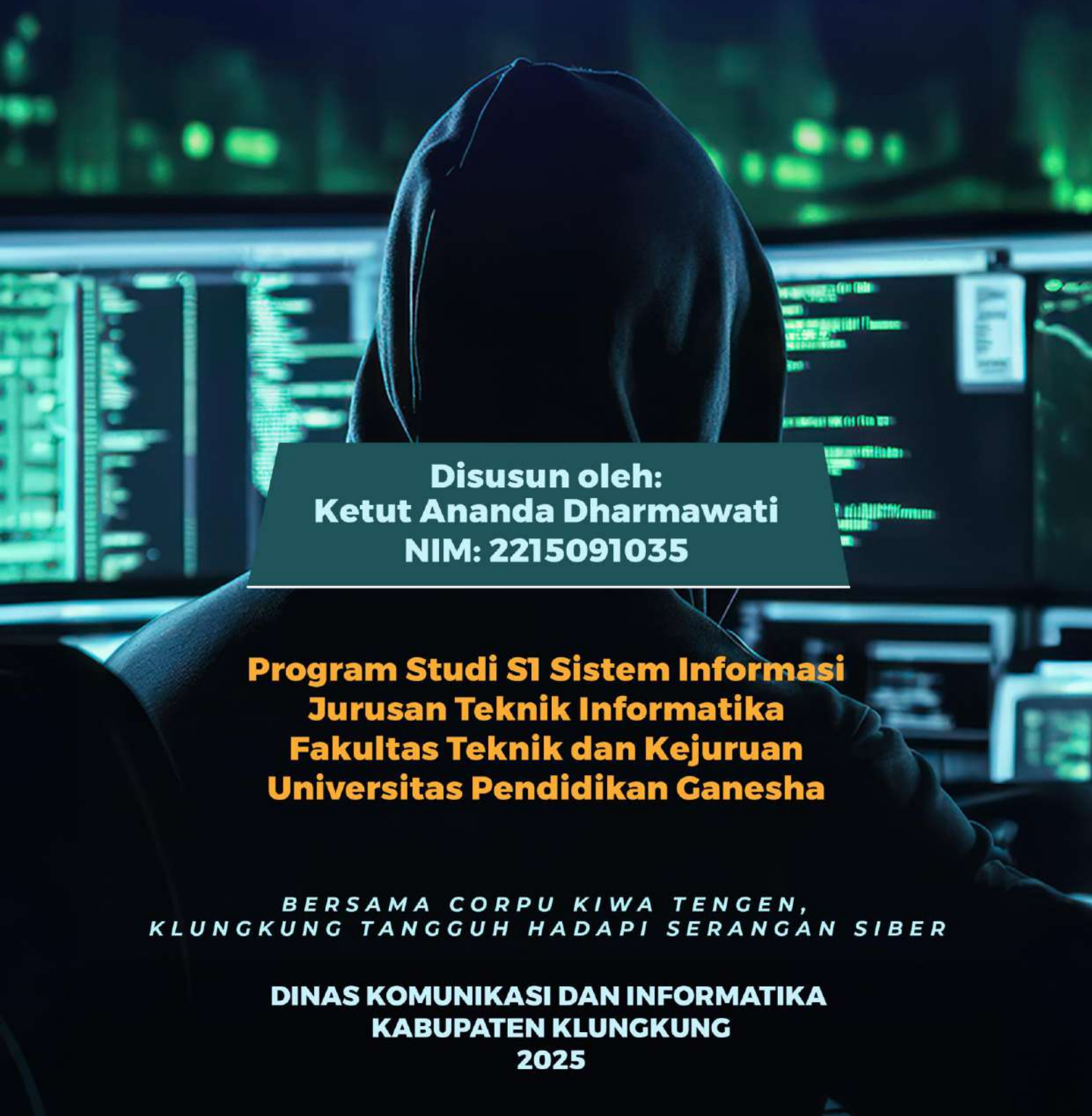
KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 2: Ancaman Siber yang Sering Terjadi

Subtopik 2.1: Phishing



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. Phishing merupakan salah satu ancaman siber paling sering terjadi di Indonesia, termasuk di lingkungan pemerintahan daerah maupun masyarakat umum. Modusnya semakin canggih dari tahun ke tahun, mulai dari email palsu, pesan WhatsApp, SMS penipuan, hingga kombinasi beberapa saluran komunikasi digital. Karena sifatnya yang menipu dan memanfaatkan kelengahan manusia, phishing berpotensi besar merugikan keuangan, mencuri data pribadi, bahkan mengganggu sistem pelayanan publik.

