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 sudah aktif menggunakan perangkat digital (HP/PC) dalam kehidupan sehari-hari namun belum sepenuhnya memahami risiko dan praktik pencegahan kebocoran data, sehingga diperlukan pendekatan berbasis studi kasus.
Materi Pelajaran: Memahami dan menjelaskan nterhadap keamanan data yang terjadi ketika menggunkan perangkat hp/pc.
Dimensi Profil Lulusan: Penalaran Kritis, Kolaborasi, Kemandirian, Cinta kepada Ilmu Pengetahuan, Cinta kepada Bangsa dan Negeri

2. Desain Pembelajaran

Capaian Pembelajaran: Peserta didik mampu menganalisis berbagai ancaman keamanan data pada perangkat digital dan menerapkan langkah-langkah perlindungan data yang efektif dan bertanggung jawab.
Lintas Disiplin Ilmu: Pendidikan Kewarganegaraan (Etika Digital dan Hukum ITE), Bahasa Indonesia (Penyusunan Laporan dan Presentasi), Bimbingan Konseling (Kesehatan Mental Digital)
Kemitraan Pembelajaran: Pakar Keamanan Siber Lokal, Komunitas IT (misalnya ID-CERT), Divisi IT Perusahaan/Instansi Pemerintah
Tujuan Pembelajaran:

1. Mengidentifikasi jenis-jenis ancaman keamanan data (phishing, malware, kebocoran) pada perangkat digital dengan teliti. (Penalaran Kritis)
2. Menganalisis cara kerja enkripsi dan autentikasi dua faktor sebagai solusi keamanan. (Cinta Ilmu Pengetahuan)
3. Mendemonstrasikan praktik pengamanan data pribadi (password manager, pengaturan privasi) secara mandiri. (Kemandirian)
4. Merumuskan dan mempresentasikan etika digital yang bertanggung jawab sebagai wujud kepedulian terhadap keamanan nasional dan individu. (Kolaborasi, Cinta Bangsa dan Negeri)

Topik Pembelajaran: Ancaman Keamanan Data Digital (HP/PC), Praktik Pengamanan Data, dan Etika Penggunaan Perangkat.
Model: Problem-Based Learning (PBL), Discovery Learning
Metode: Studi Kasus, Diskusi Kelompok, Simulasi Praktik (Setting Keamanan), Presentasi

3. Pengalaman Belajar

Kegiatan Awal:

- Salam, doa, dan pengecekan kehadiran.
- Apersepsi: Guru menampilkan berita viral terkait kebocoran data atau penipuan siber.
- Asesmen Awal (Pretest Lisan): Menanyakan seberapa sering siswa mengganti kata sandi dan risiko apa yang mereka ketahui.
- Orientasi: Guru menyampaikan tujuan pembelajaran dan kaitannya dengan Profil Pelajar Pancasila (Penalaran Kritis dan Kemandirian).

Kegiatan Inti:

- Stimulasi (Identifikasi Masalah): Siswa dibagi kelompok dan diberikan studi kasus kebocoran data yang berbeda (misalnya, akun diretas, data ponsel dicuri).
- Pengumpulan Data: Siswa mencari informasi (online/bahan ajar) tentang jenis ancaman, mekanisme serangan, dan dampaknya.
- Pengolahan Data (Kolaborasi & Kritis): Diskusi kelompok untuk merumuskan solusi teknis (misal: penggunaan VPN, sandi unik) dan solusi etika untuk mencegah ancaman tersebut.
- Pembuktian (Praktik Mandiri): Setiap siswa mempraktikkan pengaturan keamanan dasar pada perangkat mereka sendiri (misal: otentikasi 2FA, izin aplikasi yang mencurigakan).
- Generalisasi (Presentasi): Setiap kelompok mempresentasikan temuan mereka, menyoroti pentingnya keamanan data bagi diri sendiri dan negara.

Kegiatan Penutup:

- Guru dan siswa merangkum poin-poin penting mengenai praktik keamanan siber yang baik.
- Refleksi: Siswa mengisi jurnal refleksi menggunakan pertanyaan reflektif yang disediakan.
- Tindak Lanjut: Pemberian tugas mandiri untuk membuat daftar 'Do's and Don'ts' Keamanan Siber yang akan ditempel di ruang kelas.
- Penghargaan atas kolaborasi dan kemandirian siswa.

4. Asesmen Pembelajaran

Asesmen Awal: Tanya jawab lisan singkat mengenai pengalaman terkena iklan/notifikasi mencurigakan dan pretest pilihan ganda 5 soal terkait istilah dasar keamanan data.
Asesmen Proses: Observasi kerja kelompok (Kolaborasi), Penilaian Kinerja saat praktik setting keamanan (Kemandirian), dan keaktifan diskusi (Penalaran Kritis).
Asesmen Akhir: Laporan Analisis Studi Kasus Keamanan Data (Tertulis) dan Tes Keterampilan (demonstrasi penggunaan autentikasi dua faktor pada salah satu akun mereka).

Mengetahui,
Malang, 19 Januari 2026

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

Lampiran 1. LKPD (Lembar Kerja Peserta Didik)

Nama	:	.....
Kelas	:	IX- ...
Materi	:	Memahami dan menjelaskan nterhadap keamanan data yang terjadi ketika menggunkan perangkat hp/pc.

Langkah Kerja:

1. Bentuk kelompok (4-5 siswa) dan pilih salah satu studi kasus kebocoran data (HP atau PC).
2. Analisis kasus: Identifikasi jenis ancaman, mekanisme serangan, dan kerugian yang ditimbulkan (Penalaran Kritis).
3. Rancang Solusi Teknis: Cari tahu dan catat langkah-langkah pencegahan teknis (misalnya: cara mengaktifkan 2FA, tips membuat sandi kuat).
4. Praktek Pengamanan: Secara individu, terapkan salah satu solusi teknis pada perangkat Anda (misalnya pengaturan privasi aplikasi).
5. Susun laporan/slide presentasi yang berisi ancaman, dampaknya, dan solusi etis/praktis (Kolaborasi).
6. Presentasikan hasil temuan kelompok di depan kelas.

