

Meningkatkan Kesadaran Hukum Perbankan Masyarakat terhadap Tanggung Jawab Perdata atas Penipuan *Online Phishing*

**Noval Akbar Ramadhan¹, Arya Adha Saputra², Putri Novia Sulestari³, Tiara Angel
Firmansyah⁴, Rut Eliarza Simamora⁵, Edward Binsar Hamonangan Dwinanda⁶,
Daniel Hafid⁷, Deny Slamet Pribadi⁸, Ahmad Nafhani⁹**

^{1,2,3,4,5,6,7,8,9} Fakultas Hukum, Universitas Mulawarman, Indonesia

Received : 17 Juni 2026, Revised : 29 Juni 2025, Published : 21 Juli 2026

Corresponding Author

Nama Penulis: Noval Akbar Ramadhan

E-mail: novalakbar038@gmail.com

Abstrak

Meningkatnya kasus phishing dalam sektor perbankan digital saat ini menjadi persoalan serius dimana masyarakat awam seringkali menjadi korban pelaku kejahatan digital yang artinya perkembangan layanan perbankan digital di Indonesia belum sepenuhnya diimbangi dengan kesiapan keamanan siber dan literasi digital masyarakat. Phishing dalam layanan perbankan digital tidak dapat dipandang hanya sebagai bentuk kelalaian pribadi nasabah, melainkan juga berkaitan dengan kewajiban bank dalam memberikan perlindungan hukum dan keamanan sistem elektronik kepada nasabah. Oleh karena itu, pengabdian masyarakat ini sangat penting untuk meningkatkan kesadaran kepada masyarakat mengenai kejahatan perbankan digital dan juga untuk memperkuat literasi dan perlindungan hukum kepada masyarakat sebagai pengguna layanan jasa keuangan digital agar terhindar dari ancaman phishing. Metode pelaksanaan kegiatan pengabdian ini adalah metode ceramah dengan pendekatan pengambilan deskriptif kualitatif. Bahwa kesimpulan yang diperoleh dari kegiatan sosialisasi hukum perbankan dan lembaga jasa keuangan oleh Fakultas Hukum Universitas Mulawarman dengan tema "Waspada Phishing dalam Kejahatan Perbankan Digital" telah berjalan dengan baik dan memberikan manfaat bagi masyarakat warga RT 28 Kelurahan Sempaja Selatan. Melalui kegiatan sosialisasi ini, peserta memperoleh pemahaman mengenai pengertian phishing, bentuk kejahatan perbankan digital, langkah pencegahan data pribadi dan keamanan dalam penggunaan layanan perbankan digital, dan meningkatkan kesadaran masyarakat agar lebih berhati-hati.

Kata kunci - phishing, perbankan digital, pengabdian masyarakat

Abstract

The increasing number of phishing cases in the digital banking sector has become a serious issue, as ordinary members of the public are often targeted and victimized by cybercriminals. This situation indicates that the development of digital banking services in Indonesia has not been fully supported by adequate cybersecurity readiness and digital literacy among the public. Phishing in digital banking services should not merely be viewed as a result of customers' personal negligence, but also as an issue related to banks' obligations to provide legal protection and secure electronic systems for their customers. Therefore, this community service activity is essential to raise public awareness regarding digital banking crimes and to strengthen legal literacy and legal protection for users of digital financial services in order to prevent them from becoming victims of phishing attacks. The community service program was conducted using a lecture-based method with a qualitative descriptive approach. The results indicate that the legal education and awareness program on banking and financial services, organized by the Faculty of Law, Universitas Mulawarman under the theme "Beware of

Phishing in Digital Banking Crimes," was successfully implemented and provided benefits to the residents of RT 28, Sempaja Selatan Village. Through this socialization activity, participants gained an understanding of the concept of phishing, various forms of digital banking crimes, preventive measures for protecting personal data, and security practices in the use of digital banking services. Furthermore, the activity contributed to increasing public awareness and encouraging participants to be more cautious when conducting digital financial transactions.

Keywords - phishing, digital banking, community service

How To Cite : Ramadhan, N. A., Saputra, A. A., Sulestari, P. N., Firmansyah, T. A., Simamora, R. E., Dwinanda, E. B. H., Hafid, D., Pribadi, D. S., & Nafhani, A. (2026). Meningkatkan Kesadaran Hukum Perbankan Masyarakat terhadap Tanggung Jawab Perdata atas Penipuan Online Phishing. *Jurnal Pengabdian Masyarakat Bangsa*, 4(5), 2490 - 2500. <https://doi.org/10.59837/jpmba.v4i5.4638>

Copyright ©2026 Noval Akbar Ramadhan, Arya Adha Saputra, Putri Novia Sulestari, Tiara Angel Firmansyah, Rut Eliarza Simamora, Edward Binsar Hamonangan Dwinanda, Daniel Hafid, Deny Slamet Pribadi, Ahmad Nafhani

PENDAHULUAN

Perkembangan teknologi informasi telah membawa perubahan besar dalam sistem pelayanan perbankan di Indonesia. Aktivitas transaksi yang sebelumnya dilakukan secara langsung di kantor bank kini beralih ke layanan digital seperti mobile banking dan internet banking yang menawarkan kemudahan, kecepatan, serta efisiensi bagi masyarakat. Bank pada dasarnya merupakan lembaga keuangan yang memiliki peran penting dalam menghimpun dan menyalurkan dana masyarakat (Rizieq, 2024). Sebagaimana diterangkan dalam Pasal 1 angka 2 Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan yang menyatakan bahwa *"Bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak."*

