KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 2: Ancaman Siber yang Sering Terjadi

Subtopik 2.2: Malware & Ransomware

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

Tujuan Pembelajaran

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

1. Menjelaskan pengertian phishing dengan contoh nyata yang relevan.
2. Mengidentifikasi bentuk-bentuk phishing yang umum terjadi di Indonesia (2023–2025).
3. Menyadari tren baru phishing yang semakin canggih, termasuk penggunaan AI dan deepfake.
4. Menjelaskan dampak phishing terhadap ASN, masyarakat, dan sistem pemerintahan daerah.
5. Menentukan langkah praktis pencegahan serta tindakan awal jika terpapar phishing.

Sasaran Peserta

1. ASN: Agar mampu mengenali pesan phishing yang menargetkan data instansi, menjaga kerahasiaan sistem, serta segera melaporkan insiden sesuai prosedur.
2. Masyarakat: Agar lebih berhati-hati terhadap pesan palsu, tidak mudah membagikan data pribadi, dan mampu melindungi diri serta lingkungan dari potensi penipuan daring.

A. Definisi Malware & Ransomware

1. Apa itu Malware?

Malware merupakan singkatan dari ***malicious software***, yaitu **perangkat lunak berbahaya** yang dirancang untuk merusak, mengambil alih, atau mencuri data dari perangkat digital tanpa izin pengguna. *Malware* dapat menyusup ke komputer, laptop, atau ponsel melalui banyak cara, misalnya lewat lampiran email mencurigakan, situs palsu, aplikasi bajakan, atau bahkan perangkat penyimpanan eksternal seperti flashdisk. Bagi **ASN**, *malware* menjadi ancaman serius karena dapat menyerang sistem administrasi pemerintahan, aplikasi pelayanan publik, dan jaringan kantor. Jika *malware* berhasil masuk, bukan hanya data pribadi ASN yang terancam, tetapi juga dokumen penting seperti arsip kependudukan, laporan keuangan, dan surat resmi dinas. Sementara bagi **masyarakat**, *malware* biasanya muncul lewat tautan atau file yang tampak menarik, seperti "update aplikasi", "hadiah undian", atau "voucher gratis". Begitu dibuka, *malware* akan bekerja di latar belakang, mencuri data pribadi seperti NIK, foto KTP, dan akun media sosial tanpa disadari pengguna.

Secara umum, *malware* dapat dibagi menjadi beberapa jenis:

a. Virus**:** Menyebar dengan cara menempel pada file atau program lain, lalu merusak data.
b. Trojan**:** Menyamar sebagai program yang tampak berguna, padahal membuka akses bagi peretas.
c. Spyware**:** Mengintai aktivitas pengguna, mencatat ketikan (keylogger), dan mengirim informasi ke pihak lain.
d. Adware**:** Menampilkan iklan berlebihan yang bisa mengarahkan ke situs berbahaya.
e. Worm**:** Menyebar otomatis ke perangkat lain dalam jaringan tanpa interaksi pengguna.

Malware tidak hanya menyerang komputer besar atau server pemerintah, tetapi juga perangkat pribadi seperti ponsel. Tahun 2025 mencatat peningkatan signifikan *malware mobile* di Indonesia, terutama yang menyamar sebagai aplikasi keuangan atau e-commerce.

2. Apa itu Ransomware?

Ransomware adalah jenis *malware* yang **mengunci atau mengenkripsi data korban**, kemudian meminta tebusan (ransom) agar data bisa diakses kembali. Serangan ini sering disebut sebagai **"pencurian digital modern"**, karena pelaku tidak mengambil barang fisik, melainkan menahan data penting hingga korban membayar uang tebusan, biasanya dalam bentuk mata uang kripto seperti Bitcoin.

Dalam konteks **pemerintahan daerah**, *ransomware* merupakan ancaman nyata yang dapat melumpuhkan pelayanan publik. Misalnya, jika server data kependudukan atau sistem keuangan daerah terinfeksi, maka seluruh proses administrasi bisa berhenti. Bagi **masyarakat**, serangan *ransomware* bisa terjadi di perangkat pribadi, misalnya laptop atau ponsel yang digunakan untuk menyimpan dokumen, foto, atau catatan penting. Ketika file terkunci, korban tidak dapat membukanya tanpa "kunci digital" dari pelaku.

