

BIJAK DALAM BERMEDIA SOSIAL: LAWAN HOAKS & PHISHING

Wafiq Abdul Hafish ^{*1}, Aditia Fristanto ², Megasari Apriniarti ³, Fadillah Ulfa ⁴, Hasmi Suyuthi ⁵

Universitas Muhammadiyah Bengkulu, Bengkulu, Indonesia

^{1,2}Fakultas Teknik, Universitas Muhammadiyah Bengkulu

^{3,5}Fakultas Keguruan Dan Ilmu Pendidikan, Universitas Muhammadiyah Bengkulu

⁴Fakultas Agama Islam, Universitas Muhammadiyah Bengkulu

Email: *wafiqabduhafish7@gmail.com, aditiaf1rst@gmail.com, mega20sari@gmail.com

ABSTRAK

Masyarakat sekarang semakin memanfaatkan internet dalam berbagai aktivitas sehari-hari, seperti berkomunikasi, menonton hiburan, dan melakukan transaksi uang. Namun, hal ini juga membuat munculnya masalah baru, terutama berupa kejahatan siber. Salah satu bentuk kejahatan siber ini Phishing adalah tindakan penipuan di mana orang yang tidak bertanggung jawab berpura-pura menjadi pihak resmi, seperti bank atau perusahaan, untuk mencuri data pribadi atau informasi keuangan korban. Adapun mitra dalam kegiatan sosialisasi ini adalah masyarakat umum, terutama ibu-ibu PKK. Mereka masih kurang memahami cara mengenali tanda-tanda phishing, sehingga rentan menjadi korban. Masalah utamanya adalah rendahnya kemampuan literasi digital dan kurangnya kesadaran terhadap bahaya jika berbagi data di internet. Untuk mengatasi masalah itu, dilakukan kegiatan sosialisasi pada Mahakarya 1 hari. Metode yang digunakan meliputi pemaparan materi, studi kasus, diskusi, dan simulasi untuk melatih peserta dalam mengenali dan mencegah phishing. Materi yang diberikan fokus pada langkah-langkah pencegahan, seperti tidak mengklik tautan yang mencurigakan, tidak menginstal aplikasi dari sumber tidak terpercaya, tidak memberikan informasi pribadi kepada orang yang tidak dikenal. Hasil kegiatan menunjukkan adanya peningkatan pemahaman peserta, baik masyarakat umum maupun ibu-ibu PKK, terhadap bentuk dan ciri-ciri phishing serta kemampuan mereka dalam menerapkan langkah-langkah pencegahan. Dengan demikian, kegiatan ini berhasil meningkatkan kemampuan literasi digital peserta dan memberikan kontribusi nyata dalam membentuk kesadaran masyarakat agar bisa lebih bijak dan aman dalam menggunakan internet.

Kata Kunci: Bijak dalam bermedia sosial untuk menghindari hoax

I. PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat membuat internet menjadi bagian yang sangat penting dalam kehidupan sehari-hari. Saat ini, masyarakat tidak hanya menggunakan internet untuk berkomunikasi, tetapi juga untuk menonton hiburan, belajar, dan melaksanakan transaksi uang. Kondisi ini membawa banyak kemudahan dan efisiensi dalam berbagai bidang kehidupan. Namun di balik keuntungannya, ada juga risiko yang bisa menyebabkan kerugian bagi pengguna, salah satunya adalah kejahatan siber.

Menurut Chiew, Yong, dan Tan (2018), phishing merupakan salah satu bentuk serangan siber yang paling umum dengan berbagai tipe dan teknik yang digunakan untuk mengecoh korban. Kesadaran keamanan yang rendah membuat banyak pengguna mudah menjadi korban serangan phishing, dikutip dari Vadila dan Pratama (2021). Penelitian sebelumnya juga menemukan bahwa kejahatan online phishing dapat menasar institusi pemerintah maupun pendidikan melalui email palsu (Sari & Sutabri, 2023).

Untuk mengatasi masalah ini, dilakukan kegiatan sosialisasi dengan

metode seperti penyampaian materi, studi kasus, diskusi, dan simulasi pencegahan.

Dalam kegiatan ini, masyarakat diberikan pengetahuan serta keterampilan praktis untuk mengenali dan menghindari phishing, seperti tidak membuka tautan yang mencurigakan, tidak menginstal aplikasi dari sumber tidak jelas, tidak memberikan data pribadi kepada pihak yang tidak dikenal.

Tujuan utama dari kegiatan ini adalah agar masyarakat lebih paham tentang dunia digital, terutama soal keamanan siber, sehingga mereka mampu menggunakan internet dengan lebih bijak dan aman. Dengan adanya peningkatan kesadaran ini, diharapkan masyarakat bisa mengurangi risiko menjadi korban phishing serta ikut serta membangun lingkungan digital yang lebih aman.

II. METODE KEGIATAN

Kegiatan sosialisasi ini dilaksanakan kisaran Agustus 2025 di Kelurahan Tanjung Agung, dengan sasaran masyarakat umum sebagai mitra kegiatan. Durasi pelaksanaan berlangsung selama 60 menit.

