Kurikulum Merdeka

BAHAN AJAR

INFORMATIKA

Berdasarkan Kurikulum Merdeka Tahun Ajaran 2025/2026

Untuk SMP / MTs

KELAS

VIII

SEMESTER II

Nama : _____

No. Absen : _____

Kelas : _____

Sekolah : _____

KATA PENGANTAR

Puji syukur kami panjatkan kehadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat, taufik dan hidayah-Nya, sehingga kami dapat menyelesaikan penyusunan Bahan Ajar Informatika Kelas VIII Semester 2 Tahun Pelajaran 2025/2026 ini dengan baik tanpa suatu halangan yang berarti.

Bahan ajar ini berisi ringkasan materi, latihan, petunjuk praktikum, dan soal-soal evaluasi yang diharapkan dapat menjadi sarana yang efektif bagi peserta didik dalam mengasah kemampuan berpikir komputasional, berliterasi digital dalam memecahkan masalah. Penyusunan Bahan Ajar ini tidak lepas dari bantuan dari berbagai pihak. Oleh karena itu kami menyampaikan banyak terimakasih kepada semua pihak yang telah membantu penyusunan Bahan Ajar ini.

Kami berharap bahan ajar ini dapat dimanfaatkan secara optimal oleh guru sebagai panduan dalam proses pembelajaran serta oleh peserta didik sebagai sumber belajar yang mandiri dan bermakna. Kami juga menyadari bahwa bahan ajar ini masih memiliki keterbatasan dan belum sempurna. Oleh karena itu, kami dengan terbuka mengharapkan kritik dan saran yang membangun demi penyempurnaan di masa yang akan datang.

Akhir kata, semoga bahan ajar ini dapat memberikan manfaat dan kontribusi positif dalam meningkatkan kualitas pembelajaran Informatika di sekolah.

TIM PENYUSUN BAHAN AJAR INFORMATIKA

Kelas VIII Semester 2 Tahun Ajaran 2025/2026

MGMP Informatika SMP Kabupaten Kudus

Penyusun:

Dian Noor Arif, S.Kom.

Giyanto, S.Pd.

Editor

Fitriana Nur Cahyani, S.Kom.

Koordinator

Yusro, S.Pd, M.Pd.

DAFTAR ISI

BAB I
DATA DAN INFORMASI

Tujuan Pembelajaran
1. Mengetahui kredibilitas sumber informasi digital dan mengenal ekosistem media pers digital
2. Membedakan fakta dan opini
3. Menyaring informasi palsu (hoax) dalam kehidupan sehari-hari

Pertanyaan Pemantik
1. Apakah yang kalian ketahui mengenai kredibilitas sumber informasi?
2. Apakah yang kalian ketahui mengenai fakta dan opini? Apa saja perbedaannya?
3. Apakah yang dimaksud dengan informasi palsu (hoax)?

MATERI

A. Kredibilitas Data dan Informasi

Kredibilitas data dan informasi merujuk pada sejauh mana data dan informasi yang diperoleh dapat dipercaya dan diandalkan.

Hal-hal yang mempengaruhi kredibilitas data dan informasi:

1. Sumber Data dan Informasi, yang terdiri dari: otoritas sumber, yaitu sumber yang memiliki reputasi baik dan dikenal dalam bidangnya biasanya lebih dipercaya. Misalnya, jurnal ilmiah yang di-review oleh rekan sejawat (*peer-reviewed*) lebih kredibel daripada blog pribadi; afiliasi dan kredensial, dimana penulis atau sumber informasi yang memiliki afiliasi dengan institusi ternama atau memiliki kredensial yang relevan (misalnya, gelar akademis atau sertifikasi profesional) menambah kredibilitas informasi.
2. Akurasi, yang terdiri dari: akurasi/kecermatan data, dimana data harus bebas dari kesalahan dan penyimpangan. Ini berarti bahwa angka, fakta, dan statistik yang diberikan harus benar dan tepat sesuai dengan realitas; verifikasi, dimana informasi yang dapat diverifikasi melalui sumber lain atau melalui penelitian tambahan biasanya lebih dapat diandalkan. Akurasi juga ditingkatkan ketika data dikumpulkan dan disajikan dengan metodologi yang jelas dan transparan.
3. Kebaruan (*Timeliness*), yang terdiri dari: relevansi waktu, dimana data dan informasi yang terbaru seringkali lebih relevan, terutama dalam konteks yang cepat berubah seperti teknologi atau ekonomi. Informasi yang sudah usang mungkin tidak lagi mencerminkan keadaan sebenarnya dan dapat menyesatkan.
4. Ketepatan konteks, yang terdiri dari: konteks yang memadai, dimana informasi harus disajikan dalam konteks yang tepat untuk dipahami dengan benar. Informasi yang dikeluarkan dari konteksnya dapat memberikan gambaran yang salah atau menyesatkan; komprehensivitas, dimana informasi yang mencakup berbagai sudut pandang atau seluruh aspek dari suatu isu lebih kredibel dibandingkan informasi yang hanya menyajikan satu perspektif.
5. Tujuan dan Bias, yang terdiri dari objektivitas, dimana informasi yang disajikan secara objektif dan tanpa bias lebih kredibel. Sumber yang memiliki kepentingan tertentu, seperti agenda politik atau komersial, mungkin menyajikan informasi dengan bias tertentu; Pengungkapan Konflik Kepentingan, dimana sumber yang transparan tentang potensi konflik kepentingan cenderung lebih kredibel. Misalnya, penulis yang bekerja untuk perusahaan farmasi harus mengungkapkan ini saat menulis tentang obat-obatan.
6. Keterpercayaan Sumber Sekunder, yang terdiri dari: penggunaan sumber sekunder yang kredibel, dimana jika data atau informasi dikutip dari sumber lain; sumber asli harus kredibel. Informasi yang diambil dari sumber sekunder yang tidak terpercaya dapat menurunkan kredibilitas informasi yang disajikan.

7. Referensi dan Rujukan, yang terdiri dari: referensi yang dapat dilacak, dimana sumber informasi yang menyediakan referensi lengkap dan dapat dilacak ke sumber aslinya lebih kredibel. Ini memungkinkan pembaca untuk memverifikasi klaim yang dibuat; penggunaan literatur yang relevan, dimana informasi yang didasarkan pada penelitian atau literatur yang diakui di bidangnya menambah kredibilitas.
8. Etika dan Kejujuran, yang terdiri dari pengungkapan yang jujur, dimana data dan informasi yang disajikan secara jujur dan tanpa manipulasi, seperti tidak menyembunyikan data yang tidak mendukung argumen, lebih dapat dipercaya; dan penghormatan terhadap Hak Cipta dan Hak Intelektual, dimana mengutip sumber dengan benar dan tidak melakukan plagiarisme menunjukkan integritas informasi

B. Kredibilitas Sumber Data dan Informasi

Kredibilitas sumber data dan informasi mengacu pada sejauh mana suatu sumber dapat dipercaya dan diandalkan untuk menyediakan informasi yang akurat, objektif, dan relevan.

Kredibilitas sumber data dan informasi ditentukan oleh beberapa faktor sebagai berikut:

1. Reputasi Sumber: Sumber yang memiliki reputasi baik, seperti institusi akademik, lembaga riset, atau media ternama, dianggap lebih kredibel. Reputasi dibangun dari rekam jejak sumber informasi dalam memberikan data yang akurat dan dapat diandalkan.
2. Keahlian Penulis atau Kontributor: Kredibilitas sumber juga bergantung pada keahlian individu yang menghasilkan informasi. Pakar atau ahli di bidang tertentu, yang memiliki latar belakang pendidikan atau pengalaman yang relevan, lebih mungkin memberikan informasi yang akurat dan mendalam.
3. Metode Pengumpulan Data: Informasi yang dihasilkan melalui metode pengumpulan data yang valid dan reliabel lebih kredibel. Misalnya, data dari survei yang menggunakan sampel representatif dan metodologi statistik yang tepat lebih dapat dipercaya.
4. Transparansi dan Dokumentasi: Sumber yang transparan tentang bagaimana data dikumpulkan, dianalisis, dan disajikan cenderung lebih kredibel. Dokumentasi yang lengkap dan referensi yang jelas memungkinkan verifikasi informasi oleh pihak lain.
5. Konsistensi dan Verifikasi: Informasi yang konsisten dengan sumber lain yang sudah diakui kredibilitasnya atau yang dapat diverifikasi secara independen lebih dapat dipercaya

Jenis-jenis sumber data dan informasi yang kredibel antara lain:

1. Sumber Akademis

- Jurnal Ilmiah: Artikel yang dipublikasikan dalam jurnal yang di-review oleh rekan sejawat (*peer-reviewed journals*) dianggap sangat kredibel. Jurnal ini menerapkan standar ketat dalam proses seleksi dan penerbitan.
- Buku Akademik: Buku yang ditulis oleh ahli di bidang tertentu dan diterbitkan oleh penerbit ternama (misalnya, universitas) juga merupakan sumber yang kredibel.
- Lembaga Penelitian dan Pemerintah
- Laporan Penelitian: Laporan dari lembaga penelitian independen atau pemerintah, seperti *World Health Organization* (WHO), *United Nations* (UN), atau Badan Pusat Statistik (BPS), biasanya sangat kredibel karena mereka mengikuti metodologi yang ketat dan transparan.
- Data Statistik Resmi: Data yang dikeluarkan oleh lembaga pemerintah atau organisasi internasional, seperti data sensus, survei nasional, dan statistik ekonomi, dianggap sangat kredibel.

2. Media Terpercaya

- Surat Kabar dan Majalah Ternama: Media yang dikenal dengan integritas jurnalistik yang tinggi, seperti *The New York Times*, *The Guardian*, atau Kompas di Indonesia, cenderung lebih kredibel. Media ini biasanya memiliki tim editor yang ketat dan memverifikasi informasi sebelum dipublikasikan.

- Situs Berita Resmi: Portal berita online dari media yang diakui kredibilitasnya juga menjadi sumber informasi yang dapat dipercaya.
- Media Pemerintah dan Lembaga Pendidikan: Portal berita online dari media pemerintah yang biasanya diakhiri dengan ekstensi go.id, .gov, ac.id, .edu, dll.

3. Organisasi Profesional

- Publikasi dari Asosiasi Profesional: Laporan atau artikel yang dikeluarkan oleh asosiasi profesional, seperti *American Medical Association* (AMA) atau Ikatan Dokter Indonesia (IDI), biasanya sangat kredibel karena dihasilkan oleh para ahli dalam bidang tersebut.
- White Papers dan Position Papers: Dokumen ini sering disiapkan oleh organisasi professional atau industri sebagai panduan atau posisi resmi mereka dalam isu tertentu.

4. Dokumen Resmi

- Undang-Undang dan Peraturan: Teks hukum, undang-undang, peraturan, dan dokumen resmi lainnya yang dikeluarkan oleh pemerintah merupakan sumber informasi yang sangat kredibel dan diandalkan untuk memahami kerangka hukum dan kebijakan publik.
- Laporan Tahunan Perusahaan: Laporan tahunan yang diterbitkan oleh perusahaan, terutama yang sudah diaudit oleh pihak ketiga, merupakan sumber kredibel untuk informasi keuangan dan operasional.

