KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 2: Ancaman Siber yang Sering Terjadi

Subtopik 2.4: Ancaman pada Media Sosial

Disusun oleh:
Ketut Ananda Dharmawati
NIM: 2215091035

Program Studi S1 Sistem Informasi
Jurusan Teknik Informatika
Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha

BERSAMA CORPU KIWA TENGEN,
KLUNGKUNG TANGGUH HADAPI SERANGAN SIBER

DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN KLUNGKUNG
2025

KATA PENGANTAR

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat-Nya modul pembelajaran *"Keamanan Siber untuk ASN dan Masyarakat"* dapat disusun. Media sosial kini menjadi bagian dari kehidupan sehari-hari, tidak hanya sebagai sarana komunikasi pribadi, tetapi juga sebagai kanal informasi publik dan layanan pemerintahan. Namun, di balik manfaatnya, media sosial juga membuka celah besar terhadap penyalahgunaan data, penyebaran *hoaks*, penipuan daring, dan ancaman reputasi.

Subtopik ini diharapkan membantu ASN dan masyarakat memahami potensi risiko di media sosial serta cara menggunakannya secara aman, bijak, dan bertanggung jawab. Semoga materi ini memberikan manfaat nyata dalam membangun ruang digital yang sehat, aman, dan mendukung kepercayaan publik terhadap pemerintah daerah. Terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan subtopik ini. Semoga subtopik ini memberikan manfaat nyata dalam mendukung terwujudnya tata kelola pemerintahan dan kehidupan masyarakat yang lebih aman di era digital.

Kami menyadari bahwa modul ini masih memiliki keterbatasan dan belum sempurna. Oleh karena itu, kami sangat mengharapkan kritik dan saran yang membangun dari para pembaca demi penyempurnaan modul ajar ini di masa mendatang.

Klungkung, 2025

Penyusun

DAFTAR ISI

Tujuan Pembelajaran

Setelah mempelajari subtopik ini, peserta (ASN maupun masyarakat) diharapkan mampu:

1. Menjelaskan berbagai bentuk ancaman siber yang terjadi melalui media sosial.
2. Membedakan antara informasi asli dan manipulatif (*hoaks*, *phishing* media sosial, impersonasi).
3. Menerapkan langkah-langkah aman dan etis dalam menggunakan media sosial pribadi maupun institusional.

Sasaran Peserta

1. ASN: agar memahami tanggung jawab dan etika penggunaan media sosial yang mencerminkan profesionalisme instansi.
2. Masyarakat: agar lebih cerdas dan waspada terhadap ancaman penipuan dan manipulasi informasi di media sosial.

A. Pemahaman Awal tentang Ancaman di Media Sosial

Media sosial kini menjadi bagian tak terpisahkan dari kehidupan masyarakat dan pemerintahan. Bagi **ASN**, media sosial adalah sarana komunikasi publik, promosi program pemerintah, serta alat untuk mendengarkan aspirasi masyarakat. Sementara bagi **masyarakat**, platform seperti Facebook, Instagram, TikTok, dan X (Twitter) menjadi ruang berbagi informasi, hiburan, dan interaksi sosial.

Namun, di balik kemudahan itu, media sosial juga menjadi **lahan subur bagi ancaman siber yang bersifat halus dan sering kali tidak disadari.** Berbeda dengan serangan seperti *phishing* atau *malware* yang biasanya terjadi lewat email atau sistem teknis, ancaman di media sosial lebih banyak melibatkan **manipulasi perilaku, psikologi, dan emosi pengguna.**

1. Perubahan Pola Ancaman Tahun 2025

Berdasarkan laporan *Badan Siber dan Sandi Negara (BSSN, 2025)* dan hasil pemantauan *We Are Social Global Report 2025*, tingkat penggunaan media sosial di Indonesia mencapai **84% populasi**. Dengan tingginya aktivitas digital, muncul pola baru ancaman yang lebih canggih, antara lain:

a. **Deepfake dan konten manipulatif**, yang dapat digunakan untuk meniru wajah atau suara pejabat, lalu menyebarkan pesan palsu.
b. **Social engineering berbasis empati**, seperti pesan bantuan palsu yang memanfaatkan isu kemanusiaan untuk menipu warga.
c. **Pemanfaatan algoritma media sosial** untuk menyebarkan informasi tertentu secara masif dan membentuk opini publik.

Ancaman-ancaman ini sulit dideteksi hanya dengan perangkat keamanan biasa, karena menyasar **manusia sebagai titik lemahnya sistem.**

2. Media Sosial sebagai Cermin Reputasi ASN dan Pemerintah Daerah

Bagi ASN, media sosial bukan hanya tempat berbagi informasi pribadi. Setiap unggahan, komentar, atau bahkan *like* dapat merepresentasikan citra instansi

tempat ia bekerja. Itulah sebabnya **etiket digital (*digital etiquette*)** menjadi salah satu aspek penting dalam keamanan siber pemerintahan daerah.

