/10.35335/kampret.v1i1.9.

[6] H. Tabrizchi and M. K. Rafsanjani, “A survey on security challenges in cloud computing: issues, threats, and solutions,” *Springer Sci. Media*, 2020

[7] M. K. Sharma and M. J. Nene, “Two-factor authentication using biometric based quantum operations,” *Secur. Priv.*, vol. 3, no. 3, 2020, doi: 10.1002/spy2.102.

[8] K. C. Laudon and J. Laudon, *IT Infrastructure and Emerging Technologies*. 2018.

[9] C. Z. Acemyan, P. Kortum, J. Xiong, and D. S. Wallach, “2FA might be secure, but it’s not usable: A summative usability assessment of Google’s two-factor authentication (2FA) methods,” *Proc. Hum. Factors Ergon. Soc.*, vol. 2, pp. 1141–1145, 2018, doi: 10.1177/1541931218621262.

[10] D. Wang, Q. Gu, H. Cheng, and P. Wang, "The request for better measurement: A comparative evaluation of two-factor authentication schemes," *ASIA CCS 2016 - Proc. 11th ACM Asia Conf. Comput. Commun. Secur.*, no. May, pp. 475–486, 2016, doi: 10.1145/2897845.2897916.

[11] R. S. Pressman and B. R. Maxim, *Software Engineering A PRACTITIONER'S APPROACH*. McGraw-Hill, 2020.

[12] D. E. Kurniawan, M. Iqbal, J. Friadi, F. Hidayat, and R. D. Permatasari, "Login Security Using One Time Password (OTP) Application with Encryption Algorithm Performance," *J. Phys. Conf. Ser.*, vol. 1783, no. 1, 2021, doi: 10.1088/1742-6596/1783/1/012041.

[13] J. Zhang, X. Tan, X. Wang, A. Yan, and Z. Qin, "T2FA: Transparent Two-Factor Authentication," *IEEE Access*, vol. 6, pp. 32677–32686, 2018, doi: 10.1109/ACCESS.2018.2844548.

[14] N. Karapanos *et al.*, "Sound-Proof : Usable Two-Factor Authentication Based on Ambient Sound This paper is included in the Proceedings of the," *Usenix Secur.*, 2015.

[15] N. Morze, O. Buinytska, and L. Varchenko-Trotsenko, "Use of Bot-Technologies for Educational Communication At the University," *Eff. Dev. Teach. Ski. Area Ict E-Learning*, vol. 9, pp. 239–248, 2017, [Online]. Available: https://depot.ceon.pl/handle/123456789/15492.

[16] H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim, and M. A. Chaudary, "New and Simple Offline Authentication Approach using Time-based One-time Password with Biometric for Car Sharing Vehicles," *2020 IEEE Asia-Pacific Conf. Comput. Sci. Data Eng. CSDE 2020*, no. April 2021, 2020, doi: 10.1109/CSDE50874.2020.9411569.

[17] C. Adams, G. V. Jourdan, J. P. Levac, and F. Prevost, "Lightweight protection against brute force login attacks on web applications," *PST 2010 2010 8th Int. Conf. Privacy, Secur. Trust*, pp. 181–188, 2010, doi: 10.1109/PST.2010.5593241

[18] CASCAVILLA, G., TAMBURRI, D. A., & VAN DEN HEUVEL, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers and Security, 105, 102258.

[19] HAYATI, M., & FATA, D. (2021). Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan Setoolkit Melalui Teknik Phising. Djtechno Jurnal Teknologi Informasi, 2(1), 2128.https://doi.org/10.46576/djtechno.v2i1.125

[20] GULO, A. S., LASMADI, S., & NAWAWI, K. (2021). Cyber Crime dalam Bentuk PhisingBerdasarkan Undang-Undang Informasi dan Transaksi Elektronik. PAMPAS: Journal of crimimal Law 1(2) ,68-81 https/doi.org/10.22437/ pampas.v1i2.9574Criminal Law, 1(2), 68–81. https://doi.org/10.22437/pampas.v1i2