5. Sumber Primer

- Wawancara dan Kesaksian: Informasi langsung dari wawancara dengan saksi atau ahli yang berpengalaman secara langsung dalam suatu kejadian atau topik merupakan sumber primer yang kredibel.
- Dokumen Arsip: Dokumen asli seperti surat, memo, dan catatan sejarah yang disimpan di arsip resmi adalah sumber primer yang sangat kredibel.

6. Data Open-Source

- Repositori Data Publik: Repositori yang menyimpan data open-source seperti GitHub untuk proyek perangkat lunak, atau Kaggle untuk dataset ilmiah, sering kali digunakan untuk penelitian dan dianggap kredibel karena data yang tersedia dapat diverifikasi dan digunakan kembali oleh komunitas

Salah satu hal yang paling banyak dilakukan pengguna di dunia maya yang didominasi oleh media sosial adalah berbagi dan meneruskan informasi yang berharga dan menghibur bagi orang lain. Namun pada kenyataannya, seringkali informasi yang dibagikan melalui media sosial adalah informasi yang tidak akurat atau biasa disebut dengan hoaks.
Dalam publikasi UNESCO berjudul "*Journalism, Fake News and Disinformation*: *A Handbook for Journalism Education and Training*" yang dirilis pada tahun 2018, UNESCO membagi fenomena kabar bohong atau hoaks menjadi tiga kategori, yaitu:

1. Misinformasi (*Misinformation*),

Misinformasi adalah informasi yang salah atau tidak akurat yang disebarkan tanpa adanya niat untuk menipu atau merugikan. Orang yang menyebarkan misinformasi biasanya tidak sadar bahwa informasi yang mereka bagikan adalah keliru. Contoh: Menyebarkan berita tentang sebuah peristiwa atau fakta yang tidak benar karena salah paham atau kurangnya verifikasi, tetapi tanpa niat buruk. Misalnya, seseorang membagikan berita Kesehatan yang salah karena percaya bahwa itu benar, tanpa ada niat untuk merugikan.
Ciri-ciri:

a. Biasanya tidak disengaja.
b. Disebarkan oleh orang-orang yang tidak memiliki informasi lengkap atau gagal memverifikasi sumber.

2. Disinformasi (*Disinformation*)

Disinformasi adalah informasi yang salah atau tidak akurat yang sengaja dibuat dan disebarkan dengan tujuan untuk menipu atau merugikan orang lain. Disinformasi sering kali dirancang untuk memanipulasi opini publik, memicu konflik, atau mencapai tujuan tertentu, seperti politik atau ekonomi.
Contoh: Berita palsu atau kampanye propaganda yang sengaja dibuat untuk mempengaruhi hasil pemilu atau menjelekkan kelompok tertentu dengan informasi yang sepenuhnya tidak benar.
Ciri-ciri:
a. Dibuat dengan niat yang disengaja untuk menyesatkan atau menipu.
b. Digunakan untuk menciptakan kebingungan, keraguan, atau permusuhan.
c. Sering diorganisir oleh pihak-pihak dengan agenda tersembunyi

3. Malinformasi (*Malinformation*)

Malinformasi adalah informasi yang sebenarnya benar atau akurat, tetapi disebarkan dengan niat untuk merugikan atau merusak reputasi individu, kelompok, atau negara. Dalam hal ini, informasi tersebut tidak dipalsukan, tetapi disajikan dengan cara yang menyesatkan atau keluar dari konteks yang tepat untuk menimbulkan dampak negatif.
Contoh: Membocorkan informasi pribadi yang benar tentang seseorang (seperti email pribadi atau foto) untuk mempermalukan atau merusak reputasinya. Contoh lain adalah menggunakan fakta yang benar tetapi disajikan secara manipulatif untuk memperburuk situasi tertentu, seperti dalam kampanye politik atau sosial.
Ciri-ciri:
a. Informasi yang dibocorkan atau digunakan adalah benar, tetapi niat di balik penyebarannya adalah untuk menciptakan kerusakan.
b. Sering kali melibatkan pengungkapan data pribadi atau informasi sensitif secara tidak etis.

Perbedaan Utama Ketiga Kategori tersebut adalah:
Misinformasi adalah kesalahan tanpa niat buruk.
Disinformasi adalah kesalahan yang dibuat dan disebarkan dengan niat menipu atau merugikan.
Malinformasi adalah informasi yang benar tetapi digunakan untuk menyakiti atau merugikan.

Agar terhindar dari pelaku tindak penyebaran informasi yang tidak akurat, berikut beberapa cara untuk mengetahui informasi yang tidak akurat:

1. **Mengembangkan pemikiran kritis**. Salah satu alasan utama penyebaran berita palsu adalah menciptakan "kejutan" yang menyebabkan seseorang menjadi emosional, senang, marah, ketakutan, dan hal lain. Oleh karena itu, saat membaca suatu berita kita harus menjaga diri dan tidak terpancing secara emosional. Baca dan pelajari yang dilihat dan didengar secara rasional dan kritis. Pikirkan: "Mengapa cerita ini ditulis? Apakah untuk meyakinkan tentang sudut pandang tertentu? Apakah akan berujung ke pengiriman uang? Apakah saya menjadi terpengaruh dan terpicu untuk melakukan sesuatu?"

2. **Memeriksa sumber informasi**. Jika menemukan cerita dari sumber yang belum pernah didengar sebelumnya, kita harus melakukan pencarian dan penggalian informasi! Periksa alamat web halaman yang dibaca. Cermati apakah ada kesalahan ejaan nama perusahaan di alamat web tersebut, atau ekstensi dari web. Domain resmi lembaga di Indonesia biasanya berakhiran dengan go.id, gov, sch.id, ac.id, edu, dll. Lembaga komersial diakhiri dengan .com. Penggunaan *Content Management System* (CMS) gratis perlu dicurigai sebagai penyebar informasi palsu. Penyebar informasi palsu terkadang membuat halaman web, surat kabar, atau gambar palsu yang terlihat resmi, tetapi sebenarnya palsu. Misalnya, jika kita membaca postingan mencurigakan yang berasal dari WHO,

maka kita harus memeriksa situs WHO sendiri untuk memverifikasi apakah informasi itu benar ada. Beberapa situs pengecekan berita terpercaya adalah: turnbackhoax.id, cekfakta.com, cekfakta.tempo.co, www.kompas.com/cekfakta, www.liputan6.com/cek-fakta.

3. **Melakukan cek dan ricek dari liputan lain**. Apakah ada media lain yang memberitakan informasi tersebut? Apa yang dikatakan sumber lain tentang itu? Pengecekan berita bisa dimulai dengan melihat liputan di media utama (mainstream) karena media profesional mainstream memiliki pedoman editorial yang ketat dan jaringan luas wartawan yang sangat terlatih Akan tetapi, ada juga kemungkinan bahwa media utama melakukan kesalahan atau memihak (tidak berimbang), maka baik jika mencari pembanding sumber yang lain juga.

4. **Cek validitas gambar.** Saat ini perangkat lunak pengeditan gambar dan foto sudah sangat canggih dan memudahkan penggunanya untuk membuat gambar palsu yang kelihatan seperti asli. Penelitian menunjukkan bahwa ternyata setengah dari kita terkecoh dengan gambar palsu. Namun, ada beberapa hal yang dapat digunakan sebagai petunjuk palsu, seperti bayangan aneh, tepi tidak mulus, dll. Namun bisa juga terjadi, bahwa suatu gambar itu valid dan akurat tetapi digunakan dalam konteks yang salah. Misalnya, foto sampah yang menutupi pantai bisa jadi berasal dari pantai yang berbeda atau dari gambar 10 tahun yang lalu, bukan peristiwa yang terjadi baru-baru ini. Untuk mendeteksi validitas gambar bisa digunakan tools seperti Google Image Search untuk memeriksa dari mana gambar berasal dan apakah itu telah diubah.
   Cara mengecek dengan Google Images: Buka https://images.google.com , simpan foto berita hoaks yang ingin diverifikasi dengan cara melakukan screenshot artikelnya. Upload/drag and drop screenshot ke pencarian di Google Images. Setelahnya, akan muncul hasil pencarian yang menampilkan situs pertama yang mengunggah foto tersebut. Situs ini akan muncul pada posisi pencarian paling atas, dari sini kita bisa tahu siapa yang menyebarkan gambar tersebut pertama kali. Cari tahu apakah situs web yang menyebarkan gambar itu kredibel atau tidak. Informasi dari laman lembaga negara dan pemerintah adalah kredibel.

5. **Gunakan akal sehat**. Berita bohong dirancang untuk memberikan kejutan atas harapan, ketakutan, dan emosi kita. Oleh karena itu kita bisa menggunakan akal sehat kita untuk mengetahui apakah informasinya bohong. Misalnya kita mendapat hadiah mobil tanpa kita pernah mengirimkan undian apapun, atau penyedia internet membagikan voucher gratis besar-besaran kepada semua penggunanya, dll

C. Menyaring Informasi Palsu (Hoax)

Media sosial semestinya dimanfaatkan untuk bersosialisasi dan berinteraksi dengan menyebarkan konten-konten positif. Sayangnya, beberapa pihak memanfaatkannya untuk menyebarkan informasi yang mengandung konten negatif. Jika hal tersebut dibiarkan, dikhawatirkan akan membahayakan generasi muda. Pemerintah juga terus berupaya untuk mengurangi penyebaran hoax atau berita palsu dengan cara menyusun undang-undang yang di dalamnya mengatur sanksi bagi pengguna internet yang turut menyebarkan konten negatif. Selain itu, Kementerian Komunikasi dan Digital turut mengedukasi masyarakat untuk meningkatkan literasi digital.

Literasi digital ini adalah kemampuan untuk memahami dan menggunakan informasi dalam berbagai bentuk dari berbagai sumber yang sangat luas yang diakses melalui perangkat komputer. Bawden (2001) menawarkan pemahaman baru mengenai literasi digital yang berakar pada literasi komputer dan literasi informasi. Literasi komputer berkembang pada dekade 1980-an, ketika komputer mikro semakin luas dipergunakan, tidak saja di lingkungan bisnis, tetapi juga di masyarakat. Namun, literasi informasi baru menyebar luas pada dekade 1990-an manakala informasi semakin mudah disusun, diakses, disebarluaskan melalui teknologi informasi berjejaring. Dengan demikian, mengacu pada

pendapat Bawden, literasi digital lebih banyak dikaitkan dengan keterampilan teknis mengakses, merangkai, memahami, dan menyebarluaskan informasi.