Subtopik ini disusun agar ASN dan masyarakat memiliki pemahaman praktis tentang apa itu phishing, bagaimana cara mengenalinya, serta langkah-langkah sederhana untuk mencegah menjadi korban. Dengan demikian, tercipta ekosistem digital yang lebih aman, baik di birokrasi maupun dalam kehidupan sehari-hari. 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

KATA PENGANTAR ii
DAFTAR ISI iii
Tujuan Pembelajaran 4
Sasaran Peserta 4
A. Definisi Phishing 5
B. Bentuk Umum Phishing di Indonesia (2023-2025) 6
C. Tren Phishing di Tahun 2025 7
D. Dampak Phishing 9
E. Cara Mendeteksi Phishing 11
F. Contoh Kasus Phishing Terkini (2023–2025) di Indonesia 12
G. Langkah Pencegahan Praktis untuk ASN & Masyarakat 14
Pertanyaan Reflektif 15
DAFTAR PUSTAKA 16

CORPU
KIWA TENGEN

Tujuan Pembelajaran

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

1. Menjelaskan definisi keamanan siber dengan bahasa sederhana.
2. Menguraikan secara singkat perkembangan keamanan siber di Indonesia sebagai konteks pentingnya perlindungan data.
3. Memahami ruang lingkup keamanan siber dalam kehidupan sehari-hari dan birokrasi.
4. Merefleksikan peran pribadi dalam meningkatkan keamanan siber, baik sebagai ASN maupun masyarakat.

Sasaran Peserta

1. ASN: agar memahami tugas menjaga data pemerintahan sekaligus menyadari posisi strategis pemda dalam ekosistem keamanan siber nasional.
2. Masyarakat: agar lebih bijak dalam menjaga data pribadi, menghindari interaksi digital berisiko, serta mampu merefleksikan langkah kecil untuk meningkatkan keamanan digital sehari-hari.

COPPU
KIWA TENGEN

A. Definisi Phishing

Phishing adalah salah satu bentuk **kejahatan siber** yang paling sering dialami ASN dan masyarakat di Indonesia. Istilah "*phishing*" berasal dari kata *fishing* (memancing), karena pelaku mencoba "memancing" korban agar memberikan informasi pribadi secara sukarela, meskipun sebenarnya itu adalah jebakan. *Phishing* biasanya dilakukan dengan cara **menyamar sebagai pihak resmi atau terpercaya**, seperti bank, *marketplace*, lembaga pemerintah, bahkan rekan kerja. Korban dibuat percaya melalui email, pesan WhatsApp, SMS, atau situs palsu, lalu diarahkan untuk memberikan data penting seperti **Nomor Induk Kependudukan (NIK), kata sandi akun, kode OTP, atau nomor rekening bank**.

Bagi **ASN**, *phishing* sangat berbahaya karena tidak hanya menargetkan akun pribadi, tetapi juga bisa masuk ke **sistem dinas dan aplikasi pelayanan publik**. Misalnya, seorang ASN menerima email palsu yang seolah dari BSSN atau Mendagri dengan permintaan mengisi data login. Jika ASN terkecoh, data akun dinas bisa diambil alih dan sistem instansi menjadi rentan dibobol.

Bagi **masyarakat**, *phishing* biasanya hadir dalam bentuk yang lebih sederhana tetapi sama merugikannya. Contoh umum adalah pesan WhatsApp palsu yang mengaku dari bank, menawarkan hadiah undian, atau menyamar sebagai kurir paket yang meminta pembayaran tambahan. Begitu korban memberikan data atau mengklik tautan, penipu dapat mencuri uang, menyalahgunakan identitas, atau bahkan menguasai akun WhatsApp untuk menipu kontak lain.

