ABDITEKNIKA
Jurnal Pengabdian Kepada Masyarakat
Volume 4 Nomor 1 April 2024 Halaman 28-33
DOI : https://doi.org/10.31294/abditeknika.v4i1.3146 ISSN 2775-1694

Sosialisasi Penggunaan Media Sosial yang Aman dari Bahaya Phishing di Masjid Al Huda Pandeyan

Indrawan Ady Saputro[1*], Lilik Sugiarto[2], Febrianta Surya Nugraha[3], Nurhidayanto[4]

[1,2,3,4] STMIK AMIKOM Surakarta
Jl. Veteran, Dusun I, Singopuran, Kec. Kartasura, Kabupaten Sukoharjo, Jawa Tengah 57163

email korespondensi: indrawanadysaputro@gmail.com

Submit: 16-01-2024 | Revisi : 23-01-2024 | Terima : 29-01-2024

Abstrak
Ancaman penyebaran tindak kejahatan *phishing* melalui platform media sosial semakin menjadi-jadi oleh pihak-pihak yang tidak bertanggung jawab. Dampak dari kejahatan *phishing* dapat mencakup kerugian baik secara materiil, finansial, maupun psikologis. Oleh karena itu, sangat penting untuk mengambil langkah-langkah pencegahan guna melindungi diri dari potensi serangan *phishing* yang dapat terjadi. Salah satu metode yang dapat diterapkan adalah melalui kegiatan sosialisasi tentang penggunaan media sosial di Masjid Al Huda Pandeyan, bertujuan untuk memberikan perlindungan kepada jamaah dari risiko *phishing*. Tujuan utama dari kegiatan ini adalah menciptakan lingkungan di mana para jamaah dapat menggunakan media sosial dengan bijak dan aman, serta terhindar dari potensi bahaya kejahatan siber, termasuk *phishing*. Jumlah peserta dalam kegiatan sosialisasi sebanyak 25 peserta. Pendekatan yang diadopsi dalam sosialisasi ini melibatkan metode ceramah dan diskusi. Dari hasil kegiatan sosialisasi ini, bahwa sosialisasi yang telah dilakukan pada jamaah Masjid Al Huda Pandeyan mendapatkan respons positif. Dari hasil kuisioner 32% peserta menilai bahwa kegiatan tersebut berjalan dengan "baik" dan 68% menilai kegiatan tersebut "Sangat baik". Mayoritas peserta, yang sebagian besar adalah pengguna media sosial, merespon kegiatan tersebut dengan baik.

Kata Kunci : Sosialisasi, Media Sosial, *Phishing*

Abstract
The threat of spreading phishing crimes through social media platforms is increasingly being carried out by irresponsible parties. The impact of phishing crimes can include material, financial, or psychological losses. Therefore, it is very important to take precautionary steps to protect yourself from potential phishing attacks that can occur. One method that can be applied is through socialization activities about the use of social media at Masjid Al Huda Pandeyan, aimed at providing protection to worshippers from the risk of phishing. The main goal of this activity is to create an environment where pilgrims can use social media wisely and safely, and avoid the potential dangers of cybercrime, including phishing. The number of participants in the socialization activity was 25 participants. The approach adopted in this socialization involves the method of lectures and discussions. From the results of this socialization activity, that the socialization that has been carried out at the Al Huda Pandeyan Mosque congregation received a positive response. From the results of the questionnaire, 32% of participants rated the activity "good" and 68% rated it "very good". The majority of participants, most of whom were social media users, responded well to the event.

Keywords : Socialization, Social Media, Phishing

1. Pendahuluan

Penggunaan media sosial yang semakin populer telah membawa dampak signifikan pada kehidupan manusia, termasuk dalam konteks keamanan. Beberapa ancaman dari bahaya keamanan siber antara lain : *social engineering, hacking, cracking,* dan *phishing*. Pengabdian sebelumnya melakukan kegiatan sosialisasi tentang *social engineering*. Kegiatan tersebut dilaksanakan secara webinar atau daring dengan sasaran peserta ibu-ibu PKK (Tyas Darmaningrat et al., 2022). Pengabdian lainnya (Wathoni et al., 2023) melakukan kegiatan sosialisasi kesadaran keamanan siber dengan sasaran peserta guru. Berbeda dengan pengabdian sebelumnya, sasaran peserta pada pengabdian ini adalah jamaah pada Masjid Al Huda Pandeyan dan mengangakat tema sosialisasi berkaitan dengan salah satu ancaman utama yang muncul dari penggunaan media sosial adalah *phishing*. *Phishing* adalah sebuah teknik manipulasi psikologis yang digunakan oleh penyerang untuk mencuri informasi pribadi dari

