KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 2: Ancaman Siber yang Sering Terjadi

Subtopik 2.5: Social Engineering

SOCENG
Social Engineering

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. Di era digital yang semakin kompleks, serangan siber tidak selalu datang dari virus atau peretasan sistem, tetapi juga dari manipulasi psikologis manusia yang dikenal dengan istilah rekayasa sosial (social engineering)**.**

Subtopik ini membahas bagaimana penyerang memanfaatkan kepercayaan, ketidaktelitian, atau rasa takut seseorang untuk mendapatkan akses terhadap informasi atau sistem yang seharusnya dilindungi. Melalui pemahaman ini, diharapkan ASN dan masyarakat mampu mengenali pola penipuan yang semakin halus serta mengembangkan kewaspadaan dalam berinteraksi di dunia digital. Semoga materi ini dapat menjadi panduan praktis dalam memperkuat kesadaran keamanan siber di lingkungan pemerintahan maupun masyarakat Kabupaten Klungkung. 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 pengertian dan bentuk-bentuk rekayasa sosial di era digital.
2. Mengidentifikasi ciri dan tahapan serangan berbasis manipulasi psikologis.
3. Menyebutkan contoh kasus nyata di lingkungan masyarakat dan pemerintahan daerah.
4. Menentukan langkah pencegahan dan respons yang tepat terhadap serangan rekayasa sosial.
5. Mengembangkan budaya waspada dan tanggung jawab dalam menjaga informasi pribadi maupun data instansi.

Sasaran Peserta

1. ASN: agar memahami bagaimana rekayasa sosial bisa mengancam keamanan sistem pemerintah, dan mampu melindungi akses instansi dari ancaman berbasis manipulasi manusia.
2. Masyarakat: agar lebih berhati-hati terhadap taktik penipuan digital yang memanfaatkan kepercayaan, emosi, atau rasa takut, serta mampu mengenali tanda-tanda rekayasa sosial dalam kehidupan sehari-hari.

A. Pendahuluan: Evolusi Ancaman Berbasis Manusia di Era Digital 2025

Di masa kini, perkembangan teknologi membuat batas antara dunia digital dan dunia nyata semakin tipis. Masyarakat semakin bergantung pada layanan digital, baik untuk komunikasi, transaksi, hingga pelayanan publik. Namun, seiring meningkatnya kenyamanan tersebut, muncul pula ancaman baru yang tidak hanya menyerang sistem, tetapi juga **menyerang manusia sebagai titik terlemah dalam rantai keamanan siber.** Jika dulu serangan siber identik dengan *virus komputer* atau *peretasan jaringan*, maka kini pelaku lebih sering **memanipulasi manusia** agar secara sukarela memberikan akses atau informasi penting. Strategi ini dikenal dengan istilah **rekayasa sosial (*social engineering*)** suatu bentuk kejahatan digital yang memanfaatkan rasa percaya, empati, atau kelengahan seseorang untuk tujuan jahat.

Menurut laporan **BSSN (2024)**, lebih dari **70% insiden keamanan data di instansi pemerintah daerah** terjadi bukan karena kelemahan sistem, melainkan karena kesalahan manusia. Pelaku kejahatan tidak perlu menembus sistem yang rumit jika cukup dengan **menipu pengguna** agar membuka jalan masuk. Mereka menciptakan pesan yang tampak meyakinkan, berpura-pura menjadi pihak berwenang, atau memanfaatkan rasa takut agar korban segera bertindak tanpa berpikir panjang.

Tahun 2025 menandai munculnya **gelombang baru rekayasa sosial berbasis kecerdasan buatan (*AI-driven social engineering*)**. Dengan teknologi seperti *deepfake* dan *voice cloning*, pelaku kini bisa meniru suara pimpinan instansi atau membuat video yang terlihat sangat nyata untuk memancing kepercayaan korban. Fenomena ini menjadikan masyarakat dan ASN harus semakin kritis dalam memverifikasi setiap informasi yang diterima secara daring.

Serangan berbasis manusia ini tidak hanya mengakibatkan kerugian pribadi seperti pencurian data atau uang, tetapi juga berpotensi mengguncang kepercayaan

publik terhadap lembaga pemerintahan. Ketika satu pegawai tertipu dan memberikan akses ke sistem, seluruh jaringan instansi bisa terdampak. Begitu pula di masyarakat, satu pesan palsu di grup WhatsApp keluarga dapat menyebar menjadi *hoaks* massal yang menimbulkan kepanikan.

Oleh karena itu, memahami rekayasa sosial tidak cukup hanya mengetahui bentuk-bentuknya, tetapi juga **menyadari bagaimana pikiran dan emosi manusia bisa dimanfaatkan** dalam dunia digital. Kesadaran inilah yang menjadi kunci untuk membangun pertahanan siber yang kokoh, berbasis manusia yang waspada dan cerdas digital.

B. Pengertian Rekayasa Sosial (Social Engineering)

Rekayasa sosial (social engineering) adalah **upaya memanipulasi psikologis seseorang agar secara sukarela memberikan informasi, akses, atau melakukan tindakan tertentu yang merugikan dirinya sendiri atau pihak lain.** Berbeda dengan serangan teknis seperti malware atau peretasan sistem, rekayasa sosial menargetkan **manusia sebagai pintu masuk utama**. Pelaku memanfaatkan **emosi, rasa percaya, rasa takut, atau ketidaktahuan korban** untuk mencapai tujuannya.

Dalam praktiknya, social engineering bukan hanya soal kejahatan siber yang terjadi secara daring, tetapi juga bisa dilakukan secara langsung, misalnya melalui telepon, tatap muka, atau surat elektronik yang tampak resmi. Pelaku biasanya menyamar menjadi figur yang dipercaya: pejabat, rekan kerja, pihak bank, atau penyedia layanan pemerintah.

1. Unsur Utama Rekayasa Sosial

Untuk memahami cara kerja serangan ini, penting mengenali beberapa unsur utamanya:

a. **Manipulasi Psikologis:** pelaku menggunakan emosi korban seperti panik, penasaran, atau takut agar segera bertindak tanpa berpikir panjang. Contoh: pesan “akun Anda akan diblokir dalam 1 jam, klik tautan berikut untuk

verifikasi".

b. **Penyamaran atau Peniruan Identitas:** pelaku meniru identitas pihak berwenang atau lembaga resmi. Misalnya, penipu mengaku dari "Tim IT Pemda Klungkung" untuk meminta kode OTP.
c. **Eksploitasi Kepercayaan:** pelaku menargetkan pihak yang mudah dipercaya seperti pegawai front office, admin media sosial, atau masyarakat yang belum paham keamanan data.
d. **Tujuan Akhir:** mendapatkan informasi sensitif seperti NIK, kata sandi, OTP, atau akses sistem pemerintahan.

