RENCANA PELAKSANAAN PEMBELAJARAN

Nama Sekolah	:	MTs Ahmad Yani Jabung
Nama Guru	:	Muhammad Badrul Huda, S.Pd
Mata Pelajaran	:	Informatika
Kelas/Semester	:	IX A / 2
Alokasi Waktu	:	2 x 40 Menit

1. Identifikasi

Peserta didik: Sebagian besar siswa telah menggunakan internet secara aktif dan memahami konsep dasar akun daring, namun pemahaman mendalam tentang ancaman siber dan cara mitigasinya masih terbatas.
Materi Pelajaran: Memahami dan menjelaskan keamanan data dan informasi di dunia maya.
Dimensi Profil Lulusan: Penalaran Kritis, Kreativitas, Komunikasi, Cinta kepada Tuhan Yang Maha Esa, Cinta kepada Ilmu Pengetahuan

2. Desain Pembelajaran

Capaian Pembelajaran: Siswa mampu mengidentifikasi berbagai ancaman keamanan siber, menjelaskan prinsip dasar perlindungan data, dan menerapkan praktik aman dalam berinteraksi di dunia maya.
Lintas Disiplin Ilmu: Pendidikan Kewarganegaraan (Etika Digital), Bahasa Indonesia (Penulisan Laporan), Bimbingan Konseling (Dampak Sosial/Psikologis), Seni Budaya (Desain Infografis)
Kemitraan Pembelajaran: Komunitas Pegiat Siber Lokal, Praktisi IT (DU/DI), Kepolisian Sektor (mengenai undang-undang ITE)
Tujuan Pembelajaran:

1. Mengidentifikasi jenis-jenis ancaman siber (phishing, malware, dsb.) dengan tepat (Penalaran Kritis).
2. Menganalisis pentingnya penggunaan kata sandi yang kuat dan berlapis (CAIP).
3. Merancang infografis digital yang persuasif mengenai tips keamanan data (Kreativitas & Komunikasi).
4. Menjelaskan secara lisan cara melindungi privasi diri saat berinteraksi di media sosial (Komunikasi).
5. Menunjukkan sikap bertanggung jawab dan etis dalam menjaga data pribadi dan orang lain di dunia maya (Cinta kepada Tuhan Yang Maha Esa).

Topik Pembelajaran: Jenis-jenis Ancaman Siber (Malware, Phishing, Ransomware), Prinsip Dasar Keamanan Data (Kerahasiaan, Integritas, Ketersediaan), dan Etika Digital dalam Melindungi Privasi.
Model: Problem-Based Learning (PBL), Project-Based Learning (PjBL)
Metode: Studi Kasus (Simulasi), Diskusi Kelompok, Presentasi Infografis, Praktik Pengaturan Keamanan Akun.

3. Pengalaman Belajar

Kegiatan Awal:

- Guru menyapa, mengajak siswa berdoa, dan melakukan absensi (Cinta kepada Tuhan Yang Maha Esa).
- Apersepsi: Guru menampilkan berita/kasus nyata kebocoran data di Indonesia (Memantik Penalaran Kritis).
- Asesmen Awal: Tanya jawab singkat tentang "Apa hal terpenting yang harus dijaga saat online?".
- Guru menyampaikan tujuan pembelajaran.

Kegiatan Inti:

1. Orientasi Masalah: Siswa dibagi kelompok dan diberikan studi kasus (misalnya, simulasi email phishing yang tampak meyakinkan).
2. Mengorganisasi Belajar: Siswa meneliti dan mengidentifikasi karakteristik ancaman siber yang ada dalam studi kasus (CAIP).
3. Pembimbingan: Guru memfasilitasi diskusi tentang prinsip CIA Triad (Confidentiality, Integrity, Availability).
4. Mengembangkan dan Menyajikan Hasil: Siswa merancang Infografis/Poster Digital yang berisi 5 tips anti-phishing yang kreatif dan persuasif (Kreativitas).
5. Analisis dan Evaluasi: Setiap kelompok mempresentasikan infografisnya, kelompok lain memberikan umpan balik (Komunikasi & Penalaran Kritis).
6. Praktik Mandiri: Siswa mempraktikkan cara membuat kata sandi yang kuat dan mengaktifkan Two-Factor Authentication (2FA) pada akun email/media sosial mereka.

Kegiatan Penutup:

- Refleksi: Siswa menjawab pertanyaan reflektif tentang pelajaran hari ini.
- Kesimpulan: Guru dan siswa menyimpulkan prinsip-prinsip utama keamanan data dan etika digital.
- Tindak Lanjut: Guru memberikan tugas untuk menyebarkan informasi keamanan data (seperti infografis) kepada keluarga atau teman.
- Doa penutup (Cinta kepada Tuhan Yang Maha Esa).

4. Asesmen Pembelajaran

Asesmen Awal: Tanya jawab lisan (Apa itu data pribadi?) dan kuis pilihan ganda singkat tentang istilah-istilah dasar siber.
Asesmen Proses: Observasi keterlibatan kelompok dalam menganalisis studi kasus (Penalaran Kritis) dan penilaian saat penyusunan infografis (Kreativitas dan Kerjasama).
Asesmen Akhir: Penilaian Infografis (Proyek) dan tes tertulis esai singkat tentang pentingnya etika digital.
Mengetahui,

Mengetahui,
Malang, 8 Januari 2026

Kepala Sekolah	Guru
Muroihatul Jannah, M.Pd	**Muhammad Badrul Huda, S.Pd**

Lampiran 1. LKPD (Lembar Kerja Peserta Didik)

Nama	:	.....
Kelas	:	IX A
Materi	:	Memahami dan menjelaskan keamanan data dan informasi di dunia maya.