📌 *Contoh sederhana:*

Komentar ASN terhadap isu politik, atau unggahan yang menyinggung kelompok tertentu, dapat dengan cepat viral dan menurunkan kredibilitas pemerintah daerah.

Oleh karena itu:

a. ASN diharapkan **memisahkan akun pribadi dan akun kedinasan** dengan jelas.
b. Gunakan logo, nama instansi, dan pernyataan publik hanya di kanal resmi.
c. Hindari membahas hal yang sensitif atau belum terverifikasi di media sosial pribadi.

Dengan langkah-langkah sederhana ini, reputasi ASN dan kepercayaan publik terhadap pemerintah dapat lebih terjaga.

3. Tantangan Etika dan Privasi di Kalangan Masyarakat

Di sisi masyarakat, ancaman terbesar bukan hanya *hoaks* atau *penipuan daring*, tetapi juga **kurangnya kesadaran terhadap batas privasi digital.** Banyak pengguna tanpa sadar membagikan terlalu banyak informasi pribadi di media sosial mulai dari tanggal lahir, alamat rumah, hingga aktivitas harian. Informasi sederhana seperti ini bisa menjadi pintu masuk bagi pelaku kejahatan digital.

📱 *Contoh nyata:*

Penjahat siber dapat memanfaatkan foto liburan seseorang untuk mengetahui bahwa rumahnya kosong, atau menggunakan data pribadi untuk mendaftar akun pinjaman online.

Masyarakat juga sering menjadi sasaran **penipuan sosial (social scam)** dengan iming-iming hadiah, pekerjaan, atau bantuan pemerintah yang palsu. Kelemahan ini menunjukkan bahwa **keamanan siber bukan hanya soal teknologi, tetapi juga soal perilaku dan kewaspadaan.**

4. Dinamika di Kabupaten Klungkung dan Pemerintahan Daerah

Dalam konteks lokal seperti **Kabupaten Klungkung**, media sosial memainkan peran penting dalam pelayanan publik, promosi wisata, dan komunikasi kebijakan daerah. Namun, tingginya keterbukaan informasi juga memperbesar risiko penyebaran *hoaks* lokal, penyalahgunaan logo pemerintah, dan peretasan akun resmi.

BSSN bersama pemerintah daerah telah mengembangkan **program literasi siber daerah** dan **pembentukan CSIRT Klungkung**, yang salah satu tugasnya adalah **memantau ancaman di media sosial yang berpotensi mengganggu keamanan digital daerah.**

Untuk itu:

a. ASN perlu memahami **batasan konten kedinasan dan pribadi**.
b. Masyarakat perlu dilatih untuk **membedakan akun resmi dan palsu.**
c. Pemerintah daerah harus menegakkan **prosedur verifikasi konten publik digital** agar tidak menjadi sasaran manipulasi.

5. Mengapa Ancaman Media Sosial Berbeda dengan Ancaman Siber Lain

Ancaman pada media sosial bersifat **psikologis dan sosial**, bukan teknis. Kalau *malware* menyerang perangkat, dan *phishing* menyerang data, maka **ancaman media sosial menyerang kepercayaan**.

🧩 Perbedaannya terletak pada:

Jenis Ancaman	Sasaran Utama	Dampak Akhir
Phishing	Data pribadi dan akses akun	Kehilangan data atau uang
Malware	Perangkat dan sistem	Gangguan operasional
Kebocoran Data	Basis data instansi	Hilangnya privasi dan kepercayaan
Media Sosial	Opini publik dan perilaku pengguna	Manipulasi informasi, kerusuhan digital

Karena itulah, subtopik ini tidak membahas aspek teknis, tetapi menyoroti **bagaimana perilaku digital dan etika komunikasi online dapat menjadi pertahanan utama.** Ancaman di media sosial bukan lagi sekadar soal "akun diretas" atau "*hoaks* tersebar".

Di tahun 2025, ancaman ini telah berkembang menjadi **strategi digital yang mampu mengguncang kepercayaan masyarakat terhadap lembaga publik.** Baik ASN maupun masyarakat harus memiliki kesadaran baru bahwa menjaga keamanan digital bukan hanya dengan perangkat lunak, tetapi dengan **karakter, integritas, dan kehati-hatian dalam berinteraksi di dunia maya.**

B. Jenis Ancaman Media Sosial Tahun 2025

Media sosial pada tahun 2025 tidak lagi hanya menjadi tempat berbagi informasi dan hiburan, melainkan telah berubah menjadi ruang strategis yang rawan disalahgunakan. Berbagai bentuk ancaman kini semakin kompleks karena memadukan teknologi, psikologi, dan komunikasi massa. Berikut ini beberapa jenis ancaman utama yang perlu dipahami oleh ASN dan masyarakat.