Ciri-ciri umum perangkat yang terinfeksi *ransomware* antara lain:

a. File tiba-tiba tidak bisa dibuka dan berubah ekstensi (misalnya dari .docx menjadi .locked).
b. Muncul pesan di layar yang meminta pembayaran agar data bisa dipulihkan.
c. Perangkat menjadi sangat lambat atau tidak merespons.

Serangan *ransomware* di Indonesia meningkat tajam sejak 2023, terutama terhadap rumah sakit, universitas, dan kantor pemerintahan. Tahun 2025, tren ini semakin kompleks dengan munculnya ***ransomware-as-a-service*** **(RaaS)**, model bisnis di mana kelompok peretas menyediakan "paket *ransomware* siap pakai" yang bisa digunakan siapa pun dengan mudah. Ini membuat serangan semakin sering dan sulit dilacak.

3. Mengapa ASN dan Masyarakat Harus Waspada?

Karena *malware* dan *ransomware* tidak mengenal batas jabatan atau profesi. Setiap perangkat yang terhubung ke internet bisa menjadi target.

a. **ASN** harus menjaga sistem pemerintah agar tidak terganggu oleh serangan digital. Kebocoran atau gangguan data pelayanan publik bisa menurunkan kepercayaan masyarakat terhadap instansi.
b. **Masyarakat** perlu sadar bahwa data pribadi seperti NIK, nomor rekening, dan foto dokumen resmi memiliki nilai ekonomi tinggi di dunia maya. Sekali bocor, sulit dikendalikan dampaknya.

Dengan memahami pengertian *malware* dan *ransomware* secara benar, ASN dan masyarakat dapat lebih siap untuk mengenali tanda-tanda awal serangan dan melakukan langkah pencegahan sebelum terlambat.

B. Jenis-Jenis Malware yang Umum Ditemukan

Malware tidak hanya satu jenis, dan cara kerjanya pun berbeda-beda. Setiap jenis memiliki tujuan tertentu, mulai dari mencuri data hingga merusak sistem komputer. Memahami jenis-jenisnya membantu ASN dan masyarakat mengenali tanda-tanda bahaya lebih cepat sebelum kerugian terjadi.

Berikut adalah beberapa jenis *malware* yang paling sering ditemukan di Indonesia:

1. Virus Komputer

Virus merupakan jenis *malware* tertua dan paling dikenal. Cara kerjanya mirip dengan virus biologis menempel pada file atau program, lalu menyebar ke seluruh sistem. Begitu dijalankan, virus dapat merusak file, menghapus data penting, atau membuat komputer menjadi lambat.

a. **Contoh kasus:** File laporan ASN rusak setelah membuka lampiran dari email yang tidak dikenal.
b. **Tanda-tanda umum:** Komputer sering *crash*, muncul pesan error aneh, dan file hilang atau tidak bisa dibuka.

2. Trojan Horse (Kuda Troya)

Trojan adalah *malware* yang menyamar sebagai program berguna, padahal berisi kode berbahaya. Namanya diambil dari kisah Yunani kuno, musuh yang bersembunyi di dalam hadiah kuda kayu. Di dunia digital, Trojan sering disamarkan sebagai *software update*, *dokumen penting*, atau *aplikasi gratis*. Saat dibuka, Trojan membuka "pintu belakang" (backdoor) yang memberi akses ke peretas untuk mengendalikan perangkat korban.

a. **Contoh kasus:** Email palsu mengaku dari "Dinas Kepegawaian" berisi file .zip. Setelah dibuka, sistem komputer kantor langsung lambat dan data tersalin otomatis.

3. Spyware

Spyware dirancang untuk **memata-matai aktivitas pengguna** tanpa izin. Program ini mencatat informasi seperti situs yang dikunjungi, isi pesan, bahkan setiap huruf yang diketik di keyboard (keylogger).

a. **Dampak:** Data login ASN atau masyarakat bisa dicuri tanpa terasa.
b. **Ciri-ciri:** Laptop tiba-tiba lambat, muncul iklan tidak wajar, dan baterai cepat habis.

Spyware sering ditemukan pada aplikasi gratis atau versi bajakan, karena pengguna tidak membaca izin akses dengan teliti.

