MODUL AJAR DEEP LEARNING
MATA PELAJARAN : INFORMATIKA
BAB 8 : DAMPAK SOSIAL INFORMATIKA

A. IDENTITAS MODUL

Nama Sekolah	**SMP/MTs .....**
Nama Penyusun	**.....**
Mata Pelajaran	**Informatika**
Kelas / Fase / Semester	**IX / Fase D / Genap**
Alokasi Waktu	**6 JP (3 kali pertemuan)**
Tahun Pelajaran	**20... / 20...**

B. IDENTIFIKASI KESIAPAN PESERTA DIDIK

- **Pengetahuan Awal**: Peserta didik adalah pengguna aktif internet, media sosial, dan berbagai aplikasi digital. Mereka pernah mendengar istilah seperti virus, *hacker*, dan penipuan online, namun pemahamannya mungkin belum mendalam.
- **Minat**: Peserta didik memiliki minat yang tinggi terhadap topik ini karena sangat relevan dengan keamanan akun media sosial, game, dan data pribadi mereka di dunia maya.
- **Latar Belakang**: Sebagai *digital natives*, peserta didik sering berinteraksi di dunia digital namun kesadaran akan ancaman dan cara proteksi diri yang sistematis masih perlu dibangun.
- **Kebutuhan Belajar**:
  - **Visual**: Membutuhkan studi kasus nyata, diagram alur kejahatan siber, dan contoh antarmuka fitur keamanan.
  - **Auditori**: Sangat efektif belajar melalui diskusi kelompok untuk menganalisis kasus dan berbagi pengalaman.
  - **Kinestetik**: Eksplorasi langsung fitur-fitur keamanan pada peramban (*browser*) dan pengaturan privasi di gawai masing-masing.

C. KARAKTERISTIK MATERI PELAJARAN

- **Jenis Pengetahuan yang Akan Dicapai**:
  - **Konseptual**: Memahami berbagai jenis kejahatan dan kerawanan di dunia digital (*phishing*, *malware*, *ransomware*, dll), serta konsep-konsep perlindungan data (enkripsi, otentikasi, antivirus, *cookie*).
  - **Prosedural**: Mampu merancang mekanisme perlindungan data sederhana (seperti otentikasi multifaktor) dan mengelola pengaturan keamanan dasar pada peramban.
- **Relevansi dengan Kehidupan Nyata Peserta Didik**: Sangat tinggi. Materi ini membekali peserta didik dengan pengetahuan dan keterampilan esensial untuk melindungi diri dari pencurian identitas, penipuan finansial, dan pelanggaran privasi di dunia digital.
- **Tingkat Kesulitan**: Sedang. Terdapat banyak istilah teknis baru, namun konsepnya dapat dianalogikan dengan keamanan di dunia nyata sehingga lebih mudah dipahami.
- **Struktur Materi**: Materi disusun dari pengenalan ancaman (Keamanan Data dan Informasi), dilanjutkan dengan solusi (Perkakas Perlindungan), dan diakhiri dengan

praktik pencegahan (Meningkatkan Keamanan Informasi).

- **Integrasi Nilai dan Karakter**:
  - **Bernalar Kritis**: Menganalisis studi kasus kejahatan siber untuk memahami modus operandi dan dampaknya.
  - **Kemandirian**: Mengembangkan tanggung jawab untuk mengelola keamanan data dan perangkat pribadi.
  - **Kepedulian**: Menumbuhkan kesadaran untuk tidak hanya melindungi diri sendiri, tetapi juga mengingatkan orang lain (keluarga, teman) tentang potensi ancaman digital.

D. DIMENSI PROFIL LULUSAN

- **Keimanan dan Ketakwaan terhadap Tuhan Yang Maha Esa, dan Berakhlak Mulia**: Menerapkan etika digital, tidak menggunakan pengetahuan untuk merugikan orang lain.
- **Kewargaan**: Menjadi warga digital yang cerdas, bertanggung jawab, dan mampu menjaga keamanan bersama di ruang siber.
- **Penalaran Kritis**: Mampu mengidentifikasi potensi ancaman keamanan dan mengevaluasi langkah-langkah perlindungan yang paling efektif.
- **Kemandirian**: Proaktif dalam memperbarui pengaturan keamanan dan melindungi informasi pribadi.
- **Komunikasi**: Mampu menjelaskan risiko keamanan digital kepada orang lain dengan bahasa yang sederhana.