Perkembangan layanan perbankan digital tersebut kemudian melahirkan pola interaksi baru antara bank dan nasabah yang seluruh proses transaksinya dilakukan melalui sistem elektronik. Namun, kemajuan teknologi yang memberikan kemudahan tersebut juga diiringi dengan meningkatnya risiko kejahatan siber, salah satunya *phishing*. *Phishing* merupakan modus penipuan online yang dilakukan dengan cara memperoleh data pribadi nasabah, seperti PIN (*Personal Identification Number*), password, OTP (*One Time Password*), maupun data rekening melalui tautan atau media digital palsu yang menyerupai layanan resmi perbankan. Dalam aksinya, pelaku *phishing* memanfaatkan rendahnya literasi digital masyarakat untuk mengakses akun perbankan korban dan mengambil dana secara melawan hukum (Dwi & Indah, 2025). Kondisi ini menunjukkan bahwa perkembangan sistem perbankan digital tidak hanya menghadirkan kemudahan transaksi, tetapi juga menimbulkan persoalan hukum baru terkait keamanan data nasabah dan tanggung jawab pihak perbankan terhadap kerugian yang ditimbulkan akibat kejahatan digital tersebut.

Meningkatnya kasus *phishing* dalam sektor perbankan digital saat ini menjadi persoalan yang nyata di tengah masyarakat. Badan Siber dan Sandi Negara (BSSN) mencatat terdapat sekitar 102,95 juta anomali trafik serangan siber di Indonesia sepanjang Januari hingga Juli 2024, dimana sebagian besar serangan tersebut berkaitan dengan *malware* dan aktivitas pencurian data digital. Selain itu, laporan Kaspersky juga menunjukkan bahwa sepanjang tahun 2024 terdapat sekitar 649 ribu serangan siber yang secara khusus menargetkan sektor perbankan di Indonesia, dengan modus yang banyak mengarah pada pencurian data nasabah melalui *malware* dan *phishing*. Tingginya ancaman tersebut memperlihatkan bahwa perkembangan layanan perbankan digital di Indonesia belum sepenuhnya diimbangi dengan kesiapan keamanan siber dan literasi digital masyarakat. Modus yang digunakan pun semakin beragam, mulai dari pengiriman tautan palsu melalui pesan singkat, *WhatsApp*, email, hingga penyamaran identitas bank melalui media sosial. Masyarakat dalam hal ini masih menjadi

sasaran empuk pelaku kejahatan digital karena rendahnya pemahaman mengenai keamanan transaksi elektronik (Sarton, 2017).

Situasi tersebut memperlihatkan bahwa keamanan layanan perbankan digital tidak hanya menjadi tanggung jawab nasabah, tetapi juga merupakan kewajiban pihak perbankan sebagai penyedia layanan keuangan digital. Dalam hukum positif Indonesia, bank pada dasarnya memiliki kewajiban untuk menjamin keamanan layanan yang digunakan oleh nasabah (Chairunnisa, 2024). Pasal 29 ayat (4) Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan menyatakan bahwa *“Untuk kepentingan nasabah, bank wajib menyediakan informasi mengenai kemungkinan timbulnya risiko kerugian sehubungan dengan transaksi nasabah yang dilakukan melalui bank.”* Ketentuan tersebut menunjukkan bahwa bank tidak hanya bertugas menyediakan layanan transaksi digital, tetapi juga wajib memberikan perlindungan preventif melalui edukasi dan informasi mengenai risiko kejahatan digital kepada nasabah (Sugiantari, n.d.). Selain itu, Pasal 19 Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi menyebutkan bahwa kewajiban pengendalian data pribadi dan prosesor data pribadi meliputi: Setiap orang; Badan Publik; dan Organisasi Internasional. Dalam layanan perbankan digital, data nasabah merupakan bagian dari data pribadi yang wajib dijaga keamanan dan kerahasiaannya oleh pihak bank. Tidak hanya itu, tanggung jawab perdata juga dapat timbul apabila kerugian nasabah terjadi akibat adanya kelalaian dalam sistem keamanan layanan digital perbankan (Anjheli, 2025). Hal tersebut sejalan dengan Pasal 1365 Kitab Undang-Undang Hukum Perdata yang menyatakan bahwa *“Tiap perbuatan melanggar hukum yang membawa kerugian kepada orang lain mewajibkan orang yang karena salahnya menerbitkan kerugian itu, mengganti kerugian tersebut.”* Ketentuan ini memperlihatkan bahwa apabila terdapat kelemahan pengawasan, kurangnya sistem keamanan, atau minimnya edukasi yang menyebabkan nasabah mengalami kerugian akibat *phishing*, maka pihak perbankan tidak dapat sepenuhnya melepaskan diri dari tanggung jawab hukum terhadap nasabahnya (Hasanudin & Babussalam, 2024).