4. Adware

Adware menampilkan iklan pop-up secara berlebihan di perangkat. Meski tampak hanya mengganggu, beberapa adware justru menjadi pintu masuk *malware* lain atau mengarahkan pengguna ke situs palsu.

a. **Contoh:** Masyarakat yang mengunduh aplikasi "penghemat baterai" dari situs tidak resmi malah mendapat iklan judi online terus-menerus.
b. **Pencegahan:** Hindari menginstal aplikasi dari sumber tidak jelas dan gunakan pemblokir iklan (ad blocker).

5. Worm (Cacing Digital)

Worm adalah *malware* yang bisa menyebar secara otomatis tanpa bantuan pengguna. Ia menyebar melalui jaringan Wi-Fi, email, atau flashdisk yang terhubung antarperangkat.

Jika satu komputer kantor terinfeksi, worm bisa berpindah ke seluruh jaringan instansi dalam hitungan menit.

a. **Contoh:** Salah satu komputer di dinas terinfeksi worm, lalu seluruh printer dan server ikut bermasalah.
b. **Solusi:** Gunakan antivirus dengan perlindungan jaringan (network protection).

6. Rootkit

Rootkit adalah jenis *malware* yang menyembunyikan dirinya sangat dalam di sistem, sehingga sulit terdeteksi oleh antivirus biasa. Tujuannya untuk memberikan akses penuh kepada peretas tanpa terlihat.

a. **Dampak:** Data pemerintah bisa diambil secara diam-diam tanpa disadari ASN yang bertugas.
b. **Ciri-ciri:** Perangkat sering restart sendiri, pengaturan berubah tanpa sebab, dan antivirus tidak bisa dijalankan.

7. Botnet

Botnet adalah jaringan komputer yang sudah terinfeksi *malware* dan dikendalikan dari jarak jauh oleh pelaku. Biasanya digunakan untuk melancarkan serangan besar seperti **DDoS (Distributed Denial of Service)** yakni membanjiri server dengan permintaan palsu hingga layanan digital lumpuh.

a. **Contoh:** Situs pelayanan publik daerah tidak bisa diakses selama beberapa jam akibat serangan DDoS.
b. **Pencegahan:** Gunakan firewall dan pastikan perangkat selalu diperbarui.

💡 **Catatan Tren 2025:**

Badan Siber dan Sandi Negara (BSSN) mencatat peningkatan signifikan pada ***malware* berbasis mobile** dan ***ransomware* hibrida**. Serangan kini tidak lagi hanya menargetkan komputer kantor, tapi juga perangkat pribadi ASN dan masyarakat.

C. Ransomware: Ancaman yang Meningkat di Tahun 2025

Ransomware adalah salah satu bentuk ***malware* paling berbahaya di era digital saat ini**. Berbeda dengan virus atau spyware yang bekerja diam-diam, *ransomware* **menyerang secara langsung dan memblokir akses ke data korban**. Setelah data dikunci, pelaku akan meminta uang tebusan agar akses bisa dipulihkan.

Istilah "*ransomware*" berasal dari kata *ransom* (tebusan) dan *software* (perangkat lunak). Artinya, perangkat lunak ini secara sengaja dibuat untuk **menahan data penting seseorang atau organisasi demi keuntungan finansial pelaku**.

1. Cara Kerja Ransomware

Serangan *ransomware* biasanya berlangsung dalam tiga tahap:

a. Infeksi Awal

Terjadi ketika pengguna mengklik tautan, membuka lampiran email, atau mengunduh file dari sumber tidak resmi. *Ransomware* masuk ke sistem dan mulai mengenkripsi (mengunci) file penting tanpa sepengetahuan korban.

b. Enkripsi Data

Semua file seperti dokumen, foto, laporan, atau database berubah menjadi format acak yang tidak bisa dibuka. File sering berganti ekstensi (misalnya .xlsx menjadi .locked atau .crypt).

c. Permintaan Tebusan

Muncul pesan di layar yang meminta korban membayar uang tebusan, biasanya menggunakan mata uang kripto seperti Bitcoin agar sulit dilacak. Jika korban tidak membayar dalam waktu tertentu, pelaku mengancam akan menghapus data atau menyebarkannya ke publik.