Mengapa *phishing* berbahaya? Karena serangan ini **tidak membutuhkan keahlian teknis tinggi**, melainkan memanfaatkan **kelemahan manusia**: rasa percaya, tergesa-gesa, atau panik. Di tahun 2025, tren *phishing* semakin meningkat karena pelaku menggunakan **teknologi AI** untuk membuat pesan lebih meyakinkan, bebas dari kesalahan bahasa, dan sulit dibedakan dengan pesan asli.

Dengan memahami definisi *phishing* secara utuh, bukan hanya sekadar "pesan penipuan" ASN dan masyarakat akan lebih siap menghadapi ancaman ini. *Phishing*

bukan hal sepele, tetapi ancaman serius yang dapat merusak sistem pemerintahan sekaligus merugikan individu.

B. Bentuk Umum Phishing di Indonesia (2023-2025)

Phishing tidak lagi terbatas pada email palsu seperti beberapa tahun lalu. Saat ini, modusnya semakin beragam dan menyasar siapa saja, baik ASN maupun masyarakat umum. Berikut adalah bentuk-bentuk *phishing* yang paling sering ditemukan di Indonesia:

1. **Email Palsu yang Menyamar sebagai Instansi Resmi**
    a. Banyak serangan *phishing* dikirim melalui email dengan logo, kop surat, atau tanda tangan elektronik yang terlihat mirip dengan instansi pemerintah atau lembaga keuangan.
    b. Contoh: email yang mengatasnamakan *Kementerian Dalam Negeri* atau *BSSN*, meminta ASN mengisi ulang data login.
    c. Sekilas terlihat resmi, tetapi alamat pengirim biasanya memakai domain gratis (seperti @gmail.com) atau alamat yang mirip tapi palsu, misalnya @bssn-go.id (padahal asli adalah @bssn.go.id).
2. **Pesan WhatsApp atau SMS Palsu**
    a. Modus ini paling sering menargetkan masyarakat. Pesan biasanya berisi peringatan atau iming-iming, misalnya: *"Akun bank Anda akan diblokir dalam 1 jam, klik tautan ini"* atau *"Selamat, Anda memenangkan hadiah undian!"*.
    b. Pelaku menyamar sebagai bank, *marketplace*, kurir paket, bahkan pejabat pemerintah.
    c. Jika korban mengklik tautan atau memberikan kode OTP, akun bisa diambil alih dan dana dicuri.

3. **Link Undian atau Promo Palsu**
    a. Tautan palsu ini banyak beredar di media sosial atau grup WhatsApp. Korban diminta mengisi survei atau memasukkan NIK untuk mendapatkan hadiah.
    b. Faktanya, data yang dimasukkan justru dikumpulkan untuk penipuan atau dijual di forum gelap.
4. **Phishing Melalui Akun Media Sosial**
    a. Halaman login palsu yang menyerupai Facebook, Instagram, atau aplikasi pemerintah dibuat untuk mencuri *username* dan *password*.
    b. Banyak masyarakat terkecoh karena tampilannya sangat mirip dengan situs asli.
5. **Phishing dengan Menyasar ASN secara Langsung**
    a. Beberapa kasus terbaru menunjukkan ASN menjadi target langsung, misalnya melalui pesan yang mengatasnamakan pimpinan daerah, meminta dokumen, atau data internal.
    b. Karena sifatnya terlihat "perintah atasan", ASN sering merasa wajib menuruti, padahal itu jebakan.

Dengan memahami berbagai bentuk ini, ASN dan masyarakat diharapkan bisa lebih waspada, tidak tergoda oleh tampilan meyakinkan, dan selalu memeriksa keaslian sumber informasi.