Salah satu isu yang terkait dengan literasi digital adalah adanya Hoaks. Hoaks yaitu kabar bohong yang sengaja dibuat untuk disamarkan seperti layaknya kebenaran. Hoaks atau berita/kabar bohong ini sangat subur penyebarannya di dalam media sosial. Bila Masyarakat tidak dapat membedakan antara berita benar atau berita bohong, maka hal ini menjadi ladang subur penyebaran hoaks tersebut.
Untuk mengenli sebuah berita itu benar atau bohong, ada beberapa ciri yang dapat dikenali, antara lain:

1. Biasanya diawali denggan kta-kata sugestif dan heboh
2. Informasi hoaks sering mencatut nama orang atau Lembaga terkenal
3. Terdengar mustahil terjadi, sehingga sering disertai hasil penelitian palsu atau tidak sesuai konteksnya
4. Hoaks tidak muncul di media massa, biasanya hanya muncul pada sistus yang diragukan kredibilitasnya serta lewat pesan-pesan berantai
5. Kalimat yang digunakan biasanya ditulis dengan banyak huruf kapital serta tanda seru

Beberapa cara yang dapat kita lakukan untuk memeriksa apakah suatu berita itu hoaks atau bukan adalah sebagai berikut:

1. **Periksa fakta**
   Sebelum membaca berita kita harus perhatikan dari mana berita itu berasal dan siapa sumbernya. Apakah dari institusi resmi sperti KPK atau POLRI? Atau sekedar rumor yang dihembuskan oleh orang-orang tertentu?
2. **Cermati alamat situs**
   Berdasarkan catatan Dewan Pers, di Indonesia terdapat sekitar 43.000 situs yang mengklaim sebagai portal berita. Dari jumlah tersebut, yang sudah terverifikasi sebagai situs berita resmi tidak sampai 300. Artinya terdapat setidaknya puluhan ribu situs yang berpotensi menyebarkan berita palsu di internet yang perlu kita waspadai.
   Oleh karena itu, untuk informasi yang diperoleh dari website, cermatilah Alamat URL situs dimaksud. Apabila berasal dari situs yang belum terverifikasi sebagai institusi pers resmi, misalnya menggunakan domain blog, maka informasi tersebut dapat dikatakan meragukan.
3. **Cek keaslian foto**
   Sering kali para pembuat hoaks mengedit foto untuk memprovokasi pembaca. Di era teknologi digital saat ini, bukan hanya konten berupa teks yang bisa dimanipulasi, melainkan juga konten lain berupa foto atau video.
   Cara untuk mengecek keaslian foto bisa dengan memanfaatkan mesin pencari Google Image. Hasil pencarian akan menyajikan gambar-gambar serupa yang terdapat di internet sehingga bisa dibandingkan.
4. **Cari informasi di Google dengan kata kunci terkait informasi tersebut**
   Jika mendapat informasi yang diragukan kebenarannya, lakukan *cross-check* dengan menuliskan kata kunci dari informasi tersebut di mesin pencari seperti Google. Hasil pencarian akan menunjukkan informasi terkait lainnya dari berbagai sumber yang dapat digunakan untuk melihat apakah informasi tersebut benar atau tidak.
5. **Periksa informasi tersebut di situs-situs dan media sosial**
   a. Turnbackhoax.id
   b. Cekfaka.com
   c. Stophoax.id

Kita juga bisa melaporkan hoaks di situs-situs tersebut

Agar dapat terhindar dari HOAKS, ada beberapa pertanyaan yang perlu ditanyakan pada diri sendiri sebelum menyebarkan informasi yang diterima, pertanyaannya sebagai berikut:

1. Apakah berita itu benar...? jika jawabannya TIDAK maka JANGAN DISEBARKAN tapi jika jawabannya YA, silakan lanjut ke pertanyaan berikutnya.
2. Apakah berita itu bermanfaat...? jika jawabannya TIDAK maka JANGAN DISEBARKAN tapi jika jawabannya YA, silakan lanjut ke pertanyaan berikutnya.
3. Apakah berita itu mendesak untuk disebarkan...? jika jawabannya TIDAK maka JANGAN DISEBARKAN tapi jika jawabannya YA, silakan berita tersebut disebarkan lalu Tunggu dan bersabar.

Gambar 1.1. Alur tindak lanjut ketika menerima informasi

D. Fakta dan Opini

1. Fakta

Fakta adalah pernyataan yang dapat dibuktikan kebenarannya melalui bukti empiris atau data yang objektif. Fakta menggambarkan peristiwa, kejadian, atau keadaan yang benar-benar terjadi dan tidak dapat disangkal kebenarannya. Fakta bisa diverifikasi melalui pengamatan, data statistik, dokumentasi, atau laporan yang dapat diuji ulang.

Ciri-ciri Fakta:

a. Objektif: Fakta bersifat netral, tidak dipengaruhi oleh sudut pandang atau perasaan.
b. Dapat Diverifikasi: Fakta dapat dibuktikan kebenarannya dengan menggunakan sumber terpercaya, seperti dokumen, data ilmiah, atau rekaman kejadian.
c. Universal: Fakta diterima secara luas oleh orang-orang karena didukung oleh bukti yang dapat diterima.

Contoh Fakta: Semaraang adalah ibu kota provinsi Jawa Tengah, Air membeku pada suhu 0°C, Pada tahun 1969, manusia pertama kali mendarat di bulan.

2. Opini.

Opini adalah pernyataan yang mencerminkan pandangan, pendapat, interpretasi, atau keyakinan seseorang. Opini seringkali dipengaruhi oleh perasaan, kepercayaan, dan perspektif individu atau kelompok, sehingga tidak bisa diverifikasi atau dibuktikan kebenarannya secara mutlak. Opini bersifat subjektif dan tidak selalu memiliki dasar bukti kuat seperti fakta.

Ciri-ciri Opini:

a. Subjektif: Opini tergantung pada sudut pandang, perasaan, atau interpretasi individu, dan dapat berbeda antara satu orang dengan yang lain.
b. Tidak Dapat Diverifikasi: Opini tidak bisa dibuktikan benar atau salah secara pasti, karena merupakan pandangan pribadi yang tidak harus didasarkan pada bukti.
c. Bervariasi: Karena dipengaruhi oleh pengalaman dan sudut pandang masing-masing individu, opini bisa berbeda dari satu orang ke orang lain.

Contoh Opini: Jakarta adalah kota yang paling menarik di Indonesia; menurut saya, es krim rasa coklat lebih enak daripada vanila; film itu sangat membosankan.

3. Persamaan antara Fakta dan Opini

a. Keduanya adalah Pernyataan: Baik fakta maupun opini adalah bentuk pernyataan yang dibuat oleh seseorang atau ditulis dalam suatu konteks tertentu. Mereka sama-sama digunakan untuk menyampaikan ide atau informasi.
b. Dapat Digunakan untuk Mendukung Argumentasi: Fakta dan opini sering digunakan bersamaan dalam berbagai argumen, seperti dalam debat, artikel, atau diskusi, di mana fakta berfungsi untuk mendukung atau memperkuat opini.
c. Ditemukan dalam Komunikasi Sehari-hari: Fakta dan opini selalu muncul dalam percakapan sehari-hari, media, atau tulisan. Orang sering kali menggunakan keduanya untuk menyampaikan pemikiran, perasaan, atau memberikan informasi salah, dan personal atau kontekstual (opini bisa bervariasi tergantung pada individu atau konteks tertentu).

4. Perbedaan antara Fakta dan Opini

Kriteria	Fakta	Opini
Sifat	Objektif, netral, dan didukung oleh bukti	Subjektif, dipengaruhi oleh perasaan pribadi
Dapat diverifikasi	Kebenarannya tetap, tidak berubah dengan sudut pandang	Kebenaran tergantung pada pandangan individu
Penggunaan	Digunakan untuk memberikan informasi yang akurat	Digunakan untuk menyampaikan pendapat atau perasaan
Contoh	"Matahari terbit di timur."	"Matahari terbit adalah pemandangan yang indah."

Latihan 1

1. Jelaskan hal-hal yang mempengaruhi kredibilitas data dan informasi!
2. Jelaskan faktor-faktor yang mempengaruhi kredibilitas sumber data dan informasi!
3. Apakah yang dimaksud dengan fakta?
4. Jelaskan pengertian opini!
5. Sebutkan persamaan fakta dengan opini!

E. Melakukan Validasi Data (Materi Tambahan)

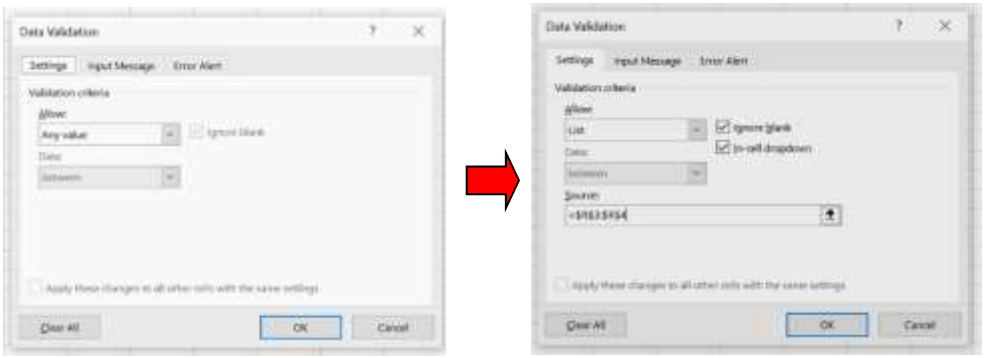
Validasi adalah proses pengecekan kesesuaian nilai yang diinput ke lembar kerja terhadap tipe data dan batasan nilai yang telah ditentukan. Validasi berguna untuk mencegah kesalahan input data secara tidak sengaja. Selain itu, proses validasi dilakukan untuk mencegah terjadinya pemasukan nilai yang salah dan menghindari terjadinya *error* (kesalahan) ketika nilai-nilai tersebut digunakan dalam penghitungan fungsi.

Berikut beberapa bentuk validasi data menggunakan Micrososft Excel yang dapat digunakan dan cara melakukannya:

1. Membatasi Data yang Diinput Hanya pada Pilihan yang Telah Ada di dalam Daftar

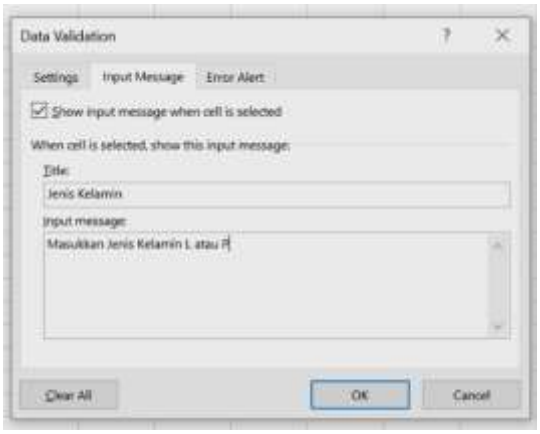
Sebagai contoh, data jenis kelamin hanya dapat diinput dari pilihan L dan P. Untuk melakukan validasi dengan nilai pilihan, dapat dilakukan dengan langkah-langkah sebagai berikut:

a. Buatlah daftar nilai yang dapat digunakan, dalam hal ini kita menempatkan nilai L di cell R3 dan P di cell R4. Dengan kata lain, cell R3:R4 merupakan daftar nilai yang diizinkan.
b. Pilih cell yang ingin diatur nilai validasinya, misalnya kita ingin mengatur validasi kolom jenis kelamin di cell E3 sampai E22. Pilih cell E3 sampai E22.
c. Pada tab Data, klik tombol Data Validation. Pada menu yang muncul, klik Data Validation. Kotak dialog Data Validation akan ditampilkan.