1. Akun Palsu Mengatasnamakan Pemerintah atau Tokoh Publik (Fake Government Account)

Ancaman ini menjadi yang paling sering terjadi di daerah. Pelaku membuat akun palsu menyerupai instansi pemerintah atau pejabat publik dengan tujuan menipu masyarakat.

Ciri-ciri akun palsu:

a. Menggunakan logo instansi tanpa izin.
b. Nama akun mirip akun resmi, tapi sedikit dimodifikasi (misalnya, @DinasSosialKlungkung_ atau @Pemda.Klungkungn).
c. Mengirim pesan pribadi yang meminta data pribadi, donasi, atau pembayaran.

📌 *Contoh kasus:*

Pada akhir tahun 2024, muncul akun palsu “Bantuan UMKM Klungkung 2024” yang menipu warga dengan meminta biaya administrasi Rp50.000. Kasus ini berhasil diungkap setelah beberapa korban melapor ke daerah.

Dampak:

a. Hilangnya kepercayaan masyarakat terhadap kanal resmi pemerintah.

b. Reputasi ASN ikut tercoreng karena publik sulit membedakan akun asli dan palsu.

Langkah pencegahan:

a. ASN wajib menggunakan akun yang diverifikasi atau dikelola resmi oleh instansi.
b. Masyarakat perlu mengecek akun pemerintah di situs atau kanal resmi (misalnya, laman web pemda atau tautan Linktree resmi).

2. Manipulasi Citra dan Deepfake

Teknologi ***deepfake*** kini menjadi salah satu ancaman serius di media sosial. Pelaku dapat memalsukan wajah atau suara seseorang menggunakan kecerdasan buatan (AI) untuk membuat video atau rekaman palsu.

🧠 *Contoh:*

Video yang tampak seperti seorang pejabat daerah mengumumkan "bantuan tunai" atau "perubahan kebijakan", padahal konten tersebut sepenuhnya buatan AI. Masyarakat yang tidak berhati-hati dapat langsung mempercayai dan menyebarkannya, memicu kepanikan atau kesalahpahaman.

Dampak:

a. Gangguan kepercayaan publik terhadap institusi resmi.
b. Potensi penyalahgunaan video palsu untuk pemerasan atau pembunuhan karakter.

Langkah pencegahan:

a. ASN dan masyarakat harus membiasakan diri **memverifikasi sumber video** sebelum membagikannya.
b. Gunakan situs pendeteksi konten AI seperti *Deepware Scanner* atau *InVID*.

3. Penipuan Investasi dan Donasi Palsu (Social Scam)

Media sosial sering digunakan untuk menyebarkan **penawaran investasi bodong**, **donasi palsu**, atau **undian berhadiah**. Penipu memanfaatkan kepercayaan dan rasa empati masyarakat, terutama ketika terjadi bencana atau isu sosial besar.

🧮 *Contoh:*

Setelah bencana alam di Bali pada awal 2025, banyak akun palsu yang membuka "donasi kemanusiaan" dengan nomor rekening pribadi. Masyarakat yang tergerak hati menyalurkan bantuan tanpa sadar menjadi korban penipuan.

Dampak:

a. Kerugian finansial masyarakat.
b. Meningkatnya ketidakpercayaan terhadap gerakan sosial yang sebenarnya sah.

Langkah pencegahan:

a. Pastikan informasi donasi berasal dari lembaga resmi dengan rekening atas nama institusi, bukan pribadi.
b. ASN diimbau membantu meluruskan informasi dengan membagikan kanal bantuan yang benar.

4. Penyebaran Hoaks dan Disinformasi

Hoaks (berita bohong) dan disinformasi masih menjadi ancaman klasik yang sulit dihapus. Namun di tahun 2025, penyebaran *hoaks* menjadi lebih terstruktur karena memanfaatkan algoritma platform untuk mempercepat jangkauan.

📊 *Tren terbaru:*

BSSN mencatat bahwa **1 dari 4 *hoaks* yang viral di Indonesia** berasal dari manipulasi konten di media sosial, termasuk potongan video, gambar tanpa konteks, dan pernyataan palsu mengatasnamakan pejabat daerah.

Dampak:

a. Gangguan stabilitas sosial di daerah.
b. Turunnya kredibilitas pemerintah jika tidak segera diklarifikasi.

Langkah pencegahan:

a. ASN harus berhati-hati membagikan konten yang belum jelas sumbernya.
b. Gunakan platform verifikasi seperti *turnbackhoax.id* atau *kominfo.go.id/cekhoaks*.

