

Literasi Media Sosial: Upaya Pencegahan Pemalsuan Identitas Digital

Nuning Kurniasih

Program Studi Perpustakaan dan Sains Informasi, Fakultas Ilmu Komunikasi, Universitas Padjadjaran, Bandung, Indonesia

Email: nuning.kurniasih@unpad.ac.id

Email Penulis Korespondensi: nuning.kurniasih@unpad.ac.id

Abstrak-Peningkatan jumlah penggunaan internet berdampak pada meningkatnya kejahatan di dunia maya. Salah satu kejahatan di dunia maya antara lain diakibatkan adanya online impersonation atau peniruan identitas secara online. Dalam kondisi demikian, penting untuk melakukan sosialisasi tentang literasi media sosial terutama dalam upaya mencegah penipuan identitas digital. Tujuan kegiatan pengabdian ini adalah untuk membekali masyarakat dengan literasi media sosial agar terhindar dari bahaya penyalahgunaan media sosial terutama yang diakibatkan oleh peniruan atau pemalsuan identitas digital. Analisis masalah dilakukan dengan mengkaji fenomena, berita dan temuan hasil riset tentang penyalahgunaan dan kejahatan di media sosial terutama yang berkaitan dengan pemalsuan identitas di Indonesia. Materi pelatihan disampaikan dalam Webinar pada Aplikasi Zoom dan disiarkan secara langsung pada kanal YouTube. Materi pelatihan atau Webinar mencakup pemahaman akan literasi media, pemahaman akan literasi media sosial, pengetahuan tentang bentuk-bentuk penyalahgunaan media sosial, penanaman kesadaran akan bahaya pemalsuan identitas digital, pengetahuan tentang jenis-jenis peniruan atau pemalsuan identitas digital dan upaya pencegahan pemalsuan identitas digital. Khalayak sasaran kegiatan pengabdian ini adalah pelajar, mahasiswa, para akademisi hingga masyarakat umum. Pemahaman khalayak sasaran terhadap materi yang disampaikan pada saat kegiatan pengabdian dapat dilihat pada saat sesi tanya jawab atau diskusi. Pada sesi tersebut terlihat khalayak sasaran menyampaikan beberapa pertanyaan yang sesuai dengan materi pelatihan yang disampaikan. Dari pengamatan penulis pada sesi Tanya jawab atau diskusi, khalayak sasaran memiliki pemahaman yang sangat baik terhadap materi pelatihan yang diterimanya

Kata Kunci: Literasi Media; Literasi Media Sosial; Online Impersonation; Penipuan Identitas; Kejahatan Di Dunia Maya

Abstract-The increase in internet usage has led to an increase in cybercrime. One of the crimes in cyberspace is caused by online impersonation. In these conditions, it is important to socialize social media literacy, especially in an effort to prevent digital identity fraud. The purpose of this community service activity is to equip the community with social media literacy in order to avoid the dangers of social media misuse, especially those caused by impersonation or digital identity forgery. The problem was analyzed by reviewing phenomena, news and research findings on social media misuse and crime, especially those related to identity forgery in Indonesia. The training or Webinar material includes an understanding of media literacy, an understanding of social media literacy, knowledge of types of social media misuse, instilling awareness of the dangers of digital identity forgery, knowledge of the types of digital identity impersonation or forgery and efforts to prevent digital identity forgery. The target audiences for this community service activity are students, academics and the general public. The training material was delivered in a Webinar on the Zoom App and broadcast live on the YouTube channel. The understanding of the target audience of the material presented during the community service activity can be seen during the question and answer session or discussion. In this session, it was seen that the target audience asked several questions that were in accordance with the training material presented. From the observations in the Q&A or discussion session, the target audience had a very good understanding of the training material they received.

Keywords: Media Literacy; Social Media Literacy; Online Impersonation; Digital Identity Fraud; Cybercrime

1. PENDAHULUAN

Peningkatan jumlah penggunaan internet berdampak pada meningkatnya kejahatan di dunia maya. Hasil riset yang dilakukan oleh Kurnia dkk (2022) menunjukkan bahwa kerentanan terhadap penipuan digital di Indonesia mencapai 98,3%. Hal ini dilihat dari data penelitian terhadap 1700 responden, dimana 1671 diantaranya pernah menerima pesan penipuan digital. Dari jumlah tersebut, 1132 responden atau 66,6% pernah menjadi korban penipuan digital (Kurnia et al., 2022).