pengguna media sosial (Ramadhan et al., 2022) (DM et al., 2022). Sosialisasi kepada masyarakat bertujuan menjelaskan cara kerja *phishing*, jenis-jenis serangan *phishing* di media sosial, dan dampaknya. Selain itu, disampaikan juga cara menghindari serangan *phishing*, seperti meningkatkan kesadaran risiko dan mengatur privasi di akun media sosial.

Phishing adalah suatu bentuk serangan keamanan siber yang menggunakan manipulasi atau tipuan untuk memperoleh informasi pribadi, seperti kata sandi, nomor kartu kredit, atau data keuangan lainnya, dari korban (Safi & Singh, 2023) (Budi et al., 2021). Penyerang yang melakukan *phishing* mencoba membuat korban percaya bahwa berinteraksi dengan entitas yang sah atau tepercaya, seperti bank, situs web e-commerce, atau layanan online lainnya (Naqvi et al., 2023) (Wahyudi et al., 2022).

Metode umum *phishing* melibatkan pengiriman pesan atau email palsu yang menyerupai komunikasi resmi dari institusi atau perusahaan tertentu, dengan tujuan agar korban mengungkapkan informasi sensitif atau mengklik tautan berbahaya (Putra Y, 2021). Tujuan akhirnya adalah untuk mencuri identitas atau informasi keuangan korban untuk kepentingan penipuan atau kejahatan siber lainnya (Desolda et al., 2023). Kesadaran dan kehati-hatian pengguna internet dalam mengenali dan menghindari serangan *phishing* menjadi kunci dalam menjaga keamanan siber pribadi (Latifahi et al., 2022).

Dengan pemahaman mengenai bahaya *phishing*, diharapkan pengguna media sosial dapat lebih berhati-hati dalam interaksi online, meningkatkan keamanan siber. Berdasarkan hasil survei APJII, pengguna internet di Indonesia mencapai 215,63 juta orang pada 2022-2023 (APJII, 2022). *Phishing*, sebagai bentuk serangan siber, merupakan ancaman serius yang mencuri informasi pribadi . Ada berbagai jenis *phishing*, seperti email, smishing, *vishing*, *spear phishing*, dan *pharming* (Wibowo & Fatimah, 2017) berikut penjelasannya :

1. *Phishing* melalui Email: Salah satu varian umum dari teknik *phishing* adalah melalui email. Dalam skenario ini, penyerang mengirimkan email palsu yang terlihat seolah-olah berasal dari sumber terpercaya, seperti lembaga keuangan atau bank. Kemudian meminta penerima email untuk memberikan informasi pribadi atau mengklik tautan yang mengarahkan ke situs web palsu (Jahankhani et al., 2014).
2. *Smishing (SMS Phishing)*: *Smishing* melibatkan penggunaan pesan teks (SMS) untuk menipu individu agar memberikan informasi pribadi atau mengklik tautan berbahaya. Pesan teks ini seringkali menyajikan situasi yang mendesak, seperti peringatan tentang masalah akun pengguna, dengan tujuan meminta tindakan segera (Soykan & Bagriyanik, 2020).
3. *Vishing* (*Voice Phishing*): *Vishing* melibatkan penggunaan panggilan suara. Penyerang dapat menelepon target dan berupaya memperoleh informasi pribadi atau rahasia dengan menyamar sebagai entitas resmi atau terpercaya. Pendekatan ini menggunakan komunikasi suara untuk menciptakan ilusi keaslian (Pranata & Ependi, 2023).
4. *Spear Phishing*: *Spear phishing* merupakan bentuk *phishing* yang diarahkan khusus pada satu individu atau organisasi tertentu. Dalam taktik ini, penyerang mengumpulkan informasi pribadi tentang target untuk menciptakan pesan yang lebih meyakinkan dan sulit dideteksi (Prasetyo et al., 2023).
5. *Pharming*: Dalam serangan *pharming*, penyerang berusaha mengarahkan lalu lintas internet dari situs web yang sah ke situs web palsu tanpa pengetahuan pengguna. Ini dapat dilakukan melalui teknik DNS spoofing atau perubahan pada file host, menciptakan kesan situs palsu yang sebenarnya terlihat otentik (Utin Indah Permata Sari, 2022).