Masalah *phishing* dalam layanan perbankan digital tidak lagi dapat dipandang hanya sebagai bentuk kelalaian pribadi nasabah dalam menjaga data perbankannya, melainkan juga berkaitan dengan kewajiban bank dalam memberikan perlindungan hukum dan keamanan sistem elektronik kepada pengguna layanan. Tingginya penggunaan mobile banking di tengah masyarakat yang tidak diimbangi dengan literasi keamanan digital menunjukkan bahwa perlindungan terhadap nasabah masih menjadi tantangan penting dalam perkembangan perbankan digital di Indonesia. Oleh karena itu, pengabdian masyarakat ini bertujuan tidak hanya terfokus untuk meningkatkan kesadaran kepada masyarakat mengenai kejahatan perbankan digital, namun juga memperkuat literasi dan perlindungan hukum kepada masyarakat sebagai pengguna layanan jasa keuangan digital agar terhindar dari ancaman *phishing*. Pengabdian ini diharapkan bisa menjadi contoh bagi daerah-daerah lain dengan tantangan dan ancaman yang serupa, agar kemajuan perbankan digital dapat berjalan dengan perlindungan hukum yang adil dan inklusif (Rahmawati & Naili, 2025).

METODE

Kegiatan pengabdian kepada masyarakat dengan judul *“Waspada Phishing dalam Kejahatan Perbankan Digital”* dilaksanakan pada Bulan Mei 2026 di Balai Bebaya, RT.28 Perumahan Rapak Binuang Indah, Kelurahan Sempaja Selatan, Kota Samarinda, Kalimantan Timur. Tim pelaksana terdiri atas dosen dan mahasiswa dari Fakultas Hukum universitas Mulawarman. Sasaran kegiatan dalam pengabdian masyarakat ini adalah masyarakat dengan rentan usia 18 – 59 Tahun yang aktif menggunakan bank digital di RT.28 Perumahan Rapak Binuang Indah, Kelurahan Sempaja Selatan, Kota Samarinda, Kalimantan Timur yang berjumlah berjumlah 32 orang. Kegiatan ini berlangsung selama satu hari dengan durasi total selama 150 menit. Metode yang digunakan dalam kegiatan pengabdian masyarakat ini adalah metode ceramah dengan pendekatan deskriptif kualitatif. Metode ini dipilih karena berfokus pada pemahaman terhadap tingkat pengetahuan dan pemahaman peserta mengenai materi yang disampaikan selama kegiatan (Annasthasya et al., 2025). Data diperoleh melalui

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

kuesioner *pre-test* dan *post-test* yang disebarakan menggunakan *Google Form* kepada peserta setelah pemaparan materi. Data yang terkumpul kemudian dianalisis secara deskriptif untuk mengetahui tingkat pemahaman peserta terhadap materi yang telah disampaikan serta mengevaluasi efektivitas kegiatan ini.

Rangkaian kegiatan ini terdiri atas tiga tahap, tahapan pertama adalah persiapan yang meliputi koordinasi dengan RT setempat, menentukan waktu dan tempat pelaksanaan kegiatan, pembagian tugas tim, dan penyusunan materi kegiatan dan kuesioner *pre-test* serta *post-test* yang akan digunakan sebagai instrumen evaluasi. Tahap kedua adalah pelaksanaan kegiatan yang terdiri atas sambutan, pemaparan materi, serta diskusi. Materi yang disampaikan meliputi pengertian *phishing*, berbagai bentuk dan contoh modus *phishing* yang sering terjadi, serta langkah-langkah pencegahan yang dapat dilakukan oleh masyarakat. Dalam kegiatan ini, peserta diarahkan untuk dapat membedakan antara pesan, tautan, atau situs web yang asli dengan yang mengandung unsur *phishing*. Selain itu, peserta juga diberikan pemahaman mengenai ciri-ciri umum *phishing*, seperti penggunaan tautan mencurigakan, permintaan data pribadi secara tidak wajar, serta modus yang mengatasnamakan lembaga atau pihak tertentu. Tahap terakhir adalah tahap evaluasi yang dilakukan melalui analisis hasil kuesioner *pre-test* dan *post-test* yang disebarakan menggunakan *Google Form* kepada seluruh peserta setelah kegiatan selesai dilaksanakan. Penggunaan *Google Form* dipilih untuk memudahkan proses pengumpulan, pencatatan, dan pengolahan data secara sistematis. Kuesioner tersebut terdiri atas enam pertanyaan, dengan satu pertanyaan berisi identitas peserta dan lima pertanyaan lainnya berkaitan dengan materi yang telah disampaikan selama sosialisasi. Pertanyaan tersebut dirancang untuk dapat mengukur sejauh mana peserta dalam memahami materi yang telah disampaikan. Selain itu, kuesioner juga memuat pertanyaan yang bertujuan untuk mengetahui apakah peserta pernah mengalami atau menjadi sasaran modus *phishing* dalam aktivitas digital mereka. Tahapan ini kemudian diakhiri dengan tanggapan peserta terhadap jalannya kegiatan, *closing statement* oleh pemateri dan moderator, dan dilanjutkan dengan dokumentasi bersama sebelum menutup kegiatan.

Tabel 1.
Tahapan Kegiatan

Tahap	Kegiatan	Tujuan
Persiapan	Koordinasi, menentukan waktu dan tempat, pembagian tugas, menyusun materi dan kuesioner <i>pre-test</i> serta <i>post-test</i>	Memastikan seluruh teknis dari kegiatan telah disiapkan
Pelaksanaan	Sambutan, pemaparan materi, diskusi	Meningkatkan pemahaman masyarakat terhadap tanggung jawab perdata serta bahaya <i>phishing</i>
Evaluasi	Pengisian kuesioner <i>pre-test</i> serta <i>post-test</i> dan tanggapan peserta	Mengukur sejauh mana pengetahuan dan pemahaman dari peserta setelah pemaparan materi