Salah satu kejahatan di dunia maya antara lain diakibatkan adanya online impersonation atau peniruan identitas online (Nafees, Pan, Chen, & Foulds, 2021; Powell, 2019; Simmons & Lee, 2020; Solo, 2019, 2020). Online impersonation dilakukan seseorang atau sekelompok orang dengan membuat identitas palsu untuk melakukan tindakan penipuan dengan tujuan menghasilkan keuntungan bagi diri sendiri dan merugikan orang lain secara online. Pada dasarnya tidak ada masalah dengan kegiatan peniruan atau penyamaran. Namun, apabila kegiatan peniruan atau penyamaran tersebut merugikan orang lain dan dilakukan secara ilegal, maka bisa jadi hal tersebut melanggar hukum.

Di Indonesia, penggunaan identitas orang lain atau pemalsuan identitas baik berupa pemalsuan nama, alamat, jabatan dan identitas lainnya yang dipergunakan untuk memperdaya korban agar percaya seakan-akan identitas palsu tersebut adalah identitas yang benar, merupakan tindak pidana (Presiden Republik Indonesia, 2022, 2023). Sementara itu dalam Undang-undang Informasi dan Transaksi Elektronik RI, regulasi tentang kejahatan pemalsuan identitas masih berfokus pada penipuan jual beli untuk transaksi elektronik dan belum menyentuh pada penipuan identitas online (Dewi & Irwansyah, 2021; Presiden RI, 2016).

Dalam kondisi demikian, penting untuk melakukan sosialisasi tentang literasi media sosial terutama dalam upaya mencegah penipuan identitas digital. Literasi media dapat membantu masyarakat mencegah bahaya penyalahgunaan media dan meningkatkan keyakinan sikap dan niat dalam menjadikan media lebih baik (Cho, Cannon, Lopez, & Li, 2022).

2. METODE PELAKSANAAN

2.1. Lokasi dan Waktu Pelaksanaan

Pelaksanaan kegiatan pengabdian kepada masyarakat ini terintegrasi dengan kegiatan Libricious 2023 yang diselenggarakan oleh mahasiswa Program Studi Perpustakaan dan Sain Informasi Fakultas Ilmu Komunikasi Universitas Padjadjaran pada Jumat, 12 Mei 2023, pukul 08.15 – 11.00 WIB.

2.2. Tahap Pengabdian

Proses pelaksanaan pengabdian ini diawali dengan adanya permintaan dari Panitia Libricious 2023 kepada penulis untuk menjadi narasumber pada kegiatan Webinar bertajuk “Literasi Bermedia Sosial: Peran Generasi Muda Mencegah Impersonation dan Spoofing”. Berdasarkan tema yang diberikan oleh panitia tersebut, penulis melakukan analisis dan identifikasi masalah. Selanjutnya, penulis menyusun materi Webinar dengan judul “Literasi Media Sosial: Upaya Pencegahan Impersonation dan Spoofing”. Materi ini kemudian disampaikan pada kegiatan Webinar melalui Aplikasi Zoom dan disiarkan secara langsung di kanal YouTube BEM Fikom Unpad. Setelah penyampaian materi, dilanjutkan dengan sesi Tanya jawab, evaluasi dan penyusunan laporan. Penyampaian materi Webinar dilakukan dengan model pembelajaran andragogi dengan ceramah sebagai teknik penyampaian materi. Model pembelajaran andragogi memiliki 4 prinsip, yaitu (a) Melibatkan peserta didik dewasa; (b) Berdasarkan pengalaman, menerapkan teori ke dalam praktek; (c) Relevansi dan dampak terhadap kehidupan peserta didik; (d) Berpusat pada masalah (Yopp, Ludwig, & Serrano, 2013).

2.3. Bahan dan Alat

Bahan dan alat yang dipergunakan dalam kegiatan pengabdian kepada masyarakat ini adalah materi presentasi berupa slides presentasi dan media pertemuan daring yaitu Aplikasi Zoom dan media streaming yaitu YouTube.

2.4. Khalayak Sasaran

Target audien atau khalayak sasaran kegiatan pengabdian ini adalah pelajar, mahasiswa, para akademisi hingga masyarakat umum. Pada saat kegiatan, lebih dari 100 peserta hadir dalam Webinar tersebut baik melalui Aplikasi Zoom maupun YouTube.

2.5. Rancangan Evaluasi Kegiatan

2.5.1. Metode Evaluasi

Untuk mengetahui apakah khalayak sasaran dapat memahami apa yang disampaikan oleh narasumber/ penulis maka pada sesi tanya jawab, penulis menanyakan apakah jawaban yang diberikan oleh penulis dapat dipahami dan diterima oleh penanya, serta apakah ada pendapat dari peserta lain untuk mengetahui perspektif lain dari peserta Webinar. Jawaban dan pendapat atau respon dari khalayak sasaran dapat menjadi bahan evaluasi tentang pemahaman audien dan efektifitas penyampaian pesan.