2. Jenis-Jenis Ransomware yang Sering Menyerang

a. *Crypto Ransomware*

Mengunci data di komputer korban dan hanya bisa dibuka dengan "kunci" yang dimiliki pelaku. Jenis ini paling umum menyerang kantor pemerintahan dan rumah sakit.

b. *Locker Ransomware*

Tidak mengenkripsi file, tetapi mengunci seluruh sistem operasi sehingga komputer tidak bisa digunakan sama sekali.

c. *Scareware*

Menipu korban dengan pesan palsu seolah komputer terinfeksi virus berat. Korban disuruh membayar untuk "membersihkan" perangkat, padahal tidak ada virus.

d. *Double Extortion Ransomware* (Tekanan Ganda)

Tren 2025: Pelaku tidak hanya mengenkripsi data, tetapi juga **mencuri dan mengancam membocorkan** data ke publik jika tebusan tidak dibayar. Jenis ini sangat berbahaya bagi instansi pemerintahan karena bisa menyebabkan kebocoran data sensitif.

3. Sasaran Utama di Tahun 2025

a. Instansi Pemerintah Daerah (Pemda):

Karena banyak sistem pelayanan publik sudah digital, seperti *e-Office*, Siak, dan aplikasi keuangan daerah. ASN menjadi target utama karena memiliki akses langsung ke dokumen penting.

b. Sektor Kesehatan dan Pendidikan:

Rumah sakit dan kampus sering diserang karena memiliki data pribadi pasien dan mahasiswa yang bernilai tinggi.

c. Masyarakat Umum:

Ransomware kini juga menyerang ponsel melalui aplikasi palsu atau file unduhan. Pelaku mengenkripsi foto, dokumen, atau kontak dan meminta tebusan dalam jumlah kecil agar korban cepat membayar.

4. Mengapa Ransomware Semakin Berbahaya?

a. Mudah Dijalankan: Kini ada layanan *Ransomware-as-a-Service (RaaS)*, di mana siapa pun bisa "menyewa" *ransomware* siap pakai dari kelompok peretas di internet gelap.
b. Sulit Dilacak: Pembayaran dilakukan dengan kripto, membuat pelaku sulit ditemukan.
c. Target Meluas: Tidak hanya perusahaan besar, tapi juga lembaga kecil dan individu biasa.
d. Kombinasi Serangan: Banyak pelaku menggabungkan *ransomware* dengan phishing atau *malware* lain agar hasilnya lebih efektif.

Ransomware di tahun 2025 bukan lagi ancaman masa depan, **ia sudah menjadi kenyataan yang mengancam keamanan data pemerintahan dan masyarakat setiap hari**. Kesadaran, kewaspadaan, dan tindakan cepat menjadi benteng utama menghadapi serangan ini.

D. Dampak Serangan Malware dan Ransomware

Serangan *malware* dan *ransomware* tidak hanya merusak perangkat, tetapi juga bisa menimbulkan efek berantai terhadap pelayanan publik, keamanan data, dan kepercayaan masyarakat. Di era digital seperti tahun 2025, dampaknya tidak lagi terbatas pada satu komputer, melainkan bisa menyebar ke seluruh jaringan instansi atau bahkan antarwilayah.

1. Dampak bagi ASN dan Instansi Pemerintah
   a. Gangguan Layanan Publik

      Ketika sistem pemerintahan terinfeksi *ransomware*, aplikasi pelayanan publik seperti *e-Office*, administrasi kependudukan, atau sistem keuangan

bisa lumpuh. Masyarakat tidak bisa mengakses layanan dasar seperti pembuatan KTP, izin usaha, atau surat administrasi. Contoh: serangan *ransomware* yang menonaktifkan sistem kependudukan daerah menyebabkan antrean panjang di kantor pelayanan karena data tidak bisa diakses.

b. Kebocoran dan Hilangnya Data Penting

Malware bisa mencuri dokumen internal instansi, data pegawai, hingga arsip perencanaan daerah. Jika data ini bocor, pelaku bisa menjualnya di forum gelap atau menggunakannya untuk manipulasi digital. Dampak jangka panjang: berkurangnya kepercayaan publik terhadap keamanan data pemerintah.

c. Kerugian Finansial dan Operasional

Pemulihan sistem setelah serangan memerlukan biaya besar: audit keamanan, pembelian perangkat baru, hingga pelatihan ulang pegawai. Selain itu, waktu pelayanan yang terbuang menimbulkan kerugian tidak langsung bagi masyarakat.

d. Reputasi Instansi Menurun

Masyarakat akan menilai instansi yang terkena serangan sebagai tidak siap secara digital. Hal ini bisa menurunkan kepercayaan publik terhadap layanan berbasis teknologi dan membuat masyarakat ragu menggunakan aplikasi resmi pemerintah.