2. Bentuk-bentuk Rekayasa Sosial yang Umum Terjadi

Beberapa teknik rekayasa sosial yang sering ditemukan di Indonesia antara lain:

a. **Pretexting:** pelaku membuat skenario palsu untuk memperoleh informasi. Misalnya, berpura-pura sebagai petugas BSSN atau bank yang meminta konfirmasi data.
b. **Baiting:** pelaku menawarkan sesuatu yang menarik agar korban mau mengklik atau membuka file berbahaya. Contoh: file "daftar penerima bantuan Klungkung 2025.pdf.exe".
c. **Impersonation:** pelaku berpura-pura menjadi seseorang yang dikenal korban. Contoh: akun palsu mengatasnamakan atasan ASN meminta data pegawai.
d. **Scareware:** pelaku menakut-nakuti korban dengan pesan ancaman. Misalnya, "sistem Anda terinfeksi virus, segera unduh aplikasi antivirus ini!".
e. **Quid Pro Quo:** pelaku menawarkan bantuan atau hadiah dengan imbalan data. Contoh: "isi survei ini dan dapatkan pulsa gratis", padahal data dikumpulkan untuk tujuan lain.

3. Mengapa Rekayasa Sosial Berbahaya

Ancaman ini berbahaya karena sulit dideteksi oleh sistem keamanan otomatis. Tidak ada antivirus yang bisa mencegah manusia dari **kecerobohan digital.** Dalam konteks pemerintahan, satu kesalahan kecil dari ASN dapat membuka celah bagi

kebocoran data besar. Di sisi masyarakat, satu klik pada tautan palsu bisa menguras tabungan dalam hitungan menit.

Selain itu, bentuk serangan ini **selalu beradaptasi dengan perkembangan teknologi dan budaya digital.** Tahun 2025, pelaku mulai menggunakan **AI (*Artificial Intelligence*)** untuk membuat pesan dan suara palsu yang meyakinkan (*deepfake scam*), membuat masyarakat semakin sulit membedakan antara yang asli dan manipulasi.

Karena itu, **kesadaran dan kewaspadaan manusia menjadi pertahanan pertama dan utama.** Tidak cukup hanya memasang sistem keamanan canggih; setiap individu harus memahami cara berpikir pelaku agar tidak menjadi korban.

C. Pola dan Tahapan Serangan Rekayasa Sosial

Rekayasa sosial bukanlah tindakan acak. Serangan ini **terencana, sistematis, dan mengikuti pola psikologis tertentu.** Pelaku mempelajari targetnya, memilih pendekatan yang sesuai, lalu melakukan manipulasi hingga korban bertindak sesuai kehendaknya.

Memahami tahapan ini penting agar ASN dan masyarakat dapat **mendeteksi ancaman lebih dini** sebelum terjadi kerugian nyata.

1. Tahap Riset (Reconnaissance)

Pelaku mulai dengan mengumpulkan informasi tentang calon korban. Untuk ASN, informasi bisa berasal dari **profil pegawai di situs instansi, postingan media sosial, atau berita lokal.** Untuk masyarakat, pelaku mungkin mencari **nomor ponsel, alamat email, atau kebiasaan belanja online.**

🔍 *Contoh:* Seorang penipu mencari daftar pegawai Kecamatan Klungkung di situs resmi, lalu menargetkan salah satu pegawai dengan pesan palsu dari “atasan”.

Pesan utama: jangan membagikan terlalu banyak informasi pribadi atau pekerjaan di internet, karena bisa menjadi bahan bagi pelaku.

2. Tahap Pendekatan (Engagement)

Setelah memiliki cukup data, pelaku mulai menjalin kontak dengan korban.

Biasanya dilakukan lewat **telepon, email, WhatsApp, atau media sosial.** Nada komunikasi dibuat ramah dan profesional agar korban tidak curiga.

💬 *Contoh:* Pelaku mengaku dari "Bagian Teknologi Informasi BSSN" dan menawarkan bantuan pembaruan sistem keamanan, padahal tujuannya mencuri data login ASN.

Pesan utama: pelaku selalu berusaha membuat kesan percaya dan mendesak agar korban tidak berpikir lama.

3. Tahap Manipulasi (Exploitation)

Di tahap ini, pelaku memanfaatkan **emosi korban.** Mereka bisa menggunakan rasa takut ("akun Anda akan diblokir"), rasa percaya ("kami dari tim pusat"), atau rasa ingin tahu ("Anda menerima bantuan dari Pemkab Klungkung"). Pelaku juga bisa membuat korban **melakukan tindakan kecil tapi berisiko besar**, seperti mengklik tautan, membuka file, atau memberikan kode OTP.

💣 *Contoh:* Pesan dari akun palsu "Dinas Dukcapil Klungkung" meminta masyarakat mengunggah KTP dan KK ke tautan tertentu dengan alasan verifikasi data.

Pesan utama: tidak ada lembaga resmi yang meminta data pribadi melalui pesan pribadi atau tautan tidak resmi.

4. Tahap Eksekusi (Execution)

Setelah berhasil memperoleh kepercayaan, pelaku melancarkan aksinya:

a. Mengambil alih akun (email, WhatsApp, sistem kerja ASN)
b. Mencuri data pribadi atau rahasia instansi
c. Menanam malware pada perangkat korban
d. Menyebarkan pesan palsu ke kontak lain untuk memperluas jangkauan serangan

🎯 *Contoh:* Setelah korban ASN tertipu dan memberikan akses ke akun kerja, pelaku menggunakan akun itu untuk mengirim pesan palsu ke seluruh pegawai seolah datang dari kepala dinas.

Pesan utama: serangan bisa menyebar dengan cepat karena pelaku menggunakan kepercayaan antarindividu sebagai senjata.

5. Tahap Pemeliharaan dan Pengulangan (Persistence)

Pelaku sering tidak langsung meninggalkan korban. Mereka **menyimpan akses jangka panjang** ke akun atau jaringan yang sudah diretas, agar bisa digunakan kembali di kemudian hari. Bisa jadi pelaku hanya menunggu waktu yang tepat untuk memanfaatkan data tersebut.

🦹 *Contoh:* Pelaku pernah mendapatkan salinan data pegawai dari flashdisk yang hilang. Beberapa bulan kemudian, data itu digunakan untuk membuat akun palsu dengan nama ASN tersebut.

Pesan utama: efek rekayasa sosial bisa berlangsung lama dan tidak selalu terlihat langsung.

D. Jenis-Jenis Rekayasa Sosial di Indonesia

Jenis-Jenis Rekayasa Sosial di Indonesia (Online & Offline)

Rekayasa sosial dapat dilakukan dengan berbagai cara, baik **melalui dunia maya (online)** maupun **secara langsung (offline).** Pelaku terus menyesuaikan pendekatannya dengan kebiasaan masyarakat dan teknologi yang digunakan. Berikut beberapa jenis rekayasa sosial yang paling sering ditemukan di Indonesia, termasuk di lingkungan pemerintahan daerah.