2.5.2. Waktu Evaluasi

Evaluasi terhadap bagaimana pemahaman peserta Webinar dan bagaimana efektifitas penyampaian pesan dilakukan pada saat sesi tanya jawab. Setelah Webinar selesai, penulis membuka kembali rekaman acara dan mengevaluasi acara secara keseluruhan.

2.6. Kriteria Keberhasilan dan Tolak Ukur Pencapaian Tujuan

Kegiatan pengabdian ini bertujuan untuk mensosialisasikan bahaya pemalsuan identitas dengan memberikan literasi bermedia sosial kepada khalayak sasaran agar dapat terhindar dari pemalsuan identitas. Adapun kriteria keberhasilan dan tolak ukur pencapaian tujuan dirumuskan sebagai berikut: khalayak sasaran dapat memahami pentingnya literasi media sosial, khalayak sasaran dapat memahami jenis-jenis penyalahgunaan media sosial, khalayak sasaran memahami jenis-jenis penipuan identitas yang merujuk pada pemalsuan identitas, khalayak sasaran memahami bagaimana mendeteksi dan menghindari pemalsuan identitas.

3. HASIL DAN PEMBAHASAN

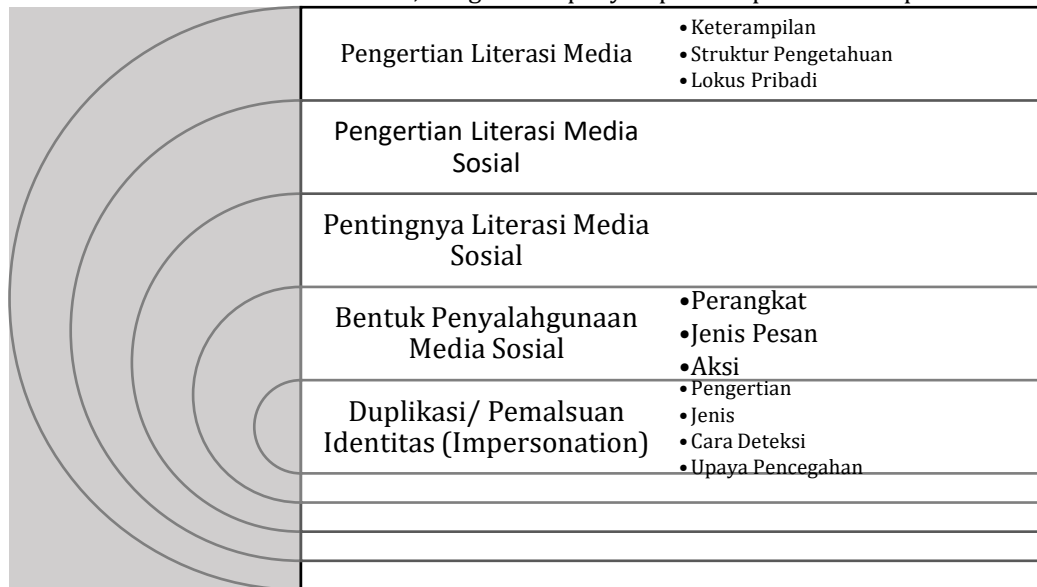
3.1. Penjelasan Kegiatan

3.1.1. Analisis dan Identifikasi Masalah

Analisis masalah dilakukan dengan mengkaji fenomena, berita dan temuan hasil riset tentang penyalahgunaan dan kejahatan di media sosial terutama yang berkaitan dengan pemalsuan identitas di Indonesia. Berdasarkan hasil analisis, maka masalah-masalah yang dinilai perlu disampaikan mencakup literasi media sosial secara umum, pemahaman pada jenis penyalahgunaan media sosial, pemahaman pada bahaya pemalsuan identitas, bagaimana cara mengidentifikasi dan menghindari bahaya pemalsuan identitas.

3.1.2. Penyampaian Materi

Penyampaian materi dilakukan melalui Webinar, dengan alur penyampaian seperti terlihat pada Gambar 1.



The diagram shows a series of concentric semi-circles on the left side, representing a flow or sequence. To the right of these circles is a table with five rows, each corresponding to a topic in the webinar. The first row is 'Pengertian Literasi Media' with sub-points: Keterampilan, Struktur Pengetahuan, and Lokus Pribadi. The second row is 'Pengertian Literasi Media Sosial'. The third row is 'Pentingnya Literasi Media Sosial'. The fourth row is 'Bentuk Penyalahgunaan Media Sosial' with sub-points: Perangkat, Jenis Pesan, Aksi, and Pengertian. The fifth row is 'Duplikasi/ Pemalsuan Identitas (Impersonation)' with sub-points: Jenis, Cara Deteksi, and Upaya Pencegahan. There are three empty rows at the bottom of the table.