Langkah Kerja:

1. Buka pengaturan keamanan pada akun email/media sosial yang Anda miliki.
2. Periksa kekuatan kata sandi Anda menggunakan fitur pemeriksaan keamanan (jika tersedia).
3. Jika kata sandi Anda lemah, ubahlah menjadi kombinasi minimal 12 karakter (huruf besar, kecil, angka, dan simbol).
4. Aktifkan fitur Otentikasi Dua Faktor (2FA) pada akun tersebut.
5. Dokumentasikan langkah-langkah yang Anda lakukan (screenshot langkah) dan laporkan hasilnya dalam bentuk narasi singkat.

Pertanyaan Reflektif:

1. Hal baru apa yang paling mengubah cara pandang Anda tentang penggunaan internet setelah mempelajari materi ini?
2. Bagaimana Anda akan menerapkan prinsip keamanan data dalam kehidupan sehari-hari dan membagikannya kepada keluarga?
3. Seberapa besar peran tanggung jawab dan etika digital (Cinta kepada Tuhan Yang Maha Esa) dalam menjaga keamanan dan privasi orang lain di dunia maya?

Lampiran 2. Bahan Ajar

A. Ringkasan Materi

Keamanan data di dunia maya sangat penting untuk melindungi Kerahasiaan, Integritas, dan Ketersediaan (CIA Triad) informasi pribadi kita. Ancaman utama meliputi Malware (perangkat lunak jahat), Phishing (penipuan untuk mendapatkan kredensial), dan peretasan. Pencegahan terbaik adalah selalu menggunakan kata sandi yang unik dan kuat, mengaktifkan otentikasi dua faktor, serta bersikap kritis (Penalaran Kritis) terhadap tautan atau lampiran yang mencurigakan. Etika digital menuntut kita untuk bertanggung jawab atas data kita sendiri dan tidak merugikan data orang lain.

B. Sumber Belajar Tambahan

Video Pembelajaran: https://www.youtube.com/watch?v=S0Tq4H7zS6E (Contoh: Video edukasi tentang pentingnya 2FA dan bahaya phishing)
Artikel/Simulasi: https://www.kominfo.go.id/content/detail/UU-ITE-dan-etika-berinternet-artikel-pendukung (Contoh: Artikel tentang undang-undang dan etika digital)

Lampiran 3. Instrumen Asesmen

A. Daftar Pertanyaan/Soal Tes

1. Jelaskan perbedaan mendasar antara Malware dan Ransomware.
2. Mengapa penggunaan Otentikasi Dua Faktor (2FA) dianggap sangat penting dalam melindungi akun daring? (Penalaran Kritis)
3. Anda menerima tautan yang menjanjikan hadiah jika mengisi data pribadi. Tindakan apa yang paling aman yang harus Anda ambil dan jelaskan alasannya.

4. Sebutkan tiga prinsip dasar (CIA Triad) dalam keamanan informasi dan jelaskan maknanya secara singkat.
5. Buatlah slogan persuasif minimal 5 kata tentang pentingnya menjaga etika digital dan Cinta kepada Ilmu Pengetahuan.

B. Rubrik Penilaian Kinerja

Aspek yang Dinilai	Skor 1 (Kurang)	Skor 2 (Cukup)	Skor 3 (Baik)	Skor 4 (Sangat Baik)
Penalaran Kritis & Pemahaman Konsep	Gagal mengidentifikasi ancaman siber dasar dan tidak mampu menjelaskan konsep keamanan.	Mampu mengidentifikasi ancaman, namun penjelasannya kurang mendalam dan terbatas pada teks.	Mampu mengidentifikasi dan menjelaskan konsep keamanan data (CIA Triad) dengan baik.	Mampu menganalisis studi kasus secara mendalam, mengaitkan konsep yang dipelajari, dan memberikan solusi yang logis.
Kreativitas dan Desain (Infografis)	Infografis tidak relevan, tidak menarik, dan informasinya salah.	Infografis relevan tetapi desainnya standar dan informasinya sedikit.	Infografis informatif, desain menarik, dan menunjukkan upaya kreatif.	Infografis sangat kreatif, orisinal, dan pesannya sangat persuasif dan mudah dipahami.
Komunikasi dan Presentasi	Presentasi tidak jelas dan siswa tidak terlibat dalam diskusi.	Presentasi terbata-bata; mampu menjawab pertanyaan dasar setelah dibantu guru.	Menyampaikan informasi dengan jelas, menggunakan bahasa yang baik, dan mampu berdiskusi secara efektif.	Menyajikan materi dengan sangat percaya diri, artikulasi jelas, dan mampu mempertahankan argumen serta mendorong diskusi aktif.
Sikap Kerja (Etika & CAIP)	Tidak menghargai pendapat teman dan tidak berusaha mencari informasi tambahan; mengabaikan etika digital.	Bekerja sama, tetapi hanya menunggu instruksi; sedikit rasa ingin tahu terhadap ilmu pengetahuan.	Aktif bekerja sama, menunjukkan inisiatif, dan berusaha mencari sumber ilmu tambahan (CAIP).	Sangat proaktif, menghormati nilai-nilai etika digital, bertanggung jawab penuh atas pekerjaannya, dan menunjukkan antusiasme tinggi terhadap pembelajaran (CAIP/CTYME).