1. Phishing (Online Manipulation)

Phishing merupakan **bentuk paling umum dari rekayasa sosial digital.** Pelaku mengirim pesan palsu melalui email, WhatsApp, atau SMS yang tampak berasal dari sumber terpercaya, dengan tujuan **mencuri data pribadi atau akses akun.**

💬 *Contoh:* Pesan dari akun WhatsApp palsu “BSSN Indonesia” yang meminta ASN memverifikasi data login sistem pemerintahan daerah. Pesan seperti ini sering menggunakan logo resmi agar terlihat meyakinkan.

🟢 **Tanda-tanda Phishing:**

a. Domain atau alamat email mencurigakan (contoh: bssn-indonesia[dot]com).
b. Pesan mendesak untuk segera bertindak (“Data Anda akan dihapus dalam 2 jam”).

c. Tautan yang mengarah ke situs palsu.

2. Pretexting (Penipuan dengan Alasan Resmi)

Pelaku menciptakan **cerita atau skenario palsu (pretext)** untuk mendapatkan informasi atau akses. Biasanya, mereka menyamar sebagai pihak berwenang seperti pejabat pemerintah, petugas bank, atau vendor teknologi.

💼 *Contoh:* Penipu menghubungi ASN dengan mengaku sebagai "staf BPK" yang sedang melakukan audit mendadak, lalu meminta file keuangan lewat email pribadi.

🟢 **Cara Menghindari:**

a. Selalu verifikasi identitas pengirim sebelum membagikan dokumen.

b. Gunakan saluran komunikasi resmi, bukan nomor pribadi.

3. Baiting (Umpan Digital)

Pelaku menawarkan sesuatu yang menarik agar korban **secara sukarela mengunduh file berbahaya atau membagikan data pribadi.**

🎁 *Contoh:* Email berisi file "Daftar ASN Klungkung yang Naik Pangkat 2025" yang ternyata mengandung malware ketika dibuka.

🟢 **Pencegahan:**

a. Jangan membuka file dari sumber yang tidak dikenal.

b. Gunakan antivirus dan sistem proteksi dokumen resmi.

4. Quid Pro Quo (Imbalan Palsu)

Pelaku menawarkan bantuan teknis atau hadiah dengan imbalan data pribadi. Bentuknya sering seperti *survey palsu* atau *bantuan teknis online.*

🎯 *Contoh:* "Sampaikan keluhan layanan publik di sini dan dapatkan saldo e-wallet Rp50.000." Padahal form tersebut mencuri data kontak dan NIK masyarakat.

🟢 **Pencegahan:**

a. Abaikan tawaran yang terdengar terlalu menguntungkan.

b. Pastikan sumber resmi sebelum mengisi formulir online.

5. Impersonation (Penyamaran Identitas)

Pelaku berpura-pura menjadi seseorang yang dipercaya korban. Di instansi pemerintahan, ini bisa sangat berbahaya karena pelaku meniru nama pejabat atau kolega.

🦹 *Contoh:* Akun media sosial mengatasnamakan kepala dinas menghubungi staf untuk meminta OTP "demi update sistem."

🟢 **Pencegahan:**

a. Jangan pernah memberikan kode OTP atau kata sandi kepada siapa pun, bahkan jika mengaku dari instansi sendiri.
b. Verifikasi langsung lewat panggilan resmi.

6. Piggybacking & Tailgating (Offline Manipulation)

Meski terdengar "fisik", ini tetap bagian dari rekayasa sosial. Pelaku **memanfaatkan sopan santun atau kelengahan** untuk masuk ke area terbatas, misalnya kantor pemerintahan.

🏛️ *Contoh:* Seseorang berpura-pura menjadi teknisi dan ikut masuk ke ruang server bersama pegawai lain tanpa izin.

🟢 **Pencegahan:**

a. Jangan membiarkan orang asing masuk tanpa tanda pengenal dan izin resmi.
b. Gunakan sistem kontrol akses dengan kartu identitas pegawai.

7. Deepfake & Voice Cloning (Tren 2025)

Teknologi **kecerdasan buatan (AI)** kini dimanfaatkan untuk membuat **video atau suara palsu yang tampak nyata.** Pelaku bisa meniru wajah atau suara pejabat untuk mengarahkan korban melakukan tindakan tertentu.

🎥 *Contoh:* Video palsu "kepala daerah" yang menginstruksikan ASN melakukan transfer dana ke rekening proyek tertentu.

🟢 **Pencegahan:**

a. Periksa sumber asli video atau pesan.

b. Gunakan kanal komunikasi resmi sebelum menindaklanjuti perintah digital.

E. Dampak Rekayasa Sosial

Rekayasa sosial sering dianggap sebagai penipuan biasa, padahal dampaknya bisa jauh lebih luas dari sekadar kehilangan uang atau akun. Serangan ini **tidak hanya menyerang individu, tetapi juga dapat mengguncang kepercayaan publik terhadap sistem pemerintahan dan keamanan digital negara.**

1. Dampak bagi ASN (Aparatur Sipil Negara)

ASN merupakan salah satu target utama pelaku rekayasa sosial karena mereka memiliki **akses langsung ke data dan sistem pemerintahan.** Sekali seorang ASN tertipu, pelaku bisa masuk ke jaringan internal dan memanfaatkan akses tersebut untuk tujuan lebih besar.

📄 **Dampak yang sering terjadi antara lain:**

a. **Kebocoran Data Instansi:** Informasi sensitif seperti data penduduk, keuangan, atau dokumen internal bocor ke pihak tidak berwenang.
b. **Kerusakan Reputasi Lembaga:** Masyarakat kehilangan kepercayaan terhadap instansi yang lalai menjaga keamanan data.
c. **Gangguan Operasional:** Sistem pelayanan publik bisa terganggu karena akses dikunci atau disusupi.
d. **Sanksi Disiplin:** ASN yang lalai dapat dikenai teguran hingga tindakan hukum, terutama jika pelanggaran mengakibatkan kebocoran data.

📍 *Contoh nyata:*

Tahun 2024, beberapa pemerintah daerah di Indonesia melaporkan kasus **phishing internal**, di mana pelaku mengaku sebagai pejabat BSSN dan berhasil memperoleh akses ke akun e-office beberapa pegawai. Akibatnya, dokumen internal bocor ke publik sebelum waktunya.

2. Dampak bagi Masyarakat

Masyarakat juga menjadi target empuk karena sebagian besar masih **belum**

memiliki kesadaran keamanan digital yang kuat. Pelaku memanfaatkan rasa panik, tergiur hadiah, atau ketidaktahuan pengguna terhadap keamanan akun digital.