C. Tren Phishing di Tahun 2025

Seiring perkembangan teknologi, teknik *phishing* juga ikut berevolusi. Jika dulu serangan *phishing* mudah dikenali karena banyak salah ejaan atau tampilan sederhana, kini pada tahun 2025 serangan ini menjadi jauh lebih canggih dan sulit dibedakan dengan komunikasi asli. Berikut beberapa tren yang paling menonjol:

1. **AI-Generated Phishing (Pesan Buatan Kecerdasan Buatan)**

a. Penipu kini memanfaatkan **Artificial Intelligence (AI)** untuk membuat pesan yang lebih rapi, bebas dari kesalahan bahasa, dan sangat meyakinkan.
b. Contoh: pesan WA yang dibuat AI bisa menyesuaikan gaya bahasa lokal, termasuk memakai bahasa daerah (misalnya Bali atau Jawa), sehingga korban merasa lebih percaya.
c. Bagi ASN, pesan AI bisa dibuat khusus seolah-olah berasal dari pimpinan instansi, lengkap dengan format resmi.

2. Deepfake Voice & Video Phishing

a. Dengan teknologi *deepfake*, pelaku bisa meniru **suara atau wajah pejabat** dalam panggilan telepon atau video singkat.
b. Contoh: seorang ASN bisa menerima telepon dengan suara yang mirip atasan, meminta kode akses sistem.
c. Masyarakat juga bisa tertipu jika menerima pesan video yang seolah-olah dari bank atau *marketplace* resmi.

3. Multi-Channel Phishing

a. Serangan kini tidak hanya melalui satu jalur, tetapi **menggabungkan beberapa kanal** sekaligus.
b. Contoh: korban menerima email peringatan, lalu ditelepon oleh "petugas layanan pelanggan palsu", dan diperkuat dengan pesan WhatsApp. Kombinasi ini membuat korban sulit membedakan mana yang asli.

4. Phishing yang Menyasar Aplikasi Mobile

a. Banyak aplikasi palsu beredar di luar Play Store/App Store resmi, yang tampilannya meniru aplikasi bank, *marketplace*, atau bahkan aplikasi pelayanan publik.
b. Masyarakat yang tidak teliti bisa mengunduh aplikasi palsu, lalu semua data login mereka dicuri.

5. **Targeted Phishing (Spear Phishing)**
    a. Tidak semua serangan dilakukan secara massal. Kini banyak serangan yang ditargetkan ke individu tertentu dengan data yang sudah dikumpulkan sebelumnya.
    b. Contoh: ASN bagian keuangan bisa menerima email palsu khusus tentang "anggaran daerah" karena pelaku tahu jabatannya.
    c. Masyarakat yang aktif di *marketplace* bisa menerima pesan khusus tentang transaksi terakhir mereka, padahal itu jebakan.

Dengan tren *phishing* di 2025 ini, **ASN perlu lebih disiplin dalam mengikuti SOP keamanan**, dan **masyarakat perlu lebih kritis terhadap setiap pesan yang diterima**, meskipun terlihat meyakinkan.

D. Dampak Phishing

Phishing sering dianggap sekadar "penipuan online biasa". Padahal dampaknya bisa sangat serius, baik terhadap **pemerintahan daerah** maupun kehidupan sehari-hari masyarakat.

1. **Dampak bagi ASN dan Pemerintah Daerah**
    a. **Kebocoran Data Publik**, Data kependudukan (NIK, KK), dokumen perencanaan, hingga arsip keuangan bisa diakses pihak tak bertanggung jawab. Jika bocor, data ini berpotensi dijual di forum gelap atau dimanfaatkan untuk tindak kriminal.
    b. **Gangguan Layanan Publik**, Jika akun ASN diretas melalui *phishing*, pelaku bisa masuk ke sistem administrasi. Akibatnya, layanan digital seperti perizinan, kependudukan, atau keuangan bisa terganggu bahkan lumpuh sementara.
    c. **Kerugian Finansial bagi Pemerintah Daerah**, Pemulihan pasca-insiden membutuhkan biaya besar, mulai dari perbaikan server, audit keamanan, hingga sosialisasi ulang ke masyarakat.

d. **Turunnya Kepercayaan Publik**, Jika masyarakat tahu bahwa data mereka tidak aman di tangan pemerintah daerah, tingkat kepercayaan terhadap layanan digital akan turun drastis. Akibatnya, transformasi digital daerah bisa terhambat.