5. Penyalahgunaan Data Pribadi dan Foto Pribadi

Media sosial sering dimanfaatkan untuk mencuri data pribadi yang secara tidak sengaja dibagikan oleh pengguna. Contoh paling umum adalah penggunaan **foto pribadi**, **alamat**, atau **nomor telepon** untuk pembuatan akun palsu atau tindak penipuan.

📌 *Contoh:*

Kasus penyalahgunaan foto ASN perempuan untuk membuat akun kencan palsu di media sosial yang kemudian digunakan untuk menipu korban lain.

Dampak:

a. Tekanan psikologis dan sosial.
b. Kerusakan reputasi pribadi dan lembaga.

Langkah pencegahan:

a. Gunakan pengaturan privasi ketat di akun media sosial.
b. Hindari membagikan foto kartu identitas, dokumen, atau anak di bawah umur secara publik.

6. Ujaran Kebencian dan Polarisasi Digital

Ancaman lain yang meningkat adalah **penyebaran ujaran kebencian dan perpecahan digital**. Isu agama, politik, dan etnis sering dimanfaatkan untuk memicu emosi publik di kolom komentar atau grup daring. Polarisasi ini berdampak langsung pada **kerukunan sosial dan citra ASN** yang harus netral secara politik.

Langkah pencegahan:

a. ASN wajib menjaga netralitas dan etika dalam berkomentar di media sosial.
b. Masyarakat diimbau tidak terpancing emosi dan segera melapor jika menemukan ujaran kebencian.

7. Serangan Psikologis (Cyber Harassment & Hate Raid)

Fenomena **perundungan digital** (cyber harassment) kini semakin meluas. Pelaku bisa saja individu anonim atau kelompok yang sengaja menyerang seseorang dengan hinaan, fitnah, atau pelecehan daring.

💬 *Contoh:*

Kasus ASN perempuan yang menjadi korban serangan komentar seksis setelah video sosialisasi programnya tersebar. Fenomena seperti ini menimbulkan tekanan mental dan membuat korban takut aktif di ruang digital.

Langkah pencegahan:

a. Gunakan fitur blokir dan laporkan akun pelaku.
b. ASN sebaiknya berkoordinasi dengan Humas instansi atau tim CSIRT jika mendapat serangan daring.

Ancaman di media sosial tahun 2025 tidak lagi bersifat sederhana. Pelaku kini menggabungkan teknologi kecerdasan buatan, rekayasa sosial, dan manipulasi informasi untuk menyerang reputasi, data, dan psikologis korban. Kesadaran individu menjadi benteng utama karena **tidak ada sistem keamanan yang lebih kuat dari kewaspadaan penggunanya.**

C. Dampak Sosial dan Psikologis Akibat Ancaman Media Sosial

Ancaman di media sosial tidak hanya berdampak pada data atau akun digital, tetapi juga **menyentuh sisi psikologis dan sosial** penggunanya. Di era digital yang serba cepat, satu unggahan bisa menyebar luas dalam hitungan detik. Jika unggahan itu bersifat salah, manipulatif, atau menyerang seseorang, dampaknya bisa sangat besar tidak hanya bagi individu, tetapi juga bagi instansi dan masyarakat luas. Berikut ini beberapa dampak utama yang perlu dipahami oleh ASN dan masyarakat.

1. Menurunnya Kepercayaan Publik terhadap Pemerintah

Salah satu dampak paling nyata dari ancaman di media sosial adalah **terganggunya kepercayaan masyarakat terhadap lembaga pemerintah**. *Hoaks*, akun palsu, dan video manipulatif (*deepfake*) yang meniru pejabat daerah dapat menimbulkan kesalahpahaman publik.

📌 *Contoh:*

Jika beredar unggahan palsu seolah-olah dari akun resmi dinas yang menyampaikan informasi bantuan fiktif, masyarakat akan kecewa dan menilai pemerintah tidak profesional. Akibatnya, meski sudah diklarifikasi, sebagian warga tetap sulit percaya pada kanal resmi.

➡️ *Dampak lanjutan:*

Turunnya tingkat partisipasi masyarakat dalam layanan digital pemerintah dan meningkatnya keraguan terhadap kebijakan publik.

2. Tekanan Psikologis bagi ASN dan Pengguna Aktif

ASN yang aktif di media sosial sering menghadapi tekanan tersendiri. Unggahan yang bermaksud baik misalnya sosialisasi kebijakan, bisa saja disalahartikan, diserang komentar negatif, atau dijadikan bahan ejekan.

⚠️ *Dampak umum yang sering terjadi:*

a. **Stres digital (digital stress)** akibat serangan komentar negatif atau fitnah daring.
b. **Kecemasan sosial** karena takut berinteraksi di ruang publik digital.
c. **Penurunan produktivitas kerja**, terutama bagi ASN yang bertugas di bidang komunikasi publik.