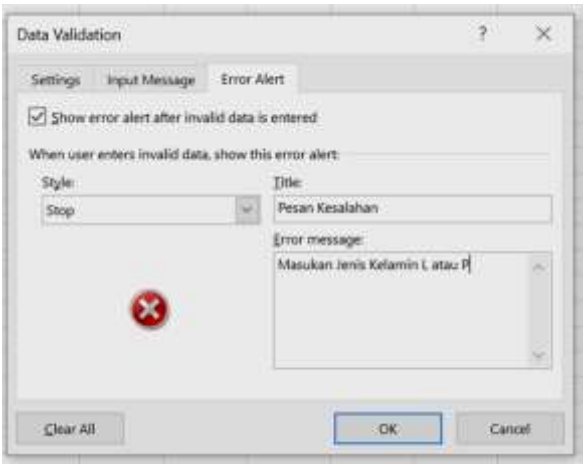
Gambar 1.2. Mengatur validasi menggunakan nilai yang ada di daftar

d. Klik tab *Input Message*, kemudian tambahkan pesan yang ingin disampaikan sebagai petunjuk kepada pengguna Ketika menginput data. Pesan akan ditampilkan Ketika pengguna memilih salah satu cell yang divalidasi.



Gambar 1.3. Mengatur pesan untuk menginput data

e. Klik tab Error Alert. Kemudian tambahkan pesan yang ingin disampaikan jika pengguna memberikan nilai yang salah.

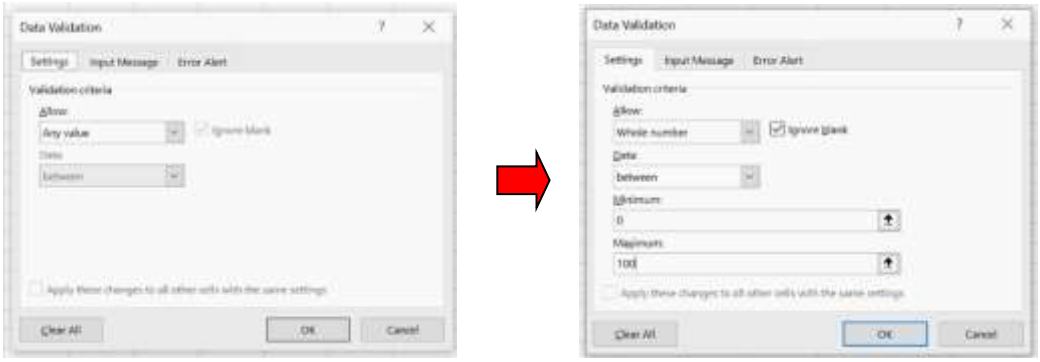


Gambar 1.4. Mengatur pesan kesalahan kepada pengguna

f. Klik tombol OK
g. Input nilai ke kolom yang telah divalidasi, kemudian coba berikan nilai yang benar dan nilai yang salah untuk memastikan pengaturan berjalan dengan baik.

2. Membaca Angka dalam Batasan Tertentu

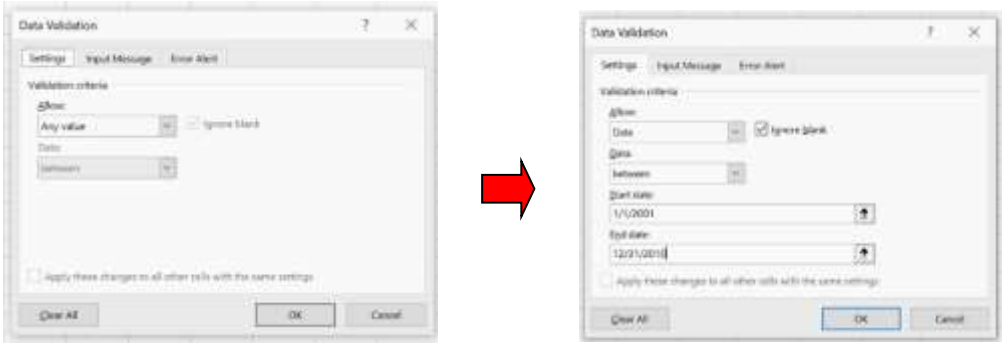
Sebagai contoh, data input nilai untuk ujian dapat dibatasi antara 0 sampai 100.



Gambar 1.5. Mengatur validasi menggunakan rentang nilai tertentu

3. Membatasi Tanggal pada Batasan Tanggal tertentu

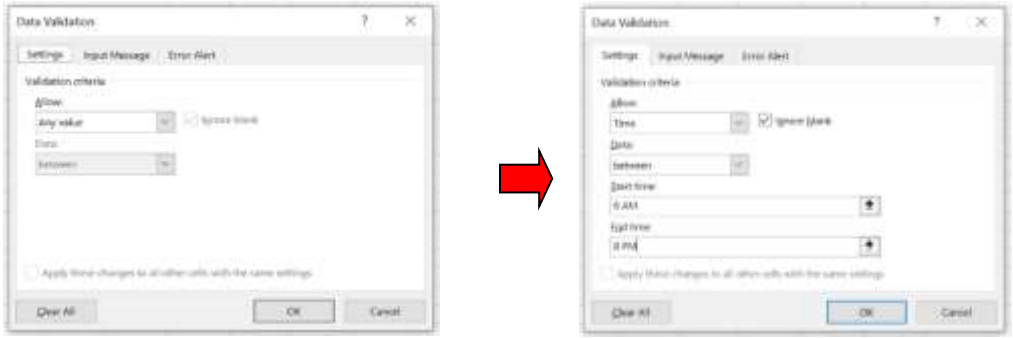
Sebagai contoh tanggal lahir dapat diatur antara tanggal 01 Januari 2001 sampai tanggal 31 Desember 2010.



Gambar 1.6. Mengatur validasi menggunakan rentang tanggal tertentu

4. Membatasi Waktu pada Batasan Waktu Tertentu

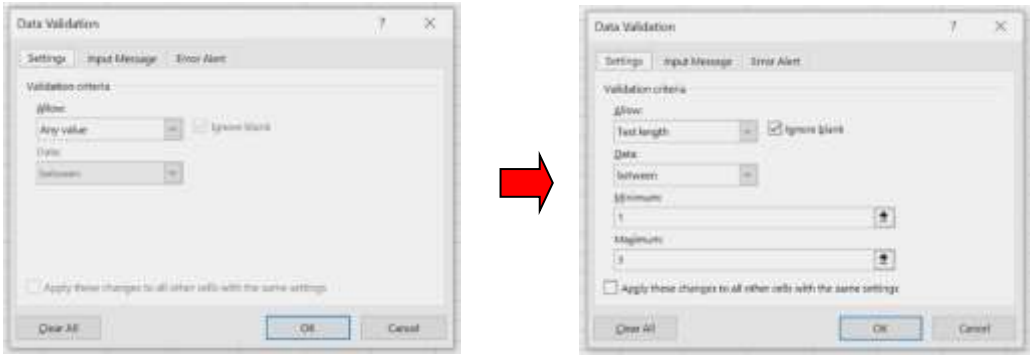
Sebagai contoh, data masuk dan pulang pegawai dapat dibatasi antara jam 6.00 AM sampai 8.00 PM.



Gambar 1.7. Mengatur validasi menggunakan rentang waktu tertentu

5. Membatasi Jumlah Karakter Teks

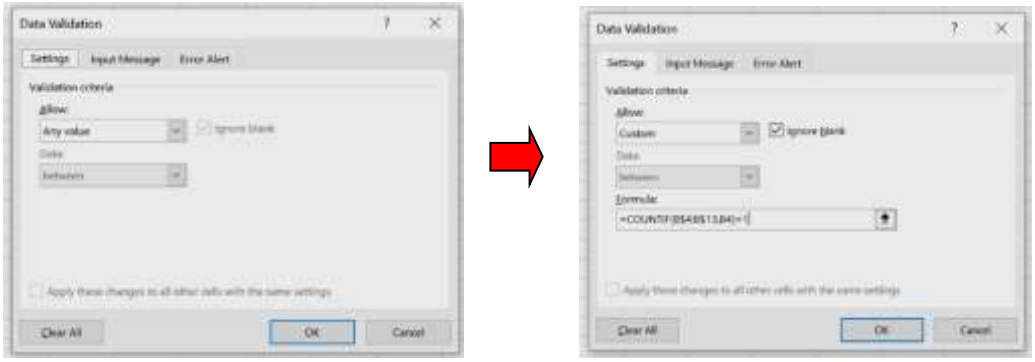
Sebagai contoh kita dapat membatasi jumlah karakter untuk kelas peserta didik (dalam angka Romawi), misalnya hanya sampai 3 karakter.



Gambar 1.8. Mengatur validasi menggunakan panjang karakter

6. Mencegah Duplikasi Data

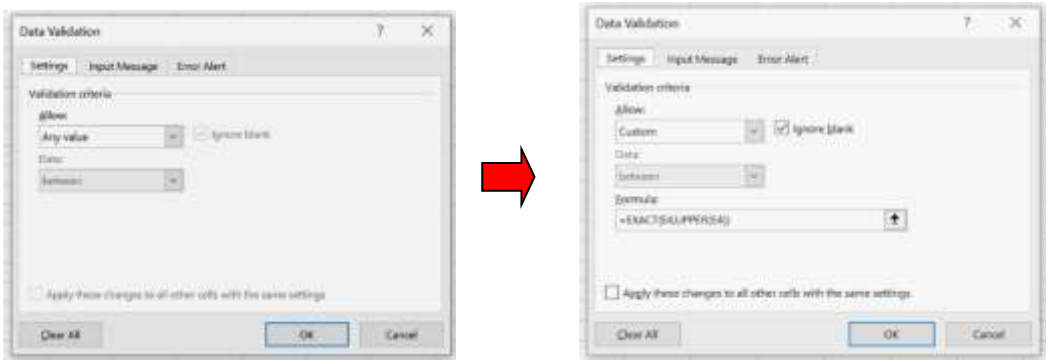
Pada kolom tertentu, tidak diizinkan ada nilai data yang sama. Sebagai contoh nilai nomor NIS, NIK, telepon, dan sebagainya tidak diizinkan sama. Rumus yang digunakan yaitu: COUNTIF(B$4:B$13,B3)=1.



