RENCANA PELAKSANAAN PEMBELAJARAN

Nama Sekolah	:	MTs Ahmad Yani Jabung
Nama Guru	:	Muhammad Badrul Huda, S.Pd
Mata Pelajaran	:	Informatika
Kelas/Semester	:	9-B / 2
Alokasi Waktu	:	2 x 40 Menit

1. Identifikasi

Peserta didik: Sebagian besar siswa Kelas 9-B sudah aktif menggunakan perangkat digital (HP dan Laptop) namun perlu pendalaman mengenai risiko dan langkah-langkah konkret perlindungan data pribadi dan etika digital.
Materi Pelajaran: Memahami keamanan data yang terjadi ketika menggunakan handphone atau laptop
Dimensi Profil Lulusan: Penalaran Kritis, Kreativitas, Komunikasi, Cinta kepada Tuhan Yang Maha Esa, Cinta kepada Ilmu Pengetahuan

2. Desain Pembelajaran

Capaian Pembelajaran: Peserta didik mampu mengidentifikasi dan menerapkan langkah-langkah praktis untuk menjaga keamanan data pribadi di perangkat digital serta memahami etika berinternet.
Lintas Disiplin Ilmu: Pendidikan Pancasila (Etika digital dan Hukum), Bahasa Indonesia (Penyusunan laporan dan presentasi), Kewirausahaan (Risiko bisnis digital).
Kemitraan Pembelajaran: Komunitas IT Lokal, Alumni yang bekerja di bidang Keamanan Siber, Dinas Komunikasi dan Informatika (Diskominfo) daerah.
Tujuan Pembelajaran:

1. Menjelaskan konsep dasar keamanan data, privasi, dan ancaman siber yang umum terjadi (Penalaran Kritis).
2. Menganalisis praktik berbahaya (phishing, malware) dan membuat rekomendasi perlindungan data yang kreatif (Kreativitas).
3. Mendemonstrasikan cara mengatur izin aplikasi dan sandi yang kuat pada perangkat (Cinta Ilmu Pengetahuan).
4. Mempresentasikan hasil analisis risiko data dengan jelas dan persuasif (Komunikasi).
5. Menyadari pentingnya menjaga data sebagai amanah (Cinta kepada Tuhan Yang Maha Esa).

Topik Pembelajaran: Ancaman Keamanan Data (Phishing, Malware, Kebocoran Data), Pengelolaan Kata Sandi dan Otentikasi Dua Faktor, Izin Aplikasi dan Privasi Digital.
Model: Problem-Based Learning (PBL), Discovery Learning
Metode: Diskusi Kelompok, Studi Kasus (Case Study), Praktikum Simulasi, Presentasi.

3. Pengalaman Belajar

Kegiatan Awal:

- Salam dan doa (Cinta kepada Tuhan YME).
- Pengecekan kehadiran.
- Apersepsi: Tanya jawab mengenai pengalaman siswa yang pernah menerima SMS/telepon asing mencurigakan (mengaitkan ke materi).
- Menyampaikan tujuan pembelajaran dan manfaat materi. (10 menit)

Kegiatan Inti:

- Orientasi Masalah: Siswa disajikan studi kasus nyata tentang kebocoran data di platform populer (PBL).
- Pengumpulan Data: Siswa secara kelompok mencari informasi tentang jenis-jenis ancaman (misal: Trojan, Ransomware) dan cara kerjanya (Penalaran Kritis).
- Pengembangan Solusi: Setiap kelompok merancang 'Panduan Aman Digital' (poster/infografis) yang berisi tips keamanan data yang kreatif (Kreativitas).
- Praktikum Mandiri: Siswa mempraktikkan audit izin aplikasi dan cara mengaktifkan 2FA pada akun media sosial mereka sendiri (Cinta Ilmu Pengetahuan).
- Presentasi dan Diskusi: Kelompok mempresentasikan hasilnya, menekankan langkah komunikasi yang efektif. (Komunikasi)

Kegiatan Penutup:

- Refleksi Guru: Menganalisis poin-poin penting yang telah dipelajari.
- Refleksi Siswa: Siswa menjawab pertanyaan reflektif tentang perubahan perilaku yang akan mereka lakukan.
- Penugasan Mandiri: Menganalisis kebijakan privasi satu aplikasi yang sering digunakan.
- Doa penutup dan ucapan terima kasih. (15 menit)

4. Asesmen Pembelajaran

Asesmen Awal: Kuis singkat via formulir digital tentang pemahaman dasar kata sandi kuat dan izin aplikasi (10 soal pilihan ganda).
Asesmen Proses: Observasi keaktifan diskusi kelompok, kedalaman analisis studi kasus, dan kolaborasi dalam pembuatan Panduan Aman Digital (Formatif).
Asesmen Akhir: Tes Tertulis (Esai Analisis) dan Penilaian Produk (Kualitas Panduan Aman Digital dan Keterampilan Presentasi).