Masyarakat di Masjid Al Huda Pandeyan, terutama takmir dan remaja, belum sepenuhnya menyadari bahaya *phishing*. Dalam penelitian ini, sosialisasi dilakukan secara berkala agar pemahaman terus berkembang. Materi sosialisasi diharapkan dapat memberikan pandangan tentang cara mencegah kejahatan internet, khususnya terkait web *phishing*. Kesadaran akan pentingnya menjaga keamanan informasi menjadi kunci dalam menghadapi dampak negatif yang mungkin ditimbulkan oleh penggunaan teknologi yang tidak bertanggung jawab.

2. Metode

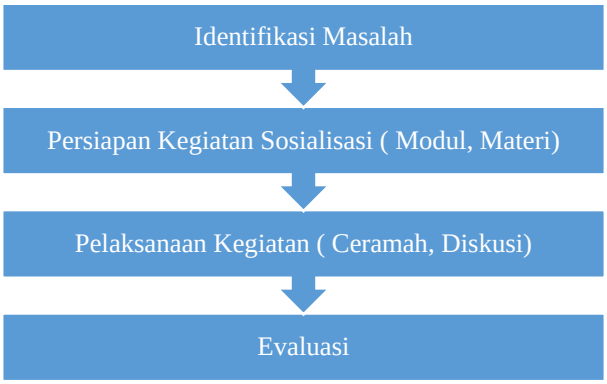
Pendekatan yang digunakan dalam kegiatan sosialisasi tentang penggunaan media sosial yang aman dari ancaman *phishing* di Masjid Al Huda Pandeyan melibatkan penyampaian informasi melalui ceramah dan pemberian ruang diskusi. Kegiatan dimulai dengan menyampaikan ceramah atau pemaparan informasi berkaitan dengan media sosial dan pengenalan *phishing* serta kasus-kasus yang diakibatkan oleh kejahatan phishing yang disebarluaskan melalui sosial media. Berikut ini tahapan pengabdian kepada masyarakat yang dilakukan dapat dilihat pada gambar 1.

Tahapan pengabdian terdiri dari identifikasi masalah, persiapan kegiatan, pelaksanaan kegiatan dan evaluasi kegiatan. Berikut ini penjelasannya :

1. Identifikasi Masalah
   Pada tahap ini tim pengabdian melakukan riset terkait permasalahan yang sedang marak terjadi pada perkembangan internet sekarang ini. Setelah mendapatkan sebuah permasalahan dilanjutkan proses observasi dan wawancara kepada pihak Takmir Masjid Al Huda Pandeyan. Berdasarkan hasil observasi dan wawancara tim pengabdian memberikan solusi terkait sosialisasi penggunaan media sosial yang aman dari bahaya *phishing*.
2. Persiapan Kegiatan

Sebelum melakukan pelaksanaan kegiatan tim pengabdian mempersiapkan modul buku untuk nanti diberikan kepada pihak takmir dan remaja masjid. Selain itu mempersiapkan materi untuk kegiatan sosialisasi di lokasi Masjid Al Huda Pandeyan.

3. Pelaksanaan Kegiatan
   Pelaksanaan kegiatan pengabdian kepada masyarakat dilaksanakan pada hari Sabtu, 20 Oktober 2023 pukul 19.30 WIB di Masjid Al Huda Pandeyan, Ngemplak, Boyolali. Kegiatan pelaksanaan berjalan dengan lancar dan diikuti sebanyak 25 peserta terdiri dari Target peserta pada kegiatan pengabdian kepada masyarakat ini adalah bapak/ibu takmir, remaja masjid dan masyarakat jama'ah Masjid Al Huda Pandeyan
4. Evaluasi
   Tahap evaluasi dilakukan pada saat akhir sesi menggunakan tanya jawab dengan peserta atau audiens kepada pemateri yang sudah memberikan materi sosialisasi.



Gambar 1. Tahapan Pengabdian Kepada Masyarakat

3. Hasil dan Pembahasan

Kegiatan ini diawali dengan pengenalan tentang media sosial (perkembangan sosial media, dampak positif dan negatif). Kemudian dilanjutkan dengan pengenalan *phishing* (jenis *phishing*, dampak berbahaya, simulasi *phishing*). Setelah itu disampaikan juga terkait kasus-kasus yang berkaitan dengan kejahatan phishing yang memanfaat media sosial untuk melakukan penyebaran. Berikut ini dokumentasi pelaksanaan seminar terlihat pada gambar 2.