Pengertian Literasi Media	<ul style="list-style-type: none">• Keterampilan• Struktur Pengetahuan• Lokus Pribadi
Pengertian Literasi Media Sosial	
Pentingnya Literasi Media Sosial	
Bentuk Penyalahgunaan Media Sosial	<ul style="list-style-type: none">• Perangkat• Jenis Pesan• Aksi• Pengertian
Duplikasi/ Pemalsuan Identitas (Impersonation)	<ul style="list-style-type: none">• Jenis• Cara Deteksi• Upaya Pencegahan

Gambar 1. Materi Pelatihan/ Webinar “Literasi Media Sosial: Upaya Pencegahan Pemalsuan Identitas Digital” oleh Nuning Kurniasih

Seperti terlihat pada Gambar 1, penyampaian materi diawali dengan pembahasan apa itu literasi media. Pada dasarnya literasi media merupakan kemampuan di dalam memahami, mencari, mengakses, menyimpan, menganalisis, mengevaluasi, mempergunakan, menciptakan atau memproduksi dan mendistribusikan pesan dalam berbagai bentuk media baik online maupun offline. Potter (2020) menyebutkan bahwa literasi media mencakup tiga hal, yaitu keterampilan, struktur pengetahuan dan lokus pribadi. Keterampilan dalam literasi media merupakan alat yang dipergunakan untuk memahami pesan di dalam media, bagaimana memahami pesan secara deduksi dan induksi, bagaimana membuat sintesis, melakukan analisis dan membuat evaluasi terhadap pesan. Pada komponen struktur pengetahuan, semua informasi yang terorganisir dalam diri individu dapat dipergunakan untuk menginterpretasikan pesan yang ada dalam media sesuai dengan koteksnya. Sementara itu lokus pribadi dipengaruhi oleh dorongan dan tujuan dari setiap individu dalam melakukan proses pencarian dan pemrosesan informasi (Potter, 2020). CML (2023) menyebutkan empat langkah dalam literasi media mulai dari kepedulian, analisis, refleksi, hingga aksi. Sebagai navigasi dalam menjalankan tahap-tahap tersebut, maka literasi media memerlukan 5 keterampilan yaitu keterampilan dalam mengakses informasi dari berbagai sumber; kemampuan analisis dan jelajah tentang bagaimana pesan dikonstruksi melalui berbagai media; keterampilan mengevaluasi pesan baik dilihat secara etika, moral dan prinsip demokratis; keterampilan dalam mengekspresikan atau menciptakan pesan dengan mempergunakan berbagai media; dan kemampuan dalam berpartisipasi di dalam budaya media global (Center for Media Literacy, 2023). Menurut Baran (2014), ketrampilan dalam literasi media mencakup pemahaman dan perhatian akan konten, mampu memfilter gangguan, menghormati kekuatan media, mampu mengelola emosi, genre, harapan pada konten, kemampuan berpikir kritis dan pengetahuan bahasa sehingga dapat menciptakan nilai (Baran, 2014). Sementara itu The European Charter for Media Literacy (2007) menyebutkan ada tujuh kompetensi dalam literasi media, yaitu kompetensi penggunaan teknologi media secara efektif untuk mengakses, menyimpan, menemukan kembali dan membagi konten; kemampuan untuk mendapatkan akses informasi dari berbagai media; kemampuan untuk memahami bagaimana dan mengapa konten dibuat; kemampuan menganalisis beragam konten dalam media; kemampuan menganalisis konten secara kritis baik dari sisi teknis, bahasa ataupun konvensi dalam media;

kemampuan untuk mengidentifikasi dan menghindari konten yang berbahaya dalam berbagai media; dan kemampuan untuk memanfaatkan media secara efektif dan bertanggung jawab (Bachmair & Bazalgette, 2007).

Dari beberapa pendapat tersebut, dapat disimpulkan bahwa literasi media memberi bekal kepada masyarakat dalam memahami peran media di masyarakat termasuk memahami bagaimana keterampilan yang diperlukan dalam mempergunakan dan mengekspresikan diri di berbagai jenis media.

Setelah menjelaskan tentang literasi media, berikutnya penulis menjelaskan tentang literasi media sosial. Konsep literasi media sosial merupakan penggabungan konsep literasi informasi, literasi media dan literasi digital. Di tengah banyaknya kekhawatiran tentang dampak negatif penggunaan media sosial, literasi media sosial membekali pengguna dengan struktur kognitif, afektif dan keterampilan secara kritis, sehat dan bertanggung jawab dalam mempergunakan media sosial. Schreurs dan Vandenbosch (2021) memperkenalkan Model Literasi Media Sosial yang disebut SMILE. Model SMILE memperkenalkan kerangka kerja literasi media sosial berdasarkan efek media, psikologi sosial, komunikasi interpersonal dan literatur pendidikan. (Schreurs & Vandenbosch, 2021).