Mengetahui,
Malang, 13 Januari 2026

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

Lampiran 1. LKPD (Lembar Kerja Peserta Didik)

Nama	:	.....
Kelas	:	9-B
Materi	:	Memahami keamanan data yang terjadi ketika menggunakan handphone atau laptop

Langkah Kerja:

1. Pilih 5 aplikasi di handphone Anda yang paling sering digunakan (misalnya: media sosial, chatting, game).
2. Buka pengaturan izin aplikasi pada perangkat Anda (Android: Pengelola Aplikasi; iOS: Pengaturan Privasi).
3. Catat izin apa saja yang diminta oleh 5 aplikasi tersebut (misalnya: Lokasi, Kamera, Kontak, Mikrofon).
4. Analisis secara kritis: Apakah semua izin tersebut benar-benar dibutuhkan aplikasi agar berfungsi optimal?
5. Lakukan penyesuaian izin (matikan izin yang dianggap berlebihan).
6. Dokumentasikan hasil audit dan jelaskan alasannya dalam laporan kelompok (maksimal 300 kata).

Pertanyaan Reflektif:

1. Setelah memahami risiko kebocoran data, perubahan apa yang paling penting yang akan Anda terapkan segera pada perangkat pribadi Anda?
2. Bagaimana pemahaman tentang keamanan data ini memengaruhi tanggung jawab Anda sebagai pengguna internet yang beretika?
3. Mengapa kesadaran dan kehati-hatian dalam berbagi data dapat dihubungkan dengan nilai-nilai spiritual (Cinta kepada Tuhan Yang Maha Esa)?

Lampiran 2. Bahan Ajar

A. Ringkasan Materi

Keamanan data pada perangkat digital sangat krusial karena hampir seluruh aktivitas kita terekam. Ancaman umum meliputi phishing (upaya memperoleh data sensitif melalui penipuan), malware (perangkat lunak jahat seperti virus atau ransomware), dan kebocoran data akibat kata sandi lemah. Untuk melindungi diri, kita harus menggunakan kata sandi yang unik dan kuat, mengaktifkan otentikasi dua faktor (2FA), dan sangat berhati-hati dalam memberikan izin akses pada aplikasi yang terpasang di handphone atau laptop. Data pribadi adalah aset yang harus dijaga dengan hati-hati, sejalan dengan etika digital bahwa kita harus bertanggung jawab atas informasi yang kita miliki dan bagikan.

B. Sumber Belajar Tambahan

Video Pembelajaran: https://www.youtube.com/watch?v=ContohLinkKeamananSiber
Artikel/Simulasi: https://www.bssn.go.id/edukasi-siber/

Lampiran 3. Instrumen Asesmen

A. Daftar Pertanyaan/Soal Tes

1. Jelaskan perbedaan antara malware dan phishing, serta berikan satu contoh konkret dari masing-masing ancaman.
2. Mengapa penggunaan kata sandi yang sama untuk berbagai akun sangat berisiko? (Penalaran Kritis).
3. Anda menemukan sebuah aplikasi game yang meminta izin akses ke kontak telepon dan mikrofon. Berikan analisis kritis apakah izin tersebut wajar atau berlebihan, dan apa risiko yang ditimbulkan jika izin diberikan?
4. Sebagai seorang pelajar yang kreatif, buatlah langkah-langkah persuasif (minimal 3 langkah) untuk meyakinkan teman Anda agar segera mengaktifkan 2FA pada akun media sosialnya.

B. Rubrik Penilaian Kinerja

Aspek yang Dinilai	Skor 1 (Kurang)	Skor 2 (Cukup)	Skor 3 (Baik)	Skor 4 (Sangat Baik)
Penalaran Kritis dan Analisis Masalah (Esai)	Jawaban dangkal, tidak dapat membedakan konsep keamanan dasar, dan tidak menyertakan contoh yang relevan.	Mampu menjelaskan konsep dasar tetapi analisis terhadap studi kasus kurang mendalam dan solusinya tidak realistis.	Mampu membedakan konsep, menganalisis studi kasus dengan baik, dan memberikan solusi yang logis.	Mampu menjelaskan kon komprehensif, melakuka kritis yang tajam, dan m solusi inovatif dan berke
Kreativitas dan Kualitas Produk (Panduan Digital)	Panduan sangat sederhana, kurang informatif, dan desain tidak menarik.	Panduan informatif tetapi minim kreativitas dalam desain dan penyajian materi.	Panduan informatif, menggunakan desain yang cukup menarik, dan pesan keamanan tersampaikan dengan jelas.	Panduan sangat kreatif, didukung data, dan men bahasa visual yang per mudah dipahami ole audiens.
Komunikasi dan Presentasi	Penyampaian gagasan tidak terstruktur, kurang percaya diri, dan sulit dipahami.	Penyampaian terstruktur tetapi kurang interaktif dan tidak mampu menjawab pertanyaan dengan baik.	Penyampaian jelas, terstruktur, dan mampu menjawab sebagian besar pertanyaan kelompok lain dengan baik.	Penyampaian sangat menggunakan teknik k yang efektif, dan memimpin diskusi serta sanggahan dengan argu kuat.
Sikap Kerja (Kolaborasi dan Etika)	Sama sekali tidak berpartisipasi dalam kelompok dan mengabaikan nilai-nilai kejujuran digital.	Kurang aktif dalam diskusi dan hanya mengikuti instruksi minimal yang diberikan.	Aktif berpartisipasi, menghargai pendapat teman, dan menunjukkan tanggung jawab dalam mencari ilmu pengetahuan.	Sangat proaktif, menja penggerak menunjukkan semanga yang tinggi (Cint Pengetahuan), serta men digital dan kejujuran d kepada Tuhan Yang Mah