DESAIN PEMBELAJARAN

A. CAPAIAN PEMBELAJARAN (CP)

Pada akhir Fase D, murid memiliki kemampuan sebagai berikut:

- **Berpikir Komputasional**
  Menerapkan berpikir komputasional untuk problem dalam kehidupan sehari-hari maupun dalam menghadapi masalah komputasi; memahami konsep himpunan data terstruktur dalam kehidupan sehari-hari; memahami konsep lembar kerja pengolah data; menerapkan berpikir komputasional dalam menyelesaikan persoalan yang mengandung himpunan data berstruktur sederhana dengan volume kecil; serta menuliskan sekumpulan instruksi dengan menggunakan sekumpulan kosakata terbatas atau simbol dalam format pseudocode.
- **Literasi Digital**
  Memahami cara kerja dan penggunaan mesin pencari di internet; mengetahui kualitas informasi dan kredibilitas sumber informasi digital; mengenal ekosistem media pers digital; membedakan fakta, opini, dan hoaks; memahami pemanfaatan perangkat teknologi pengolah dokumen, lembar kerja, dan presentasi; mampu mendeskripsikan komponen, fungsi, dan cara kerja komputer; memahami konsep dan penerapan konektivitas jaringan lokal dan internet baik kabel maupun nirkabel; mengetahui jenis ruang publik virtual; memahami pemanfaatan perangkat teknologi digital untuk produksi dan diseminasi konten; memahami pentingnya menjaga rekam jejak digital, mengamalkan toleransi dan empati di dunia digital, memahami dampak perundungan digital, membuat kata sandi yang aman; memahami pengamanan perangkat dari berbagai jenis malware, memilah informasi yang bersifat privat dan publik, melindungi data pribadi dan identitas digital serta memiliki kesadaran penuh (*mindfulness*) dalam dunia digital.

B. LINTAS DISIPLIN ILMU

- **PPKn**: Hak dan kewajiban warga negara dalam melindungi data pribadi, serta aspek hukum dari kejahatan siber (UU ITE).
- **Bahasa Indonesia**: Kemampuan membaca dan menganalisis teks studi kasus kejahatan siber secara kritis.

C. TUJUAN PEMBELAJARAN

- **Pertemuan 1**: Peserta didik mampu mengidentifikasi berbagai jenis kejahatan dan kerawanan di dunia digital (Aktivitas DSI-K9-01 & DSI-K9-02).
- **Pertemuan 2**: Peserta didik mampu menjelaskan fungsi berbagai perkakas perlindungan data seperti enkripsi, antivirus, dan otentikasi (Aktivitas DSI-K9-04).
- **Pertemuan 3**: Peserta didik mampu menerapkan cara meningkatkan keamanan informasi melalui pengaturan pada peramban (*browser*) dan memahami cara kerja *cookie* (Aktivitas DSI-K9-03).

D. TOPIK PEMBELAJARAN KONTEKSTUAL

- Studi kasus penipuan *phishing* yang marak di Indonesia.
- Cara kerja otentikasi multifaktor pada aplikasi e-commerce atau game.

- Mengatur privasi dan *cookie* di peramban yang sering digunakan.

E. KERANGKA PEMBELAJARAN

PRAKTIK PEDAGOGIK

- **Model Pembelajaran**: Pembelajaran Berbasis Masalah (*Problem-Based Learning*), Studi Kasus.
- **Pendekatan**: Deep Learning (Mindful, Meaningful, Joyful Learning).
- **Metode Pembelajaran**: Diskusi kelompok, studi kasus, eksplorasi, demonstrasi.
- **Strategi Pembelajaran Berdiferensiasi**:
  - **Diferensiasi Proses**: Diskusi kelompok memungkinkan peserta didik dengan pemahaman berbeda untuk saling belajar. Peserta didik dapat memilih situs web yang berbeda untuk dieksplorasi pada materi *cookie*.
  - **Diferensiasi Produk**: Hasil rancangan otentikasi (Aktivitas DSI-K9-04) dapat disajikan dalam bentuk diagram alur, poin-poin deskriptif, atau cerita skenario.

F. LANGKAH-LANGKAH PEMBELAJARAN BERDIFERENSIASI

PERTEMUAN 1 (2 JP : 80 MENIT)

Topik : Keamanan Data, Informasi, dan Ancaman Digital

KEGIATAN PENDAHULUAN (15 MENIT)

- **Orientasi & Doa**.
- **Apersepsi**: Guru bertanya, "Siapa yang pernah mendapat SMS/WA 'Selamat Anda memenangkan hadiah...' atau 'Paket Anda tertahan...'? Menurut kalian, apa tujuan pesan seperti itu?". Diskusi diarahkan ke konsep penipuan dan pencurian data. (*Meaningful*)
- **Penyampaian Tujuan**.

KEGIATAN INTI (55 MENIT)

- **Diskusi Terbimbing (Aktivitas DSI-K9-01)**: Peserta didik dibagi menjadi kelompok-kelompok kecil. Mereka mendiskusikan dua topik pada aktivitas: (1) Siapa yang bertanggung jawab atas keamanan sistem? (2) Analogi antara gangguan internet dan kemacetan lalu lintas. (*Bernalar Kritis, Kolaborasi*)
- **Studi Kasus (Aktivitas DSI-K9-02)**: Masih dalam kelompok, peserta didik menganalisis kasus *phishing* email di Indonesia. Mereka diminta membuat ringkasan cara kerja *phishing*, mengidentifikasi dampaknya, dan mengusulkan solusi pencegahan. (*Meaningful*)
- **Presentasi Kelompok**: Setiap kelompok mempresentasikan hasil diskusi dan analisis studi kasusnya.