HASIL DAN PEMBAHASAN

Pelaksanaan kegiatan pengabdian kepada masyarakat dengan tema “Waspada *Phishing* dalam Kejahatan Perbankan Digital” dilaksanakan pada bulan Mei 2026 di Balai Bebaya RT.28 Perumahan Rapak Binuang Indah, Kelurahan Sempaja Selatan, Kota Samarinda, Kalimantan Timur. Kegiatan ini diselenggarakan oleh tim pelaksana yang terdiri atas dosen dan mahasiswa Fakultas Hukum Universitas Mulawarman sebagai bentuk kontribusi perguruan tinggi dalam meningkatkan literasi hukum dan keamanan digital masyarakat. Pelaksanaan kegiatan ini dilatarbelakangi oleh semakin meningkatnya penggunaan layanan perbankan digital yang diikuti dengan berkembangnya berbagai modus kejahatan siber seperti salah satunya adalah *phishing*. Kemudahan transaksi melalui layanan digital telah memberikan manfaat yang signifikan bagi masyarakat, namun pada saat yang sama juga

meningkatkan risiko penyalahgunaan data dan pencurian informasi pribadi oleh pelaku kejahatan siber (Semarang) et al., 2025).

Berdasarkan hasil observasi awal dan komunikasi dengan pengurus lingkungan setempat, diketahui bahwa hampir seluruh masyarakat di RT.28 Perumahan Rapak Binuang Indah telah memanfaatkan layanan perbankan digital untuk berbagai kebutuhan transaksi sehari-hari, seperti transfer dana, pembayaran tagihan, dan pembelian produk atau jasa secara daring. Akan tetapi, tingkat pemahaman masyarakat mengenai risiko keamanan digital, terkait modus *phishing* masih beragam. Sebagian masyarakat telah mengetahui bahwa terdapat berbagai bentuk penipuan yang mengatasnamakan bank atau lembaga tertentu, namun belum seluruhnya memahami ciri-ciri *phishing*, cara kerja pelaku, serta langkah-langkah yang harus dilakukan untuk melindungi data pribadi dan keamanan akun perbankan mereka. Kondisi ini menunjukkan bahwa peningkatan penggunaan teknologi keuangan belum sepenuhnya diimbangi dengan peningkatan literasi keamanan digital di tingkat masyarakat.



Gambar 1.
Pemaparan materi

Sebagai bagian dari evaluasi kegiatan, dilakukan pengumpulan data melalui kuesioner *pre-test* dan *post-test* yang disebarkan kepada seluruh peserta menggunakan *Google Form*. Kuesioner ini bertujuan untuk mengidentifikasi karakteristik responden, mengetahui pengalaman peserta terkait modus *phishing*, serta mengukur tingkat pemahaman peserta terhadap materi yang telah disampaikan selama kegiatan sosialisasi. Terdapat sebanyak 32 orang yang menjadi peserta dalam kegiatan ini dengan latar belakang yang beragam sebagai berikut.

Tabel 2.
Responder

Indikator	Jumlah	Persentase
Jenis Kelamin		
Laki-laki	5 orang	15,62%
Perempuan	27 orang	84,37%
Umur		
17 – 25 Tahun	2 orang	6,25%
26 – 40 Tahun	2 orang	6,25%
41 – 50 Tahun	8 orang	25%
> 50 Tahun	20 orang	62,5%
Pekerjaan		
ASN	2 orang	6,25%
Swasta	6 orang	18,75%
Pensiunan Swasta	1 orang	3,12%
Ibu Rumah Tangga (IRT)	23 orang	71,87%

Berdasarkan data *responder* dari 32 peserta kegiatan, diperoleh gambaran mengenai karakteristik demografis peserta yang mengikuti kegiatan “Waspada *Phishing* dalam Kejahatan Perbankan Digital.” Dari aspek jenis kelamin, peserta didominasi oleh perempuan sebanyak 27 orang (84,37%), sedangkan peserta laki-laki berjumlah 5 orang (15,62%). Dominasi peserta perempuan ini menunjukkan tingginya partisipasi perempuan, khususnya ibu rumah tangga, dalam kegiatan edukasi yang berkaitan dengan keamanan digital dan penggunaan layanan perbankan digital. Ditinjau dari kelompok usia, mayoritas peserta berusia di atas 50 tahun, yaitu sebanyak 20 orang (62,5%). Selanjutnya, peserta yang berusia 41–50 tahun berjumlah 8 orang (25%), sedangkan peserta yang berusia 17–25 tahun dan 26–40 tahun masing-masing berjumlah 2 orang (6,25%). Data tersebut menunjukkan bahwa sebagian besar peserta berada pada kelompok usia dewasa akhir hingga lanjut usia yang saat ini juga telah menjadi pengguna aktif layanan perbankan digital untuk berbagai kebutuhan transaksi keuangan sehari-hari.

Berdasarkan jenis pekerjaan, mayoritas peserta berprofesi sebagai ibu rumah tangga sebanyak 23 orang (71,87%). Adapun peserta yang bekerja di sektor swasta berjumlah 6 orang (18,75%), aparatur sipil negara (ASN) sebanyak 2 orang (6,25%), dan pensiunan swasta sebanyak 1 orang (3,12%). Komposisi tersebut menunjukkan bahwa kegiatan sosialisasi menjangkau kelompok masyarakat yang secara aktif menggunakan layanan digital dalam kehidupan sehari-hari, namun tidak selalu memiliki latar belakang pendidikan atau pekerjaan yang berkaitan dengan teknologi informasi dan keamanan siber. Karakteristik peserta tersebut menunjukkan bahwa kegiatan sosialisasi telah menjangkau kelompok masyarakat yang memiliki tingkat kerentanan cukup tinggi terhadap kejahatan *phishing*. Kelompok usia yang lebih tua umumnya menghadapi tantangan dalam beradaptasi dengan perkembangan teknologi digital yang berlangsung sangat cepat, sehingga berpotensi lebih rentan terhadap berbagai modus penipuan berbasis teknologi informasi. keterbatasan literasi digital dan rendahnya pemahaman mengenai keamanan siber dapat meningkatkan risiko menjadi korban *phishing* (Desi Ananta et al., 2024).