Gambar 2. Pelaksanaan Sosialisasi

Rincian kegiatan sosialisasi pada takmir dan remaja masjid Al Huda Pandeyan terlihat pada tabel 1.

Tabel 1. Rincian Kegiatan Sosialisasi

Jadwal	Kegiatan
19.30-19.45	Pembukaan
19.45-20.15	Materi Pengenalan Sosial Media
	Sesi Tanya Jawab
20.15-20.45	Materi Pengenalan *Phishing*
	Sesi Tanya Jawab

Jadwal	Kegiatan
20.45-21.30	Materi Simulasi dan Pencegahan *Phishing* Sesi Tanya Jawab
21.30-21.40	Evaluasi
21.40-21.45	Penutup

Hasil pelaksanaan kegiatan menjelaskan tentang beberapa materi yaitu pengenalan sosial media, phishing, simulasi dan pencegahannya. Materi Pengenalan Sosial Media mencakup konsep dan definisi sosial media, contoh platform populer, diskusi peran sosial media sehari-hari dengan dampaknya pada hubungan personal dan profesional, identifikasi potensi risiko keamanan, penjelasan risiko privasi, pencurian identitas, dan penipuan online, serta panduan praktis untuk menjaga keamanan akun beserta pemahaman konfigurasi privasi dan kontrol di berbagai platform. Materi Pengenalan *Phishing* melibatkan definisi dan penjelasan konsep phishing, perbandingan dengan serangan siber lainnya, tahapan serangan *phishing* dari awal hingga akhir beserta contoh skenario di media sosial, pengenalan tanda-tanda umum serangan *phishing*, cara mengenali pesan atau tautan palsu, serta penjelasan tentang berbagai metode *phishing* yang sering terjadi di platform sosial media.

Selain materi-materi tersebut, pelatihan juga mencakup aspek simulasi dan pencegahan phishing dengan mendemonstrasikan serangan *phishing* secara langsung. Tujuan dari simulasi ini adalah untuk meningkatkan pemahaman peserta tentang modus serangan yang mungkin dihadapi, serta memberikan pengenalan mendalam tentang cara mengidentifikasi dan menghindari jebakan *phishing*. Dalam bagian ini, peserta akan terlibat dalam serangkaian simulasi serangan *phishing* yang realistis, memberi pengalaman praktis dalam menghadapi situasi nyata. Melalui simulasi ini, peserta dapat melatih keterampilan dalam mengenali tanda-tanda serangan phishing, seperti pesan email yang mencurigakan atau situs web palsu.

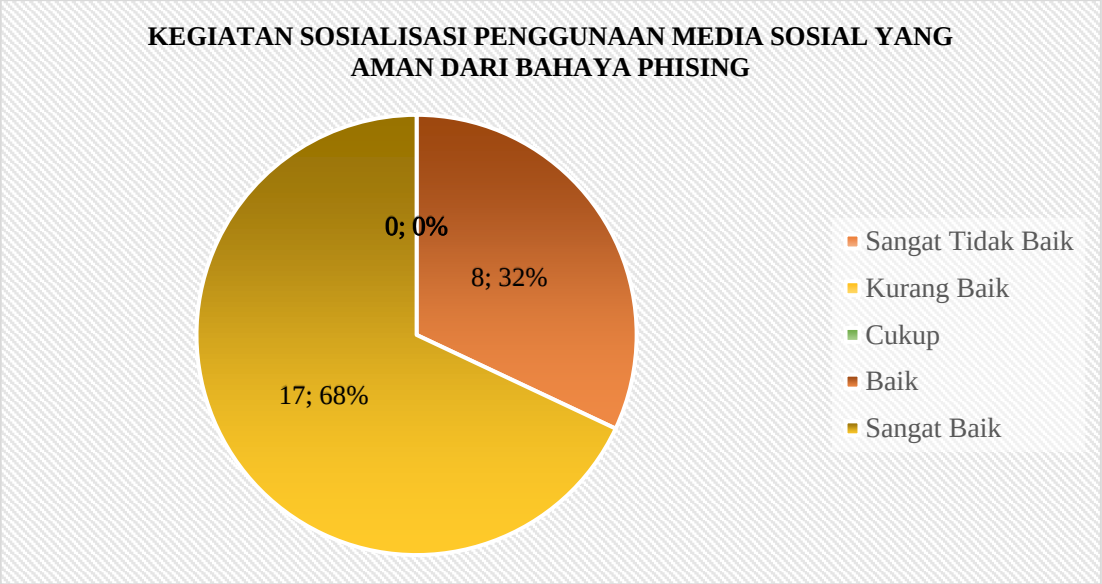
Selanjutnya, materi ini juga menyajikan panduan langkah-langkah konkret untuk pencegahan phishing yang dapat diambil oleh pengguna. Salah satu poin utama adalah penekanan pada penggunaan keamanan ganda (two-factor authentication) sebagai langkah tambahan untuk melindungi akun. Peserta diajak untuk memahami peran keamanan ganda dalam menanggulangi ancaman keamanan digital dan mengimplementasikannya secara efektif. Selama pelatihan, pentingnya kesadaran pengguna juga dijelaskan sebagai kunci utama dalam mengatasi risiko *phishing*. Peserta diberi pemahaman mendalam tentang pentingnya bersikap waspada dan skeptis terhadap pesan atau tautan yang mencurigakan, serta pentingnya untuk tidak mengungkapkan informasi pribadi atau kredensial login tanpa verifikasi yang jelas.