Selanjutnya peserta diajak untuk memahami mengapa literasi media terutama literasi media sosial diperlukan. Menurut penulis, ada beberapa hal yang membuat literasi media penting, yaitu pertama melalui literasi media kita akan dapat memahami media, bagaimana media membangun budaya populer dan bagaimana media mempengaruhi keputusan pribadi; kedua, literasi media akan membangun kesadaran, tidak hanya tentang media tetapi juga tentang pesan yang diterima; ketiga, literasi media sosial akan membantu pengguna berpikir kritis sehingga pengguna dapat mengenali, menyaring persepsi dan keyakinan terhadap media sekaligus pesan yang ada di dalamnya; keempat, dengan literasi media, pengguna tidak hanya berperan aktif sebagai konsumen informasi, tetapi dapat aktif dan kreatif menciptakan konten-konten di berbagai media; kelima, literasi media mempermudah khalayak dalam mengakses media; keenam, literasi media akan membangun kesadaran pengguna untuk aktif dalam mencegah dan menghindari penyalahgunaan media; ketujuh literasi media membri bekal khalayak untuk bijak dan sehat bermedia, memahami etika, moral dan aturan main ketika menggunakan media, pengguna media dapat mengetahui apa yang bisa dan tidak bisa dilakukan ketika mempergunakan media.

Penulis menyampaikan kepada khalayak sasaran, bahwa setidaknya ada tiga jenis penyalahgunaan media sosial, yaitu penyalahgunaan melalui perangkat yang dipergunakan, penyalahgunaan melalui jenis pesan baik berupa teks, gambar, suara, video, dll, dan penyalahgunaan aksi dalam arti penyalahgunaan melalui tindakan atau perilaku bermedia seperti cybercrime, cyberstalking, cyberbullying, penyebaran hoax, pelecehan, penipuan, peniruan dan pemalsuan identitas.

Terkait pemalsuan identitas, penulis menyampaikan maraknya korban online impersonation saat ini. Impersonation merupakan sebuah tindakan peniruan yang merujuk pada penggunaan identitas palsu yang dipergunakan oleh seseorang atau sekelompok orang yang dimaksudkan untuk menipu, sehingga mendapatkan keuntungan pribadi dan merugikan orang lain. Online impersonation yang dimaksudkan untuk menyamarkan sebuah akun asli dan kemudian menyerang media sosial dengan konten palsu merupakan entitas yang jahat (Zarei, Farahbakhsh, Crespi, & Tyson, 2020). Oleh karena itu, apabila ada sebuah penggemar atau akun parodi harus mencantumkan keterangan bahwa akun tersebut bukanlah akun asli dari artis atau figur publik lainnya, tetapi merupakan akun penggemar atau akun parodi. Adapun jenis-jenis dari online impersonation dapat dilihat pada Tabel 1.

Tabel 1. Jenis-jenis Online Impersonation (Peniruan/ Pemalsuan Identitas) di Media Sosial

No.	Jenis-jenis Impersonation	Keterangan
1.	Akun palsu.	Merupakan jenis penyalahgunaan media sosial dengan membuat akun palsu atas nama seseorang atau sebuah lembaga seakan-akan akun tersebut akun asli dari orang atau lembaga yang akunnnya dipalsukan.
2.	Masuk ke akun orang lain dan mempergunakannya tanpa ijin.	Merupakan jenis penyalahgunaan media sosial dengan menyusup masuk ke dalam akun orang lain, kemudian mempergunakan akun tersebut seakan-akan penyusup tersebut adalah pemilik akun tersebut. Kata sandi adalah kunci masuk rahasia yang hanya boleh diketahui oleh pemilik akun. Karena sifatnya rahasia, kata sandi tidak boleh dibagikan kepada orang lain. Namun demikian ada kasus-kasus dimana seseorang membagikan kata sandinya kepada orang-orang terdekat. Walaupun hal tersebut tidak dibenarkan, apabila hal ini terjadi, ada baiknya orang yang diberi akses meminta ijin terlebih dahulu kepada pemilik akun ketika akan mempergunakan akun tersebut. Kasus lainnya adalah sebuah akun yang dijalankan oleh beberapa administrator. Untuk kasus seperti ini sebaiknya setiap admin mencantumkan inisial ketika mempergunakan akun tersebut. Hal ini untuk mempermudah pengawasan penanggung jawab pengguna akun.