💸 **Beberapa dampak yang sering dialami masyarakat:**

a. **Kerugian Finansial:** Uang tabungan, saldo e-wallet, atau dana bantuan sosial bisa dicuri melalui tautan palsu.
b. **Penyalahgunaan Identitas:** Data pribadi seperti NIK, foto, atau nomor rekening digunakan untuk membuka akun pinjaman online atau tindak kriminal lainnya.
c. **Gangguan Psikologis:** Korban penipuan digital sering mengalami stres, malu, bahkan takut menggunakan layanan digital kembali.
d. **Penyebaran Hoaks:** Pesan palsu atau video manipulatif membuat masyarakat ikut menyebarkan informasi salah tanpa sadar.

📍 *Contoh nyata:*

Kasus *"penipuan bantuan sosial"* di beberapa wilayah Bali pada awal 2025, di mana pelaku menggunakan pesan WhatsApp palsu dengan logo pemerintah daerah untuk mengumpulkan data NIK dan OTP masyarakat.

3. Dampak bagi Pemerintah Daerah

Serangan rekayasa sosial yang menargetkan ASN dan masyarakat **secara tidak langsung melemahkan sistem pemerintahan daerah.** Jika dibiarkan, hal ini dapat mengganggu stabilitas pelayanan publik dan merusak citra pemerintah.

🏛️ **Dampak utama yang perlu diwaspadai:**

a. **Turunnya Kepercayaan Publik:** Warga kehilangan keyakinan terhadap kemampuan pemerintah dalam melindungi data mereka.
b. **Gangguan Layanan Digital:** Sistem administrasi seperti e-office, pelayanan kependudukan, dan keuangan daerah bisa lumpuh akibat penyalahgunaan akses.
c. **Risiko Hukum dan Etik:** Pemerintah daerah dapat diminta pertanggungjawaban jika kebocoran data disebabkan oleh kelalaian internal.
d. **Melemahnya Kolaborasi Antar-Instansi:** Ketika kepercayaan antar lembaga

terganggu, koordinasi keamanan siber menjadi sulit dilakukan.

📍 *Contoh relevan:*

Dalam laporan BSSN tahun 2024, 1 dari 3 serangan siber yang melibatkan instansi daerah **berawal dari rekayasa sosial terhadap pegawai non-teknis**, seperti staf administrasi atau petugas pelayanan publik.

4. Dampak Sosial dan Psikologis

Selain dampak teknis dan finansial, rekayasa sosial juga menimbulkan **dampak sosial yang nyata.** Masyarakat menjadi mudah curiga terhadap pesan resmi, ASN menjadi takut berkomunikasi secara digital, dan lingkungan kerja kehilangan rasa saling percaya.

🧠 **Beberapa dampak yang sering muncul:**

a. **Rasa Takut dan Paranoid:** Korban enggan berinteraksi secara online karena khawatir tertipu.
b. **Menurunnya Produktivitas:** ASN yang menjadi korban sering kehilangan semangat kerja atau mengalami tekanan psikologis.
c. **Erosi Kepercayaan Sosial:** Hubungan antara pemerintah dan masyarakat menjadi renggang karena adanya kecurigaan berlebihan.

Rekayasa sosial bukan sekadar “penipuan online”, tetapi ancaman multidimensi yang bisa merusak kepercayaan, reputasi, dan stabilitas sistem pemerintahan. Baik ASN maupun masyarakat harus memahami bahwa **setiap interaksi digital membawa risiko**, dan **setiap tindakan ceroboh dapat berdampak luas** pada ekosistem keamanan daerah. Kesadaran, verifikasi informasi, dan kehati-hatian dalam berbagi data adalah langkah paling efektif untuk mencegah kerugian yang lebih besar di masa depan.

F. Psikologi di Balik Serangan Rekayasa Sosial

Rekayasa sosial bukan hanya persoalan teknologi ini adalah **permainan psikologi manusia.** Pelaku tidak perlu meretas sistem yang rumit; cukup memahami **cara berpikir,**

merasa, dan bereaksi korban, lalu memanipulasinya agar melakukan apa yang diinginkan. Di balik setiap pesan palsu, panggilan penipuan, atau tautan mencurigakan, selalu ada **strategi psikologis yang dirancang untuk menekan tombol emosi manusia.** Berikut beberapa prinsip psikologis utama yang sering dimanfaatkan pelaku:

1. Prinsip Kepercayaan (Trust Bias)

Manusia cenderung mempercayai pesan yang **terlihat resmi, sopan, dan meyakinkan.** Pelaku memanfaatkan hal ini dengan meniru gaya bahasa, logo, dan tanda tangan instansi resmi agar korban tidak curiga.

📍 *Contoh:*

Pesan dengan kop surat "Pemerintah Kabupaten Klungkung" yang menawarkan program bantuan digital padahal palsu.

🧩 *Pelajaran:*

Jangan menilai keaslian hanya dari tampilan visual. Lihat domain, nomor kontak, dan sumber resmi.

2. Prinsip Urgensi (Sense of Urgency)

Pelaku menekan korban dengan waktu agar **tidak sempat berpikir panjang.** Emosi panik atau takut membuat orang cenderung langsung mengikuti instruksi tanpa memverifikasi.

📍 *Contoh:*

"Data Anda akan terhapus dalam 10 menit jika tidak dikonfirmasi!"

🧩 *Pelajaran:*

Instansi resmi tidak pernah menekan masyarakat untuk segera bertindak tanpa prosedur.

3. Prinsip Kepatuhan terhadap Otoritas (Authority Bias)

Kita cenderung mematuhi perintah dari orang yang terlihat berkuasa pejabat, atasan, atau pihak berwenang. Pelaku menggunakan teknik ini dengan **menyamar sebagai figur otoritatif.**

📍 *Contoh:*

Penipu mengaku sebagai kepala dinas atau petugas BSSN dan meminta data sensitif "untuk audit sistem".

🧩 *Pelajaran:*

Setiap perintah resmi memiliki jalur administrasi dan dokumen pendukung yang jelas, jangan percaya hanya pada pesan digital.

4. Prinsip Timbal Balik (Reciprocity)

Pelaku menciptakan situasi di mana korban merasa "berutang budi." Misalnya, setelah memberikan bantuan kecil, pelaku meminta imbalan berupa data pribadi.

📍 *Contoh:*

"Terima kasih sudah ikut survei kami. Sebagai apresiasi, mohon kirim NIK Anda agar hadiah bisa dikirim."

🧩 *Pelajaran:*

Hadiah atau imbalan dari sumber tidak resmi sering kali hanyalah umpan.