Terakhir, materi mencakup penyusunan rencana tanggap darurat. Peserta diberikan langkah-langkah konkret yang harus diambil jika menjadi korban serangan *phishing*, termasuk melaporkan insiden dan segera mengamankan akun. Keseluruhan pelatihan ini bertujuan untuk meningkatkan keamanan digital peserta melalui pengetahuan yang diperoleh dan pemahaman praktis dalam menghadapi ancaman *phishing*.

Setelah menyelesaikan kegiatan, tim pengabdian dan peserta seminar mengadakan sesi foto bersama sebagai langkah dokumentasi kegiatan, sebagaimana yang tampak pada Gambar 3. Selanjutnya, tim pengabdian melaksanakan diskusi internal untuk mengevaluasi seluruh aspek kegiatan, termasuk persiapan, materi, dan tingkat antusiasme peserta.

Gambar 3. Foto Bersama Kegiatan Sosialisasi

Hasil evaluasi dari kegiatan pengabdian kepada masyarakat tersebut menggunakan kuisioner. Beberapa kriteria yang digunakan dalam kuisioner tersebut adalah penilaian tentang materi, presentasi, pemahaman tentang media sosial, materi tentang *phishing*. Berikut hasil dari kuisioner yang diberikan kepada 25 peserta kegiatan didapatkan hasil bahwa sebanyak 32% (8 orang) dari peserta memilih opsi "Baik" dan sebanyak 68% (17 orang) memilih opsi "Sangat baik" terhadap sosialisasi yang sudah dilakukan. Jadi, secara keseluruhan, peserta memberikan respons positif terhadap sosialisasi tersebut. Berikut ini diagram terkait penilaian peserta terhadap sosialisasi dapat dilihat pada gambar 4.



Gambar 4. Penilaian peserta terhadap sosialisasi

4. Kesimpulan

Dari hasil ini, dapat disimpulkan bahwa peserta, bahwa sosialisasi yang dilakukan pada jamaah Masjid Al Huda Pandeyan telah mendapatkan respons positif, dengan 32% peserta menilai kegiatan tersebut berjalan dengan "Baik" dan 68% menilai kegiatan sosialisasi berjalan dengan "Sangat Baik". Mayoritas peserta, yang sebagian besar adalah pengguna media sosial, merespon kegiatan tersebut dengan baik. Kegiatan sosialisasi ini memberikan wawasan baru tentang cara menjaga keamanan online dan melindungi diri dari bahaya *phishing*. Peserta juga berhasil memperoleh pengetahuan baru tentang tanda-tanda dan risiko yang terkait dengan serangan *phishing* di lingkungan media sosial. Penulis merekomendasikan agar kegiatan serupa dapat diadakan secara berkala, mungkin dalam beberapa bulan sekali. Hal ini akan memastikan bahwa jamaah terus memperbarui pengetahuan terkait keamanan media sosial dan dapat menjaga ketahanan terhadap ancaman *phishing* yang terus berkembang. Semakin sering jamaah terlibat dalam sosialisasi semacam ini, semakin tinggi kemungkinan dapat mengenali potensi risiko dan mengambil langkah-langkah yang tepat untuk melindungi diri dan komunitas dari serangan online.

