SPIRIT VOL 17 NO 1 (2025) 12 – 23
JURNAL SPIRIT
0173/C3/DT.05.00/2025

e-ISSN 2721-057X
p-ISSN 2085-3092

SMISHING GUARD: STRATEGI PENGEMBANGAN SISTEM DETEKSI DAN RESPONS ANCAMAN SMS PHISHING

Slamet[1]
Prodi S1 Sistem Informasi [1] (Universitas Dinamika, Surabaya, Indonesia)
slamet@dinamika.ac.id

Naskah diterima: 1 Mei 2025 ; Direvisi : 21 Mei 2025 ; Disetujui : 23 Mei 2025

Abstrak

Dalam beberapa tahun terakhir, serangan SMS phishing (smishing) telah menunjukkan peningkatan signifikan secara global, termasuk di Indonesia, dengan modus yang semakin variatif dan kompleks. Serangan ini mengeksploitasi kelemahan dalam sistem perpesanan seluler dan rendahnya literasi keamanan digital untuk memperoleh informasi sensitif dari korban. Penelitian ini mengusulkan Smishing Guard, sebuah strategi terintegrasi berbasis kecerdasan buatan yang dirancang untuk mendeteksi dan merespons ancaman SMS phishing secara adaptif dan kontekstual. Sistem ini dikembangkan dengan memanfaatkan data dari SMS public gateway sebagai sumber informasi awal, yang merepresentasikan pesan-pesan mencurigakan yang kerap digunakan dalam skema phishing. Melalui pendekatan pembelajaran mesin dan analisis berbasis fitur linguistik dan metadata, Smishing Guard mampu mengidentifikasi pola serangan dengan tingkat akurasi yang tinggi. Selain itu, strategi respons yang diusulkan mencakup notifikasi real-time kepada pengguna serta penyusunan basis data phishing dinamis sebagai upaya mitigasi jangka panjang. Hasil penelitian ini menunjukkan potensi signifikan dalam memperkuat ekosistem keamanan siber, khususnya dalam menanggulangi ancaman smishing yang kian kompleks di era digital.

Kata kunci: SMS phishing, deteksi ancaman, sistem keamanan, SMS public gateway

Abstract

In recent years, SMS phishing (smishing) attacks have shown a significant increase globally, including in Indonesia, with increasingly varied and complex modes. These attacks exploit weaknesses in mobile messaging systems and low digital security literacy to obtain sensitive information from victims. This study proposes Smishing Guard, an integrated strategy based on artificial intelligence designed to detect and respond to SMS phishing threats adaptively and contextually. This system is developed by utilizing data from the SMS public gateway as an initial source of information, which represents suspicious messages that are often used in phishing schemes. Through a machine learning approach and linguistic and metadata feature-based analysis, the Smishing Guard is able to identify attack patterns with a high level of accuracy. In addition, the proposed response strategy includes real-time notification to users and the compilation of a dynamic phishing database as a long-term mitigation effort. The results of this study show significant potential in strengthening the cybersecurity ecosystem, especially in dealing with increasingly complex smishing threats in the digital era.

Keywords: SMS phishing, threat detection, security system, SMS public gateway

PENDAHULUAN

Dalam era digital yang semakin terhubung, keamanan informasi menjadi aspek krusial dalam menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) [1] data pribadi maupun institusional. Salah satu bentuk ancaman siber yang kian meningkat dalam beberapa tahun terakhir adalah serangan *phishing*, khususnya melalui pesan singkat atau *Short Message Service* (SMS). Serangan ini umumnya memanfaatkan *social engineering* [2] untuk mengecoh korban agar memberikan informasi sensitif seperti data perbankan, kode *one time password* (OTP), hingga data identitas pribadi.

Di Indonesia, fenomena SMS *phishing* [3] menunjukkan tren yang mengkhawatirkan. Menurut laporan dari Badan Siber dan Sandi Negara (BSSN) [4] tahun 2023, serangan siber berbasis rekayasa sosial termasuk SMS *phishing* mengalami peningkatan signifikan sebesar 37% dibandingkan tahun sebelumnya. Modus yang digunakan semakin beragam, mulai dari pengakuan palsu sebagai petugas layanan keuangan, hingga pemberitahuan hadiah palsu yang mengarahkan korban pada tautan berbahaya. Tidak jarang, serangan ini disertai dengan manipulasi nomor pengirim yang menyerupai instansi resmi (*spoofing*), sehingga meningkatkan tingkat keberhasilan penipuan.