Oleh karena itu, sebelum pemaparan materi sosialisasi dilakukan, tim pelaksana terlebih dahulu melaksanakan *pre-test* untuk memperoleh gambaran awal mengenai tingkat pengetahuan dan pemahaman peserta terkait *phishing* dan keamanan perbankan digital. *Pre-test* tersebut bertujuan untuk menggali informasi mengenai pengalaman peserta dalam menghadapi berbagai modus *phishing*, termasuk untuk mengetahui apakah peserta pernah menjadi korban atau hampir menjadi korban *phishing* dalam penggunaan layanan perbankan digital. *Pre-test* ini juga bertujuan untuk mengidentifikasi sejauh mana pemahaman peserta mengenai pengertian *phishing*. Hasil *pre-test* ini menjadi data awal yang digunakan untuk menilai tingkat pengetahuan peserta sebelum masuk ke rangkaian pemaparan materi. Hasil dari *pre-test* tersebut adalah sebagai berikut.

Tabel 3.

Pre-test

Indikator	Jumlah	Persentase
Apakah menggunakan <i>mobile banking</i> dalam sehari-hari?		
Menggunakan	29	90,62%
Tidak Menggunakan	3	9,37%
Apakah pernah mendengar mengenai <i>phishing</i>?		
Pernah	14	43,75%
Tidak pernah	18	56,25%
Apakah pernah menjadi korban <i>phishing</i>?		
Pernah	1	3,12%
Tidak pernah	31	96,87%
Apakah pernah mengalami dan menjadi calon korban <i>phishing</i>?		
Pernah	21	65,62
Tidak pernah	11	43,37%

Hasil *pre-test* menunjukkan bahwa sebagian besar peserta telah memanfaatkan layanan mobile banking dalam aktivitas sehari-hari. Dari 32 responden yang mengikuti kegiatan sosialisasi, sebanyak 29 orang (90,62%) menyatakan menggunakan mobile banking untuk berbagai kebutuhan transaksi keuangan, sedangkan 3 orang (9,37%) menyatakan tidak menggunakan layanan tersebut. Tingginya tingkat penggunaan mobile banking menunjukkan bahwa layanan perbankan digital telah menjadi bagian dari kehidupan masyarakat dalam melakukan transaksi keuangan secara praktis dan efisien. Berbagai fitur yang tersedia, seperti transfer dana, pembayaran tagihan, pembelian pulsa, dan pengecekan saldo, menjadi faktor yang mendorong masyarakat untuk beralih dari layanan perbankan konvensional ke layanan berbasis digital. Namun, tingginya penggunaan mobile banking juga perlu diimbangi dengan pemahaman yang memadai mengenai keamanan digital agar pengguna dapat terhindar dari berbagai ancaman kejahatan siber yang menyasar layanan perbankan digital.

Pre-test tersebut juga menunjukkan bahwa tingkat pengetahuan peserta mengenai *phishing* masih beragam. Sebanyak 18 orang (56,25%) menyatakan telah mengetahui atau pernah mendengar istilah *phishing* sebelumnya, sedangkan 14 orang (43,75%) mengaku belum memahami atau belum pernah mengetahui mengenai *phishing*. Temuan ini menunjukkan bahwa meskipun sebagian besar peserta telah menggunakan layanan perbankan digital, pemahaman mengenai salah satu bentuk kejahatan siber yang paling sering menargetkan pengguna layanan tersebut masih belum merata. Kondisi ini menunjukkan adanya kesenjangan antara tingkat penggunaan teknologi keuangan dengan tingkat literasi keamanan digital masyarakat. Padahal, pemahaman mengenai *phishing* merupakan salah satu aspek penting dalam melindungi data pribadi dan keamanan akun perbankan digital dari penyalahgunaan oleh pihak yang tidak bertanggung jawab.

Berkaitan dengan pengalaman responden terhadap *phishing*, hasil *pre-test* menunjukkan bahwa hanya 1 orang (3,12%) yang mengaku pernah menjadi korban *phishing*, sedangkan 31 orang (96,87%) menyatakan belum pernah menjadi korban. Meskipun jumlah korban yang teridentifikasi relatif kecil, data tersebut tidak serta-merta menunjukkan rendahnya ancaman *phishing* di lingkungan masyarakat. Sebaliknya, hasil survei memperlihatkan bahwa sebanyak 21 orang (65,62%) pernah mengalami situasi yang mengarah pada upaya *phishing* atau hampir menjadi korban *phishing*, sementara 11 orang (34,37%) menyatakan belum pernah mengalaminya. Temuan ini menunjukkan bahwa upaya *phishing* telah cukup sering menyasar masyarakat, meskipun tidak selalu berakhir pada keberhasilan pelaku dalam memperoleh data atau melakukan penipuan.