2. **Dampak bagi Masyarakat**
   a. **Kehilangan Uang**, Korban sering diarahkan untuk mentransfer uang ke rekening penipu, atau data rekeningnya dicuri sehingga saldo terkuras.
   b. **Pencurian Identitas**, NIK, nomor rekening, hingga akun media sosial bisa dipakai untuk pinjaman online ilegal, pembukaan rekening fiktif, atau tindak kriminal lain.
   c. **Akun Digital Diambil Alih**, WhatsApp, email, atau akun *marketplace* korban bisa diretas. Setelah itu, pelaku sering menggunakan akun tersebut untuk menipu teman/keluarga korban.
   d. **Dampak Psikologis**, Selain kerugian finansial, banyak korban mengalami trauma, malu, bahkan takut menggunakan layanan digital lagi. Ini bisa menurunkan tingkat adopsi masyarakat terhadap layanan publik berbasis teknologi.
3. **Dampak bagi Negara secara Luas**

   Phishing tidak hanya merugikan individu atau instansi, tetapi juga bisa mengancam **ketahanan siber nasional**. Jika serangan meluas, kepercayaan internasional terhadap keamanan digital Indonesia bisa melemah, dan ini berdampak pada investasi maupun kerja sama digital.

Dari sini terlihat bahwa *phishing* bukan sekadar pesan iseng, tetapi **ancaman serius yang bisa menimbulkan kerugian finansial, sosial, dan reputasi** baik bagi ASN maupun masyarakat.

E. Cara Mendeteksi Phishing

Phishing sengaja dirancang agar terlihat mirip dengan pesan resmi. Namun, selalu ada tanda-tanda yang bisa dikenali jika kita teliti. Berikut beberapa cara mendeteksinya:

1. **Perhatikan Alamat Pengirim**
    a. **ASN:** pastikan email resmi selalu menggunakan domain pemerintah, misalnya @klungkungkab.go.id. Jika ada variasi aneh (contoh: @klungkungkab.co.id atau @gmail.com), patut dicurigai.
    b. **Masyarakat:** waspada jika ada pesan WhatsApp mengaku dari bank/ojol tetapi nomor yang digunakan adalah nomor pribadi, bukan nomor resmi yang sudah diverifikasi centang hijau.
2. **Cek Tautan (Link) dengan Teliti**

    Banyak pesan *phishing* berisi tautan palsu. **Cara mengecek:** arahkan kursor ke link (jangan langsung klik) → lihat alamat sebenarnya. Jika alamatnya panjang, aneh, atau tidak sesuai dengan situs resmi, itu indikasi *phishing*. Contoh: https://bank-indonesia.verifikasi.com bukanlah alamat resmi Bank Indonesia.
3. **Waspadai Bahasa yang Mendesak atau Mengancam**

    Phishing sering menggunakan kalimat seperti:
    a. "Akun Anda akan diblokir dalam 24 jam!"
    b. "Segera transfer agar transaksi tidak dibatalkan!"

    Pesan resmi pemerintah atau bank tidak pernah menggunakan ancaman atau paksaan.
4. **Periksa Lampiran atau File**
    a. **ASN:** jangan sembarangan membuka lampiran (misalnya .zip atau .exe) dari email yang tidak jelas. File itu bisa berisi malware.
    b. **Masyarakat:** hati-hati jika ada file dari WA/SMS mengaku sebagai undangan pernikahan, voucher hadiah, atau update aplikasi. Banyak di antaranya mengandung virus.

5. **Verifikasi dengan Sumber Resmi**

   Jika ragu, **hubungi langsung instansi atau pihak resmi** melalui nomor/website yang tercantum di sumber terpercaya.

   a. **ASN:** laporkan ke tim IT atau CSIRT daerah.
   b. **Masyarakat:** hubungi call center bank atau instansi terkait, jangan membalas pesan mencurigakan.

6. **Gunakan Fitur Keamanan Digital**

   Aktifkan ***two-factor authentication*** **(2FA)** di email, media sosial, dan aplikasi keuangan. Gunakan antivirus dan pastikan aplikasi diperbarui secara rutin.