Fenomena serupa juga terjadi di berbagai negara lain. Di Amerika Serikat, *Federal Trade Commission* (FTC) [5] mencatat kerugian lebih dari USD 330 juta akibat serangan *smishing* pada tahun 2022, meningkat hampir dua kali lipat dibandingkan tahun sebelumnya. Sementara itu, di Inggris, *National Cyber Security Centre* (NCSC) [6] melaporkan bahwa lebih dari 90 juta SMS mencurigakan telah dilaporkan oleh masyarakat sejak diluncurkannya program pelaporan pesan penipuan pada tahun 2020. Negara-negara seperti India, Australia, dan Jerman juga mengalami peningkatan signifikan dalam jumlah laporan SMS *phishing*, dengan pola serangan yang secara umum memanfaatkan celah psikologis korban dan keterbatasan validasi identitas dalam sistem perpesanan seluler.

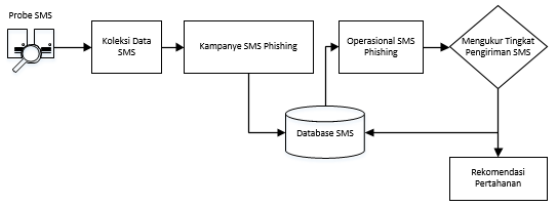
Peningkatan prevalensi serangan SMS *phishing* secara global menunjukkan adanya kebutuhan mendesak untuk mengembangkan sistem deteksi dan mitigasi yang adaptif dan berbasis teknologi mutakhir. Tantangan utama dalam mengidentifikasi dan menangkal SMS *phishing* terletak pada dinamika pola serangan, keterbatasan data untuk pelatihan sistem deteksi otomatis, serta

kurangnya kesadaran keamanan digital di kalangan masyarakat.

Oleh karena itu, penelitian yang berfokus pada pendekatan cerdas dan kontekstual dalam mendeteksi serta mencegah SMS *phishing* menjadi sangat penting untuk mendukung ekosistem keamanan siber yang berkelanjutan. Untuk memperluas pemahaman tentang SMS *Phishing* digunakan SMS *Public Gateway*: *website* yang memungkinkan pengguna untuk melihat pesan yang dikirim ke nomor yang dimiliki oleh *gateway* melalui *interface web*. SMS *Public Gateway* sering memfasilitasi penipuan atau melewatkan verifikasi bukti-bukti kemanusiaan [7].

METODE PENELITIAN

Bagian ini menjelaskan proses penelitian dari Arsitektur *Smishing Guard*, dimulai dengan proses pengumpulan data, menggabungkan pesan-pesan individual ke dalam kampanye, dan mengidentifikasi operasional dari serangan SMS *phishing*[8] [9]. Kemudian dijelaskan eksperimen pengukuran pertahanan SMS dan pengaturan *crawling* untuk mengurai data yang diambil melalui *Public* SMS *Service Provider*[10].



Gambar 2. Arsitektur *Smishing Guard*: Sistem Pertahanan Serangan SMS *Phising*

Gambar 2 menunjukkan arsitektur sistem pertahanan terhadap serangan SMS *phishing* yang disebut *Smishing Guard* [11]. Cara ini dirancang untuk mendeteksi, menganalisis, dan memberikan rekomendasi terhadap potensi ancaman [12] [13]. Proses dimulai dari tahap *probe* SMS atau pengambilan data-data SMS, yaitu aktivitas pengawasan aktif untuk menangkap lalu lintas pesan yang mencurigakan. Data yang diperoleh kemudian dikirim ke modul koleksi data SMS, yang bertugas mengumpulkan dan menyimpan pesan-pesan yang terindikasi sebagai bagian dari serangan *phishing* [14] [15].

Selanjutnya, data hasil koleksi mulai dianalisis pada tahap kampanye SMS *phishing* dengan mengidentifikasi pola, struktur pesan, dan karakteristik kampanye serangan yang sedang berlangsung. Informasi ini digunakan untuk mendukung tahapan berikutnya, yaitu operasional SMS *phishing*, yang merepresentasikan simulasi atau rekonstruksi proses serangan [16]. Tahap ini untuk memahami bagaimana pesan-pesan *phishing* disebarluaskan secara

sistematis kepada calon korban [17] [18] [19].

Tahap pengukuran tingkat pengiriman SMS kemudian dilakukan untuk mengevaluasi skala dan intensitas distribusi serangan, yang menjadi indikator utama dalam menilai potensi risiko keamanan. Semua data dan hasil analisis dari proses kampanye dan operasional disimpan dalam *database* SMS, yang berfungsi sebagai pusat informasi untuk mendukung pengambilan keputusan [20] [21] [22].

