

LEMBAR KERJA SISWA

Keamanan Data Pribadi di Dunia Digital

Mata Pelajaran: Informatika

Data Kelompok

Nama kelompok : _____

Anggota Kelompok : _____

A. TUJUAN PEMBELAJARAN

1. Siswa dapat **mengidentifikasi** berbagai jenis ancaman terhadap keamanan data pribadi (Scam, Spam, Phising, Malware, Hacking, Ghosting).
2. Siswa dapat **menganalisis** contoh-contoh nyata dari ancaman keamanan digital.
3. Siswa dapat **menerapkan** langkah-langkah praktis untuk menjaga keamanan data pribadi.

B. STIMULUS — AYO MENGAMATI!

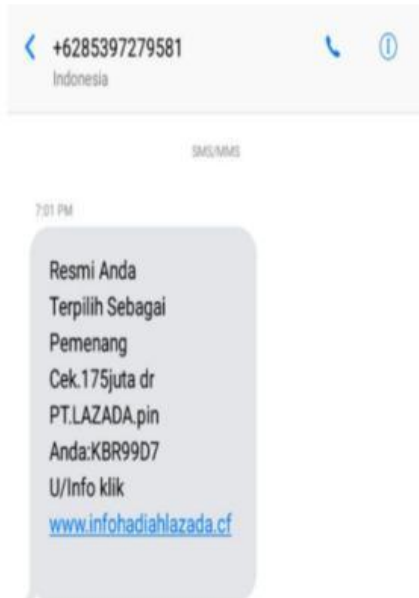
Dunia digital menawarkan banyak kemudahan, namun juga menyimpan bahaya tersembunyi. **Data pribadi kita adalah aset berharga** yang diincar oleh pihak-pihak yang tidak bertanggung jawab. Mari kita pelajari cara melindunginya!

1. Kenali Ancamannya — Amati Gambar Berikut!

Perhatikan gambar-gambar di bawah ini yang merupakan contoh nyata ancaman keamanan digital. Analisis setiap gambar dengan cermat!

Gambar 1 — Pesan Mencurigikan

Perhatikan pesan WhatsApp yang mengirimkan SMS yang mengabarkan hadiah ratusan juta rupiah.



Gambar 2 — Panggilan Tidak Dikenal

Perhatikan daftar panggilan masuk dari nomor-nomor tidak dikenal yang ditandai sebagai **"Suspected Spam"** oleh sistem.



Gambar 3 & 4 — Situs Web Palsu (Phising)

Bandingkan alamat situs resmi vs situs palsu. Perhatikan perbedaan kecil pada URL (<https://perusahaan.com> vs <http://perusahaaan.com>) dan penggunaan **https** vs **http**.



Gambar 4.15 Contoh Situs dengan Perbedaan Satu Huruf

Sumber: Tangkapan layar situs kikibca.com dan kicbca.com

Gambar 5 — File Berbahaya (Malware)

Perhatikan pesan WhatsApp yang meminta mengunduh file **.apk** seperti **"Suratundanganpernikahan.apk"** dari nomor tidak dikenal.



2. Tonton dan Pelajari — Video Pembelajaran

 **Link Video:**

Setelah menonton video, jawablah pertanyaan berikut:

1. Apa pesan utama yang disampaikan dalam video tersebut?

2. Sebutkan satu modus penipuan dalam video yang TIDAK ada dalam gambar di atas!

C. MATERI PEMBELAJARAN — AYO MEMBACA!

I. Jenis Ancaman terhadap Data Pribadi

Bacalah ringkasan materi berikut dengan saksama untuk memperdalam pemahamanmu tentang ancaman keamanan digital.

1

SCAM

Strategi penipuan yang memanfaatkan empati dan kelengahan pengguna. Metodenya beragam, bisa melalui telepon, SMS, WhatsApp, email, maupun surat berantai.

✦ **Contoh:** Pesan WhatsApp dari nomor asing mengabarkan bahwa Anda memenangkan hadiah tabungan Rp. 125 juta dan meminta Anda klik link tertentu.

2

SPAM

Perilaku mengganggu yang dilakukan secara terus-menerus dan berulang. Bermula dari mengganggu, spam bisa berlanjut menjadi penipuan dan pencurian data.

✦ **Contoh:** Panggilan berulang dari nomor tak dikenal yang ditandai sistem sebagai 'Suspected Spam', atau email promosi massal yang terus membanjiri kotak masuk.

3

PHISING

Upaya mendapatkan data sensitif (nama, usia, alamat, username, password, data finansial) dengan teknik pengelabuan menggunakan situs web atau email palsu yang sangat menyerupai aslinya.

✦ **Contoh:** Situs palsu facebook0k.com yang tampilannya persis sama dengan facebook.com asli, namun URL-nya berbeda dan tidak menggunakan HTTPS.

4

MALWARE

Perangkat lunak berbahaya yang dirancang khusus untuk menyusup, merusak, atau mencuri data dari komputer, server, data Handphone tanpa izin pemiliknya.

✦ **Contoh:** File 'Cek Resi J&T.apk' atau 'LIHAT Foto Paket.apk' yang dikirim melalui WhatsApp dari nomor tidak dikenal. Jika diinstal, dapat mencuri data pribadi.

5

HACKING

Aktivitas mengeksplorasi, memodifikasi, atau memanipulasi sistem komputer, jaringan, atau perangkat digital untuk menemukan dan mengeksploitasi celah keamanan.