5. Prinsip Kelangkaan (Scarcity)

Pelaku membuat korban percaya bahwa **kesempatan terbatas,** sehingga merasa harus segera bertindak.

📍 *Contoh:*

"Hanya 50 orang pertama yang akan menerima bantuan digital!"

🧩 *Pelajaran:*

Informasi resmi tidak pernah menekan masyarakat dengan iming-iming waktu singkat.

6. Prinsip Rasa Takut dan Ancaman (Fear Appeal)

Ketika manusia merasa takut, kemampuan berpikir logis menurun drastis. Pelaku memanfaatkan hal ini dengan menciptakan ancaman palsu agar korban segera menuruti permintaan.

📍 *Contoh:*

“Jika tidak mengisi formulir ini, akun Anda akan diblokir dan gaji ditahan.”

🧩 *Pelajaran:*

Ancaman digital harus selalu dikonfirmasi melalui saluran resmi, bukan ditanggapi secara spontan.

7. Prinsip Validasi Sosial (Social Proof)

Pelaku menciptakan kesan bahwa “semua orang sudah melakukannya,” sehingga korban ikut tanpa ragu.

📍 *Contoh:*

“Tiga rekan ASN Anda sudah memperbarui data di tautan berikut, silakan ikut.”

🧩 *Pelajaran:*

Jangan mengikuti tindakan orang lain tanpa verifikasi sumber informasi.

G. Strategi Pencegahan dan Edukasi Digital di Lingkungan Pemerintah & Masyarakat

Rekayasa sosial tidak dapat dihilangkan sepenuhnya, tetapi **dapat dicegah dengan kebiasaan digital yang benar dan sistem pengamanan yang disiplin.** Kunci utamanya adalah **kesadaran, verifikasi, dan komunikasi yang bijak.** Berikut strategi yang relevan untuk ASN dan masyarakat di Kabupaten Klungkung berdasarkan tren ancaman tahun 2025:

1. Verifikasi Sebelum Percaya

Setiap pesan, panggilan, atau tautan harus **diverifikasi sumbernya** sebelum direspons. ASN maupun masyarakat wajib membiasakan diri untuk *mengecek dua kali sebelum bertindak.*

🔍 **Langkah praktis:**

a. Pastikan domain email atau situs web berakhiran *.go.id* untuk lembaga pemerintah.
b. Jangan klik tautan langsung dari pesan; buka situs resmi secara manual.

c. Untuk ASN, konfirmasi instruksi melalui atasan langsung atau CSIRT Klungkung.

2. Jaga Kerahasiaan Informasi Pribadi

Data pribadi seperti **NIK, KK, nomor rekening, OTP, password, dan foto identitas** adalah target utama pelaku. Sekali bocor, data tersebut dapat digunakan untuk berbagai kejahatan digital.

🛡️ **Langkah praktis:**

a. Jangan pernah membagikan kode OTP, meskipun pengirim mengaku dari lembaga resmi.
b. Hindari mengunggah dokumen pribadi ke media sosial atau grup publik.
c. Gunakan perangkat kerja (HP/laptop) yang terpisah dari perangkat pribadi bagi ASN.

3. Gunakan Saluran Resmi Pemerintah

Pelaporan dan komunikasi terkait data pemerintahan harus dilakukan melalui **kanal resmi.** Di Klungkung, sudah tersedia **CSIRT (Computer Security Incident Response Team)** yang siap menangani laporan insiden siber.

📞 **Langkah praktis:**

a. Laporkan setiap pesan mencurigakan ke **CSIRT Klungkung** atau Dinas Komunikasi dan Informatika setempat.
b. Jangan menindaklanjuti perintah yang datang dari nomor pribadi pejabat tanpa konfirmasi resmi.

4. Waspadai Manipulasi Emosi

Pelaku selalu memanfaatkan **emosi manusia**, terutama rasa takut, panik, atau tergiur hadiah. Maka, langkah pertama untuk mencegah jebakan adalah **menenangkan diri.**

🧠 **Langkah praktis:**

a. Jangan langsung menanggapi pesan yang mengandung ancaman atau iming-iming hadiah.
b. Ambil jeda beberapa menit sebelum memutuskan untuk mengklik atau

membalas pesan.

c. Ingat: pemerintah tidak pernah mengirim pesan dengan ancaman blokir data atau hadiah instan.

5. Edukasi dan Simulasi Berkala

BSSN dan pemerintah daerah telah mendorong **pelatihan keamanan siber berbasis manusia.** ASN perlu dilatih agar paham bentuk-bentuk rekayasa sosial, sementara masyarakat perlu sosialisasi agar lebih kritis terhadap pesan digital.

Langkah praktis:

a. Lakukan simulasi phishing atau pelatihan keamanan digital internal tiap triwulan bagi ASN.

b. Untuk masyarakat, adakan edukasi di tingkat banjar atau desa melalui *literasi digital*.

c. Gunakan media sosial pemerintah untuk mengingatkan masyarakat soal modus-modus baru.

6. Terapkan Prinsip "Zero Trust"

Prinsip ini berarti **tidak langsung mempercayai siapa pun atau pesan apa pun sebelum diverifikasi.** Dalam konteks ASN, setiap permintaan data, akses, atau dokumen harus melalui izin berjenjang.

Langkah praktis:

a. Setiap permintaan data internal wajib melalui surat tugas atau sistem resmi.

b. Untuk masyarakat, hindari berbagi data ke pihak ketiga tanpa kejelasan tujuan.

c. Anggap setiap permintaan mendadak sebagai potensi ancaman sampai terbukti aman.

7. Gunakan Teknologi Keamanan Dasar

Meski fokusnya manusia, perlindungan teknis tetap penting sebagai lapisan tambahan.

Langkah praktis:

a. Aktifkan autentikasi dua langkah (2FA) di semua akun penting.

b. Gunakan password berbeda untuk setiap platform.
c. Rutin memperbarui sistem operasi dan antivirus.

8. Budaya Laporkan, Bukan Diam

Banyak korban enggan melapor karena malu atau takut disalahkan. Padahal, laporan cepat justru membantu mencegah korban berikutnya.

📣 **Langkah praktis:**

a. ASN wajib melapor ke tim IT instansi atau CSIRT daerah jika menemukan indikasi serangan.
b. Masyarakat dapat melapor ke kanal pengaduan resmi pemerintah atau kepolisian siber.
c. Gunakan laporan sebagai bahan pembelajaran, bukan untuk saling menyalahkan.

Strategi pertahanan terhadap rekayasa sosial bukan hanya soal teknologi, tetapi **soal kebiasaan digital yang disiplin.** Kunci utamanya adalah *berpikir sebelum bertindak*, *verifikasi sebelum percaya*, dan *lapor sebelum terlambat.*

Jika ASN dan masyarakat Kabupaten Klungkung mampu menerapkan tiga prinsip itu, maka mereka sudah membangun **tembok pertahanan siber berbasis kesadaran manusia** yang jauh lebih kuat daripada sekadar perangkat lunak keamanan.