Penghargaan

Terima kasih pada LPPM STMIK Amikom Surakarta atas dukungan dana dan memfasilitasi kegiatan publikasi pengabdian kepada masyarakat ini.

Referensi

APJII. (2022). *Hasil Survei Penetrasi dan Perilaku Pengguna Internet*. Asosiasi Penyelenggara Jasa Internet Indonesia. https://apjii.or.id/survei

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*(November), 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Desolda, G., Aneke, J., Ardito, C., Lanzilotti, R., & Costabile, M. F. (2023). Explanations in warning dialogs to help users defend against phishing attacks. *International Journal of Human-Computer Studies*, *176*, 103056. https://doi.org/https://doi.org/10.1016/j.ijhcs.2023.103056

DM, M. Y., Addermi, & Lim, J. (2022). Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia. *Jurnal Pendidikan Dan Konseling*, *4*, 8022.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics.

Cyber Crime and Cyber Terrorism Investigator's Handbook, *September 2017*, 149–164. https://doi.org/10.1016/B978-0-12-800743-3.00012-8

Latifahi, F. N., Mawardi, I., & Wardhana, B. (2022). Ancaman Pencurian Data (Phishing) Di Tengah Trend Pengguna Fintech Pada Pandemic Covid-19. *Perisai*, *6*(1), 73–85. https://doi.org/10.21070/perisai.v6i1.

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, *132*, 103387. https://doi.org/https://doi.org/10.1016/j.cose.2023.103387

Pranata, E. J., & Ependi, L. (2023). Phising Terhadap Website Bank Bca. *Jurnal Trends*, *01*(01), 34–40. https://ejurnal.ibisa.ac.id/index.php/jsd/article/view/293

Prasetyo, A. D., Seta, H. B., & Pradnyana, I. W. W. (2023). Analisis Digital Forensik Spear Phishing Menggunakan Metode National Institute of Justice (Studi Kasus: Instagram Verified Account). *Informatik : Jurnal Ilmu Komputer*, *19*(1), 58–67. https://doi.org/10.52958/iftk.v19i1.4675

Putra Y, V. F. (2021). Modus Operandi Tindak Pidana Phising Menurut UU ITE. *Jurist-Diction*, *4*(6), 2525. https://doi.org/10.20473/jd.v4i6.31857

Ramadhan, A., Alhafidh, M. A., & Firmansyah, M. D. (2022). Penyebaran Link Phising Kuota Kemendikbud Terhadap Kesadaran Informasi Pribadi Di Kalangan Mahasiswa UNINUS. *Kampret Journal*, *1*(1), 11–15. https://doi.org/10.35335/kampret.v1i1.9

Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. *Journal of King Saud University - Computer and Information Sciences*, *35*(2), 590–611. https://doi.org/https://doi.org/10.1016/j.jksuci.2023.01.004

Soykan, E. U., & Bagriyanik, M. (2020). The effect of SMiShing attack on security of demand response programs. *Energies*, *13*(17). https://doi.org/10.3390/en13174542

Tyas Darmaningrat, E. W., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. *Sewagati*, *6*(2). https://doi.org/10.12962/j26139960.v6i2.92

Utin Indah Permata Sari. (2022). Kebijakan Penegakan Hukum Dalam Upaya Penanganan Cyber Crime Yang Dilakukan Oleh Virtual Police Di Indonesia. *Jurnal Studia Legalia*, *2*(01), 58–77. https://doi.org/10.61084/jsl.v2i01.7

Wahyudi, D., Niswar, M., Ais, A., & Alimuddin, P. (2022). Website Phising Detection Application Using Support Vector Machine (Svm). *Journal of Information Technology and Its Utilization*, *5*(2), 2022.

Wathoni, M., Efendi, Y., Maulana, A., Anfa, E. N., Alegra, V. P., Rifki, M., & Fauzan, A. (2023). Kesadaran Keamanan Siber (Cyber Security Awareness) Pada Smp Labschool Fip Umj. *Jurnal Universitas Muhammadiyah Jakarta*, *Volume 2*(No 3). http://jurnal.umj.ac.id/index.php/semnaskat

Wibowo, M. H., & Fatimah, N. (2017). Ancaman Phishing Terhadap Pengguna Sosial Media dalam Dunia Cyber Crime. *JoEICT (Journal of Education And ICT)*, *1*(1), 1–5. https://jurnal.stkippgritulungagung.ac.id/index.php/joeict/article/view/69