Fenomena ini menunjukkan bahwa keamanan siber tidak hanya soal melindungi data, tetapi juga **melindungi kesehatan mental pengguna digital.**

3. Perpecahan Sosial dan Polarisasi di Dunia Maya

Ancaman di media sosial sering memecah belah masyarakat. Isu politik, agama, atau suku dapat dimanfaatkan oleh pihak tertentu untuk menciptakan *polarization* atau perpecahan opini di ruang publik digital. Masyarakat tanpa disadari terbawa arus komentar yang memicu permusuhan.

📱 *Contoh nyata:*

Ketika unggahan anonim memicu perdebatan antara kelompok warga di kolom komentar, kemudian berlanjut menjadi ketegangan di lingkungan nyata.

➡️ *Dampak sosial:*

Menurunnya toleransi digital, meningkatnya ujaran kebencian, dan terganggunya kerukunan sosial di tingkat lokal.

4. Hilangnya Privasi dan Keamanan Pribadi

Privasi adalah fondasi dari rasa aman di dunia digital. Namun di media sosial, banyak orang tidak menyadari bahwa mereka telah membuka terlalu banyak informasi pribadi seperti lokasi rumah, jadwal kegiatan, atau data keluarga. Ketika informasi ini jatuh ke tangan yang salah, bisa digunakan untuk tindak kriminal.

📌 *Kasus yang sering terjadi:*

Penjahat digital memanfaatkan unggahan seseorang yang sedang bepergian untuk melakukan perampokan di rumah kosong. Ada pula kasus pelecehan daring yang dimulai dari pembocoran foto pribadi.

➡️ *Dampak jangka panjang:*

Rasa tidak aman, trauma digital, dan ketakutan untuk kembali aktif di media sosial.

5. Rusaknya Reputasi Digital ASN dan Lembaga Pemerintah

Setiap ASN adalah wajah dari instansinya, termasuk di ruang digital. Satu komentar yang tidak pantas, unggahan tanpa verifikasi, atau tanggapan emosional terhadap isu publik dapat langsung beredar luas dan berdampak pada reputasi lembaga.

💬 *Contoh:*

Seorang ASN di daerah menulis pendapat pribadi yang dianggap berpihak secara politik. Unggahan itu disebarkan ulang oleh media daring dan menimbulkan anggapan bahwa instansi terkait tidak netral. Padahal, itu dilakukan di akun pribadi.

➡️ *Pelajaran penting:*

ASN perlu memahami bahwa **etika digital** bukan sekadar aturan, tetapi juga cerminan integritas dan profesionalisme.

6. Kelelahan Informasi (Information Fatigue)

Di era media sosial yang serba cepat, pengguna sering kewalahan dengan banjir informasi. Banyaknya konten palsu, berita sensasional, dan pesan berantai membuat masyarakat kesulitan membedakan mana informasi benar, mana yang salah.

Akibatnya:

a. Pengguna menjadi mudah lelah secara mental.
b. Cenderung acuh terhadap peringatan resmi pemerintah.
c. Enggan membaca klarifikasi atau edukasi digital.

7. Efek Domino terhadap Ekosistem Digital Daerah

Kebocoran kepercayaan publik di media sosial dapat mempengaruhi **ekosistem digital daerah** secara keseluruhan. Ketika warga kehilangan rasa aman untuk berinteraksi online, partisipasi dalam program digital pemerintah daerah (seperti aplikasi pengaduan publik, layanan administrasi online, dan *e-participation*) ikut menurun.

Bagi daerah seperti Klungkung yang sedang memperkuat tata kelola digital, hal ini dapat menjadi hambatan serius bagi kemajuan pemerintahan berbasis elektronik.

D. Strategi Aman dan Etis Menggunakan Media Sosial bagi ASN dan Masyarakat

Di era digital yang serba cepat, **keamanan media sosial tidak hanya soal menghindari serangan siber**, tetapi juga tentang bagaimana setiap individu menjaga **integritas, tanggung jawab, dan etika digitalnya.** ASN dan masyarakat perlu memahami bahwa keamanan digital tidak tercipta dari teknologi saja, tetapi dari **kebiasaan dan perilaku pengguna.** Berikut strategi yang dapat diterapkan oleh ASN dan masyarakat untuk menggunakan media sosial secara **aman, bijak, dan bertanggung jawab.**

1. Gunakan Media Sosial Sesuai Peran dan Kebutuhan

Media sosial memiliki fungsi yang berbeda bagi setiap orang:

a. **ASN** menggunakan media sosial sebagai sarana komunikasi publik, sosialisasi kebijakan, dan layanan masyarakat.

b. **Masyarakat** memanfaatkannya untuk berinteraksi, mencari informasi, dan membangun jejaring sosial.