Berdasarkan keterangan yang diberikan responden, bentuk percobaan *phishing* yang paling sering ditemui antara lain berupa telepon dari pihak yang mengatasnamakan bank atau instansi tertentu, pesan singkat yang berisi tautan mencurigakan, informasi undian atau hadiah palsu, permintaan kode OTP, serta pesan melalui aplikasi *WhatsApp* dan media sosial yang meminta data pribadi maupun informasi rekening. Beragamnya modus yang dialami peserta menunjukkan bahwa pelaku *phishing* terus menyesuaikan metode yang digunakan dengan perkembangan teknologi dan pola komunikasi masyarakat. Oleh karena itu, hasil *pre-test* ini mengindikasikan bahwa kegiatan sosialisasi mengenai *phishing* sangat relevan dan diperlukan untuk meningkatkan pemahaman masyarakat mengenai karakteristik, modus operandi, serta langkah-langkah pencegahan yang dapat dilakukan dalam penggunaan layanan perbankan digital secara aman. Temuan tersebut sekaligus menjadi dasar untuk menilai efektivitas kegiatan sosialisasi melalui perbandingan dengan hasil *post-test* yang dilakukan setelah penyampaian materi dan sesi diskusi selesai dilaksanakan.

Tabel 4.

Post-test

Indikator	Paham	Cukup	Tidak Paham
Pengertian <i>phishing</i>	7 orang (21,87%)	17 orang (53,12%)	8 orang (25%)
Bentuk <i>phishing</i>	3 orang (9,37%)	29 orang (90,62%)	0
Pencegahan <i>phishing</i>	7 orang (21,87%)	23 orang (71,87%)	2 orang (6,25%)

Hasil *post-test* menunjukkan bahwa tingkat pemahaman awal peserta mengenai *phishing* masih berada pada kategori yang beragam. Dari 32 responden yang mengikuti kegiatan sosialisasi, sebanyak 17 orang (53,12%) memiliki tingkat pemahaman yang tergolong cukup, 7 orang (21,87%) berada pada kategori paham, dan 8 orang (25%) menyatakan belum memahami atau belum mengenal *phishing* secara memadai. Data tersebut menunjukkan bahwa sebagian besar peserta hanya memiliki pengetahuan dasar mengenai *phishing* tanpa memahami secara lebih mendalam karakteristik, modus operandi, maupun risiko yang dapat ditimbulkan terhadap keamanan data pribadi dan layanan perbankan digital. Selain itu, masih terdapat seperempat dari total peserta yang belum memahami *phishing* sama sekali. Temuan ini mengindikasikan bahwa literasi keamanan digital masyarakat, khususnya terkait ancaman *phishing*, masih perlu ditingkatkan melalui kegiatan edukasi yang berkelanjutan. Oleh karena itu, kegiatan sosialisasi ini dirancang untuk memberikan pemahaman yang lebih komprehensif mengenai *phishing*, termasuk berbagai bentuk dan strategi yang digunakan pelaku dalam melancarkan aksinya.

Setelah pelaksanaan sosialisasi dan sesi diskusi, dilakukan *post-test* untuk mengukur tingkat pemahaman peserta terhadap materi yang telah disampaikan. Hasil *post-test* menunjukkan adanya peningkatan pemahaman peserta mengenai bentuk-bentuk *phishing* dalam kejahatan perbankan digital. Sebanyak 29 orang (90,62%) menyatakan telah cukup memahami berbagai bentuk *phishing* yang sering terjadi di era digital, sedangkan 3 orang (9,37%) menyatakan telah memahami materi dengan baik dan mampu menjelaskan kembali bentuk-bentuk *phishing* beserta karakteristiknya. Menariknya, tidak terdapat peserta yang menyatakan tidak memahami materi yang telah disampaikan. Hasil tersebut menunjukkan bahwa seluruh peserta telah memiliki pemahaman dasar mengenai *phishing* setelah mengikuti kegiatan sosialisasi. Peningkatan ini menunjukkan bahwa penyampaian materi dan diskusi yang dilakukan selama kegiatan mampu membantu peserta mengenali berbagai modus *phishing*, seperti penipuan melalui telepon yang mengatasnamakan pihak bank, pesan berisi tautan mencurigakan, permintaan kode OTP, serta berbagai bentuk rekayasa sosial yang bertujuan memperoleh data pribadi dan informasi perbankan korban (Arisanty et al., 2025).

Selain mengukur pemahaman mengenai bentuk-bentuk *phishing*, *post-test* juga digunakan untuk mengetahui pemahaman peserta mengenai langkah-langkah yang perlu dilakukan apabila mengalami atau menghadapi indikasi *phishing*. Hasil evaluasi menunjukkan bahwa sebanyak 23 orang (71,87%) telah memahami tindakan yang harus dilakukan ketika menghadapi *phishing*, seperti tidak memberikan kode OTP kepada pihak lain, segera mengganti kata sandi akun yang berpotensi terdampak, menghubungi pihak bank untuk melakukan pengamanan rekening, serta melaporkan kejadian kepada pihak yang berwenang. Selanjutnya, sebanyak 7 orang (21,87%) memiliki pemahaman yang cukup mengenai langkah-langkah penanganan dan pencegahan *phishing*, sedangkan 2 orang (6,25%) masih belum memahami secara optimal tindakan yang perlu dilakukan apabila menjadi sasaran *phishing*. Meskipun masih terdapat sebagian kecil peserta yang memerlukan pendalaman materi lebih lanjut, secara umum hasil *post-test* menunjukkan bahwa kegiatan sosialisasi telah berhasil meningkatkan pengetahuan dan kesadaran peserta mengenai bahaya *phishing*, bentuk-bentuk kejahatan yang digunakan pelaku, serta langkah-langkah perlindungan yang dapat diterapkan dalam penggunaan layanan perbankan digital secara aman dan bertanggung jawab.



