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: Siswa sudah aktif menggunakan berbagai platform digital namun memiliki pemahaman yang bervariasi mengenai pentingnya privasi dan ancaman siber yang mengintai data pribadi mereka.
Materi Pelajaran: Menjaga keamanan data diri dari ancaman kejahatan dunia digital
Dimensi Profil Lulusan: Keimanan dan Ketakwaan terhadap Tuhan YME, Penalaran Kritis, Kemandirian, Cinta kepada Ilmu Pengetahuan, Cinta kepada Bangsa dan Negeri

2. Desain Pembelajaran

Capaian Pembelajaran: Siswa mampu menganalisis berbagai ancaman keamanan data diri di dunia digital dan secara mandiri menerapkan solusi perlindungan yang efektif.
Lintas Disiplin Ilmu: PPKN (Hukum dan Etika Digital), Bahasa Indonesia (Penyusunan Laporan dan Infografis), Sosiologi (Dampak sosial kejahatan siber)
Kemitraan Pembelajaran: Praktisi Keamanan Siber (Narasumber), Komunitas IT Lokal, Pihak Kepolisian (Divisi Siber)
Tujuan Pembelajaran:

1. Menganalisis secara kritis jenis-jenis ancaman keamanan data diri (phishing, malware, rekayasa sosial).
2. Menerapkan praktik terbaik dalam membuat dan mengelola kata sandi yang kuat serta otentikasi dua faktor (2FA).
3. Menjelaskan pentingnya menjaga etika digital sebagai bentuk tanggung jawab pribadi dan nasional (Cinta Bangsa).
4. Merumuskan langkah-langkah pencegahan dan penanggulangan dini terhadap kebocoran data.

Topik Pembelajaran: Keamanan Data Pribadi dan Pencegahan Kejahatan Siber (Cybercrime) di Era Digital.
Model: Problem-Based Learning, Project-Based Learning
Metode: Studi Kasus, Diskusi Kelompok, Simulasi Praktik, Presentasi Hasil.

3. Pengalaman Belajar

Kegiatan Awal:

1. Pembukaan dan Doa bersama (Keimanan dan Ketakwaan).
2. Apersepsi: Guru menampilkan berita atau studi kasus kebocoran data viral di Indonesia.
3. Ice breaking: Pertanyaan pemicu 'Apakah Anda yakin data Anda aman?'
4. Penyampaian tujuan pembelajaran dan relevansi materi dengan pengembangan Penalaran Kritis dan Kemandirian siswa.

Kegiatan Inti:

1. Orientasi Masalah: Siswa dibagi kelompok dan diberikan studi kasus kejahatan siber (misalnya, akun diretas karena mengklik tautan palsu).

2. Pengorganisasian Belajar: Siswa merumuskan pertanyaan kunci: Bagaimana data diri bisa tercuri? dan Bagaimana cara mencegahnya? (Penalaran Kritis).
3. Pembimbingan Individu/Kelompok: Siswa melakukan riset mengenai terminologi dan teknik keamanan (kata sandi, 2FA, enkripsi).
4. Pengembangan dan Penyajian Hasil: Setiap kelompok membuat daftar 'Lima Dosa Digital' (kesalahan fatal dalam keamanan data) dan solusinya.
5. Analisis dan Evaluasi: Praktik simulasi penerapan 2FA pada perangkat, diikuti oleh diskusi kritis terhadap proses yang dilakukan (Kemandirian, Cinta Ilmu Pengetahuan).

Kegiatan Penutup:

1. Refleksi Individu: Siswa mencatat 3 poin penting yang mengubah cara pandang mereka tentang keamanan data.
2. Kesimpulan: Guru bersama siswa merangkum langkah-langkah utama dalam menjaga privasi data (etika digital).
3. Penugasan: Membuat infografis digital/poster cetak (proyek) yang berisi tips keamanan data diri yang mudah dipahami publik (Cinta Bangsa dan Negeri).
4. Doa penutup dan salam.

4. Asesmen Pembelajaran

Asesmen Awal: Tanya jawab lisan tentang istilah 'phishing' dan 'privasi' untuk mengukur pengetahuan dasar siswa.
Asesmen Proses: Observasi keaktifan diskusi, kemampuan analisis studi kasus, dan kolaborasi dalam kelompok (Penalaran Kritis dan Kemandirian).
Asesmen Akhir: Penilaian Proyek (Infografis/Poster Keamanan Data) dan Tes Tertulis (esai) mengenai analisis kasus dan solusi perlindungan data.

Jabung, 26 Januari 2026

Mengetahui,

Kepala Madrasah	**Guru Mata Pelajaran**,
Muroihatul Jannah, M.Pd	**Muhammad Badrul Huda, S.Pd**

Lampiran 1. LKPD (Lembar Kerja Peserta Didik)

Nama	:	.....
Kelas	:	IX -
Materi	:	Menjaga keamanan data diri dari ancaman kejahatan dunia digital

Langkah Kerja:

1. Tentukan satu akun digital (Email/Media Sosial) yang sering Anda gunakan.
2. Lakukan evaluasi kekuatan kata sandi Anda saat ini menggunakan alat online atau kriteria 12+ karakter dan kombinasi unik.
3. Akses pengaturan keamanan dan aktifkan Otentikasi Dua Faktor (2FA) menggunakan aplikasi otentikator atau SMS.
4. Simulasikan skenario lupa kata sandi dan bagaimana proses pemulihan akun Anda bekerja.
5. Dokumentasikan hasil evaluasi kata sandi, proses aktivasi 2FA, dan identifikasi potensi kelemahan yang masih ada.