H. Kolaborasi ASN–Masyarakat dalam Mencegah Manipulasi Digital

Keamanan siber bukan hanya tanggung jawab satu pihak. Tidak ada sistem yang benar-benar aman jika hanya dijaga oleh teknologi atau tim IT. **Pertahanan terbaik justru muncul dari kolaborasi antara ASN dan masyarakat** dua pihak yang setiap hari berinteraksi dalam ekosistem digital pemerintahan dan pelayanan publik.

1. ASN sebagai Garda Depan Keamanan Data Publik

Sebagai penyelenggara pelayanan, ASN memiliki peran penting dalam menjaga keamanan informasi yang dikelola oleh instansi pemerintah. Namun, tanggung jawab ASN tidak berhenti pada penggunaan sistem dengan benar. ASN juga harus menjadi **teladan literasi digital dan etika komunikasi daring.**

🏛️ **Langkah nyata untuk ASN:**

a. Menyampaikan edukasi ringan kepada masyarakat saat memberikan pelayanan digital.
b. Tidak membagikan data atau dokumen masyarakat tanpa prosedur resmi.
c. Melakukan verifikasi ganda setiap kali menerima permintaan data internal.
d. Menjadi sumber informasi yang benar ketika ada kabar palsu atau pesan menyesatkan beredar di masyarakat.
e. ASN yang melek digital bukan hanya pegawai yang paham teknologi, tetapi **pegawai yang mampu mengamankan kepercayaan publik**.

2. Masyarakat sebagai Mitra Pengawas dan Pengaman Digital

Masyarakat tidak hanya sebagai penerima layanan, tetapi juga **pengguna aktif ruang digital pemerintah.** Mereka berperan penting dalam menjaga keamanan dengan menjadi **pengawas sosial digital (digital social guardian)** memastikan informasi yang beredar benar, dan melaporkan hal mencurigakan.

👥 **Langkah nyata untuk masyarakat:**

a. Tidak menyebarkan tautan atau pesan yang belum diverifikasi.
b. Melaporkan pesan mencurigakan yang mengatasnamakan instansi pemerintah.
c. Mengedukasi lingkungan sekitar, seperti keluarga dan tetangga, agar lebih hati-hati dalam berbagi data pribadi.
d. Menjadi pengguna layanan digital pemerintah yang aktif memberikan masukan dan kritik membangun.
e. Masyarakat yang sadar digital akan memperkuat benteng pertahanan ASN dari sisi luar sistem.

3. Peran Pemerintah Daerah sebagai Penghubung

Pemerintah daerah, khususnya melalui **CSIRT Klungkung dan Dinas Komunikasi dan Informatika**, berperan sebagai **jembatan antara ASN dan masyarakat** dalam memperkuat budaya keamanan siber. Pemerintah tidak hanya menyiapkan sistem perlindungan, tetapi juga harus menciptakan lingkungan yang transparan dan edukatif.

🛡️ **Langkah strategis:**

a. Menyelenggarakan pelatihan gabungan ASN–masyarakat tentang rekayasa sosial dan keamanan data pribadi.
b. Mengembangkan kanal aduan online satu pintu untuk laporan insiden siber.
c. Menyebarkan informasi edukatif melalui media sosial resmi dengan bahasa yang sederhana.
d. Melibatkan desa, sekolah, dan organisasi masyarakat dalam kampanye *"Klungkung Aman Digital"*.
e. Dengan langkah kolaboratif, keamanan digital menjadi **budaya bersama**, bukan sekadar aturan teknis.

4. Keamanan Siber sebagai Ekosistem Sosial

Rekayasa sosial memanfaatkan kelemahan manusia maka pertahanannya juga harus bersumber dari **kekuatan manusia: kepercayaan, kerja sama, dan kesadaran.** ASN yang teliti dan masyarakat yang kritis akan menciptakan **lingkaran keamanan digital yang saling melindungi.**

🌐 **Kunci sukses kolaborasi:**

a. ASN menjadi sumber informasi yang valid.
b. Masyarakat menjadi pelapor aktif jika menemukan indikasi manipulasi digital.
c. Pemerintah daerah menjadi penggerak sistem keamanan dan literasi.
d. Dengan begitu, Kabupaten Klungkung dapat menjadi contoh **pemerintahan daerah yang tangguh terhadap ancaman sosial digital**, di mana setiap warga merasa aman untuk beraktivitas di dunia maya.

Ketika ASN dan masyarakat bekerja sama, saling melindungi, dan saling mengingatkan, maka ruang digital tidak lagi menjadi tempat yang menakutkan,

melainkan ruang yang produktif, aman, dan penuh kepercayaan.

I. Tren Baru: Rekayasa Sosial Berbasis AI (AI-Driven Social Engineering)

Perkembangan teknologi kecerdasan buatan (AI) telah membawa banyak manfaat, mulai dari mempercepat pelayanan publik, meningkatkan efisiensi administrasi, hingga mempermudah masyarakat mengakses informasi. Namun, di sisi lain, **AI juga dimanfaatkan oleh pelaku kejahatan siber untuk melakukan manipulasi yang jauh lebih canggih dan sulit dideteksi.** Fenomena ini dikenal sebagai **rekayasa sosial berbasis AI (*AI-driven social engineering*).**

1. Apa Itu Rekayasa Sosial Berbasis AI

Rekayasa sosial berbasis AI adalah **penggunaan algoritma kecerdasan buatan untuk mempelajari perilaku, bahasa, dan kebiasaan korban**, kemudian menciptakan pesan atau interaksi yang tampak sangat meyakinkan. Jika dulu pesan penipuan mudah dikenali dari bahasa yang janggal, maka kini **AI mampu meniru gaya bicara, nada tulisan, bahkan emosi seseorang** dengan sangat alami.

🤖 *Contoh:*

a. Sistem AI mengirimkan email otomatis dengan gaya bahasa yang sama seperti pimpinan instansi.
b. Bot AI meniru suara pejabat pemerintah untuk meminta konfirmasi data melalui telepon.
c. Deepfake video memperlihatkan sosok yang tampak seperti kepala daerah memberikan instruksi tertentu.

2. Jenis Ancaman AI yang Berkaitan dengan Rekayasa Sosial

Beberapa bentuk baru yang muncul akibat perkembangan AI di tahun 2025 antara lain:

🧠 **a. Deepfake Manipulation**, AI mampu membuat video atau audio palsu dengan

tingkat kemiripan yang tinggi. Pelaku dapat menipu ASN atau masyarakat dengan menampilkan “bukti visual” yang seolah asli.