2. Dampak bagi Masyarakat

a. Kehilangan Data Pribadi

Malware dapat mencuri data penting seperti NIK, KK, nomor rekening, dan dokumen pribadi. *Ransomware* bahkan bisa mengunci seluruh file di HP atau laptop sehingga tidak dapat diakses lagi. Contoh nyata: masyarakat yang kehilangan akses ke file pekerjaan atau foto keluarga karena terkena *ransomware* dari aplikasi bajakan.

b. Kerugian Finansial

Banyak korban yang terjebak membayar tebusan atau kehilangan saldo rekening setelah membuka tautan mencurigakan. Pelaku sering meminta nominal yang tampak kecil agar korban tergoda untuk segera membayar.

c. Penyalahgunaan Identitas

Data pribadi yang bocor dapat digunakan untuk tindakan ilegal, seperti pinjaman online atas nama korban, pembuatan akun palsu, atau penipuan di media sosial.

d. Dampak Psikologis dan Sosial

Selain kerugian materi, korban sering merasa malu, stres, dan kehilangan rasa percaya terhadap teknologi digital. Hal ini bisa menghambat adopsi layanan publik berbasis online di daerah.

3. Dampak bagi Pemerintahan dan Negara

Serangan *malware* dan *ransomware* terhadap sistem pemerintahan daerah bukan hanya masalah teknis, tetapi juga **masalah strategis nasional**. Jika banyak instansi daerah lumpuh bersamaan, koordinasi layanan publik bisa terganggu. Kebocoran data warga dapat melemahkan keamanan nasional di ruang siber. Reputasi pemerintah di mata masyarakat maupun mitra internasional bisa menurun.

4. Dampak Jangka Panjang

a. **Menurunnya Kepercayaan Digital:** Masyarakat ragu menggunakan aplikasi pemerintah.

b. **Biaya Pemulihan Besar:** Pemerintah daerah perlu waktu lama dan biaya tinggi untuk memulihkan sistem.

c. **Risiko Reinfeksi:** Jika sistem tidak diperbarui dengan benar, serangan dapat terulang.

E. Contoh Kasus Terkini (Indonesia 2023-2025)

Ancaman *malware* dan *ransomware* di Indonesia terus meningkat setiap tahun. Data dari **Badan Siber dan Sandi Negara (BSSN)** menunjukkan bahwa serangan siber dengan pola *ransomware* dan *malware* menjadi salah satu insiden paling sering dilaporkan oleh instansi pemerintahan maupun sektor swasta. Berikut beberapa contoh kasus aktual yang dapat menjadi pembelajaran bagi ASN dan masyarakat.

1. **Serangan Ransomware pada Rumah Sakit (2023)**

   Kronologi: Beberapa rumah sakit di Jawa dan Sulawesi mengalami serangan *ransomware* yang menyebabkan sistem rekam medis tidak bisa diakses selama beberapa hari. Semua data pasien terkunci dan pelayanan harus dilakukan secara manual.

   Dampak: Penundaan tindakan medis, hilangnya sebagian data, dan meningkatnya beban kerja petugas.

   Pelajaran: *Ransomware* tidak hanya menyerang lembaga keuangan, tetapi juga layanan vital seperti kesehatan. Backup data berkala dan pembaruan sistem sangat penting.

2. **Serangan ke Pemerintah Daerah (2024)**

   Kronologi: Beberapa pemerintah kabupaten dan kota melaporkan gangguan serius pada server data perizinan dan kepegawaian akibat *ransomware*. Pelaku meminta tebusan dalam bentuk Bitcoin senilai ratusan juta rupiah.

   Dampak: Layanan digital tidak bisa diakses masyarakat selama hampir satu minggu. ASN tidak dapat mengunggah laporan dan masyarakat tidak bisa memproses perizinan.

   Pelajaran: Pemerintah daerah perlu memiliki **CSIRT (Computer Security Incident Response Team)** aktif dan sistem cadangan (backup) offline untuk mengantisipasi situasi darurat.