Gambar 1.9. Mengatur agar tidak ada duplikasi data

7. Mengatur Huruf Kapital atau Huruf Kecil

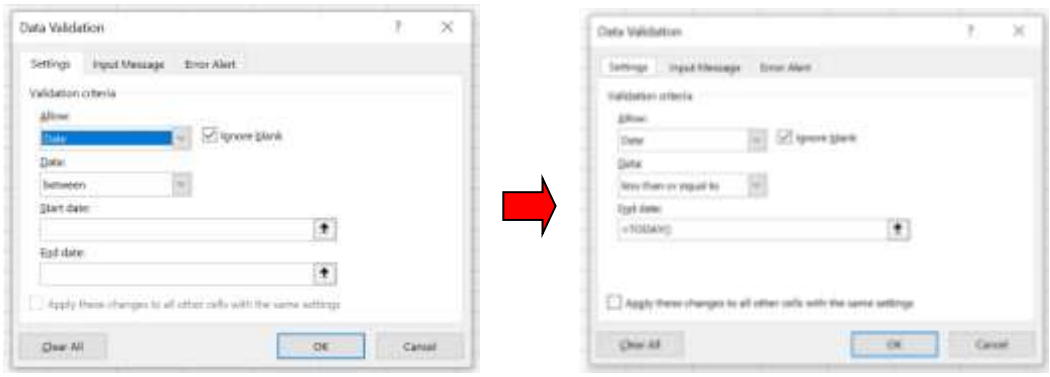
Sebagai contoh, kita dapat mengatur cell E4:E23 hanya menerima data yang berupa huruf kapital dengan menggunakan fungsi UPPER. Sebaliknya untuk mengatur agar data selalu berupa huruf kecil, kita dapat menggunakan fungsi LOWER.



Gambar 1.10. Mengatur agar nilai data selalu huruf kapital

8. Mengatur Agar Tanggal yang Diinput Tidak Melebihi Hari Ini

Cara mengatur agar tanggal yang diinput tidah melewati batas hari ini adalah seperti gambar di bawah ini.



Gambar 1.11. Mengatur agar batasan tanggal tidak melebihi hari ini

9. Mengatur Nilai Data Berupa Teks atau Bilangan

Rumus yang digunakan untuk mengatur agar nilai di suatu kolom berupa teks atau bilangan saja yaitu =ISTEXT atau =ISNUMBER.

Gambar 1.12. Mengatur agar nilai data selalu berupa teks atau bilangan

Praktikum

BEKERJA DENGAN DATA

Tujuan:

- Melakukan Validasi Data

Dalam praktikum ini, siswa membuat Daftar Nama yang telah disajikan dengan membuat validasi pada range sesuai jenis datanya.

Langkah-langkah Praktikum:

1. Ketiklah data di bawah ini dengan program Microsoft Excel!
2. Pada setiap kolom buatlah validasi sesuai ketentuan berikut:
   a. Kolom Nomor buat validasi supaya data yang bisa diinput hanya beupa angka!
   b. Kolom Nama buat validasi supaya data yang bisa diinput hanya beupa teks!
   c. Kolom NIS buat validasi supaya data yang diinput tidak boleh ada yang sama!
   d. Kolom Jenis Kelamin buat validasi supaya hanya bisa diisi dengan data L atau P saja!

DAFTAR NAMA SISWA SMP KUDUS

Nomor	Nama	NIS	Jenis Kelamin
1	RAMA AINUN NAJIB	7730	L
2	S MU'TASHIM SUTRISNO	7851	L
3	RAIHAN MUZAKKI	7848	L
4	SABRINA AGNI MAULIDA	7732	P
5	SALISA ALIFFIA PUTRI	7792	P
6	SHAKAYLA NAIRA PUTRI	7733	P
7	SIFA AULIA CAHYANI	7853	P
8	TSANIYA DEVANI FAILASHUFA	7824	P
9	YUMNA NADYA SHAFWAH	7883	P
10	ZULFA KUMALASARI	7943	P

UJI KOMPETENSI BAB I

I. Berilah tanda silang (X) pada huruf a, b, c, atau d pada jawaban yang tepat!

1. Berikut ini yang merupakan indikator terpenting untuk menilai kredibilitas sumber informasi adalah …
   A. Informasi sering dibagikan di media sosial
   B. Penulisnya memiliki banyak pengikut online
   C. Penulis atau organisasi adalah otoritas yang tepercaya dalam bidang tersebut
   D. Informasinya terlihat menarik dan berwarna-warni
2. Di bawah ini merupakan hal-hal yang mempengaruhi kredibilitas data dan informasi, *kecuali* ….
   A. Sumber Data dan Informasi
   B. Akurasi
   C. Ketepatan tempat
   D. Referensi dan Rujukan
3. Salah satu alasan validasi informasi sangat penting dilakukan sebelum menyebarkan atau menggunakannya adalah ….
   A. Karena semua informasi di internet pasti palsu
   B. Supaya proses pencarian informasi menjadi lebih cepat
   C. Untuk memastikan bahwa informasi tersebut akurat, benar, dan dapat dipercaya
   D. Agar informasi terlihat lebih banyak di internet
4. Berikut ini yang tidak menjadi indikator sebuah sumber informasi yang kredibel adalah ….
   A. Sumber informasi tersebut berasal dari lembaga yang terpercaya.
   B. Informasi yang disampaikan didukung oleh data dan fakta yang jelas.
   C. Penulis atau penyebar informasi memiliki keahlian di bidangnya.
   D. Informasi tersebut sering dibagikan di media sosial.
5. Salah satu ciri utama sumber informasi yang kredibel adalah ...
   A. Informasi tersebut disebarkan melalui media sosial pribadi
   B. Kontennya didukung oleh data, fakta, atau referensi yang jelas dan teruji
   C. Memiliki banyak emoji dan huruf kapital
   D. Penulis atau penerbitnya tidak jelas dan anonim
6. Sebelum mempercayai sebuah informasi yang baru kita baca, sebaiknya kita ....
   A. Langsung membagikannya ke teman-teman.
   B. Memeriksa kebenaran informasi tersebut dengan cepat.
   C. Mencari informasi yang sama dari sumber lain.
   D. Mengabaikan informasi tersebut.
7. Di bawah ini merupakan ciri-ciri fakta, *kecuali* ….
   A. Objektif
   B. Dapat Diverifikasi
   C. Universal
   D. Subjektif
8. Teknik validasi informasi dengan cara membandingkan atau mencocokkan informasi yang sama dari minimal dua atau lebih sumber yang berbeda disebut teknik ...
   A. Emotional Reading
   B. Lateral Reading
   C. Deep Reading
   D. Cross-Checking (Cek Silang)
9. Informasi yang sering kita temui di internet, seperti berita atau artikel, sebaiknya kita nilai dari segi….
   A. Keakuratan dan relevansi informasinya
   B. Keterbacaan tulisannya
   C. Keunikan gambar yang menyertainya
   D. Jumlah komentar yang diberikan pembaca
10. Pernyataan berikut yang paling akurat mengenai kredibilitas data adalah ….
    A. Data selalu kredibel jika berasal dari situs resmi pemerintah
    B. Kredibilitas tidak hanya bergantung pada sumber, tetapi juga pada cara penyampaian informasi
    C. Informasi yang selalu diulang-ulang di media massa pasti kredibel
    D. Seorang penulis yang pandai menulis pasti kredibel

11. Berikut ini yang bukan merupakan ciri dari berita bohong (hoax) adalah ….
    A. Judul yang provokatif dan mencolok.
    B. Sumber informasi yang jelas dan dapat dipertanggungjawabkan.
    C. Informasi yang tidak logis atau sulit dipercaya.
    D. Bahasa yang digunakan cenderung emosional.
12. Ketika Anda menemukan sebuah artikel berita dari situs yang asing, kemudian kita membuka tab baru dan mencari tahu reputasi situs tersebut di Google, tindakan ini dikenal sebagai teknik....
    A. Fact-Checking
    B. Vertical Reading
    C. Lateral Reading (Membaca Lateral)
    D. Source-Only Reading
13. Alasan pentingnya menilai kredibilitas suatu sumber informasi adalah ….
    A. Agar kita terlihat pintar di depan teman-teman.
    B. Agar kita tidak ketinggalan informasi terbaru.
    C. Agar kita tidak menyebarkan informasi yang salah.
    D. Agar kita dapat membedakan informasi yang penting dan tidak penting.
14. Pernyataan berikut yang merupakan fakta adaah ….
    A. Artikel ini adalah yang terbaik yang pernah saya baca.
    B. Ibukota Provinsi Jawa Timur adalah Surabaya.
    C. Warna hijau adalah warna yang paling menyejukkan.
    D. Belajar informatika itu sangat menyenangkan.
15. Perbedaan mendasar antara 'akurasi' dan 'objektivitas' dalam validasi informasi adalah ....
    A. Akurasi berkaitan dengan kecepatan, sementara objektivitas berkaitan dengan sumber
    B. Akurasi adalah tentang ketepatan fakta, sedangkan objektivitas adalah tentang kebebasan dari bias atau pandangan pribadi
    C. Akurasi adalah kriteria yang lebih penting daripada objektivitas
    D. Objektivitas hanya berlaku untuk berita, sementara akurasi berlaku untuk semua jenis informasi
16. Di bawah ini merupakan ciri-ciri opini, *kecuali* ….
    A. Subjektif
    B. Tidak Dapat Diverifikasi
    C. Bervariasi
    D. Objektif
17. Di bawah ini merupakan bentuk-bentuk cyberbullying, *kecuali* ….
    A. Flaming
    B. Harassment
    C. *Disintegration*
    D. *Denigration*
18. Pernyataan "Hujan deras menyebabkan banjir" termasuk ke dalam kategori….
    A. Opini, karena didasarkan pada perasaan.
    B. Fakta, karena dapat dibuktikan secara empiris.
    C. Teori, karena masih perlu penelitian lebih lanjut.
    D. Hipotesis, karena merupakan dugaan sementara.
19. Pernyataan berikut yang merupakan opini adalah ….
    A. Air mendidih pada suhu 100 derajat Celcius.
    B. Voly adalah olahraga yang paling seru.
    C. Bumi berputar mengelilingi matahari.
    D. Makhluk hidup membutuhkan oksigen untuk bernapas.
20. Pernyataan "Minum susu setiap hari membuat tulang kuat" termasuk ke dalam kategori….
    A. Fakta, karena sudah banyak penelitian yang membuktikannya.
    B. Opini, karena masih banyak perdebatan tentang hal ini.
    C. Teori, karena masih perlu penelitian lebih lanjut.
    D. Hipotesis, karena merupakan dugaan sementara.

II. Jawablah pertanyaan-pertanyaan di bawah ini dengan singkat dan jelas!

1. Sebutkan jenis-jenis sumber data dan informasi yang kredibel!
2. Jelaskan perbedaan antara misinformasi dan disinformasi!
3. Jelaskan perbedaan fakta dan opini!
4. Sebutkan 4 (empat) cara yang dapat kita lakukan untuk memeriksa apakah suatu berita itu hoaks atau bukan!
5. Jelaskan 3 (tiga) ciri fakta!