Dengan membiasakan diri memeriksa hal-hal di atas, ASN dan masyarakat akan lebih siap menghadapi *phishing*, meskipun serangannya makin canggih di tahun 2025.

F. Contoh Kasus Phishing Terkini (2023–2025) di Indonesia

Agar lebih mudah dipahami, berikut beberapa kasus *phishing* yang sempat ramai di Indonesia dalam 2 tahun terakhir.

1. **Phishing Bank Digital (2023–2024)**
   a. **Modus:** korban menerima SMS atau WhatsApp yang mengaku dari bank digital populer. Pesan berisi tautan ke halaman login palsu.
   b. **Tujuan:** mencuri *username*, *password*, dan kode OTP untuk menguras saldo rekening.
   c. **Dampak:** ribuan nasabah melapor kehilangan dana karena tanpa sadar mengisi data di situs palsu.
2. **Pesan WhatsApp Palsu Kurir Paket (2023)**
   a. **Modus:** pesan masuk mengaku dari jasa ekspedisi (JNE, J&T, Pos Indonesia) yang menyebutkan paket tidak bisa dikirim karena “alamat salah” atau “butuh verifikasi”.

b. **Ciri khas:** link yang diberikan mengarah ke aplikasi berbahaya, bukan situs resmi.
c. **Dampak:** HP korban terkunci oleh malware atau data pribadi dicuri.

3. **Penipuan Lowongan Kerja ASN Palsu (2024)**
   a. **Modus:** calon korban mendapat pesan/email lowongan kerja ASN dengan logo resmi kementerian/instansi, disertai link pendaftaran palsu.
   b. **Tujuan:** mencuri data pribadi seperti KTP, KK, dan ijazah.
   c. **Dampak:** data bocor bisa dipakai untuk pemalsuan dokumen atau pinjaman online ilegal.
4. **Phishing melalui Media Sosial (2024–2025)**
   a. **Modus:** akun palsu yang mirip akun resmi instansi pemerintah membuat postingan berisi tautan pendaftaran bantuan sosial (bansos) atau subsidi internet.
   b. **Tujuan:** mengumpulkan data masyarakat (NIK, nomor rekening).
   c. **Dampak:** banyak masyarakat terjebak karena mengira program itu resmi dari pemerintah.
5. **Serangan Phishing Hybrid (2025)**
   a. **Modus terbaru:** penyerang menggabungkan beberapa saluran (SMS, WA, email, media sosial) secara bersamaan. Misalnya, korban mendapat email berisi tautan, lalu ditelepon langsung oleh pelaku yang berpura-pura petugas bank untuk meyakinkan.
   b. **Ciri khas:** tampak sangat meyakinkan, bahkan menggunakan bahasa formal dan logo resmi.
   c. **Dampak:** korban lebih mudah percaya karena “terdorong” dari banyak arah sekaligus.

Kasus-kasus ini menunjukkan bahwa *phishing* semakin **canggih, bervariasi, dan menyasar semua lapisan masyarakat maupun ASN**. Karena itu, kewaspadaan dan literasi digital menjadi kunci pencegahan.

G. Langkah Pencegahan Praktis untuk ASN & Masyarakat

Mencegah lebih baik daripada menyesal setelah menjadi korban *phishing*. Berikut beberapa langkah sederhana namun efektif:

1. **Selalu Gunakan Sumber Resmi**
    a. **ASN:** gunakan aplikasi dan email resmi pemerintah dengan domain .go.id. Jangan mengakses tautan dari sumber tidak jelas.
    b. **Masyarakat:** hanya gunakan situs/akun resmi bank, *marketplace*, atau instansi (cek centang biru atau domain resmi).
2. **Jangan Mudah Percaya dengan Pesan Mendesak**

    Hindari terburu-buru. Jika ada pesan mengaku dari bank/instansi dengan ancaman akun akan diblokir, **tenang dan verifikasi** ke call center resmi.
3. **Amankan Identitas Digital**