No.	Jenis-jenis Impersonation	Keterangan
3.	Manipulasi teknologi.	Merupakan jenis penyalahgunaan media sosial dengan memanfaatkan teknologi seperti dengan mempergunakan kecerdasan buatan untuk meniru suara atau wajah, menyamar, mengumpulkan dan menyebarkan informasi yang berbahaya, melanggar privacy dan hukum.
4.	Bukti palsu.	Merupakan jenis penyalahgunaan media sosial dengan membuat bukti atau pesan palsu.
5.	Email palsu.	Merupakan jenis penyalahgunaan media sosial dengan membuat dan menggunakan email palsu, biasanya menggunakan nama email yang mirip dengan nama email asli. Diperlukan ketelitian untuk melihat apakah email dikirim dari email asli atau palsu.
6.	Spoofing	Merupakan jenis penyalahgunaan media sosial dengan menggunakan nomor telepon, SMS, Whatsapp, email, IP, domain dan aplikasi palsu. Biasanya menggunakan nomor atau akun yang mirip dengan nomor atau akun asli. Bentuk spoofing lainnya adalah serangan siber yang terjadi pada saat pelaku mencegat proses komunikasi diantara dua pihak secara diam-diam, atau disebut Man in The Middle (MitM). Malware MitM yang tengah menyerang seringkali memantau dan mengubah informasi individu/rahasia yang baru disadari oleh kedua pengguna tersebut (Mallik, Ahsan, Shahadat, & Tsou, 2019).
7.	Phishing	Merupakan jenis penyalahgunaan media sosial dengan meniru atau menyamar sebagai karyawan sebuah perusahaan atau sebuah merek. Peniruan ini dimaksudkan untuk menipu konsumen perusahaan, mereka berusaha mendapatkan data atau informasi pelanggan yang sifatnya sensitif atau pribadi seperti nomor rekening bank berikut kata sandinya. Bentuk phising lainnya adalah berupa URL yang mengandung malware.
8.	Counterfeiting	Merupakan jenis penyalahgunaan media sosial dengan meniru dan membuat halaman palsu sebuah merek untuk menipu konsumennya dengan menjual produk palsu.
9.	Fake News	Merupakan jenis penyalahgunaan media sosial dengan melakukan peniruan dan membuat akun palsu dan menyamar sebagai selebritas, figur publik atau sebuah lembaga dengan tujuan menyebarkan dan mengungkap informasi atau berita palsu.
10.	Scams	Merupakan jenis penyalahgunaan media sosial dengan melakukan peniruan dan penipuan dari hasil pencurian identitas untuk mendapatkan sejumlah uang atau barang dari korban.
11.	Catfishing	Merupakan jenis penyalahgunaan media sosial dengan berpura-pura menunjukkan perasaan tertarik kepada orang lain dan biasa terjadi dalam kecan online.
12.	Peniruan identitas pada Ujian Online/ Jarak Jauh	Merupakan jenis penyalahgunaan media pembelajaran dimana siswa mengundang pihak ketiga untuk meniru atau membantu selama ujian berlangsung. Salah satu upaya untuk mengatasi hal ini adalah dengan mempergunakan Principal Componen Analysis/ PCA yaitu dengan melakukan identifikasi dan otentifikasi peserta didik secara langsung selama ujian (R, R, & M, 2017)

Setelah khalayak sasaran mengetahui jenis-jenis peniruan atau pemalsuan identitas, selanjutnya penulis menjelaskan bagaimana cara mendeteksi pemalsuan identitas digital, Cara mendeteksi pemalsuan identitas digital tersebut antara lain dengan meneliti alamat email, URL, nomor telepon atau jenis akun lainnya yang diterima. Hal yang perlu diperhatikan adalah peniru biasanya mempergunakan nama, foto, deskripsi, tagar dan postingan sama dengan nama, foto, deskripsi, tagar dan postingan dari akun asli, sehingga masyarakat harus benar-benar meneliti keaslian akun. Ciri lainnya, penyamar atau penipu biasanya meminta data yang bersifat rahasia dan pribadi seperti nomor rekening beserta kata sandinya, kemudian mengajukan permintaan yang tidak biasa seperti minta ditransfer uang dengan nada mendesak. Selain itu, apabila penipu menggunakan teks, biasanya banyak tulisan yang salah ketik atau typo. Peniruan identitas seperti peniruan email dapat juga dideteksi dengan mempergunakan alat deteksi otomatis, pemantauan terhadap isu-isu tentang serangan atau kejahatan siber yang sedang marak, mempergunakan rekayasa sosial untuk dapat mengenali penipu dan peretas serta mendeteksi serangan duplikasi dan penipuan identitas yang membahayakan.