BAB II

SISTEM KOMPUTER

Tujuan Pembelajaran
1. Mendeskripsikan komponen, fungsi, dan cara kerja komputer
2. Mendeskripsikan jenis-jenis software komputer berdasarkan lisensi dan bentuknya

Pertanyaan Pemantik
1. Apakah yang kalian ketahui mengenai sistem komputer?
2. Sebutkan jenis-jenis software komputer?

MATERI

A. Perangkat Keras (Hardware)

Perangkat keras merupakan peralatan fisik dari sebuah komputer yang dapat disentuh dan dipindahkan. Perangkat keras terdiri atas empat bagian, yaitu:

1. Perangkat masukan (input device)

Contoh:

- *mouse* untuk memindahkan kursor di layar dan memilih atau mengklik objek atau menu yang ada.
- *keyboard* untuk memasukkan data, memberikan perintah, dan berinteraksi dengan sistem komputer
- *microphone* untuk memasukkan suara ke komputer.
- *touch screen* menjadi alat input untuk ponsel pintar (smartphone) atau jam pintar (smartwatch).
- *sensor inframerah (infrared)* pada remote control untuk mengendalikan televisi, AC, dan perangkat elektronik lainnya.
- *scanner* perangkat yang digunakan untuk mengubah gambar fisik atau dokumen cetak menjadi format digital yang dapat disimpan, diedit, dan ditampilkan pada komputer.

2. Perangkat keluaran (output device)

Contoh :

- *monitor* untuk menampilkan informasi visual dari komputer atau perangkat lainnya.
- *speaker* untuk menghasilkan suara atau output audio.
- *printer* untuk mencetak atau menghasilkan salinan fisik dari dokumen elektronik atau gambar digital.
- *LCD proyektor* menampilkan gambar atau video dari komputer, DVD player, atau perangkat lainnya ke layar besar atau permukaan datar.
- *antena pada smartphone* yang mungkin jarang kita sadari antena tersebut menghasilkan keluaran berupa gelombang radio yang dapat diterima oleh BTS (Base Transceiver Station) dari provider telekomunikasi.

3. Perangkat pemrosesan (processing device)

Bagian utama dari perangkat komputer adalah unit pemrosesan berupa prosesor yang berfungsi sebagai otak dari sebuah komputer. *Prosesor terdiri atas tiga bagian yaitu:*

a. Unit kontrol (Control Unit)

Merupakan bagian prosesor yang bertugas untuk mengendalikan perangkat yang terpasang pada komputer, dari alat input, output, dan penyimpanan. *Berikut adalah beberapa fungsi utama Control Unit :*

- *Mengatur eksekusi instruksi*
  Control Unit bertanggung jawab untuk mengambil instruksi dari memori dan menginterpretasikannya, dan mengatur eksekusi instruksi satu per satu kemudian memastikan urutan operasi yang benar.
- *Mengendalikan aliran data*
  Control Unit mengendalikan aliran data antara unit-unit pemrosesan utama dalam CPU, seperti Arithmetic Logic Unit (ALU) dan Register, dan memastikan pengiriman data yang tepat pada waktu yang tepat dan ke tempat yang tepat dalam proses pemrosesan.
- *Mengatur urutan instruksi*
  Control Unit menentukan urutan instruksi yang harus dieksekusi oleh CPU, dalam artian mengatur aliran instruksi dan menentukan instruksi mana yang akan dilakukan berikutnya berdasarkan program yang sedang dijalankan.
- *Menerjemahkan instruksi*
  Control Unit menerjemahkan instruksi yang diterima dari memori menjadi sinyal-sinyal kontrol yang dapat dipahami oleh unit-unit pemrosesan lainnya dalam CPU. Sehingga bisa mengubah instruksi menjadi aksi fisik yang dilakukan oleh komponen-komponen CPU.
- *Mengelola clock CPU*
  Control Unit menghasilkan sinyal clock yang mengatur kecepatan operasi CPU. Sinyal clock ini memberikan timing yang sinkron untuk setiap operasi dalam CPU, memastikan bahwa semua komponen bekerja secara terkoordinasi.
- *Mengelola interupsi*
  Control Unit mengelola interupsi eksternal dan internal yang terjadi dalam sistem komputer. Ini memungkinkan CPU untuk merespon kejadian mendadak dan menjalankan rutinitas interupsi yang sesuai.
- *Mengendalikan akses memori*
  Control Unit mengendalikan akses ke memori utama. Ini memastikan bahwa data dan instruksi yang diperlukan oleh CPU dapat diambil dari memori dan ditulis kembali dengan benar.
- *Mengelola pemrosesan pipelining*
  Control Unit dapat mengimplementasikan teknik pemrosesan pipelining dimana beberapa instruksi dieksekusi secara bersamaan dalam tahap-tahap yang berbeda. Ini meningkatkan kecepatan pemrosesan dan efisiensi CPU secara keseluruhan.
- *Mengatur penggunaan sumber daya CPU*
  Control Unit dapat mengatur dan mengalokasikan sumber daya CPU, seperti register dan buffer, untuk menjalankan instruksi dengan efisien.

b. Unit aritmatika dan logika (Arithmetic Logic Unit)

Komponen utama dalam Central Processing Unit (CPU) yang bertanggung jawab untuk melakukan operasi aritmatika dan logika dalam pemrosesan data. *Berikut adalah beberapa fungsi utama dari ALU:*

- *Operasi Aritmatika*
  ALU melakukan operasi matematika dasar seperti penjumlahan, pengurangan, perkalian, dan pembagian.
- *Operasi Logika*
  ALU juga melakukan operasi logika, termasuk AND, OR, NOT, XOR, dan operasi logika lainnya. Operasi logika ini digunakan dalam pemrosesan data untuk membandingkan, memanipulasi, atau menggabungkan nilai-nilai bit.
- *Operasi Pembanding*

ALU memiliki kemampuan untuk membandingkan dua nilai atau data. Dalam artian dapat digunakan untuk memeriksa kesetaraan, perbandingan numerik (lebih besar, lebih kecil, sama dengan), atau operasi perbandingan lainnya.

- *Operasi Logika Bit*
  ALU mampu melakukan operasi logika bit pada tingkat bit individu. Ini meliputi operasi AND bit, OR bit, XOR bit, NOT bit, dan operasi bit lainnya.
- *Operasi Penanganan Overflow*
  ALU juga memiliki mekanisme untuk menangani kasus overflow, yaitu ketika hasil operasi aritmatika melebihi kapasitas bit yang ditetapkan. ALU dapat mendeteksi dan mengambil tindakan yang sesuai untuk menangani overflow, seperti menghasilkan carry atau flag overflow.

c. Register

Unit penyimpanan kecil dengan kecepatan yang sangat tinggi yang terdapat dalam Central Processing Unit (CPU) komputer. Fungsi utama register adalah menyimpan dan memanipulasi data sementara dalam proses pemrosesan komputer. *Berikut adalah beberapa fungsi penting dari register:*

- *Penyimpanan Data*
  Register digunakan untuk menyimpan data yang sedang diproses atau yang akan diproses oleh CPU. Data yang disimpan dalam register dapat berupa angka, karakter, alamat memori, atau instruksi program.
- *Penyimpanan Hasil Sementara*
  Register digunakan untuk menyimpan hasil sementara dari operasi aritmatika, logika, atau pemrosesan data lainnya. Misalnya, register dapat digunakan untuk menyimpan hasil penjumlahan dua angka atau hasil logika dari operasi AND.
- *Penyimpanan Alamat Memori*
  Register khusus seperti Instruction Register (IR) digunakan untuk menyimpan alamat memori instruksi yang sedang dieksekusi. Hal ini memungkinkan CPU untuk mengakses instruksi selanjutnya dalam urutan yang tepat.

Ketika kalian bermain game yang meminta kalian menggerakkan karakter atau objek di layar dengan mouse atau ketukan papan kunci, komponen dalam alat pemrosesan inilah yang dapat memproses gerakan mouse dan ketukan jari pada keyboard yang kalian lakukan agar permainan dapat berjalan. Contoh lain ialah ketika kalian suka mendengarkan musik melalui aplikasi di ponsel, alat pemrosesan inilah yang akan membaca daftar lagu (playlist) yang sudah disusun, lalu mengirimkan sinyal suara ke earphone atau headset sehingga kalian dapat mendengarkan musiknya. Komponen alat pemrosesan ini juga yang dapat mampu memproses gerakan swipe jari kalian ketika membuka aplikasi sosial media, hingga melakukan unggahan foto ke teman-teman atau follower kalian.

4. Perangkat penyimpanan (storage device)

Contoh:

- *Hard Drive (HDD)* perangkat penyimpanan yang menggunakan media magnetik untuk menyimpan data dalam bentuk digital.
- *Solid State Drive (SSD)* perangkat penyimpanan yang menggunakan teknologi flash memory untuk menyimpan data.
- *USB Flash Drive* perangkat penyimpanan portabel yang menggunakan teknologi flash memory.
- *Memory Card* kartu kecil yang digunakan untuk penyimpanan portabel dalam perangkat elektronik seperti kamera digital, smartphone, tablet, dan perangkat audio portabel.
- *Optical Disc* seperti CD (Compact Disc), DVD (Digital Versatile Disc), dan Blu-ray Disc digunakan untuk penyimpanan data optik.

- *Cloud Storage* layanan penyimpanan online yang memungkinkan pengguna menyimpan, mengakses, dan mencadangkan data melalui internet. *Layanan cloud storage yang populer adalah* Google Drive, Dropbox, OneDrive, iCloud dan Amazon S3. Data disimpan di server jarak jauh dan dapat diakses dari berbagai perangkat dengan koneksi internet.

B. Perangkat Lunak (*Software*)

Perangkat lunak adalah sekumpulan instruksi, data, atau program yang digunakan untuk mengoperasikan komputer dan menjalankan tugas-tugas tertentu. Perangkat lunak dapat dikategorikan ke dalam beberapa jenis utama berdasarkan fungsi dan kegunaannya. Berikut ini adalah penjelasan tentang jenis-jenis perangkat lunak dan contoh serta penggunaannya:

1. Perangkat lunak system

a. Sistem Operasi

Setiap komputer harus mempunyai system operasi. Secanggih apapun perangkat keras yang dimiliki oleh komputer, tanpa adanya system operasi maka komputer tersebut menjadi tidak berguna.

Tugas utama yang dilakukan oleh system operasi Adalah melakukan manajemen sumber daya agar penggunaannya berlangsung efisien dan konsisten. Selain itu system operasi juga berfungsi untuk mengendalikan proses-proses yang ada di computer supaya berjalan seperti seharusnya.

Contoh sistem operasi: MS DOS, MS Windows (dengan berbagai generasi), Macintosh, LINUX (dengan berbagai distribusi).

b. Driver Perangkat

Mengizinkan sistem operasi berkomunikasi dengan perangkat keras seperti printer, kartu grafis, dan perangkat input.

c. Firmware

Software khusus yang tertanam dalam perangkat keras untuk mengendalikan fungsi dasar perangkat. Contoh: BIOS pada komputer.