3. **Malware di Aplikasi Bajakan (2023–2025)**

   Kronologi: Banyak masyarakat tanpa sadar memasang aplikasi bajakan di HP

atau laptop, seperti versi gratis dari perangkat lunak premium. Sebagian besar aplikasi tersebut ternyata berisi *malware* pengintai data.

Dampak: Data login, kontak, dan foto pribadi tersimpan di server asing tanpa izin pengguna.

Pelajaran: Gunakan hanya aplikasi resmi dari Google Play Store, App Store, atau penyedia terpercaya. Versi bajakan bisa jadi lebih berbahaya daripada sekadar ilegal.

4. **Kasus Email Dinas Terinfeksi Trojan (2024)**

   Kronologi: Seorang ASN menerima email dengan subjek "Surat Edaran Terbaru Mendagri". File lampiran berformat .docx ternyata berisi Trojan yang secara otomatis mengirim salinan data ke pihak luar negeri.

   Dampak: Beberapa dokumen internal bocor, dan butuh waktu untuk membersihkan sistem instansi.

   Pelajaran: ASN perlu lebih berhati-hati membuka email, bahkan jika terlihat datang dari instansi resmi. Selalu cek domain pengirim dan laporkan ke tim IT jika mencurigakan.

5. **Ransomware di Laptop Pribadi (2025)**

   Kronologi: Seorang masyarakat di Bali melaporkan laptopnya terkunci setelah mengunduh file undangan dari grup WhatsApp. Semua foto dan dokumen berubah ekstensi dan muncul pesan tebusan.

   Dampak: Kehilangan data pribadi dan kerugian finansial karena korban sempat membayar tebusan.

   Pelajaran: Jangan pernah membuka lampiran dari sumber tak dikenal, dan rutin lakukan **backup data penting** di penyimpanan eksternal.

6. **Serangan Hybrid (Gabungan) 2025**

   Kronologi: Jenis serangan terbaru memadukan ***phishing + ransomware + trojan***. Pelaku mengirim tautan melalui email palsu, yang setelah diklik langsung menanam *malware* dan mengenkripsi data korban.

Dampak: Serangan jenis ini lebih sulit dideteksi karena menggunakan kecerdasan buatan (AI) untuk menyamarkan jejak.

Pelajaran: Keamanan digital tidak cukup hanya dengan antivirus, tapi memerlukan kewaspadaan manusia sebagai "tembok pertama" pertahanan.

Serangan siber bukan lagi hal yang jauh dari kehidupan sehari-hari. Baik ASN maupun masyarakat harus sadar bahwa **setiap perangkat digital adalah pintu masuk potensial bagi kejahatan siber**. Kedisiplinan, kehati-hatian, dan kebiasaan digital yang aman adalah benteng paling kuat untuk melindungi diri.

F. Cara Pencegahan yang Efektif

Serangan *malware* dan *ransomware* tidak hanya bisa dicegah dengan teknologi, tetapi juga dengan **perilaku digital yang disiplin dan bijak**. Pencegahan harus dilakukan di semua level individu, instansi, dan masyarakat karena ruang digital saling terhubung. Berikut langkah-langkah pencegahan yang paling relevan:

1. **Gunakan Perangkat dan Aplikasi Resmi**
    a. Unduh aplikasi hanya dari sumber terpercaya seperti **Google Play Store, App Store, atau situs resmi pengembang.**
    b. Hindari aplikasi bajakan (cracked software), karena 7 dari 10 aplikasi ilegal mengandung *malware* tersembunyi.
    c. ASN wajib memastikan bahwa aplikasi yang digunakan untuk pekerjaan berasal dari **kanal resmi instansi atau pemerintah pusat (misalnya BSSN, Kominfo, atau CSIRT Daerah).**

    💡 *Contoh baik:* Gunakan sistem surat elektronik resmi dengan domain pemerintah (.go.id) daripada email gratisan untuk surat menyurat kedinasan.
2. **Rutin Melakukan Pembaruan Sistem dan Antivirus**
    a. Pastikan sistem operasi (Windows, Android, iOS, Linux) selalu diperbarui secara otomatis.
    b. Gunakan antivirus dan aktifkan fitur **real-time protection**.

c. Untuk instansi pemerintah, disarankan memiliki sistem pemantauan terpusat agar bisa mendeteksi ancaman lebih cepat.