Karena itu, **setiap pengguna harus menyesuaikan gaya berkomunikasi dan batasan informasi yang dibagikan.**

Contoh Praktik Baik:

a. ASN menggunakan akun resmi instansi untuk menyampaikan informasi layanan, bukan untuk pendapat pribadi.
b. Masyarakat menggunakan akun pribadi untuk menyampaikan aspirasi secara sopan dan konstruktif, bukan menyerang.

2. Lindungi Akun dengan Keamanan Berlapis

Berdasarkan laporan BSSN tahun 2025, **lebih dari 60% serangan siber di media sosial berasal dari lemahnya keamanan akun pengguna.** Langkah-langkah sederhana berikut bisa sangat membantu:

a. Aktifkan **verifikasi dua langkah (*Two-Factor Authentication*)** di setiap akun.
b. Gunakan **kata sandi kuat** dan jangan gunakan ulang di platform lain.
c. Hindari membuka tautan mencurigakan dari pesan pribadi atau komentar.
d. Jangan bagikan data pribadi (seperti NIK, alamat, atau nomor telepon) di ruang publik digital.

Ingat: Keamanan digital dimulai dari langkah paling kecil dari kata sandi hingga cara berbagi informasi.

3. Bedakan Antara Akun Pribadi dan Akun Kedinasan

ASN memiliki tanggung jawab moral dan etik dalam menggunakan media sosial. Untuk mencegah kesalahpahaman publik:

a. Gunakan akun kedinasan **hanya untuk urusan resmi**, dan kelola sesuai standar komunikasi instansi.
b. Hindari membahas isu politik, SARA, atau topik sensitif di akun pribadi yang bisa dikaitkan dengan instansi.

c. Bila membuat konten pribadi, sertakan penegasan seperti “Pendapat ini bersifat pribadi, bukan representasi instansi.”

🏛️ *Tujuannya:* menjaga profesionalisme ASN dan kepercayaan publik terhadap pemerintah daerah.

4. Pahami Etika Digital (Digital Etiquette)

Etika digital mencakup **cara berkomunikasi, menghormati privasi orang lain, dan menjaga sopan santun di ruang daring.**

Prinsip 5 “S” etika digital yang bisa diterapkan ASN dan masyarakat:

1. **Santun**: Gunakan bahasa yang sopan, tidak kasar, dan tidak menyinggung SARA.
2. **Saring**: Verifikasi sebelum membagikan informasi atau tautan.
3. **Smart**: Gunakan media sosial untuk hal produktif, bukan konflik.
4. **Sigap**: Hapus atau laporkan konten berbahaya, jangan ikut menyebarkan.
5. **Selamatkan Data**: Lindungi data pribadi dari penyalahgunaan.

📱 *Penerapan sederhana:* Sebelum menulis komentar, tanya diri sendiri: “Apakah ini akan membantu, menyakiti, atau mempermalukan orang lain?”

5. Bangun Reputasi Digital yang Positif

Baik ASN maupun masyarakat perlu menyadari bahwa **jejak digital bersifat permanen.** Setiap unggahan, foto, komentar, atau *like* dapat ditelusuri dan berpotensi membentuk persepsi publik tentang karakter seseorang atau lembaga.

🧠 *Langkah praktis membangun reputasi digital:*

a. Gunakan media sosial untuk membagikan hal positif seperti prestasi kerja, kegiatan sosial, atau inovasi layanan.
b. Hindari perdebatan yang tidak produktif di kolom komentar.
c. Respon kritik publik dengan tenang dan berdasarkan fakta.

🌿 *Ingat:* Di dunia digital, kepercayaan dibangun bukan dengan banyaknya pengikut, tapi dengan **konsistensi integritas.**

6. Bijak dalam Berbagi Informasi dan Foto

Banyak kasus penyalahgunaan data berawal dari **unggahan yang tampak sepele**. Foto di kantor dengan dokumen terbuka, atau status yang menampilkan lokasi pribadi, bisa menjadi celah keamanan.

💡 *Tips praktis:*

a. Pastikan latar belakang foto tidak menampilkan informasi sensitif (surat, layar komputer, dokumen).
b. Jangan unggah identitas diri seperti KTP, kartu pegawai, atau tiket perjalanan.
c. Hindari *tag location* saat berada di tempat pribadi.

7. Jadilah Teladan Digital (Digital Role Model)

ASN dan masyarakat sama-sama memiliki peran penting dalam membangun budaya digital yang aman dan sehat. Dengan menjadi contoh yang baik, kita bisa memengaruhi lingkungan sekitar untuk lebih berhati-hati di dunia maya.