Gambar 2.

Foto bersama setelah kegiatan

Hasil kegiatan menunjukkan adanya peningkatan pemahaman masyarakat mengenai *phishing* dan berbagai bentuk kejahatan yang menasar pengguna layanan perbankan digital. Meskipun sebagian besar peserta telah menggunakan layanan mobile banking dalam kehidupan sehari-hari, masih banyak peserta yang belum memahami karakteristik, modus operandi, dan risiko yang ditimbulkan oleh serangan *phishing*. Kondisi tersebut menunjukkan bahwa tingginya penggunaan layanan perbankan digital belum sepenuhnya diimbangi dengan tingkat literasi keamanan digital yang memadai. Setelah mengikuti kegiatan sosialisasi, seluruh peserta menunjukkan peningkatan pemahaman mengenai *phishing*, baik dari segi pengertian, bentuk-bentuk *phishing*, maupun cara mengenali indikasi penipuan digital yang sering digunakan oleh pelaku kejahatan siber. Peningkatan pemahaman tersebut terlihat dari hasil *post-test* yang menunjukkan bahwa seluruh peserta telah memahami bentuk-bentuk *phishing* yang umum terjadi di era digital. Sebanyak 90,62% peserta menyatakan cukup memahami berbagai modus *phishing*, sedangkan 9,37% peserta menyatakan telah memahami materi secara lebih mendalam dan mampu menjelaskan kembali karakteristik serta jenis-jenis *phishing* yang sering digunakan pelaku. Dalam sesi diskusi, peserta juga mampu mengidentifikasi berbagai bentuk serangan *phishing* yang pernah mereka temui, seperti pesan singkat yang berisi tautan mencurigakan, telepon yang mengatasnamakan pihak bank, permintaan kode OTP, pemberitahuan hadiah atau undian palsu, serta pesan melalui aplikasi *WhatsApp* dan media sosial yang meminta data pribadi maupun informasi rekening. Temuan ini menunjukkan bahwa kegiatan sosialisasi tidak hanya meningkatkan pengetahuan teoritis peserta, tetapi juga meningkatkan kemampuan mereka dalam mengenali ancaman *phishing* yang berpotensi terjadi dalam kehidupan sehari-hari.

Selain meningkatkan pemahaman mengenai bentuk-bentuk *phishing*, kegiatan sosialisasi juga berhasil meningkatkan kesadaran peserta mengenai pentingnya menjaga keamanan data pribadi dan informasi perbankan digital. Peningkatan kesadaran peserta juga terlihat dari pemahaman mengenai langkah-langkah yang harus dilakukan apabila menghadapi atau menjadi sasaran *phishing*. Hasil *post-test* menunjukkan bahwa sebagian besar peserta telah memahami tindakan yang perlu dilakukan, seperti tidak memberikan kode OTP kepada pihak mana pun, segera mengganti kata sandi akun yang berpotensi terdampak, menghubungi pihak bank untuk mengamankan rekening, serta melaporkan kejadian kepada pihak yang berwenang. Meningkatnya pemahaman tersebut menunjukkan bahwa kegiatan sosialisasi telah berhasil memberikan bekal pengetahuan praktis kepada masyarakat dalam menghadapi ancaman kejahatan siber. Dengan demikian, kegiatan pengabdian kepada masyarakat ini tidak hanya meningkatkan literasi keamanan digital peserta, tetapi juga mendorong terbentuknya sikap yang lebih waspada dan bertanggung jawab dalam menggunakan layanan perbankan digital sehingga dapat meminimalkan risiko menjadi korban *phishing* di masa mendatang.

KESIMPULAN

Kegiatan sosialisasi hukum perbankan dan lembaga jasa keuangan yang diselenggarakan oleh Fakultas Hukum Universitas Mulawarman dengan tema "Waspada *Phishing* dalam Kejahatan

Perbankan Digital" telah berjalan dengan baik dan memberikan manfaat bagi masyarakat, khususnya warga RT.28 Kelurahan Sempaja Selatan, Kota Samarinda, Kalimantan Timur. Kegiatan ini dilaksanakan sebagai bentuk pengabdian kepada masyarakat untuk meningkatkan pemahaman mengenai bahaya *phishing* dalam layanan perbankan digital.

Berdasarkan hasil penyuluhan dan data kuisioner berupa *pre-test* dan *post-test*, diketahui bahwa sebagian besar peserta telah menggunakan layanan mobile banking dalam aktivitas sehari-hari, namun tingkat pemahaman mengenai *phishing* masih tergolong rendah. Banyak peserta yang belum memahami bentuk, modus, serta cara pencegahan *phishing* dengan tepat, bahkan sebagian besar pernah mengalami atau hampir menjadi korban penipuan digital yang mengatasnamakan pihak perbankan. Kegiatan ini bertujuan untuk memberikan pemahaman dan meningkatkan kesadaran kepada masyarakat RT.28 Kelurahan Sempaja Selatan, Kota Samarinda, Kalimantan Timur mengenai *phishing*, bentuk-bentuk kejahatan perbankan digital, serta langkah-langkah pencegahan yang dapat dilakukan untuk melindungi data pribadi dan keamanan dalam penggunaan layanan perbankan digital.