Metode yang digunakan adalah sosialisasi berupa penyampaian pengetahuan tentang bahaya hoaks dan penipuan phishing. Kegiatan ini bertujuan untuk meningkatkan literasi digital masyarakat agar lebih waspada dalam menggunakan internet, terutama dalam berinteraksi melalui media sosial.

Adapun langkah-langkah pelaksanaan kegiatan meliputi:

1. Penyampaian materi mengenai bentuk-bentuk hoaks dan phishing yang sering terjadi di media sosial.
2. Penjelasan interaktif mengenai risiko membuka tautan dari pihak yang tidak dikenal.
3. Studi kasus dengan menunjukkan contoh situs web palsu yang biasa digunakan untuk melakukan penipuan.

4. Diskusi dan tanya jawab untuk memberikan ruang kepada peserta berbagi pengalaman serta memperoleh solusi praktis.

Melalui metode ini, masyarakat diharapkan mampu memahami ciri-ciri modus penipuan digital, menghindari tautan mencurigakan, serta meningkatkan kewaspadaan dalam menjaga data pribadi agar terhindar dari phishing.



Gambar 1. Sesi Pembukaan.

III. HASIL DAN PEMBAHASAN

Kegiatan sosialisasi “Bijak dalam Bermedia Sosial: Lawan Hoaks & Phishing” telah dilaksanakan kisaran Agustus 2025 di Kelurahan Tanjung Agung, Kecamatan Sungai Serut, Kota Bengkulu. Peserta kegiatan terdiri dari masyarakat umum dan ibu-ibu PKK sebagai target utama. Kegiatan berlangsung selama 60 menit dengan suasana aktif dan partisipatif.

1. Penyampaian Materi

Pada tahap awal, tim pengabdian menyampaikan materi mengenai bentuk-bentuk hoaks dan phishing yang marak terjadi. Peserta diperkenalkan pada ciri-ciri umum phishing seperti:

- Tautan (link) mencurigakan yang mirip dengan website resmi.
- Permintaan data pribadi secara tidak wajar.

- Penawaran hadiah dengan syarat mengklik tautan tertentu.

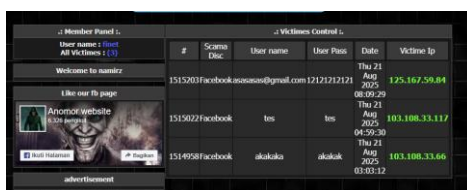
2. Studi Kasus:

Website Palsu Peserta diperlihatkan contoh website palsu yang dibuat mirip dengan situs resmi perbankan atau marketplace. Biasanya pelaku meminta pengguna login agar data pribadi dan password bisa dicuri.

- Kontribusi: Memberikan pemahaman bagaimana membedakan website resmi dengan palsu, misalnya dengan mengecek URL dan sertifikat keamanan (https).
- Dampak: Peserta memahami cara cepat mengecek keaslian situs sebelum memasukkan data penting.



Gambar 2. Contoh Phishing media sosial.



Gambar 3. Contoh Phishing ketika menginput data.

3. Penipuan WhatsApp

Peserta juga dikenalkan pada modus penipuan WhatsApp dengan imbalan hadiah, seperti mobil gratis atau undian berhadiah. Pelaku biasanya mengirim pesan massal dengan link klaim hadiah, lalu meminta korban mengisi data

pribadi atau mentransfer uang untuk "biaya administrasi".

- Kontribusi: Memberikan pemahaman bahwa perusahaan resmi tidak pernah memberikan hadiah tanpa prosedur yang jelas.
- Dampak: Peserta lebih berhati-hati dan tidak mudah tergiur janji hadiah palsu. Terutama ibu-ibu PKK, yang sebelumnya mengaku sering menerima pesan serupa.



Gambar 4. Contoh Penipuan di WhatsApp.

IV. KESIMPULAN DAN SARAN

Kesimpulan

Kegiatan sosialisasi tentang "Bijak dalam Menggunakan Media Sosial: Mengenali Hoaks & Phishing" yang diadakan di Kelurahan Tanjung Agung berhasil meningkatkan pemahaman masyarakat tentang dunia digital, terutama para ibu-ibu PKK dan warga umum. Peserta kegiatan berhasil memahami berbagai bentuk phishing, mengenali tanda-tanda penipuan online, serta mengetahui cara-cara mencegahnya, seperti tidak membuka tautan yang tidak jelas, tidak memberikan data pribadi secara sembarangan, dan lebih berhati-hati

terhadap tipu daya hadiah palsu di media sosial. Dengan meningkatnya pengetahuan tersebut, masyarakat menjadi lebih waspada terhadap ancaman kejahatan siber dan mampu memanfaatkan internet dengan bijak serta aman.