📍 *Contoh:*

Video palsu kepala dinas meminta ASN mentransfer dana operasional, padahal hasil editan AI.

🧠 **b. Voice Cloning Scam**, AI dapat meniru suara seseorang hanya dengan cuplikan pendek. Penipu bisa menelpon korban dengan suara seperti rekan kerja atau anggota keluarga.

📍 *Contoh:*

Telepon dengan suara yang identik dengan atasan meminta password sistem atau data login.

🧠 **c. AI Chatbot Fraud**, Chatbot palsu kini dapat berbicara seperti manusia. Banyak korban tidak sadar sedang berbicara dengan bot yang memancing informasi sensitif.

📍 *Contoh:*

Bot yang berpura-pura menjadi “layanan pelanggan e-KTP digital” dan meminta unggahan dokumen pribadi.

🧠 **d. AI-Generated Phishing Email**, AI digunakan untuk membuat ribuan email phishing dengan bahasa yang sangat rapi, tanpa kesalahan ejaan, dan menyesuaikan konteks lokal.

📍 *Contoh:*

Email “update sistem absen ASN” lengkap dengan logo instansi dan nama pejabat lokal **yang valid.**

3. Mengapa AI-Driven Social Engineering Lebih Berbahaya

Serangan berbasis AI jauh lebih sulit dideteksi karena:

a. Pesannya tampak **alami dan kontekstual**, meniru gaya komunikasi target.
b. Pelaku dapat **mensimulasikan identitas digital palsu** dengan cepat dan dalam jumlah banyak.

c. Serangan bisa **berlangsung otomatis 24 jam**, tanpa campur tangan manusia secara langsung.

Dampaknya meluas karena **AI mampu menyesuaikan pesan untuk ribuan korban berbeda.**

💬 **Menurut laporan BSSN 2025**, tren kejahatan digital berbasis AI meningkat lebih dari **60%** dibanding tahun sebelumnya, terutama pada kasus peniruan suara dan video.

4. Cara ASN dan Masyarakat Menghadapinya

Tidak ada sistem yang benar-benar kebal terhadap manipulasi AI, tetapi dengan kesadaran dan ketelitian, kita dapat meminimalkan risikonya.

🔐 **Langkah praktis untuk ASN:**

a. Verifikasi identitas setiap instruksi penting, terutama jika disampaikan lewat pesan suara atau video digital.
b. Gunakan sistem komunikasi resmi dengan autentikasi ganda.
c. Jangan menyebarkan video atau pesan internal tanpa memastikan sumbernya.

👥 **Langkah praktis untuk masyarakat:**

a. Jangan langsung percaya pada video, foto, atau suara yang beredar di media sosial.
b. Periksa kembali melalui situs resmi atau media pemerintah sebelum membagikan informasi.
c. Laporkan konten mencurigakan ke pihak berwenang (Diskominfo/CSIRT).

5. Edukasi Digital sebagai Pertahanan Utama

AI dapat menipu sistem, tetapi **tidak dapat menipu manusia yang sadar dan kritis.** Oleh karena itu, edukasi digital menjadi fondasi penting dalam menghadapi era *AI-driven social engineering.*

Pemerintah daerah dapat:

a. Menyelenggarakan pelatihan *AI Awareness* bagi ASN dan masyarakat.
b. Membentuk *tim literasi digital desa* untuk membantu masyarakat mengenali konten palsu berbasis AI.

c. Mengintegrasikan sistem deteksi deepfake pada kanal komunikasi resmi.

Jika dulu korban tertipu karena ketidaktahuan, kini korban bisa tertipu karena **AI membuat kebohongan terlihat sangat meyakinkan.** Maka, kunci utama perlindungan di era ini bukan hanya firewall atau sistem keamanan, tetapi **kecerdasan emosional, logika kritis, dan kebiasaan memverifikasi informasi.** Dengan kolaborasi ASN, masyarakat, dan pemerintah daerah, Kabupaten Klungkung dapat menjadi **contoh daerah yang tangguh menghadapi manipulasi digital berbasis AI.**

J. Studi Kasus Ilustratif (2024–2025)

Memahami ancaman melalui kisah nyata agar kewaspadaan meningkat. Kasus-kasus berikut diambil dari berbagai sumber nasional dan laporan lembaga keamanan siber seperti **BSSN (2024–2025)**, **Kominfo**, serta pemberitaan terpercaya. Tujuannya bukan untuk menakut-nakuti, tetapi untuk **memberikan pembelajaran nyata tentang bagaimana rekayasa sosial bekerja di dunia nyata.**

1. Kasus "Pegawai Terpercaya" – Penipuan Melalui Video Palsu Kepala Dinas (2024)

📍 *Lokasi: Jawa Tengah (Kasus Serupa Potensial di Daerah Lain)*

Seorang ASN menerima video singkat dari akun WhatsApp yang menampilkan wajah dan suara mirip kepala dinasnya. Video tersebut meminta ASN tersebut mentransfer dana "darurat operasional" ke rekening tertentu untuk kepentingan dinas. Karena video tampak meyakinkan dan menggunakan gaya bicara yang sangat mirip, ASN tersebut mengikuti perintah tanpa verifikasi.

🧩 **Analisis:**

Video tersebut adalah **deepfake** hasil manipulasi AI.

Pelaku memanfaatkan rasa percaya ASN terhadap atasannya.

Tidak ada sistem internal verifikasi yang memastikan setiap perintah keuangan lewat prosedur resmi.

💡 **Pelajaran:**

Teknologi deepfake kini sangat realistis. ASN harus selalu mengonfirmasi perintah penting secara langsung melalui jalur resmi, bukan pesan pribadi.

2. Kasus "Bantuan Sosial Digital" – Formulir Online Palsu (2025)

📍 *Lokasi: Bali dan Jawa Timur (termasuk laporan di Klungkung)*

Masyarakat menerima tautan WhatsApp berisi formulir "Pendaftaran Bantuan Sosial Digital 2025." Formulir tampak meyakinkan, menggunakan logo BSSN dan Kementerian Sosial, dan meminta warga mengisi NIK, foto KTP, serta nomor rekening. Beberapa hari kemudian, saldo rekening penerima justru berkurang, dan data pribadinya tersebar di forum online.

🧩 **Analisis:**

Ini adalah bentuk **phishing** dengan *pretext* bantuan pemerintah.

Masyarakat tertipu karena terbiasa mengikuti tautan dari grup WhatsApp tanpa verifikasi.

Tidak ada kampanye literasi digital aktif di tingkat desa saat itu.

💡 **Pelajaran:**

Layanan resmi pemerintah **tidak pernah meminta data pribadi lewat tautan publik atau pesan pribadi.**

Masyarakat perlu memeriksa sumber informasi melalui situs resmi (.go.id).