📌 *Catatan:* Banyak *ransomware* memanfaatkan **celah keamanan lama** yang sebenarnya sudah diperbaiki lewat pembaruan, tapi belum dipasang oleh pengguna.

3. **Waspadai Email dan Tautan Mencurigakan**
   a. Jangan asal klik tautan (link) atau unduhan dari email tak dikenal.
   b. Cek alamat pengirim banyak pelaku memalsukan nama domain agar terlihat seperti instansi resmi.
   c. Jika ragu, **konfirmasi ke rekan kerja atau instansi terkait** sebelum membuka lampiran.

🧠 *Ingat: Ransomware* sering kali masuk lewat file yang tampak biasa, seperti "Surat Edaran", "Invoice", atau "Laporan Keuangan".

4. **Lakukan Backup Data Secara Rutin**
   a. Simpan salinan data penting di media eksternal (hard drive, flashdisk, atau penyimpanan cloud yang aman).
   b. Gunakan prinsip **3-2-1 Backup:** 3 salinan data, 2 media penyimpanan berbeda, dan 1 disimpan di lokasi terpisah.
   c. Pastikan data cadangan tidak selalu terhubung ke internet agar tidak ikut terinfeksi.

🔐 *Contoh:* Instansi pemerintah bisa menjadwalkan backup mingguan untuk server dan sistem administrasi.

5. **Gunakan Kata Sandi yang Kuat dan Unik**
   a. Gunakan kombinasi huruf besar, huruf kecil, angka, dan simbol.
   b. Jangan gunakan kata sandi yang sama di semua akun.
   c. Ganti kata sandi secara berkala dan aktifkan **verifikasi dua langkah (2FA)** bila tersedia.

💡 *Tip cepat:* Gunakan pengelola kata sandi (password manager) agar lebih mudah dan aman.

6. **Edukasi dan Sosialisasi Keamanan Siber**
    a. ASN harus menjadi contoh dalam penerapan kebiasaan digital aman di lingkungan kerja.
    b. Pemerintah daerah dapat mengadakan pelatihan rutin tentang keamanan siber minimal dua kali setahun.
    c. Masyarakat perlu diedukasi tentang bahaya *malware* sederhana, misalnya lewat kampanye digital, media sosial, atau siaran lokal.

📣 *Contoh inisiatif:* "Gerakan Klungkung Aman Siber" dapat melibatkan sekolah, perangkat desa, dan pelaku UMKM agar lebih sadar risiko serangan digital.

7. **Laporkan Insiden Secepatnya**
    a. Jika menemukan indikasi serangan (misalnya file terkunci, sistem melambat, atau muncul pesan tebusan), **jangan panik dan jangan membayar tebusan.**
    b. Segera laporkan ke **CSIRT Kabupaten Klungkung** atau petugas IT instansi.
    c. Dokumentasikan pesan dan file terkait, namun jangan membuka atau menghapus file tersebut agar bisa dianalisis.

⚠️ *Penting:* Tindakan cepat dalam 24 jam pertama sangat menentukan keberhasilan pemulihan sistem.

Mencegah *malware* dan *ransomware* bukan hanya urusan teknis, tetapi juga **soal kesadaran dan tanggung jawab bersama.** ASN menjaga data pemerintahan, sementara masyarakat menjaga data pribadi, keduanya memiliki peran penting dalam menjaga keamanan digital di Klungkung. Kedisiplinan kecil seperti tidak sembarangan klik tautan, memperbarui sistem, dan rutin melakukan backup bisa menjadi benteng besar menghadapi serangan siber modern tahun 2025.

Pertanyaan Reflektif

1. Jika suatu hari sistem komputer instansi Anda tiba-tiba terkunci dan muncul pesan meminta tebusan, langkah pertama apa yang sebaiknya dilakukan? Mengapa langkah tersebut penting?
2. Banyak masyarakat dan ASN masih menunda memperbarui perangkat dengan alasan “takut error” atau “malas restart”. Menurut Anda, apa dampak kebiasaan ini terhadap keamanan data?
3. Bayangkan Anda menerima file “Laporan Kinerja ASN 2025” dari rekan kerja, tetapi dikirim lewat email pribadi, bukan dari domain resmi instansi. Apa yang akan Anda lakukan?
4. Dalam pandangan Anda, siapa yang paling berperan besar dalam mencegah serangan *ransomware*: pihak IT, pimpinan instansi, atau setiap individu pengguna? Jelaskan alasannya.
5. Jika Anda diminta memberikan satu pesan singkat kepada teman kerja atau keluarga tentang cara menghindari *malware*, apa yang akan Anda sampaikan?