Akhirnya, sistem memberikan rekomendasi pertahanan berdasarkan data historis dan hasil pengukuran, yang dapat digunakan oleh entitas keamanan siber untuk merancang strategi mitigasi, peningkatan sistem deteksi dini, serta edukasi pengguna terhadap ancaman smishing.Arsitektur ini bersifat iteratif dan adaptif, memungkinkan sistem untuk terus memperbarui basis datanya seiring dengan evolusi taktik pelaku kejahatan siber, serta menyediakan umpan balik guna memperkuat kebijakan pertahanan yang diterapkan.

HASIL DAN PEMBAHASAN

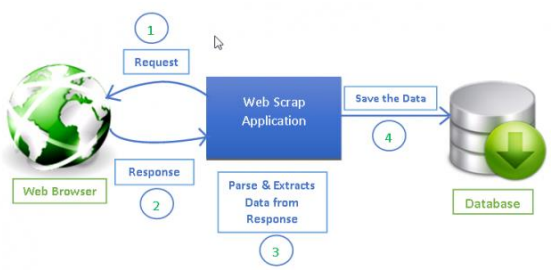
1. Pengumpulan Data

Data pesan SMS dikumpulkan dengan menelusuri (*crawling*) lima SMS gateway yang dapat diakses melalui *browser*. Pesan yang diterima oleh SMS gateway ditampilkan di *websites* yang telah di-*hosting* pada *domain* tertentu, sebagaimana tercantum dalam tabel 1.

Tabel 1. SMS *gateway* yang digunakan dan jumlah SMS *phishing* pada setiap *gateway*

Nama SMS Gateway	Jumlah Pesan	Jumlah pesan phishing
Afreesms.com	1.010.000	2.200
www.smsgatewayhub.com	650.000	1.010
textlocal.com	16.500.015	72.000
SendAnonymousSMS.com	230.000	3.201
gosmsgateway.com	1.003	10

Untuk melakukan ekstraksi *(crawling)* data dari *website* digunakan aplikasi *open source* bernama Scrapy [17]. Halaman *web* ini menampilkan isi pesan mentah dengan fitur seperti: URL, OTP, dan menjelaskan informasi metadata yang berguna tentang pesan tersebut. Metadata untuk setiap pesan berisi nomor telepon sumber, nomor telepon tujuan, dan waktu. Berbagai model *gateway* menerapkan bidang ini dengan cara berbeda, namun pada *crawler* ini mengekstrak metadata dan isi pesan dari setiap *gateway*, kemudian menyimpannya dalam *data base* lokal. Cara kerja dari SMS *crawling* dapat dilihat pada gambar 3.



Gambar 3. Cara kerja sistem SMS *crawling*
Sumber: https://www.datacamp.com/

Pada saat melakukan *crawling*, data yang dihimpun sempat berhenti diterima dari salah satu SMS *gateway* karena *provider reverse-proxy* memblokir IP Address penelitian. Selain itu, sebagian besar SMS *gateway* tidak menampilkan meta waktu yang tepat. Namun, SMS *gateway* ini menampilkan meta waktu relatif (misalnya satu jam yang lalu, 3 hari yang lalu, dan sebagainya). Unit meta waktu yang tampil digunakan untuk menghitung jendela waktu untuk setiap pesan ketika meta waktu yang tepat tidak tersedia. Data dikumpulkan dari lima SMS *gateway* yang berbeda, *gateway* ini terkadang berisi nomor telepon tujuan yang sama. Oleh karena itu, isi pesan dan jendela waktu digabungkan untuk membuang pesan duplikat yang dikumpulkan oleh *crawler*.

Data mentah yang dikumpulkan dari gateway diperkaya dengan melakukan *post processing* metadata dan isi pesan. Negara, tempat, dan nomor telepon tujuan diidentifikasi dengan menggunakan kode negara dan format penomoran. *Post processing* juga melakukan ekstraksi URL, alamat email, nomor telepon, dan OTP yang disematkan di dalam isi pesan.

URL yang diekstrak dari isi pesan dinyatakan (dideteksi) berbahaya atau tidak berbahaya dengan menggunakan *VirusTotal*[18], dan *Google Safe Browsing*[19]. URL ditandai berbahaya sebagai Pesan SMS berbahaya jika *VirusTotal* menandai URL sebagai berbahaya, demikian juga jika *Google Safe Browsing* menandai URL sebagai Pesan SMS *phishing*. Peneliti menghapus perilaku seperti penipuan lebih lanjut yang mungkin tidak sepenuhnya *phishing*, seperti aplikasi pinjaman *online*, dan unduhan file berbahaya.