Pertanyaan Reflektif:

1. Berdasarkan studi kasus hari ini, seberapa besar tanggung jawab individu dalam mencegah kejahatan siber?
2. Mengapa etika digital dan kejujuran (Keimanan) sangat krusial saat berurusan dengan data pribadi orang lain?
3. Sebagai generasi muda, langkah konkret apa yang akan Anda ambil besok untuk memastikan lingkungan digital Anda lebih aman?

Lampiran 2. Bahan Ajar

A. Ringkasan Materi

Keamanan data diri adalah tindakan melindungi informasi sensitif seperti nama lengkap, alamat, NIK, dan kredensial akun dari akses yang tidak sah. Ancaman utama meliputi phishing (penipuan berkedok), malware (perangkat lunak jahat), dan rekayasa sosial (manipulasi psikologis). Perlindungan terbaik melibatkan kombinasi teknologi (password kuat, 2FA, enkripsi) dan kesadaran diri (tidak mudah percaya, cek sumber informasi). Menjaga data diri bukan hanya urusan individu, tetapi juga kontribusi pada ketahanan siber nasional.

B. Sumber Belajar Tambahan

Video Pembelajaran: https://www.youtube.com/watch?v=y78X9_KeamananDataPribadi
Artikel/Simulasi: https://kominfo.go.id/content/artikel/panduan_perlindungan_data_pribadi_di_media_sosial

Lampiran 3. Instrumen Asesmen

A. Daftar Pertanyaan/Soal Tes

1. Jelaskan secara rinci tiga jenis kejahatan siber yang paling sering mengincar data pribadi siswa SMP.
2. Mengapa menggunakan manajer kata sandi lebih dianjurkan daripada mencatat kata sandi di kertas atau di notes ponsel?
3. Jelaskan hubungan antara Penalaran Kritis dan pencegahan rekayasa sosial (social engineering).
4. Beri contoh kasus di mana seseorang menunjukkan Cinta kepada Bangsa dan Negeri melalui kepeduliannya terhadap keamanan data siber.
5. Anda menerima pesan darurat dari 'bank' yang meminta konfirmasi PIN melalui tautan. Bagaimana Anda mengevaluasi keaslian pesan ini?

B. Rubrik Penilaian Kinerja

Aspek yang Dinilai	Skor 1 (Kurang)	Skor 2 (Cukup)	Skor 3 (Baik)	Skor 4 (Sangat Baik)
Analisis dan Pemahaman Ancaman (Penalaran Kritis)	Tidak mampu mengidentifikasi ancaman utama atau gagal membedakan jenis kejahatan siber.	Mampu mengidentifikasi beberapa ancaman dasar, namun penjelasan tidak sistematis.	Mampu mengidentifikasi, membedakan, dan menjelaskan ancaman siber dengan cukup baik serta menunjukkan analisis yang logis.	Mampu menganalisis studi kasus secara mendalam, menghubungkan ancaman dengan potensi risiko, dan menunjukkan penalaran kritis yang kuat.
Keterampilan Praktis (Kemandirian)	Gagal melaksanakan langkah-langkah praktik (misalnya 2FA) atau membutuhkan bantuan penuh.	Melaksanakan langkah praktik dengan bantuan minimal, hasil belum optimal.	Mampu melaksanakan praktik keamanan (2FA, evaluasi password) secara mandiri dan hasilnya efektif.	Mampu melaksanakan praktik, menguji keamanannya, dan memberikan rekomendasi perbaikan yang orisinal dan efektif.
Hasil Proyek/Infografis (Cinta Ilmu Pengetahuan, Cinta Bangsa)	Infografis tidak relevan dengan topik atau tidak informatif.	Infografis cukup informatif, namun tata letak kurang menarik dan target audiens tidak jelas.	Infografis informatif, desain menarik, dan pesan keamanan data tersampaikan dengan jelas dan benar.	Infografis sangat kreatif, memuat informasi yang akurat dan terperinci, serta menunjukkan upaya edukasi yang tinggi kepada masyarakat luas (Cinta Bangsa).
Sikap dan Etika Digital (Keimanan dan Ketakwaan)	Tidak menunjukkan tanggung jawab dalam diskusi atau cenderung meremehkan isu keamanan data.	Cukup bertanggung jawab namun kurang konsisten dalam bersikap etis selama proses pembelajaran.	Menunjukkan etika digital yang baik, menghargai privasi teman, dan bertanggung jawab terhadap data yang diolah.	Secara konsisten menunjukkan integritas dan etika digital yang sangat tinggi, serta secara aktif mengingatkan rekan tentang pentingnya Keimanan dan etika dalam menjaga data.