Pertanyaan Reflektif:

- Apa pelajaran terbesar yang Anda dapatkan hari ini tentang nilai data pribadi?
- Bagaimana pengetahuan ini mengubah cara Anda menggunakan perangkat HP atau PC ke depannya?
- Mengapa menjaga keamanan data pribadi dan data negara menjadi bentuk dari 'Cinta kepada Bangsa dan Negeri'?

Lampiran 2. Bahan Ajar

A. Ringkasan Materi

Keamanan data digital adalah upaya melindungi informasi dari akses, penggunaan, pengungkapan, gangguan, atau penghancuran yang tidak sah. Ancaman utama meliputi *phishing* (penipuan untuk mendapatkan data sensitif), *malware* (program jahat seperti virus dan ransomware), dan kebocoran data akibat kelemahan sistem atau kelalaian pengguna. Perangkat HP dan PC adalah target utama, di mana pengguna seringkali rentan karena menggunakan sandi lemah atau mengunduh aplikasi tidak resmi. Pencegahan memerlukan kombinasi teknologi dan etika. Secara teknologi, penting untuk selalu memperbarui sistem operasi, menggunakan autentikasi dua faktor (2FA), dan mengelola kata sandi menggunakan *password manager*. Secara etika, pengguna harus kritis (Penalaran Kritis) terhadap setiap tautan atau permintaan informasi sensitif, serta memahami bahwa data yang mereka kelola memiliki dampak luas, termasuk pada keamanan siber nasional (Cinta Bangsa dan Negeri). Kemandirian dalam mengelola keamanan adalah kunci untuk menghindari kerugian.

B. Sumber Belajar Tambahan

Video Pembelajaran: https://www.youtube.com/watch?v=yYf-S-0J4QY
Artikel/Simulasi: https://kominfo.go.id/content/detail/36109/tips-aman-berinternet-dari-direktorat-jenderal-aptika-kemenkominfo/0/tips_dan_trik

Lampiran 3. Instrumen Asesmen

A. Daftar Pertanyaan/Soal Tes

1. Jelaskan perbedaan mendasar antara *phishing* dan *malware*. Berikan contoh bagaimana keduanya dapat menyerang HP dan PC.
2. Mengapa penggunaan autentikasi dua faktor (2FA) sangat disarankan untuk akun penting?
3. Sebagai seorang warga negara yang sadar akan keamanan data, jelaskan minimal tiga langkah preventif yang harus Anda lakukan sebelum mengunduh aplikasi baru di Play Store/App Store?
4. Studi Kasus: Rina menerima email yang mengaku dari banknya dan memintanya mengklik tautan untuk verifikasi akun segera. Jelaskan bagaimana Penalaran Kritis dapat membantu Rina dalam menyikapi email ini?
5. Bagaimana konsep 'Cinta kepada Bangsa dan Negeri' berhubungan dengan praktik menjaga keamanan data digital?

B. Rubrik Penilaian Kinerja

Aspek yang Dinilai	Skor 1 (Kurang)	Skor 2 (Cukup)	Skor 3 (Baik)	Skor 4 (Sangat Baik)
Pemahaman Konsep (Penalaran Kritis)	Tidak mampu membedakan jenis ancaman atau menjelaskan mekanismenya.	Mampu membedakan jenis ancaman, namun penjelasannya kurang akurat dan tidak relevan dengan studi kasus.	Mampu menjelaskan jenis ancaman dengan akurat dan memberikan contoh relevan yang menghubungkan HP/PC.	Mampu menganalisis kasus ancaman secara komprehensif, merumuskan dampak, dan menyimpulkan solusi dengan tepat.
Kolaborasi dan Komunikasi	Pasif dan tidak berkontribusi dalam kelompok, laporan disusun secara individu.	Berkontribusi minimal; ide kurang jelas saat dikomunikasikan dan tidak mendukung anggota kelompok.	Aktif berdiskusi dan mampu mempresentasikan ide dengan jelas, serta mendengarkan pendapat teman.	Sangat aktif, memimpin diskusi, mengintegrasikan ide-ide kelompok, dan mampu menginspirasi anggota lain dalam menemukan solusi.
Keterampilan Praktik (Kemandirian)	Tidak mampu mengikuti langkah-langkah praktik pengamanan, membutuhkan bantuan penuh.	Mampu melakukan praktik (misal setting 2FA) dengan banyak bantuan guru/teman dan hasilnya belum optimal.	Mampu menerapkan langkah-langkah pengamanan data secara mandiri dan hasilnya sesuai standar yang diminta.	Mampu menerapkan langkah-langkah pengamanan dan menjelaskan justifikasi mengapa tindakan tersebut penting tanpa bantuan.
Etika dan Tanggung Jawab (Cinta Ilmu/Bangsa)	Tidak menunjukkan kesadaran etika dalam penggunaan data dan tidak peduli terhadap dampak kebocoran.	Menunjukkan sedikit kesadaran etika, namun tidak terhubung dengan pentingnya keamanan data nasional/ilmu pengetahuan.	Merumuskan etika digital yang baik dan menyadari pentingnya data bagi keamanan diri, serta antusias mencari tahu solusi teknis.	Merumuskan etika digital yang komprehensif dan secara jelas mengaitkan pentingnya keamanan data individu dengan keamanan siber nasional dan mendalami pengetahuan teknis yang ditemukan.