KEGIATAN PENUTUP (10 MENIT)

- **Refleksi**: Guru bertanya, "Setelah mengetahui berbagai modus kejahatan, sikap apa yang perlu kita ubah saat beraktivitas di internet?" (*Mindful*)
- **Rangkuman**: Guru menyimpulkan jenis-jenis ancaman digital yang paling umum.

PERTEMUAN 2 (2 JP : 80 MENIT)

Topik : Perkakas untuk Melindungi Data dan Informasi

KEGIATAN PENDAHULUAN (10 MENIT)

- **Orientasi & Doa**.

- **Apersepsi**: Mengulas kembali pertemuan sebelumnya tentang ancaman. Guru bertanya, "Jika ada banyak pencuri, apa yang biasanya kita lakukan untuk melindungi rumah kita?". Jawaban (kunci, gembok, alarm) dianalogikan dengan perkakas keamanan digital.

KEGIATAN INTI (60 MENIT)

- **Eksplorasi Konsep**: Guru menjelaskan konsep dan cara kerja perkakas perlindungan: Enkripsi, Antivirus, Aplikasi Terpercaya, dan Otentikasi (termasuk biometrik dan multifaktor).
- **Aktivitas Perancangan (Aktivitas DSI-K9-04)**: Secara berkelompok, peserta didik merancang model otentikasi multifaktor untuk sebuah "Ruang Rahasia". Mereka harus memilih minimal dua metode otentikasi dari kategori yang berbeda dan menjelaskan alasannya. (*Kreativitas, Bernalar Kritis*)
- **Presentasi Rancangan**: Setiap kelompok mempresentasikan model otentikasi yang mereka rancang.

KEGIATAN PENUTUP (10 MENIT)

- **Refleksi**: "Menurut kalian, mengapa menggunakan satu kata sandi saja terkadang tidak cukup aman?"
- **Rangkuman**: Guru merangkum pentingnya menggunakan perlindungan berlapis untuk data-data penting.

PERTEMUAN 3 (2 JP : 80 MENIT)

Topik : Meningkatkan Keamanan Informasi Praktis

KEGIATAN PENDAHULUAN (10 MENIT)

- **Orientasi & Doa**.
- **Apersepsi**: Guru bertanya, "Siapa yang pernah merasa aneh karena setelah mencari sepatu di sebuah toko online, iklan sepatu muncul di semua media sosial kalian? Bagaimana itu bisa terjadi?". Diskusi diarahkan ke konsep *cookie* dan pelacakan.

KEGIATAN INTI (60 MENIT)

- **Demonstrasi**: Guru mendemonstrasikan cara mengakses fitur keamanan dan privasi pada peramban (*browser*) yang umum digunakan, khususnya cara mengelola *cookie* dan mengaktifkan "Do Not Track".
- **Aktivitas Eksplorasi (Aktivitas DSI-K9-03)**: Peserta didik secara individu atau berpasangan melakukan eksplorasi di internet untuk mencari 5 situs yang menggunakan *cookie* dan menginformasikannya. Mereka menganalisis manfaat *cookie* dan apakah ada opsi untuk menolaknya. (*Kinestetik, Mandiri*)
- **Berbagi Hasil**: Beberapa siswa membagikan temuan situs mereka dan menjelaskan fungsi *cookie* di situs tersebut.

KEGIATAN PENUTUP (10 MENIT)

- **Refleksi**: "Setelah mengetahui tentang *cookie*, apakah kalian akan mengubah pengaturan di peramban kalian? Mengapa?" (*Mindful*)
- **Rangkuman**: Guru menyimpulkan langkah-langkah praktis yang bisa dilakukan pengguna untuk meningkatkan keamanan saat berinternet.

G. ASESMEN PEMBELAJARAN

ASESMEN DIAGNOSTIK

- **Tanya Jawab**: Diskusi apersepsi di awal setiap pertemuan untuk mengukur pemahaman dan pengalaman awal siswa.

ASESMEN FORMATIF

- **Observasi**: Menilai keaktifan, kualitas argumen, dan kolaborasi siswa selama diskusi kelompok.
- **Produk (Proses)**: Menilai hasil eksplorasi situs web (Aktivitas DSI-K9-03) dan draf rancangan otentikasi.

ASESMEN SUMATIF

- **Produk (Proyek)**:
  - **Rancangan Otentikasi**: Menilai kelogisan, kreativitas, dan pemenuhan syarat otentikasi multifaktor pada rancangan kelompok.
- **Tes Tertulis**: Menggunakan soal Uji Kompetensi dari buku (menjodohkan dan uraian) untuk mengukur pemahaman konseptual siswa terhadap keseluruhan materi bab ini.