Selain itu, perlunya melibatkan berbagai pemangku kepentingan, seperti pihak perbankan, Otoritas Jasa Keuangan (OJK), pemerintah daerah, serta instansi yang bergerak di bidang keamanan siber. Keterlibatan berbagai pihak tersebut dapat memberikan informasi yang lebih komprehensif mengenai bentuk-bentuk ancaman digital terkini, mekanisme perlindungan konsumen sektor jasa keuangan, serta prosedur pelaporan yang dapat dilakukan apabila masyarakat mengalami atau menjadi sasaran *phishing*. Dengan adanya kolaborasi yang berkelanjutan antara perguruan tinggi, lembaga keuangan, dan masyarakat, diharapkan upaya pencegahan kejahatan perbankan digital dapat terlaksana secara lebih efektif.

UCAPAN TERIMA KASIH

Tim pelaksana pengabdian kepada masyarakat mengucapkan terima kasih kepada Ketua RT.28 Perumahan Rapak Binuang Indah, Kelurahan Sempaja Selatan, Kota Samarinda, Kalimantan Timur, beserta seluruh masyarakat yang telah berpartisipasi dan bersedia menjadi peserta dalam pelaksanaan kegiatan pengabdian kepada masyarakat dengan tema "Waspada *Phishing* dalam Kejahatan Perbankan Digital." Ucapan terima kasih juga disampaikan kepada Fakultas Hukum Universitas Mulawarman, para dosen, mahasiswa, serta seluruh pihak yang telah memberikan dukungan, bantuan, dan kerja sama selama proses persiapan, pelaksanaan, hingga evaluasi kegiatan. Dukungan dan partisipasi yang diberikan telah berkontribusi terhadap kelancaran dan keberhasilan pelaksanaan kegiatan pengabdian kepada masyarakat ini.

DAFTAR PUSTAKA

- Anjheli, D. (2025). Privasi Digital dan Kejahatan Phishing di Indonesia : Evaluasi Kritis terhadap Efektivitas UU ITE dan UU PDP Berdasarkan laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2023. *Staatsrecht Jurnal Hukum Kenegaraan Dan Politik Islam*, 4(1), 165–189. <https://ejournal.uin-suka.ac.id/syariah/Staatsrecht/article/view/3964>
- Annasthasya, D., Alfindoria, I., Rahayu, S., & Khair, O. I. (2025). Metodologi Penelitian Kualitatif: Tinjauan Literatur Dalam Konteks Pendidikan. *Jurnal Ilmiah Multidisipin*, 3(7), 423–429. <https://doi.org/10.60126/jim.v3i7.1070>
- Arisanty, M., Riady, Y., Anastassia, S., Kharis, A., Permatasari, S. M., Sukatmi, S., Perpustakaan, S. I., Hukum, F., Terbuka, U., Matematika, P. S., Terbuka, U., Statistika, P. S., Terbuka, U., Studi, P., Anak, P., & Dini, U. (2025). Cerdas Dan Aman Bermedia Digital : Peningkatan. *Jurnal Abdimas Patikala*, 4(4), 1407–1418.
- Chairunnisa, S. (2024). Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia. *Ilmu Hukum Dan Sosial*, 2(1).
- Desi Ananta, K., Ambodo, T., & Tohawi, A. (2024). Pengaruh Media Sosial terhadap Peningkatan Kejahatan Siber di Indonesia. *Islamic Law: Jurnal Siyash*, 9(2).

This work is licensed under Creative Commons Attribution License 4.0 CC-BY International license

- <https://doi.org/10.53429/iljs.v9i2.858>
- Sari, R. D. N. I. (2025). *Pengaruh transformasi sistem keamanan dan penggunaan teknologi baru terhadap serangan siber pada data nasabah* (Skripsi Sarjana, Institut Agama Islam Negeri Curup). Repository IAIN Curup.
- Hasanudin, A. F., & Babussalam, A. B. (2024). *Upaya Hukum Bagi Korban Kejahatan Phising Yang Menguras Saldo M-Banking*. 6(01).
- Rahmawati, A. F., & Naili, Y. T. (2025). *Penguatan Literasi Digital dan Kesadaran Hukum Pidana Bagi UMKM Sebagai Kaum Rentan Terhadap Kejahatan Siber Berbasis AI di Wilayah Banyumas*. 4(4). <https://doi.org/10.35960/pimas.v1i2.2037>
- Rizieq, M. (2024). Transformasi Layanan Perbankan dari Antrian Panjang Menuju Banking in Your Pocket. *BanKu: Jurnal Perbankan Dan Keuangan*, 5(2), 76–89. <https://doi.org/10.37058/banku.v5i2.13217>
- Sarton, G. (2017). Islamic science. *Near Eastern Culture and Society*, 83–98. <https://doi.org/10.1515/9781400886845-007>
- Semarang), R. A. A. (Universitas N., Semarang), N. S. F. (Universitas N., Semarang), A. H. H. (Universitas N., & Semarang), M. P. (Universitas N. (2025). Penyalahgunaan Data Pribadi dalam Teknologi Transaksi Digital di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia). *Jurnal Multidisiplin Ilmu Akademik*, 2(1), 1.
- Sugiantari, A. A. P. W., & Julianti, L. (2021). Tanggung jawab hukum pihak perbankan dalam pencurian data pribadi nasabah dengan teknik *phishing* pada transaksi perbankan. *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasarakswati Denpasar 2020*, 1(1), 96–105.