Saran

1. Untuk masyarakat: Diharapkan terus meningkatkan kewaspadaan dan tidak mudah tergiur oleh iming-iming hadiah atau pesan mencurigakan. Penting juga untuk membiasakan mengecek kebenaran informasi sebelum membagikannya.
2. Untuk pemerintah/instansi terkait: Perlu adanya program berkelanjutan dalam bentuk pelatihan literasi digital di tingkat RT/RW atau kelompok (Vadila & Pratama, Analisis kesadaran keamanan terhadap ancaman phishing, 2021) keamanan data semakin merata.
3. Untuk tim pelaksana: Kegiatan serupa sebaiknya dikembangkan dengan materi lebih variatif, misalnya simulasi interaktif menggunakan aplikasi nyata, agar peserta lebih terampil dalam menghadapi potensi serangan phishing. (Budiastanti, 2017)
4. Untuk penelitian/pengabdian berikutnya: Disarankan memperluas target peserta ke kalangan pelajar dan remaja yang juga rentan menjadi korban hoaks dan penipuan digital.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada seluruh anggota KKN 13 Universitas Muhammadiyah Bengkulu yang telah bekerja sama dengan baik dalam merancang dan melaksanakan kegiatan sosialisasi ini. Ucapan terima kasih juga disampaikan kepada ibu-ibu PKK, masyarakat Kelurahan Tanjung Agung, serta pihak kelurahan yang telah memberikan dukungan penuh sehingga kegiatan dapat berjalan lancar. Tidak lupa

penulis menghaturkan terima kasih kepada Ketua Lurah, Ketua RT 1–3, dan Ketua RW di Kelurahan Tanjung Agung yang telah memfasilitasi dan membantu proses koordinasi dengan warga. Berkat dukungan semua pihak, kegiatan sosialisasi “*Bijak dalam Bermedia Sosial: Lawan Hoaks & Phishing*” dapat terlaksana dengan baik dan memberikan manfaat bagi masyarakat dalam meningkatkan literasi digital serta kewaspadaan terhadap kejahatan siber.

DAFTAR PUSTAKA

- Bagus Dewanto, M. A., Fathurrahman, M., Firdaus, D. R., & Setiawan, A. (2024). Penipuan Penambah Followers Instagram: Analisis Serangan Phising dan Dampaknya pada Keamanan Data. *Journal of Internet and Software Engineering*, 1-11.
- Bodhi, S., & Tan, D. (2022). Keamanan Data Pribadi dalam Sistem Pembayaran E-Wallet terhadap Ancaman Penipuan dan Pengelabuan (Cybercrime). *UNES Law Review (UnesRev)*, 297–308.
- Budiastanti, D. E. (2017). Perlindungan hukum terhadap korban tindak pidana penipuan melalui internet. *Jurnal Cakrawala Hukum*, 22-32.
- Chiew, K. L., Yong, K. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, 1-20.
- Iskandar, O., & Kelas 4A4. (2024). Analisis Kejahatan Online Phishing pada Masyarakat. *Leuser: Jurnal Hukum Nusantara*, 34–36.
- Kusuma, F. A., Limantara, V., Gracia, G., & Sudimin, T. (2004). Etika Periklanan pada Era Digital: Hoax dan Penipuan. *JURNAL LOCUS*:

- Penelitian & Pengabdian*, 2026–2039.
- Rafiq, A. (2020). Dampak Media Sosial terhadap Perubahan Sosial Suatu Masyarakat. *Global Komunika: Jurnal Ilmu Sosial dan Ilmu Politik*, 18-29.
- Rahardja, U., Lutfiani, N., & Alpansuri, M. (2018). Pemanfaatan Google Formulir Sebagai Sistem Pendaftaran Anggota Pada Website Aptisi. *Jurnal Ilmiah SISFOTENIKA (STMIK Pontianak)*, 128-139.
- Rahmanto, T. Y. (2018). PENEGAKAN HUKUM TERHADAP TINDAK PIDANA PENIPUAN. *Jurnal Penelitian Hukum*, 31-51.
- Ramadhan, I. H., & Nurnawati, E. K. (2022). Analisis ancaman phishing dalam layanan e-commerce. *PROSIDING SNAST*, 31-41.
- Sahfitri, A., & Rosmalinda. (n.d.). Penipuan Digital Melalui Tautan Phishing. *Jurnal Dialektika Hukum*, 2024.
- Sari, P., & Sutabri, T. (2023). Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari. *Jurnal Digital Teknologi Informasi*, 6(1).
- Sumenge, M. (2013). Penipuan Menggunakan Media Internet Berupa Jual-Beli Online. *Lex Crimen*, 102-112.
- Vadila, N., & Pratama, A. R. (2021). Analisis kesadaran keamanan terhadap ancaman phishing. *AUTOMATA*, 2(2).
- Wahyuni, N. A., Cahayani, P. P., Wicaksana, I. N., & Wijayanti, I. K. (n.d.). Analisis kerentanan kejahatan online phising menggunakan tools Zphisher, Shellphish dan Whphisher: Phising. *Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer*.
- Yustitiana, R. (2021). Pelaksanaan pengaturan hukum tindak kejahatan fraud phishing transaksi elektronik sebagai bagian dari upaya penegakan hukum di Indonesia dikaitkan dengan teori efektivitas hukum. *Jurnal Hukum Visio Justisia*, 98-126.