Terakhir, penulis menyampaikan upaya pencegahan agar khalayak sasaran terhindar dari bahaya impersonation atau duplikasi dan penipuan identitas online. Upaya agar terhindar dari bahaya penipuan identitas digital tersebut antara lain dengan menjaga data pribadi, mempergunakan verifikasi ganda atau otentikasi ganda pada akun media sosial yang dimiliki, melakukan test phishing secara berkala, mempergunakan teknologi yang dapat mendeteksi peniruan identitas secara realtime, apabila terdapat indikasi akun telah ada yang meniru maka hapus infrastruktur peniruan atau penipuan dengan cepat, gunakan fitur “Report” untuk melaporkan akun yang ditiru ataupun yang meniru, membentengi merek, logo dan identitas lainnya dengan perlindungan hak cipta atau paten, menerapkan operasional sesuai Standard Operating Procedure (SOP) bagi perusahaan, teliti tautan sebelum mengkliknya, berhati-hati dalam membuka file dari pengirim yang tidak dikenal serta menonaktifkan fitur autodownload, hanya mengunduh aplikasi resmi, menghindari penggunaan aplikasi dari pihak ketiga, dan menggunakan koneksi internet pribadi untuk transaksi keuangan.

3.2. Tingkat Pemahaman tentang Kegiatan yang Berlangsung

Pemahaman khalayak sasaran terhadap materi yang disampaikan pada saat kegiatan pengabdian dapat dilihat pada saat sesi tanya jawab atau diskusi. Pada sesi tersebut terlihat khalayak sasaran menyampaikan beberapa pertanyaan yang sesuai dengan materi yang disampaikan. Khalayak sasaran ingin mengetahui lebih jauh tentang materi yang disampaikan. Beberapa pertanyaan dari khalayak sasaran atau dalam hal ini adalah peserta Webinar adalah:

- Apabila terlihat lokasi pada perangkat gadget kita berbeda dengan lokasi yang sebenarnya dimana kita berada, apakah ini mengindikasikan bahwa akun kita diretas orang lain?
- Apakah benar akun dompet e-money kita bisa dibajak orang lain apabila kita menggunakan wifi umum?
- Bagaimana mengetahui bahwa e-money kita dipergunakan oleh orang lain?

Pertanyaan-pertanyaan tersebut berkaitan dengan salah satu hal yang dibahas oleh penulis yaitu aspek keamanan digital. Setelah penulis memberikan jawaban, penulis kembali bertanya kepada penanya, apakah jawaban dari penulis dapat diterima? Respon dari penanya baik dengan menjawab “Ya” atau dengan memberikan pertanyaan lanjutan dapat dinilai sebagai pemahaman terhadap materi yang disampaikan. Dari pengamatan penulis pada sesi Tanya jawab atau diskusi, khalayak sasaran memiliki pemahaman yang sangat baik terhadap materi yang disampaikan oleh penulis.

3.3. Dokumentasi

Dokumentasi kegiatan pengabdian ini berupa:

- Materi presentasi berjudul “Literasi Media Sosial: “Upaya Pencegahan Impersonation dan Spoofing”. Materi tersebut dapat diakses pada tautan berikut :
https://www.academia.edu/10199944/LITERASI_MEDIA_SOSIAL
- Video pelaksanaan kegiatan dapat diakses pada Youtube BEM Fikom Unpad dan cuplikan penyampaian materi dapat diakses di akun YouTube penulis dengan tautan sebagai berikut:
<https://www.youtube.com/watch?v=aSUVXQuB6eE>
- Tangkapan layar pada saat kegiatan berlangsung melalui Aplikasi Zoom seperti terlihat pada Gambar 2.



Gambar 2. Tangkapan Layar Penyampaian Materi pada Kegiatan Pengabdian melalui Aplikasi Zoom

4. KESIMPULAN

Literasi media tidak hanya tentang kemampuan teknis mempergunakan media, lebih dari itu literasi media menuntun pengguna untuk mempergunakan media dengan bijak. Literasi media sosial memberi bekal kepada masyarakat dalam memahami peran media sosial di masyarakat termasuk membekali masyarakat dengan keterampilan dalam mempergunakan media sosial dengan baik, menuntun masyarakat mempergunakan pengetahuan yang dimiliki untuk menilai media sosial secara kritis serta memberikan kesadaran bahwa faktor individu berpengaruh dalam membangun media sosial yang sehat dan bernilai guna. Literasi media sosial diharapkan mampu menjadi benteng bagi pengguna media sosial agar terhindar dari bahaya penyalahgunaan media sosial, termasuk dari bahaya penipuan identitas digital.