✦ **Contoh:** Peretas berhasil masuk ke sistem database sebuah perusahaan dan mencuri jutaan data pelanggan termasuk nomor kartu kredit.

6

GHOSTING

Memutus komunikasi secara sepihak dan tiba-tiba tanpa pemberitahuan, seringkali setelah adanya kesepakatan atau transaksi yang sudah dibuat.

✦ **Contoh:** Pembeli pesan desain logo, setelah logo selesai dibuat dan dikonfirmasi, pembeli tersebut tiba-tiba menghilang dan tidak menjawab pesan.

II. Cara Menjaga Data Tetap Aman

Berikut adalah langkah-langkah praktis yang dapat kamu terapkan untuk meminimalisir ancaman keamanan data:



1. Gunakan Password yang Kuat dan Unik

Password yang baik tidak mudah ditebak. Hindari kata umum seperti **"123456"** atau nama sendiri.

- Kombinasikan huruf besar, huruf kecil, angka, dan simbol
- Panjang minimal 8 karakter
- Gunakan password berbeda untuk setiap akun
- 💡 Tips: Gunakan singkatan kalimat. Contoh: "Saya suka makan bakso tahun 2026!" → **"SsmbT2026!"**



2. Autentikasi Dua Faktor (2FA)

Password saja tidak cukup kuat! Aktifkan 2FA sebagai lapisan keamanan tambahan.

- Saat login, pengguna harus memasukkan kode OTP yang dikirim ke ponsel/email
- Ibarat kunci gembok dua lapis: kunci + sidik jari — hanya pemiliknya yang bisa masuk!



3. Selalu Perbarui Perangkat dan Aplikasi

Pembaruan rutin berisi perbaikan celah keamanan yang bisa dimanfaatkan peretas.

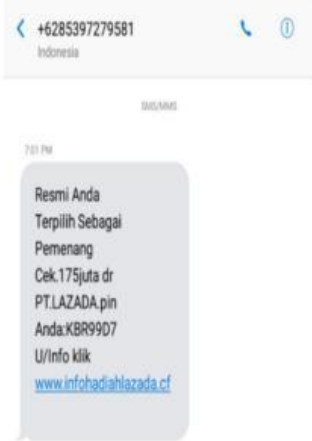
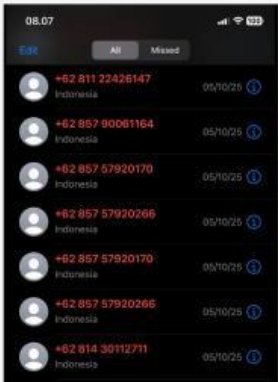
- Perangkat yang tidak diperbarui lebih rentan terhadap serangan siber
- Biasakan selalu instal pembaruan agar sistem tetap aman dan terlindungi

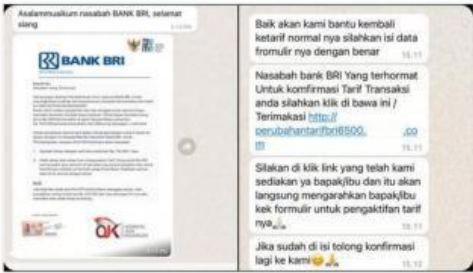
D. AKTIVITAS SISWA — AYO BERLATIH!



Aktivitas 1 — Analisis Kasus (Berdasarkan Gambar)

Berdasarkan pengamatanmu pada gambar-gambar di bagian stimulus dan materi yang telah dibaca, isilah tabel berikut ini!

No	Sumber Gambar	Jenis Ancaman	Ciri-ciri / Modus yang Terlihat	Tindakan yang Harus Dilakukan
1				
2				

No	Sumber Gambar	Jenis Ancaman	Ciri-ciri / Modus yang Terlihat	Tindakan yang Harus Dilakukan
3				
4				
5				

Aktivitas 2 — Tantangan Membuat Password Kuat

Gunakan teknik **singkatan kalimat** untuk membuat 3 password yang kuat dan unik. Tuliskan kalimat ide dan password yang dihasilkan pada tabel berikut

 **Contoh:**

Kalimat Ide: "Saya suka makan bakso tahun 2026!" → **Password:** **SsmbT2026!**

No	Kalimat Ide	Password yang Dihasilkan
1		
2		
3		

Aktivitas 3 — Refleksi dan Diskusi

Jawablah pertanyaan-pertanyaan berikut dengan pendapatmu sendiri secara jujur dan lengkap!

1 Mengapa kita tidak boleh sembarangan mengklik link atau mengunduh file .apk dari orang yang tidak dikenal?

2 Mengapa fitur Autentikasi Dua Faktor (2FA) dianggap sangat penting, bahkan jika kita sudah memiliki password yang kuat?

3 Buatlah satu SLOGAN KEAMANAN DIGITAL pribadimu untuk mengingatkan diri sendiri agar selalu waspada di internet!

 Slogan saya:

E. KESIMPULAN

Tuliskan 3 hal terpenting yang kamu pelajari hari ini tentang cara menjaga keamanan data pribadimu.

1. Hal Pertama yang saya pelajari:

2. Hal ke-2 yang saya pelajari:

3. Hal ke-3 yang saya pelajari:

Nilai:

 Jaga Data Pribadimu, Jaga Masa Depanmu! 