2. Program Utilitas

Merupakan program khusus yang berfungsi sebagai perangkat pemeliharaan komputer, seperti anti virus, partisi hardisk, manajemen hardisk, dan lain-lain. Contoh produk program utilitas: Norton Utilities, PartitionMagic, McAfee, dan lain-lain.

3. Program Aplikasi

- Aplikasi yang membantu pengguna menyelesaikan tugas-tugas sehari-hari. Contoh: Microsoft Office (Word, Excel, PowerPoint), Google Workspace.
- Aplikasi untuk kreasi konten seperti grafis, audio, video, dan desain. Contoh: Adobe Creative Suite (Photoshop, Illustrator, Premiere Pro).
- Aplikasi untuk berkomunikasi dengan orang lain. Contoh: Zoom, Microsoft Teams, WhatsApp.
- Software untuk mengakses dan menjelajahi internet. Contoh: Google Chrome, Mozilla Firefox, Safari.

4. Bahasa Pemrograman

Merupakan perangkat lunak untuk pembuatan atau pengembangan perangkat lunak lain. Bahasa pemprograman dapat diklasifikasikan menjadi tingkat rendah, tingkat sedang, dan tingkat tinggi. Pergeseran dari tingkat rendah ke tinggi menunjukkan kedekatan dengan bahasa manusia. Bahasa tingkat rendah (atau biasa disebut bahasa assembly) merupakan bahasa dengan pemetaan satu persatu terhadap instruksi komputer. Contoh bahasa tingkat tinggi: Pascal, BASIC, Prolog, Java dan lain-lain. Contoh bahasa tingkat menengah: bahasa C.

C. Lisensi Perangkat Lunak

Lisensi software merupakan hak cipta dari pemilik atau pembuat software yang nantinya bisa digunakan oleh orang lain atau juga pihak-pihak yang membutuhkan software ini. Pada dasarnya, software maupun aplikasi yang beredar saat ini sama nilai, sama berharganya dengan benda-benda yang bernilai

tinggi lainnya. Jenis-jenis lisensi perangkat lunak di komputer yang sudah dikenal saat ini meliputi hal-hal sebagai berikut:

1. **Lisensi Commercial**
   Sesuai dengan namanya, lisensi commercial ini dibuat untuk semua software yang tujuannya untuk komersial alias jualan. Maka dari itu, untuk dapat menggunakan software atau aplikasi yang memiliki lisensi commercial, dia harus membelinya atau bisa juga dengan mendapatkan izin dari sang pemilik hak cipta software atau aplikasi tersebut. Contoh paling mudah untuk software lisensi commercial ini di antaranya Sistem Operasi Windows yang dibuat Microsoft.
2. **Lisensi Trial**
   Maksud dari Trial ini adalah versi demo atau bisa dibilang versi uji coba dari software. Jadi pada software yang menggunakan lisensi trial ini, calon pembeli ataupun pengguna akan mendapatkan software yang masih dalam bentuk demo. Tujuan dibuatkan demo ini agar pengguna dapat merasakan terlebih dahulu pelayanan yang ada pada software atau aplikasi tersebut. Hanya saja, pada aplikasi versi trial ini, para pengguna diberikan batas waktu untuk menggunakannya. Batas waktunya pun bermacam-macam, ada yang 15 hari, 20 hari, 30 hari, dan lain-lain. Maka dari itu, untuk dapat menggunakan layanan secara penuh dari software yang diinginkan, calon pembeli atau pengguna harus membeli software atau aplikasi tersebut.
3. **Lisensi Non-Commercial**
   Jika ada software yang ditujukan untuk mencari keuntungan, maka ada juga software yang dibuat tidak semata-mata mencari keuntungan. Sebab, pada dasarnya, software atau aplikasi ini dibuat sebagai bentuk pelayanan untuk publik. Contohnya, software atau aplikasi yang digunakan untuk rumah sakit, sekolah, yayasan, dan lain-lain. Biasanya software yang menggunakan lisensi non commercial ini gratis yang artinya tidak dipungut biaya.
4. **Lisensi Shareware**
   Lisensi shareware memberikan kebebasan untuk pengguna dalam menggunakan, menyebarluaskan, dan menggandakan software atau aplikasi yang dipakai. Hebatnya lagi, pengguna pun tidak harus mendapatkan izin dari sang pemilik atau pembuat hak cipta software atau aplikasi. Fitur pada software atau aplikasi yang menggunakan lisensi shareware ini dapat digunakan cukup lengkap. Meskipun begitu, Software yang menggunakan lisensi shareware ini memiliki fitur yang lebih lengkap jika sang pengguna membeli software atau apikasi tersebut. Namun ini berbeda dengan trial. Pada trial, pengguna sama sekali tidak bisa menggunakan fitur pada aplikasi jika tidak membayar. Sedangkan pada shareware, aplikasi dan software dibagi menjadi dua yakni versi gratis dan versi berbayar. Contoh software atau aplikasi yang menggunakan lisensi ini adalah Winrar dan Microsoft Office.
5. **Lisensi Freeware**
   Software dan aplikasi yang dapat digunakan secara penuh fitur-fiturnya dan juga lengkap bisa ditemukan pada software dan aplikasi yang berlisensi freeware. Perbedaan yang jelas antara shareware dan freeware adalah pada fitur yang diberikan. Meskipun sama-sama gratis, software dan aplikasi yang menggunakan lisensi freeware ini benar-benar gratis dengan fitur yang lengkap. Uniknya lagi, bagian-bagian plugin pun dapat kita dapatkan juga secara gratis di situs resminya dan itu juga bisa kita dapatkan secara gratis. Contohnya saja macam-macam software gratis pada browser seperti Mozilla, Opera, Google Chrome, dan lain-lain. Lalu aplikasi chatting seperti Whatsapp dan Line. maupun software gratis untuk edit video seperti Windows Moviemaker.
6. **Lisensi Open Source**
   Untuk lisensi yang satu ini tentunya tidak asing buat kamu yang sudah berkecimpung di dunia teknologi dan informasi. Lisensi open source berarti aplikasi atau software tersebut dapat digunakan, dikembangkan, diubah dan disebarkan secara gratis dan juga mudah didapatkan dari sumber-sumber internet. Tentunya hal ini tidak perlu melalui persetujuan dari sang pembuat atau pemilik hak cipta. Sebab, tujuan dari software dan aplikasi yang berlisensi open source memang ditujukan

untuk publik. Contoh paling mudah software dan aplikasi yang menggunakan lisensi adalah Ubuntu, Linux, dan Notepad ++.

D. Bentuk Perangkat Lunak/*Software*

1. Open Source

Perangkat lunak *open source* adalah perangkat lunak yang kode sumbernya dapat diakses secara publik dan dapat diperiksa, dimodifikasi, serta didistribusikan ulang secara bebas oleh siapa saja, dengan tetap mematuhi ketentuan lisensi yang berlaku. Perangkat ini memungkinkan kolaborasi terbuka antara pengembang dan pengguna untuk mengembangkan dan memperbaikinya secara berkelanjutan. Contohnya termasuk sistem operasi Linux dan browser Mozilla Firefox.

Kelebihan *Open Source*

a. Biaya Ringan: Biasanya aplikasi lisensi open source memiliki biaya lebih ringan dan terkadang mengandalkan sekali pembayaran untuk penggunaan lifetime.

b. Modifikasi dan Pengembangan yang Lebih Bebas: Anda dapat menggunakan sumber daya apa pun yang tersedia sehari-hari untuk memenuhi kebutuhan komunitas atau individu Anda.

c. Bantuan Komunitas yang Luas: Jika ada masalah pada aplikasi, Anda tidak perlu khawatir karena sudah banyak panduan dan bantuan melalui forum .

Kekurangan *Open Source*

a. Keamanan Kurang Terjamin: Meskipun open source menawarkan keuntungan dalam pengembangan, hal ini juga merupakan masalah keamanan yang perlu diperhatikan. Sumber kode yang terbuka memungkinkan pihak yang tidak bertanggung jawab untuk melihat alur kodenya dan melakukan eksploitasi atau testing keamanan program.

b. Informasi Bantuan dari *Developer*: Jika Anda menghadapi masalah atau kesalahan dengan aplikasi, mungkin Anda tidak akan mendapatkan dukungan dari developer. Ini wajar karena aplikasi open source biasanya tidak menawarkan bantuan tingkat lanjut. Jadi, Anda harus mencari informasi tentang kendalanya di forum-forum sendiri.

c. Kualitas Perangkat Lunak/Aplikasi: Tak sedikit aplikasi *open source* dirilis tanpa pengecekan kualitas kode atau memperdulikan keamanan dan fitur yang diperlukan. Untuk menanggulanginya, Anda wajib memiliki *basic* yang cukup mumpuni dalam pemrograman dan perbaikan kode.

2. Clouse Source

Bentuk *closed source* software komputer adalah perangkat lunak yang kode sumbernya tidak tersedia untuk umum dan dilindungi hak cipta, yang berarti pengguna tidak dapat melihat, mengubah, atau mendistribusikannya secara bebas. Contohnya termasuk sistem operasi seperti Microsoft Windows dan macOS, aplikasi perkantoran seperti Microsoft Office, dan perangkat lunak desain grafis seperti Adobe Photoshop.

Contoh *Closed Source* Berdasarkan Kategori

- Sistem Operasi: Microsoft Windows, Apple macOS, Apple iOS
- Aplikasi Kantor: Microsoft Office (Word, Excel, PowerPoint)
- Perangkat Lunak Desain Grafis: Adobe Photoshop, Adobe Illustrator
- Perangkat Lunak Keamanan: Antivirus komersial (Norton, McAfee)
- Basis Data: Microsoft SQL Server
- Peramban (Browser): Microsoft Edge, Safari
- Lain-lain: Snapchat, Google Earth, Skype

Ciri-ciri Utama Software Closed Source

- **Kode sumber tertutup:**

  Kode sumber program disimpan dan tidak tersedia untuk umum. Pengguna hanya menerima file biner yang diperlukan untuk menjalankan program.

- **Kepemilikan hak cipta:**

  Hak untuk menggunakan, memodifikasi, dan menyalin perangkat lunak sepenuhnya dipegang oleh pengembangnya.

- **Lisensi pengguna:**

  Pengguna hanya membeli lisensi untuk menggunakan program tersebut dan tidak diizinkan untuk memodifikasi atau mendistribusikannya.

- **Model bisnis:**

  Seringkali merupakan perangkat lunak berbayar (proprietary software), meskipun ada juga yang gratis dengan batasan lisensi.

Latihan 1

1. Sebutkan dan jelaskan 4 (empat) jenis perangkat keras komputer!
2. Jelaskan pengertian perangkat lunak/software komputer!
3. Sebutkan 4 (empat) jenis lisensi perangkat lunak di komputer!
4. Jelaskan kelebihan software *Open Source!*
5. Sebutkan 4 (empat) ciri utama Software Closed Source!