Rata-rata, SMS gateway ini menerima 15 pesan *phishing* per hari, menjadikan *honeypot* berhasil mengisolasi sebanyak 6.559 pesan *phishing*. Persentase rata-rata pesan *phishing* untuk satu hari adalah 0,025% dengan median 0,015% (dari lalu lintas hari itu).

2. Kampanye SMS *Phishing*

Kampanye SMS *phishing* [20] didefinisikan sebagai kumpulan pesan *phishing* identik tetapi memiliki pengenal berbeda. Pengenal ini mencakup URL, nomor telepon, alamat email, dan OTP. Kampanye SMS *phishing* dilakukan dengan menggabungkan pesan *phishing* individual yang menggunakan bahasa identik sambil bersikap agnostik terhadap perubahan

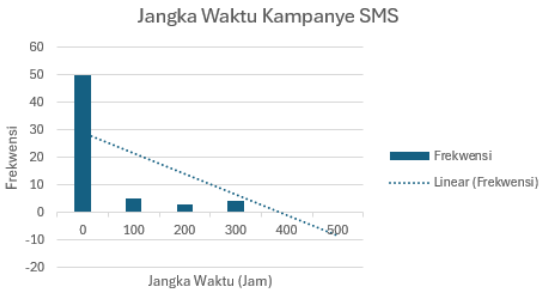
apapun pada pengenal yang ada dalam pesan. Teknik agregasi pesan *phishing* dilakukan terlebih dahulu dengan menormalisasi pesan individual seperti mengganti nomor telepon, alamat email, OTP, dan URL dengan token khusus yang sesuai. Misalnya, "OTP Anda adalah 2345 diubah menjadi "OTP Anda adalah #OTP", dan "Periksa penawaran ini di abcde[.]com menjadi "Periksa penawaran ini di #URL".

Setelah melakukan normalisasi pesan, pesan *phishing* yang identik dikelompokkan untuk kampanye *phishing*. Dengan menggabungkan pesan-pesan *phishing* individual ke dalam kampanye SMS *phishing*, variasi di berbagai kampanye dan evolusinya dapat dipelajari. Pada tabel 2 berikut adalah lima konten teratas yang digunakan kampanye.

Tabel 2. Lima Kampanye SMS *Phishing*

No	Kampanye Phising
1	Pelanggan Yth. Nomor# Nanti malam tepat pukul 12, semua +2000 COIN PULSA Anda Hangus! SEGERA ambil di *500*55# Dan tukar jadi PULSA 2x lipat!* Hubungi *500*55# sekarang.
2	Dapatkan 5rb saldo Gopay/LinkAja bagi 500 responden pertama dengan ikuti survei singkat! Klik untuk berpartisipasi: https://tsurvey.id/s/GD8w4f S&K berlaku.
3	Pelanggan Yth, Selamat nomor Anda resmi mendapat Hadiah 150 Juta berkat isi ulang pulsa dari XX no PIN;25e452 u/ info klik; www.xxx.xxx
4	Nasabah Bank BRI Yth; No. Rek Anda mendapat hadiah Cek Rp.27Jt dari BRI Untung Beliung BRITAMA Pin Anda: (ijh7455k1) Infor klik www.info-.xxx
5	Kejutan TikTok Bonus No Anda Terpilih mendapatkan 45Jt. dari Aplikasi TIK TOK. Info Lebih lanjut Hub WA:0812345xxxx

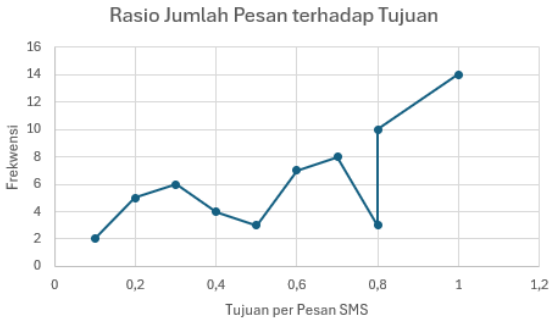
Pada periode ini dilakukan sebanyak 538 kampanye SMS *phishing*. Hasilnya rata-rata kampanye *phishing* berlangsung selama 9 hari dengan masa aktif rata-rata 0,32 hari. Pada gambar 4 ditunjukkan distribusi masa aktif kampanye SMS *phishing*.