DAFTAR PUSTAKA

Ananda Khairunnisa, P., Annisa, N., Parhusip, J., Kampus, A., Yos Sudarso, J., Jekan Raya, K., Palangka Raya, K., Tengah, K., & Penulis, K. (2024). Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI: Studi Kasus di Indonesia. *Teknik: Jurnal Ilmu Teknik Dan Informatika*, *4*(2), 9–16. https://journal.stiestekom.ac.id/index.php/TEKNIK/article/view/570

Asbath, R. G. A., Ilpan, Anugrah, R. P., & Setiawan, A. (2025). Analisis Dampak Ransomware Pada Keamanan Data. *JURNAL KUMPULAN ILMU KOMPUTER DAN PERUBAHAN DIGITAL*, *1*(1), 17–23.

Ayu, R. S., Rivai, M. M., Mubarak, N. Al, & Pratama, D. (2025). KEAMANAN INFRASTRUKTUR TEKNOLOGI INFORMASI: ANALISIS ANCAMAN SIBER DAN PENDEKATAN MITIGASI. *Pediaqu : Jurnal Pendidikan Sosial Dan Humaniora*, *4*(2), 195–222. https://doi.org/10.1201/9781032622408-13

Budiyanto, D., & Mabruri, M. (2025). Pentingnya Keamanan Siber dalam Era Digital: Tinjauan Global dan Kondisi di Indonesia. *Prosiding Seminar Nasional Sains Dan Teknologi Seri III Fakultas Sains Dan Teknologi, Universitas Terbuka*, *2*(1), 981–994.

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains Dan Teknologi*, *2*(02), 55–62. https://doi.org/10.56741/bst.v2i02.353

Iriani, L., Agung, R. P., Supriyanto, J., Sugandi, A., & Aulia, M. I. (2025). Pengetahuan Mahasiswa Mengenai Isu Keamanan Sekuriti pada Pusat Data Nasional : Ransomware. *Journal of Cyber Health and Computer (JOCHAC)*, *3*(1), 1–5. https://doi.org/10.64163/jochac.v3i1.73

Mubarak, A. S., Insirat, M. N., & Lutfiya, M. N. (2024). Ransomware: Evolution, Classification, Attack Phase, Detection and Prevention. *Seminar Nasional Teknik Elektro, Sistem Informasi Dan Teknik Informatika V (SNESTIK V)*, 1–6. https://doi.org/10.31284/p.snestik.2024.5588

Pika, D., Batu, L., Siahaan, P. G., Ramadhan, T., & Silitonga, A. I. (2025). Serangan Malware Ransomware Dalam Perspektif Transnational Crime. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, *5*(2), 2025. https://doi.org/10.53363/bureau.v5i2.615

Prasetyo, S. E., Aripradono, H. W., & Ricardo. (2025). Ransomware Attack Analysis in Cybersecurity. *Jurnal E-Komtek*, *9*(1), 302–312. https://doi.org/10.37339/e-komtek.v9i1.2279

Sulubara, S. M. (2024). Perlindungan Data Pribadi dalam Kasus Ransomware : Apa Kata Hukum ? Seri Mughni Sulubara Latar belakang penelitian berjudul " Perlindungan Data Pribadi dalam Kasus serta rekomendasi untuk perbaikan regulasi yang ada . Penelitian ini dilatarbelakangi oleh. *Eksekusi: Jurnal Ilmu Hukum Dan Administrasi Negara*, *2*(November), 426–434.

Tommy, S., Irwan, M., & Nasution, P. (2025). EVALUASI MANAJEMEN RISIKO KEAMANAN SIBER PADA INFRASTRUKTUR DIGITAL PEMERINTAH : STUDI KASUS PUSAT DATA NASIONAL (PDN) Prodi Manajemen , Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri Sumatera Utara I . Pendahuluan Dalam era transformasi dig. *Jurnal Manajemen Ekonomi Dan Bisnis (JMEB)*, *04*(01), 1–26.