    Jangan pernah membagikan **NIK, nomor rekening, OTP, atau *password*** kepada siapa pun.
    a. **ASN:** jangan mengunggah dokumen resmi ke platform sembarangan.
    b. **Masyarakat:** jangan posting foto KTP/KK di media sosial meskipun untuk syarat tertentu.
4. **Gunakan Password Kuat & 2FA**
    a. Gunakan *password* kombinasi huruf, angka, simbol.
    b. Aktifkan ***two-factor authentication*** **(2FA)** di email, WhatsApp, dan aplikasi perbankan.
5. **Laporkan Insiden Segera**
    a. **ASN:** laporkan ke CSIRT (*Computer Security Incident Response Team*) daerah jika ada email mencurigakan.
    b. **Masyarakat:** segera hubungi bank, operator, atau instansi terkait jika akun atau data terancam.
6. **Edukasi Lingkungan Sekitar**
    a. **ASN:** bagikan informasi keamanan siber di instansi.

b. **Masyarakat:** saling mengingatkan keluarga/teman agar tidak mudah percaya pesan palsu.

7. Perbarui Sistem & Aplikasi

Pastikan HP, laptop, dan aplikasi selalu diperbarui untuk menutup celah keamanan yang bisa dimanfaatkan penjahat siber.

Jika langkah-langkah ini diterapkan secara konsisten, maka ASN dan masyarakat Klungkung akan lebih siap menghadapi serangan *phishing* yang semakin canggih di tahun 2025.

Pertanyaan Reflektif

1. Pernahkah Anda atau instansi Anda menerima email/WA mencurigakan yang mengaku dari pihak resmi? Apa reaksi pertama Anda saat itu?
2. Menurut Anda, apa yang lebih berbahaya: tautan palsu dalam pesan *phishing* atau ajakan pelaku lewat telepon langsung (*voice phishing*)? Mengapa?
3. Jika suatu hari Anda tidak sengaja membuka tautan *phishing*, apa langkah pertama yang paling tepat dilakukan agar kerugian bisa diminimalkan?
4. Sebagai ASN atau masyarakat, siapa pihak pertama yang akan Anda hubungi bila mendapati indikasi *phishing*?
5. Menurut pengalaman Anda, mengapa masih banyak orang yang percaya pesan *phishing* meskipun sudah sering ada peringatan dari pemerintah dan media?

CORPU
KIWA TENGEN

DAFTAR PUSTAKA

Fitrian, H. P., Abidah, L., Zahra, K. W., & Hafidudin, W. H. (2025). PENGARUH KESADARAN PENGGUNA TERHADAP KEBERHASILAN SERANGAN PHISHING DI JARINGAN PERBANKAN. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(2), 1888–1892.

Jamaludin, A., & Permana, F. A. (2023). Personal Data Vulnerability in the Digital Era: Study of Modus Operandi and Mechanisms to Prevent Phishing Crimes. *Jurnal Al-Hakim: Jurnal Ilmiah Mahasiswa, Studi Syariah, Hukum Dan Filantropi*, *5*(2), 201–216. https://doi.org/10.22515/jurnalalhakim.v5i2.7074

Lokapala, Y. H., Nurfauzi, F. J., & Widowaty, Y. (2024). Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia. *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, *5*(1), 19–24. https://doi.org/10.18196/ijclc.v5i1.19853

Nur'aini, R. J., & Simanjuntak, M. (2025). Phishing Awareness and Security Concerns: Analyzing the Role of Anti-Phishing Knowledge and Internet Experience in Online Banking Users. *Jurnal Ilmu Keluarga Dan Konsumen*, *18*(2), 121–133. https://doi.org/10.24156/jikk.2025.18.2.121

Nurmansyah, G., Natamiharja, R., & Setiawan, I. (2025). Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach. *Pancasila and Law Review*, *6*(1), 15–44.

Wijaya, L., & Nurnawati, E. K. (2022). Analisis Kesadaran Mahasiswa YogyakartaTentang Phishing Pada Online Banking. *Jurnal Dinamika Informatika*, *11*(2), 113–122.