Gambar 4. Jangka waktu antara pesan *phishing* pertama dan terakhir

Selain itu, Kampanye SMS *phishing* cenderung memiliki rasio pesan tiga, dua atau satu ke tujuan. Distribusi trimodal ditemukan dari rasio tujuan terhadap jumlah pesan dalam kampanye dan jumlah tujuan yang ditargetkan. Beberapa kampanye menargetkan satu kali, dua kali, atau tiga sampai empat kali angka yang sama.

Pada gambar 5 terlihat distribusi rasio jumlah pesan terhadap jumlah tujuan (1 berarti untuk setiap nomor yang ditargetkan, artinya kampanye mengirimkan satu pesan, sementara 0,2 berarti kampanye mengirimkan lima pesan untuk setiap satu tujuan,). Aktor jahat dapat melakukan spam pada nomor yang sama beberapa kali untuk mengimbangi tingkat pengiriman yang buruk; tidak ada pekerjaan sebelumnya yang mengukur tingkat pengiriman untuk penyedia pesan massal.



Gambar 5. Distribusi rasio jumlah pesan terhadap jumlah tujuan.

3. Operasi SMS *Phishing*

Pada tahap ini diproyeksikan pesan *phishing* dan infrastruktur web yang digunakan oleh pesan-pesan ini ke dalam grafik bipartit *non-directional*. Operasi SMS *phishing* dilakukan dengan mengekstrak komponen-komponen grafik yang terhubung. Grafik bipartit, menurut definisi, memiliki dua jenis *node*, yaitu *node* konten dan *node* infrastruktur. *Node* konten mewakili isi pesan *phishing*, dan *node* infrastruktur mewakili URL *phishing* yang diidentifikasi sebelumnya. Konstruksi grafik bipartit mengungkapkan hubungan antara *node* konten dan *node* infrastruktur yang sesuai. Untuk setiap *node* konten, *edge* digambar untuk menghubungkan *node* konten ke *node* infrastruktur yang sesuai yang mewakili URL yang tertanam dalam konten pesan. Kemudian komponen yang terhubung dari grafik diekstrak untuk menampilkan operasi SMS.

Pendekatan berbasis grafik untuk memastikan bahwa koneksi antara pesan dan infrastruktur web bersifat non-probabilistik, sehingga menghilangkan tantangan yang terkait dengan pemilihan algoritma pengelompokan yang tepat atau *tuning hyperparameter*. Dalam penelitian ini diungkap banyak kampanye yang isi pesannya lengkap adalah URL, tanpa konten lain.

Beberapa kampanye lain berisi beberapa karakter teks tambahan beserta URL. Kampanye ini (tercantum dalam tabel 3) dihapus dari grafik bipartit karena tidak adanya isi pesan yang menyertai URL. Dalam mengenal entitas digunakan SpaCy 3.5 [21] untuk mengekstrak referensi ke merek dan organisasi dalam isi pesan. Bahasa yang digunakan dalam isi pesan diidentifikasi menggunakan polyglot [22].

Tabel 3. Karakter teks dan URL dalam kampanye

No	Kampanye Phising
1	#URL #URL #URL: #URL dear #URL Hi! #URL #URL plan #URL #OTP 2 : #URL fyavyayvayva #URL Confirm: #URL HII: #URL W0W #URL

Terdapat 5.123 pesan ke dalam 152 operasi. Dengan melihat kumpulan data kampanye SMS *phishing* kami sebagai grafik kampanye *phishing* dan URL, komponen yang terhubung dari grafik diisolasi sebagai operasi SMS *phising*. Dari 152 operasi, ditemukan bahwa rata-rata, sebagian besar operasi berlangsung singkat (kurang dari satu jam).

4. Mengukur Tingkat Pengiriman SMS

Tingkat pengiriman SMS diukur dari layanan *Application-to-Peer* (A2P) ke telepon selular. Pesan-pesan ini dibuat dengan cara yang terkendali menggunakan *service provider* pesan massal dan dikirim ke beberapa nomor telepon HP yang berbeda di berbagai operator, seperti yang ditunjukkan pada tabel 4. Jenis penipuan SMS *phishing* yang terkenal (penipuan pengiriman paket) digunakan untuk menyusun isi pesan. Isi pesan juga berisi URL yang tidak berbahaya. Pesan yang dibuat adalah "Ambil sesegera mungkin! Paket Anda sedang menunggu untuk dikirim dalam satu jam. Harap konfirmasikan informasi pengiriman #URL." Meskipun URL di setiap pesan ini menggunakan *domain* tingkat atas yang sama, *subdomain* yang berbeda juga digunakan untuk setiap pesan. Permintaan yang dibuat dicatat ke *subdomain* ini. Hal ini digunakan untuk mempelajari permintaan apa pun yang dibuat ke *subdomain* tertentu saat SMS melintasi jaringan hingga dikirim ke tujuan.