🏅 *Peran ASN:*

a. Menjadi sumber informasi resmi dan terpercaya.
b. Memberikan edukasi sederhana kepada warga tentang keamanan digital.

🤝 *Peran Masyarakat:*

a. Tidak mudah percaya pada unggahan yang viral tanpa verifikasi.
b. Melaporkan konten berbahaya atau akun palsu kepada pihak berwenang.

8. Gunakan Kanal Resmi Pemerintah untuk Klarifikasi dan Pengaduan

Apabila menemukan akun mencurigakan atau hoaks yang menyerang instansi pemerintah, segera:

a. Laporkan melalui kanal resmi **CSIRT Klungkung** atau **BSSN Indonesia**.
b. Jangan membalas unggahan palsu, karena dapat memperluas jangkauannya.
c. Simpan bukti tangkapan layar (screenshot) untuk pelaporan resmi.

E. Studi Kasus Nyata

1. Kasus Akun Palsu Mengatasnamakan Instansi Pemerintah Daerah (2024)

Pada akhir tahun 2024, terjadi kasus pembuatan akun Instagram palsu yang mengaku sebagai “Dinas Sosial Kabupaten Klungkung”. Akun tersebut membagikan tautan palsu program “Bantuan Tunai Digital” dan meminta data pribadi serta biaya pendaftaran.

📉 **Dampak:** Sebagian warga menjadi korban penipuan dan kepercayaan terhadap instansi menurun.

2. Kasus Penyebaran Video Deepfake Pejabat Publik (2025)

Pada Maret 2025, beredar video di platform TikTok yang menampilkan seorang pejabat daerah mengumumkan kebijakan fiktif tentang kenaikan pajak. Video tersebut ternyata hasil rekayasa AI (*deepfake*) yang dibuat untuk menimbulkan ketidakpercayaan masyarakat.

📉 **Dampak:** Terjadi perdebatan publik dan serangan komentar ke akun resmi pemerintah.

3. Kasus Perundungan Digital Terhadap ASN (2024)

Seorang ASN perempuan yang aktif mempromosikan program layanan publik melalui media sosial mengalami *cyber harassment* setelah videonya viral. Komentar seksis dan fitnah menyebar di berbagai platform.

📉 **Dampak:** Tekanan psikologis dan gangguan produktivitas kerja.

4. Kasus Hoaks Bantuan Sosial Nasional (2025)

Hoaks yang mengaku sebagai program “Bantuan Langsung Tunai BSSN” beredar di grup WhatsApp dan Facebook lokal. Pesan tersebut mengandung tautan berbahaya yang mengumpulkan data pribadi pengguna.

📉 **Dampak:** Kebocoran data warga dan peningkatan laporan penipuan ke CSIRT.

F. Penutup

Media sosial adalah ruang terbuka yang penuh peluang sekaligus risiko. Ia bisa menjadi **alat komunikasi publik yang efektif**, namun juga **pintu masuk ancaman digital** jika tidak dikelola dengan hati-hati. Bagi ASN, media sosial adalah perpanjangan tangan lembaga tempat di mana profesionalisme, integritas, dan etika tercermin. Bagi masyarakat, media sosial adalah wadah interaksi sosial yang harus dijaga agar tetap sehat dan aman.

Pada tahun 2025, ancaman seperti **akun palsu pemerintah, video *deepfake*, penyebaran hoaks, hingga ujaran kebencian** terus berkembang dengan teknologi yang semakin canggih. Namun, langkah pencegahannya tidak selalu rumit. Kesadaran, kehati-hatian, dan sikap bertanggung jawab dalam berinteraksi menjadi benteng paling kuat.

Dengan memahami materi ini, diharapkan setiap ASN dan masyarakat dapat:

a. Menjadi pengguna media sosial yang **cerdas, beretika, dan waspada.**
b. Mendorong terciptanya **lingkungan digital yang sehat dan terpercaya.**
c. Berperan aktif dalam **mencegah penyebaran hoaks dan menjaga citra positif daerah.**

Keamanan media sosial tidak hanya tentang “jangan diretas”, tetapi juga tentang bagaimana kita semua menjaga **kepercayaan digital**, kepercayaan antara warga dan pemerintah, antara pengguna dan platform, antara dunia nyata dan dunia maya.