DAFTAR PUSTAKA

- Bachmair, B., & Bazalgette, C. (2007). The European Charter for Media Literacy: Meaning and Potential. *Research in Comparative and International Education*, 2(1), 80–87. <https://doi.org/10.2304/rcie.2007.2.1.80>
- Baran, S. J. (2014). *Introduction to Mass Communication: Media Literacy and Culture* (8th ed.). New York: McGraw-Hill Education.
- Center for Media Literacy. (2023). *Education Philosophy*. Retrieved from About CML | Center for Media Literacy | Empowerment through Education | CML MediaLit Kit™ | website: <http://www.medialit.org/about-cml>
- Cho, H., Cannon, J., Lopez, R., & Li, W. (2022). Social media literacy: A conceptual framework. *New Media and Society*. <https://doi.org/10.1177/14614448211068530>
- Dewi, N. S. P. S., & Irwansyah, I. (2021). Regulasi terhadap Penipuan Identitas: Studi Fenomena ‘Catfish’ pada Social Networking Sites (SNS). *Jurnal Studi Komunikasi (Indonesian Journal of Communications Studies)*, 5(1), 267. <https://doi.org/10.25139/jsk.v5i1.2612>
- Kurnia, N., Rahayu, R., Wendratama, E., Monggilo, Z. M. Z., Damayantu, A., Angendari, D. A. D., ... Desmalind, D. (2022). Penipuan Digital di Indonesia: Modus, Medium dan Rekomendasi (Vol. 0). Retrieved from https://acadstaff.ugm.ac.id/karya_files/penipuan-digital-di-indonesia-dcfd07e645d245babe887e5e2daa016
- Mallik, A., Ahsan, A., Shahadat, M. M. Z., & Tsou, J. C. (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*, 3(2), 77–92. <https://doi.org/10.5267/j.ijdns.2019.1.001>
- Nafees, M., Pan, S., Chen, Z., & Foulds, J. R. (2021). Impostor GAN: Toward Modeling Social Media User Impersonation with Generative Adversarial Networks. *Communications in Computer and Information Science*, 1296 CCIS, 157–165. https://doi.org/10.1007/978-3-030-91779-1_11
- Potter, W. J. (2020). *Media Literacy* (9th ed.). Los Angeles: SAGE Publications, Inc.
- Powell, K. (2019). PROTECTING VICTIMS OF CYBERSTALKING, CYBERHARASSMENT, AND ONLINE IMPERSONATION THROUGH PROSECUTIONS AND EFFECTIVE LAWS. *Richmond Journal of Law & Technology*, XXV(3), 1–32. Retrieved from <https://jolt.richmond.edu/files/2019/04/Powell-Final-Edit.pdf>
- Presiden Republik Indonesia. Undang-undang perlindungan data pribadi. , (2022).
- Presiden Republik Indonesia. UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 1 TAHUN 2023 TENTANG KITAB UNDANG-UNDANG HUKUM PIDANA. , (2023).
- Presiden RI. (2016). Undang-undang Nomor 19 tahun 2016 tentang informasi dan transaksi elektronik. Retrieved from [https://web.kominfo.go.id/sites/default/files/users/4761/UU 19 Tahun 2016.pdf](https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf)
- R, H., R, A., & M, K. (2017). Detection of Impersonation in Remote Online Examination. 3(4), 2394–0697. Retrieved from <https://www.ijste.org/articles/IJSTEV319080.pdf>
- Schreurs, L., & Vandenbosch, L. (2021). Introducing the Social Media Literacy (SMILE) model with the case of the positivity bias on social media. *Journal of Children and Media*, 15(3), 320–337. <https://doi.org/10.1080/17482798.2020.1809481>
- Simmons, M., & Lee, J. S. (2020). Catfishing: a look into online dating and impersonation. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 12194 LNCS, 349–358. https://doi.org/10.1007/978-3-030-49570-1_24
- Solo, A. M. G. (2019). Combating Online Impersonation in the United States. 2019 International Conference on Computational Science and Computational Intelligence (CSCI). <https://doi.org/10.1109/CSCI49370.2019.00292>
- Solo, A. M. G. (2020). Fighting Online Defamation, Doxing, and Impersonation. *International Conferences Internet Technologies & Society*, 93–97. https://doi.org/10.33965/its_ste2020_202001r013
- Yopp, A., Ludwig, R., & Serrano, T. (2013). *The “ Super Six ” Principles of Andragogy : Take Your Program from Good to Great The “ Super Six ” Principles of Andragogy*. Virginia: IPDAE.
- Zarei, K., Farahbakhsh, R., Crespi, N., & Tyson, G. (2020). Impersonation on Social Media: A Deep Neural Approach to Identify Ingenuine Content. *Proceedings of the 2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2020, (October)*, 11–15. <https://doi.org/10.1109/ASONAM49781.2020.9381437>