Tabel 4. Rating pengiriman SMS massal

No	Nama Provider	Dikirim Personal	Dikirim melalui A2P
1	Telkom	Diterima	Diterima
2	Indosat	Diterima	Diterima
3	XL	Diterima	Diterima
4	Three	Diterima	Diterima
5	Axis	Diterima	Diterima
6	SmartFren	Diterima	Diterima

5. Rekomendasi Perbaikan

Peneliti merumuskan rekomendasi berikut berdasarkan temuan studi ini. Rekomendasi ini bertujuan untuk memberikan solusi atas kerentanan pengguna yang menjadi target dalam serangan *phishing*.

Berikut adalah beberapa rekomendasi perbaikan:

a. Perangkat seluler tidak dapat mendeteksi tautan berbahaya yang dikirim melalui SMS. Pengguna yang menjadi target harus berhati-hati saat mengeklik tautan mencurigakan dari nomor yang tidak dikenal karena tidak ada deteksi kesalahan yang muncul dari pengiriman melalui SMS. Di perangkat seluler, URL berbahaya juga ditampilkan sebagian yang dapat membuat pengguna yang menjadi target berpikir bahwa situs tersebut asli. Hal terbaik yang dapat dilakukan untuk mencegah serangan dan mengurangi risiko adalah dengan menghindari SMS berbahaya yang dikirim, baik dari kontak tepercaya maupun tidak dikenal karena nomor kontak mereka dapat disusupi. Pengguna yang menjadi target juga harus waspada dan melihat URL tujuan dari tautan yang dikirim.
b. Integrasi *Google Tag Manager* dan *Google Analytics* dalam *website* palsu dapat melewati deteksi kesalahan *Facebook Messenger*, serta Standar Keamanan Google Mail. *Google Analytics* dapat digunakan sebagai alat pengintaian

yang mendeteksi informasi sensitif dari pengguna yang menjadi target. Hal ini dapat dihindari dengan mewaspadai tautan yang dikirim di media sosial. Pencantuman URL dalam daftar hitam dan putih juga dapat meminimalkan risiko membuka URL yang tidak tepercaya. Pengguna yang menjadi target dapat mengizinkan atau memblokir URL tertentu di Google Chrome, yang mencegah mereka mengakses URL yang ditolak dan mengizinkan URL tepercaya.

c. Waspada dan Bersikap Skeptis. Saat menerima pesan SMS atau email, bersikap hati-hati sangatlah penting, terutama saat pesan tersebut meminta informasi pribadi atau mendesak tindakan segera. Penting untuk memverifikasi identitas pengirim sebelum menanggapi atau mengeklik tautan apa pun.
d. Waspada terhadap pesan teks yang tidak diminta, terutama yang menawarkan hadiah, diskon, atau permintaan mendesak yang tidak terduga, karena pesan tersebut dapat berupa serangan *smishing* untuk menipu agar membagikan informasi atau mengunduh konten yang berbahaya. Meskipun pengirimnya tampak familier, bersikap skeptis terhadap pesan teks yang meminta informasi pribadi dapat dilakukan karena organisasi yang sah biasanya tidak meminta informasi sensitif melalui pesan teks.
e. Mengaktifkan 2FA (Autentikasi Dua Faktor) di Semua Perangkat. Mengaktifkan 2FA pada akun daring pribadi dan bisnis merupakan langkah penting untuk melindungi diri dari *smishing* dan *phishing*. Untuk mengakses akun memerlukan langkah verifikasi kedua, biasanya berupa kode unik yang dikirim ke ponsel. Bahkan jika penyerang berhasil mendapatkan kata sandi, *intruder* tetap memerlukan kode tambahan tersebut untuk masuk. Langkah tambahan ini secara drastis mengurangi risiko akses tidak sah, meningkatkan keamanan akun dan membuatnya jauh lebih sulit untuk dibobol.
f. Tidak Membagikan Informasi Sensitif dalam Pesan yang Tidak Aman. Tidak membagikan data sensitif melalui pesan teks SMS atau email yang tidak aman, baik untuk data pribadi atau perusahaan. Individu atau organisasi yang sah tidak akan pernah meminta untuk memberikan informasi semacam ini melalui saluran mana pun. Meskipun telah memiliki akun email yang aman, harus dilakukan verifikasi pengirim sebelum memberikan data sensitif.
g. Menggunakan Perangkat Lunak Keamanan Terbaru. Ponsel, komputer pribadi, dan komputer kantor harus