3. Kasus "Akun Palsu Vendor IT Pemerintah" – Manipulasi ASN Bidang Teknis (2024)

📍 *Lokasi: Kalimantan Timur*

Pelaku membuat akun LinkedIn dan email menyerupai perusahaan penyedia jasa IT nasional. Ia menghubungi beberapa ASN bidang pengadaan untuk menawarkan *update patch keamanan sistem e-office.* Saat file dikirim dan dijalankan, ternyata itu adalah *malware* yang memberikan pelaku akses ke server instansi.

🧩 **Analisis:**

Teknik yang digunakan: kombinasi *pretexting* dan *baiting.*

Pelaku menyasar ASN yang memiliki akses langsung ke sistem server.

Ketiadaan SOP pengujian keamanan file membuat serangan berhasil.

💡 **Pelajaran:**

Jangan pernah memasang perangkat lunak atau file dari sumber tidak resmi, sekalipun mengaku dari rekanan pemerintah.

4. Kasus "Suara Anak Minta Tolong" – Penipuan AI Voice Cloning (2025)

📍 *Lokasi: Jakarta, Yogyakarta, dan Denpasar*

Beberapa orang tua menerima telepon dengan suara mirip anak mereka yang menangis dan mengatakan sedang disandera. Pelaku lalu meminta tebusan uang melalui transfer cepat. Ternyata suara itu hasil **AI voice cloning** yang dibuat dari potongan video anak korban di media sosial.

🧩 **Analisis:**

Pelaku menggunakan kecerdasan buatan untuk meniru suara korban.

Masyarakat masih belum paham bahwa manipulasi suara kini bisa dilakukan hanya dari cuplikan video 10 detik.

💡 **Pelajaran:**

Hindari mempublikasikan terlalu banyak video pribadi di media sosial, terutama yang menampilkan suara jelas atau wajah anak.

5. Kasus "Hoaks ASN Korupsi" – Manipulasi Citra Digital (2025)

📍 *Lokasi: Sulawesi Selatan*

Sebuah akun media sosial menyebarkan tangkapan layar palsu percakapan WhatsApp antara ASN dan pihak swasta yang seolah membahas proyek ilegal. Padahal, percakapan tersebut hasil **rekayasa digital dengan bantuan AI generator.** Hoaks ini menimbulkan kericuhan publik sebelum akhirnya terbukti palsu.

🧩 **Analisis:**

Pelaku menggunakan *social proof* (bukti sosial palsu) untuk menyerang reputasi seseorang.

Tidak semua masyarakat mampu membedakan gambar hasil editan dan bukti asli.

💡 **Pelajaran:**

Jangan langsung mempercayai tangkapan layar atau bukti digital yang beredar tanpa verifikasi ke instansi resmi.

Kasus-kasus di atas menunjukkan bahwa **rekayasa sosial semakin sulit dikenali karena tampilannya semakin canggih dan realistis.** Pelaku kini menggabungkan **psikologi manusia dengan kecerdasan buatan,** sehingga korban bisa berasal dari siapa saja, ASN, pejabat, bahkan masyarakat biasa.

Namun, kunci pencegahan tetap sama:

a. **Verifikasi sumber.**
b. **Tenangkan diri sebelum bereaksi.**
c. **Laporkan segera jika menemukan kejanggalan.**

Dengan kesadaran kolektif, Kabupaten Klungkung dapat menjadi **daerah yang tangguh terhadap manipulasi digital**, sekaligus teladan nasional dalam literasi keamanan siber berbasis manusia.

Pertanyaan Reflektif

1. Ketika Anda menerima pesan mendesak dari atasan melalui WhatsApp pribadi yang meminta data penting atau dana operasional, langkah apa yang paling aman Anda lakukan sebelum menindaklanjuti?
2. Sebagai ASN, bagaimana Anda bisa membantu masyarakat agar tidak mudah tertipu oleh pesan palsu atau tautan bantuan sosial yang beredar di grup WhatsApp desa?
3. Sebagai masyarakat digital, seberapa penting menurut Anda untuk membatasi informasi pribadi yang dibagikan di media sosial, terutama data seperti suara, wajah, dan alamat?
4. Bagaimana pendapat Anda tentang tren rekayasa sosial berbasis AI (seperti deepfake dan voice cloning)? Apakah teknologi ini lebih banyak memberi manfaat atau risiko? Jelaskan alasan Anda.
5. Jika Anda menemukan kerabat atau rekan kerja menjadi korban manipulasi digital, apa langkah nyata yang bisa Anda lakukan untuk menolong dan mencegah kasus serupa?
6. Rekayasa sosial seringkali berhasil karena manusia tidak waspada, bukan karena sistem lemah. Menurut Anda, bagaimana cara membangun budaya “verifikasi sebelum percaya” di lingkungan kerja maupun masyarakat?

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara (BSSN). (2024). *Laporan Tahunan Keamanan Siber Indonesia 2024.* Jakarta: BSSN. https://bssn.go.id

European Union Agency for Cybersecurity (ENISA). (2024). *Threat Landscape 2024: Social Engineering and Human Factors.* https://www.enisa.europa.eu/publications

Google Indonesia. (2025). *Tren Keamanan Digital dan Rekayasa Sosial di Indonesia 2025.* https://safety.google/intl/id

Kementerian Komunikasi dan Digital (Komdigi). (2025). *Panduan Literasi Digital Nasional: Waspada Rekayasa Sosial di Dunia Maya.* https://komdigi.go.id

Kurniawan, A., & Hidayati, S. (2024). *Analisis Serangan Rekayasa Sosial dan Strategi Mitigasinya di Lingkungan Pemerintahan. Jurnal Teknologi dan Keamanan Informasi,* 10(2), 55–68. DOI: 10.33387/jtki.v10i2.8421

Microsoft Security Intelligence. (2024). *The Human Element in Cyber Threats: Social Engineering in 2024.* https://www.microsoft.com/security/blog

Nugroho, A., & Dewi, F. (2025). *Pemanfaatan Kecerdasan Buatan dalam Serangan Rekayasa Sosial: Studi Kasus Deepfake Voice dan Chatbot Penipuan. Jurnal Keamanan Siber Indonesia,* 5(1), 44–59. DOI: 10.21009/jksi.v5i1.1194

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.* Jakarta: Kementerian Hukum dan HAM. https://peraturan.bpk.go.id/Home/Details/216819

Suryadin, A. (2025). *Peran Literasi Digital dalam Menghadapi Ancaman Rekayasa Sosial di Indonesia. Jurnal Media Teknologi Informasi,* 13(1), 102–118. DOI: 10.36787/jmti.v13i1.5542

Trend Micro Research. (2024). *The Rise of AI-Powered Social Engineering: Global Threat Report.* https://www.trendmicro.com