Pertanyaan Reflektif

1. Sebagai ASN atau masyarakat, seberapa sering Anda menggunakan media sosial untuk urusan pekerjaan atau komunikasi publik? Apakah Anda merasa aman saat melakukannya?
2. Apa langkah pertama yang bisa Anda lakukan untuk memperkuat keamanan akun media sosial pribadi Anda?
3. Pernahkah Anda membagikan informasi dari media sosial tanpa memeriksa kebenarannya? Bagaimana perasaan Anda setelah tahu ada risiko di baliknya?
4. Menurut Anda, apakah etika digital seharusnya menjadi bagian dari pembinaan ASN secara formal? Mengapa hal ini penting atau tidak penting?
5. Bagaimana Anda bisa membantu orang di sekitar (keluarga, teman, rekan kerja) agar lebih bijak dan aman menggunakan media sosial?
6. Jika suatu hari Anda menemukan akun palsu yang menggunakan nama instansi atau pejabat daerah, apa langkah konkret yang sebaiknya dilakukan?
7. Bagaimana peran kolaborasi antara ASN, masyarakat, dan pemerintah daerah bisa memperkuat keamanan ruang digital Klungkung?

DAFTAR PUSTAKA

Akhtar, H. (2020). Perilaku Oversharing di Media Sosial: Ancaman atau Peluang? *Psikologika : Jurnal Pemikiran Dan Penelitian Psikologi*, *25*(2), 257–270. https://doi.org/10.20885/psikologika.vol25.iss2.art7

Ardy, L. A. F., Istiqomah, I., Ezer, A. E., & Neyman, S. N. (2024). Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial. *Journal of Internet and Software Engineering*, *1*(4), 11. https://doi.org/10.47134/pjise.v1i4.2753

Aris Sarjito. (2024). Hoaks, Disinformasi, dan Ketahanan Nasional: Ancaman Teknologi Informasi dalam Masyarakat Digital Indonesia. *Journal of Governance and Local Politics*, *5*(2), 175–186.

Dr. Hj. Mudji Estiningsih, S.H, M. H. (2023). Indonesia Cakap Digital Melalui Kegiatan Literasi Digital Bagi Seluruh Aparatur Sipil Negara (Asn). *J-MAS: Jurnal Pengabdian Masyarakat*, *1*(5), 695–704. https://melatijournal.com/index.php/jmas/article/view/277

Halawa, L. J., Hulu, P. H., & Halawa, O. Z. (2025). Generasi Bijak Bermedia Sosial. *Jurnal Pengabdian Masyarakat Dan Riset Pendidikan*, *4*(1), 830–833. https://doi.org/10.31004/jerkin.v4i1.1655

Megiati, Y. E., Komari Pratiwi, N., Nurdiansyah, D., Yusuf, S., & Fauzi, T. R. (2024). Kapas : Kumpulan Artikel Pengabdian Masyarakat Bijak Bermedia Sosial sebagai Bentuk Pemanfaatan Internet Sehat. *Kapas : Kumpulan Artikel Pengabdian Masyarakat*, *2*(3), 332–340.

Nisa, A. Z. K., Febryantyo, B. N., & Nupus, H. (2025). Penyuluhan Bijak Bermedia Sosial : Cerdas , Aman , dan Bertanggung Jawab. *Aksi Kita Jurnal Pengabdian Masyarakat*, *1*(5), 1472–1477. https://doi.org/10.63822/dxhd6606

Putri, A. . P. D. T., I Kadek Puriartha, S.Sn., M. S., & I Nyoman Payuyasa, S.Pd., M. P. (2025). Penciptaan iklan layanan masyarakat dengan tema bijak bermedia sosial. *JURNAL CALACCITRA*, *05*(01), 33–41.

Rahayu, B. A., Wijaya, N. H., Maulana, N., Maria, D. Y., Yulina, R., & Lani, A. (2025). KESEHATAN MENTAL DAN KEHIDUPAN SOSIAL. *MARTABE : Jurnal Pengabdian Masyarakat*, *8*(8), 3292–3297. https://doi.org/10.31604/jpm.v8i8.3292-3297

Ridho Ramadhan Arfi, & Elly Nielwaty. (2024). Implementasi UU ITE dalam Meningkatkan Literasi Digital Etika Bermedia Sosial Oleh Dinas Komunikasi Informatika Statistik dan Persandian Kota Pekanbaru. *Sosial Dan Humaniora*, *01*(02), 108.

Suriadi, H. (2025). Krisis Kepercayaan Masyarakat terhadap Lembaga Publik di Era Disinformasi Digital. *Journal of Social, Educational and Religious Studies*, *1*(1), 38–52.

Yopita Desriana Butar. (2024). Analisis Penyebaran Hoax Di Media Sosial Dan Dampaknya Terhadap Masyarakat Masyarakat Indonesia Anti Fitnah , Septiaji Eko Nugroho menjelaskan bahwa hoax adalah sebuah informasi yang direkayasa . Informasi tersebut dibuat untuk menutup – nutupi fakta . Ah. *Jurnal Pendidikan, Bahasa Dan Budaya*, *3*(2), 252–258. https://doi.org/10.55606/jpbb.v3i2.3201