memiliki perangkat lunak anti-virus dan anti-malware yang tangguh dengan versi terbaru. Perangkat lunak ini akan melindungi perangkat dan data jika terjadi pemasangan *malware* atau virus melalui serangan *smishing* atau *phishing*. Solusi terbaik juga menawarkan pendeteksian, penyaringan, dan pelaporan SMS dan pesan email yang mencurigakan.

h. Mencegah *Smishing* dan *Phishing* dengan Kesadaran Keamanan. Salah satu cara terbaik untuk menghentikan *smishing* dan *phishing* adalah melalui pendidikan dan pelatihan keamanan siber karyawan yang membantu menciptakan budaya kesadaran. Budaya keamanan yang kuat dapat menurunkan risiko dari ancaman siber dengan memotivasi personel untuk menganggap serius keamanan, melatih orang tentang praktik terbaik, dan menanamkan rasa tanggung jawab untuk mengamankan data sensitif.

PENUTUP

Penelitian ini berhasil mengembangkan pendekatan sistematis dalam mengumpulkan, mengkategorikan, dan menganalisis data SMS *phishing* dengan mengandalkan lima SMS *gateway* sebagai sumber utama. Dengan menggunakan teknik *crawling* berbasis Scrapy, data pesan berhasil diekstraksi dan diperkaya melalui pemrosesan metadata serta deteksi URL berbahaya menggunakan *VirusTotal* dan *Google Safe Browsing*. Hasilnya, sebanyak 6.559 pesan phishing berhasil diisolasi dengan tingkat kemunculan rata-rata 0,025% per hari.

Analisis kampanye *phishing* menunjukkan bahwa serangan sering dilakukan dalam bentuk pesan-pesan yang memiliki konten serupa namun menggunakan pengenal yang berbeda, dengan masa aktif kampanye relatif singkat dan pola distribusi trimodal dalam rasio pesan terhadap tujuan. Pemetaan operasi *phishing* melalui grafik bipartit mengungkapkan hubungan yang erat antara isi pesan dan infrastruktur URL, dan sebanyak 152 operasi berhasil diidentifikasi, dengan durasi operasi umumnya kurang dari satu jam.

Eksperimen pengukuran tingkat pengiriman SMS menunjukkan tantangan dalam mendeteksi dan menghalau pesan phishing, meskipun pesan dikirim melalui penyedia layanan massal yang sah. Selain itu, analisis lebih lanjut menyoroti kelemahan perangkat seluler dalam mendeteksi tautan berbahaya dan mengekspos pengguna terhadap risiko tinggi.

Berdasarkan temuan ini, penelitian merekomendasikan berbagai strategi

mitigasi, termasuk peningkatan kesadaran pengguna terhadap smishing, penerapan autentikasi dua faktor (2FA), penggunaan perangkat lunak keamanan terbaru, dan pembentukan budaya keamanan siber di tingkat individu maupun organisasi. Implementasi langkah-langkah ini diharapkan dapat mengurangi risiko serangan phishing berbasis SMS secara signifikan dan meningkatkan ketahanan pengguna terhadap ancaman keamanan siber di masa depan.

DAFTAR PUSTAKA

[1] K. Y. Chai and M. F. Zolkipli, "Review on Confidentiality, Integrity and Availability in Information Security," *Journal of ICT In Education*, vol. 8, no. 2, pp. 34–42, 2021, doi: 10.37134/jictie.vol8.2.4.2021.

[2] S. Slamet, "Pertahanan Pencegahan Serangan Social Engineering Menggunakan Two Factor Authentication (2Fa) Berbasis Sms (Short Message System)," *Spirit*, vol. 14, no. 2, pp. 23–29, 2023, doi: 10.53567/spirit.v14i2.260.

[3] A. A. C.Meenakshi, "SmishSMS- The Latest Detection of SMS Phishing Trends," *Tuijin Jishu/Journal of Propulsion Technology*, vol. 44, no. 4, pp. 796–806, 2023, doi: 10.52783/tjjpt.v44.i4.936.

[4] Id-SIRTII /CC, "Lanskap Keamanan Siber Indonesia," *Id-SIRTII /CC*, no. 70, pp. 1–107, 2023.

[5] Federal Trade Commission, "Annual Performance Report for Fiscal Year 2022 and Annual Performance Plan for Fiscal Years 2023 to 2024," 2023, [Online]. Available: https://www.ftc.gov/system/files/ftc_gov/pdf/p859900fy22apr_fy23-24app.pdf.

[6] S. Pokhrel, "Annual Review 2024," *Αγαη*, vol. 15, no. 1, pp. 37–48, 2024.

[7] B. Reaves, N. Scaife, D. Tian, L. Blue, P. Traynor, and K. R. B. Butler, "Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways," *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, pp. 339–356, 2016, doi: 10.1109/SP.2016.28.

[8] E. N. Ekwonwune and V. C. Enyinnaya, "Design and Implementation of End to End Encrypted Short Message Service (SMS) Using Hybrid Cipher Algorithm," *Journal of Software Engineering and Applications*, vol. 13, no. 03, pp. 25–40, 2020, doi: 10.4236/jsea.2020.133003.

[9] O. Corporation, "Oracle ® Communications Convergent Charging Controller SMS Center Technical Guide," no. October, 2023.

[10] S. M. Peer-to-peer and P. Specification, "Short Message Peer-to-Peer Protocol Specification Version 5.0," 2023, [Online]. Available: www.smsforum.net.

[11] H. O. Lasisi, O. Oladepo, T. T. Awofolaju, and K. G. Olalekan, "Enhancement of Signaling System Number 7 for Improved Quality of Service in Mobile Communication Network," vol. 6, no. 1, pp. 197–204, 2023.

[12] A. J. Kouam, A. C. Viana, and A. Tchana, "SIMBox Bypass Frauds in Cellular Networks: Strategies, Evolution, Detection, and Future

Directions," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 4, pp. 2295–2323, 2021, doi: 10.1109/COMST.2021.3100916.

[13] D. C. Dewi, V. Y. Utami, and S. Y. M. Yusuf, "Peningkatan Kinerja Aparatur Melalui Sistem Informasi SHORT MESSAGE SERVICES (SMS) GATEWAY Pada Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kota Makassar," *Ranah Publik Indonesia Kontemporer*, vol. 1, no. 2, pp. 1–12, 2021.

[14] R. Zieni, L. Massari, and M. C. Calzarossa, "Phishing or Not Phishing? A Survey on the Detection of Phishing Websites," *IEEE Access*, vol. 11, no. January, pp. 18499–18519, 2023, doi: 10.1109/ACCESS.2023.3247135.

[15] W. Li, S. Manickam, S. U. A. Laghari, and Y. W. Chong, "Uncovering the Cloak: A Systematic Review of Techniques Used to Conceal Phishing Websites," *IEEE Access*, vol. 11, no. June, pp. 71925–71939, 2023, doi: 10.1109/ACCESS.2023.3293063.

[16] B. Tejaswi, N. Samarasinghe, S. Pourali, M. Mannan, and A. Youssef, "Leaky Kits: The Increased Risk of Data Exposure from Phishing Kits," *eCrime Researchers Summit, eCrime*, vol. 2022-Novem, 2022, doi: 10.1109/eCrime57793.2022.10142092.

[17] T. Mynttinen, "Long Tran DATA SCRAPING APPLICTION WITH SCRAPY," 2023.

[18] B. Improve, "VirusTotal Enterprise," 2021.

[19] T. Gerbet and A. Kumar, "On the (In) security of Google Safe Browsing," pp. 1–20, 2022.

[20] E. B. Blancaflor, A. B. Alfonso, K. N. U. Banganay, G. A. B. D. Cruz, K. E. Fernandez, and S. A. M. Santos, "Let's Go Phishing: A Phishing Awareness Campaign Using Smishing, Email Phishing, and Social Media Phishing Tools," *Proceedings of the International Conference on Industrial Engineering and Operations Management*, no. Sanchez 2020, pp. 260–269, 2021, doi: 10.46254/ap01.20210108.

[21] N. A. F. ICHIDA, "Optimasi Algoritma Simplified Lesk Dengan Spacy Untuk Word Sense Disambiguation Pada Kalimat Bahasa Inggris," *Jurnal Khatulistiwa Informatika*, vol. 12, no. 1, pp. 13–18, 2024, doi: 10.31294/jki.v12i1.21404.

[22] N. Nystrom, M. R. Clarkson, and A. C. Myers, "Polyglot: An extensible compiler framework for Java," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2622, pp. 138–152, 2003, doi: 10.1007/3-540-36579-6_11.