UJI KOMPETENSI BAB II

I. Berilah tanda silang (X) pada huruf a, b, c, atau d pada jawaban yang tepat!

1. Peralatan fisik dari sebuah komputer yang dapat disentuh dan dipindahkan merupakan pengertian dari ….
   A. Perangkat lunak
   B. Perangkat Keras
   C. Software
   D. Brainware
2. Sistem komputer terdiri dari tiga komponen utama, yaitu…
   A. Hardware, software, brainware
   B. Monitor, CPU, keyboard
   C. Input, proses, output
   D. RAM, ROM, harddisk
3. Berikut ini yang merupakan perangkat input komputer adalah ….
   A. Scanner
   B. HDD
   C. Printer
   D. ALU
4. Berikut ini merupakan perangkat keluaran (output device) pada komputer, *kecuali* ….
   A. *Monitor*
   B. *Microphone*
   C. Printer
   D. *LCD proyektor*
5. Berikut ini yang termasuk perangkat keras (*hardware*) adalah ….
   A. Windows
   B. Microsoft Word
   C. Mouse
   D. Antivirus
6. Unit penyimpanan kecil dengan kecepatan yang sangat tinggi yang terdapat dalam Central Processing Unit (CPU) komputer disebut ….
   A. ALU
   B. CU
   C. HDD
   D. Register
7. Sekumpulan instruksi, data, atau program yang digunakan untuk mengoperasikan komputer dan menjalankan tugas-tugas tertentu merupakan pengertian dari ....
   A. Perangkat lunak
   B. Perangkat Keras
   C. Hardware
   D. Brainware
8. Program yang digunakan untuk mengatur dan mengendalikan perangkat keras komputer disebut….
   A. Aplikasi
   B. Sistem operasi
   C. Driver
   D. Utility
9. Program khusus yang berfungsi sebagai perangkat pemeliharaan komputer merupakan pengertian dari ….
   A. Program Aplikasi
   B. Program System
   C. Program Utilitas
   D. Program Bahasa Pemrograman
10. Berikut ini merupakan jenis-jenis lisensi perangkat lunak di komputer, *kecuali* ….
    A. Commercial
    B. Shareware
    C. Trial
    D. Malware
11. Berikut ini yang termasuk sistem operasi yang bersifat *open source* adalah ….
    A. Windows
    B. MacOS
    C. Linux
    D. Chrome OS
12. Berikut ini merupakan kelebihan *Software Open Source, kecuali ….*
    A. Biaya ringan
    B. Royalty yang besar bagi pembuatnya
    C. Modifikasi dan pengembangan yang lebih bebas
    D. Bantuan komunitas yang luas
13. Perangkat berikut yang berfungsi mengubah suara menjadi sinyal digital adalah…
    A. Webcam
    B. Speaker
    C. Mikrofon
    D. Headset
14. Bagian komputer yang berfungsi menyimpan data sementara adalah ….
    A. Harddisk
    B. SSD
    C. RAM
    D. Flashdisk

15. Berikut ini yang merupakan ciri utama software closed source Adalah ….
    A. Adanya lisensi pengguna
    B. Tidak memiliki hak cipta
    C. Kode sumber program terbuka
    D. Model sosial

II. Jawablah pertanyaan-pertanyaan di bawah ini dengan singkat dan jelas!

1. Sebutkan 4 (empat) perangkat masukan (input device) pada computer!
2. Mengapa Central Processing Unit (CPU) sering disebut sebagai 'otak' dari komputer? Jelaskan peran utamanya dalam sebuah sistem komputer!
3. Sebutkan 3 (tiga) jenis perangkat lunak (software)!
4. Jelaskan kekurangan software *Open Source!*
5. Jelaskan perbedaan mendasar antara Software Sistem Operasi dan Software Aplikasi!

BAB III
KONEKTIVITAS DAN JARINGAN KOMPUTER

Tujuan Pembelajaran
Setelah mempelajari bab ini murid mampu memahami :
1. Jaringan lokal dan jaringan internet.
2. Cara kerja pengiriman data dalam konektivitas jaringan internet.
3. Jenis – jenis transmisi dalam jaringan lokal maupun internet.

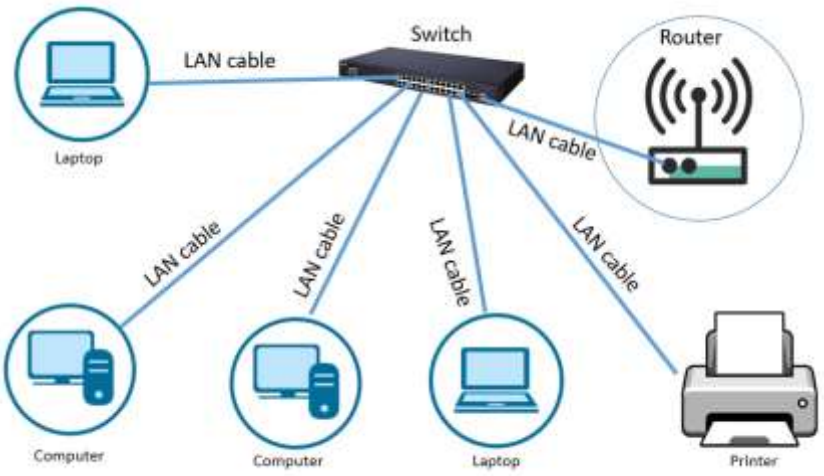
Pertanyaan Pemantik
Tahukah kalian, jaringan komputer terdiri atas banyak perangkat yang terhubung, bagaimana cara kerja dalam pengiriman data dari satu perangkat ke perangkat lain?

MATERI

A. Jaringan Komputer

Jaringan komputer adalah sebuah arsitektur di mana dua atau lebih komputer terhubung satu sama lain dan digunakan untuk berbagi data. Jaringan komputer memungkinkan pengguna untuk mentransfer data, berbagi file, mencetak dokumen bersama, mengakses internet. Jaringan komputer dibangun dengan kombinasi hardware dan software. Setiap perangkat yang terhubung pada jaringan komputer akan memiliki identitas unik untuk membedakan perangkat yang disebut alamat IP (Internet Protocol). Berdasarkan pada jangkauan areanya, secara umum jaringan komputer dapat dibagi menjadi dua jenis :

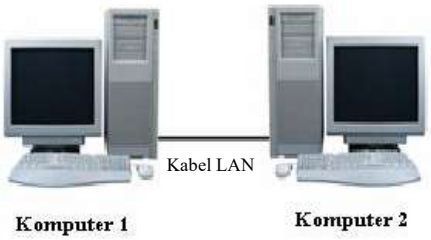
1. Jaringan Lokal



Gambar 3.1 Local Area Network (LAN)

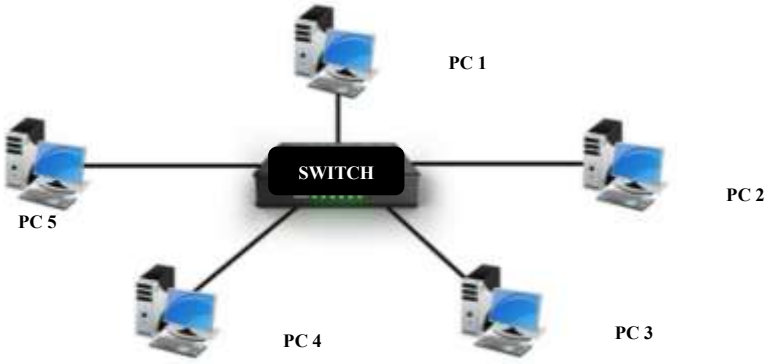
Jaringan lokal adalah jaringan komputer berkabel maupun nirkabel yang menghubungkan komputer dengan perangkat lainnya dalam wilayah terbatas seperti dalam rumah, sekolah, kampus, universitas, atau gedung kantor. Untuk mengakses perangkat pada jaringan lokal, perangkat yang kita miliki harus terhubung terlebih dahulu dengan jaringan lokal tersebut. Jaringan lokal ini disebut juga sebagai jaringan LAN (local area network).

Dalam level paling sederhana, jaringan lokal hanya terdiri atas dua perangkat yang terhubung menggunakan kabel atau tanpa kabel.



Gambar 3.2. Jaringan Komputer Dua Perangkat

Jika ingin menghubungkan lebih dari dua perangkat dalam jaringan yang sama, dibutuhkan perangkat tambahan yaitu switch.



Gambar 3.3. Jaringan Komputer Lebih Dari Dua Perangkat

Berikut adalah perangkat keras (Hardware) Jaringan Lokal :

a. Komputer Server.

Komputer pusat yang mengatur dan menyimpan data dalam jaringan. Komputer server menyediakan layanan seperti penyimpanan file, akses internet, dan printer.

Gambar 3.4. Komputer Server

b. Komputer Client.

Perangkat yang digunakan oleh pengguna untuk mengakses jaringan, layanan atau sumber daya dari komputer server. Contoh: komputer siswa, laptop, tablet.

Tablet Smartphone Personal Computer Laptop

Gambar 3.5. Komputer Client

c. Network Interface Card (NIC) / Kartu Jaringan.

Komponen yang menghubungkan komputer ke jaringan melalui kabel atau sinyal nirkabel. Contoh: LAN card, Wi-Fi adapter.

Gambar 3.6. NIC (Network

d. Switch.

Perangkat yang digunakan untuk menghubungkan beberapa perangkat dalam suatu jaringan lokal (LAN). Switch bertanggung jawab untuk meneruskan data dari satu perangkat ke perangkat lain di dalam jaringan lokal.

Gambar 3.7. Switch

e. Router.

Perangkat yang menghubungkan beberapa jaringan komputer yang berbeda dan mengarahkan lalu lintas data di antara jaringan tersebut untuk memastikan paket data sampai ke tujuan yang benar.

Gambar 3.7. Router

f. Kabel Jaringan Komputer.

Kabel yang digunakan untuk menghubungkan komputer, switch, dan router dalam jaringan LAN (Local Area Network), untuk memungkinkan komunikasi dan pertukaran data. Jenis kabel jaringan komputer yang umum digunakan meliputi :

- Twisted Pair (UTP/STP) : Jenis yang paling umum digunakan dalam jaringan LAN (Local Area Network), seperti di kantor atau rumah. Terdiri dari beberapa pasang kabel tembaga yang dililit satu sama lain untuk mengurangi interferensi.
- Fiber Optic : Menggunakan serat kaca atau plastik tipis untuk mentransmisikan data dalam bentuk cahaya. Kabel ini menawarkan kecepatan transfer data yang sangat tinggi dan jangkauan yang lebih jauh, sering digunakan untuk koneksi internet berkecepatan tinggi atau jaringan perusahaan besar.
- Coaxial : Jenis kabel yang lebih tua, dulu populer untuk jaringan komputer dan TV kabel. Terdiri dari inti tembaga padat yang dikelilingi oleh lapisan isolasi dan pelindung logam.

Kabel Twisted Pair

Kabel Fiber Optic

Kabel Coaxial

Gambar 3.8. jenis kabel jaringan

g. Access Point (AP).

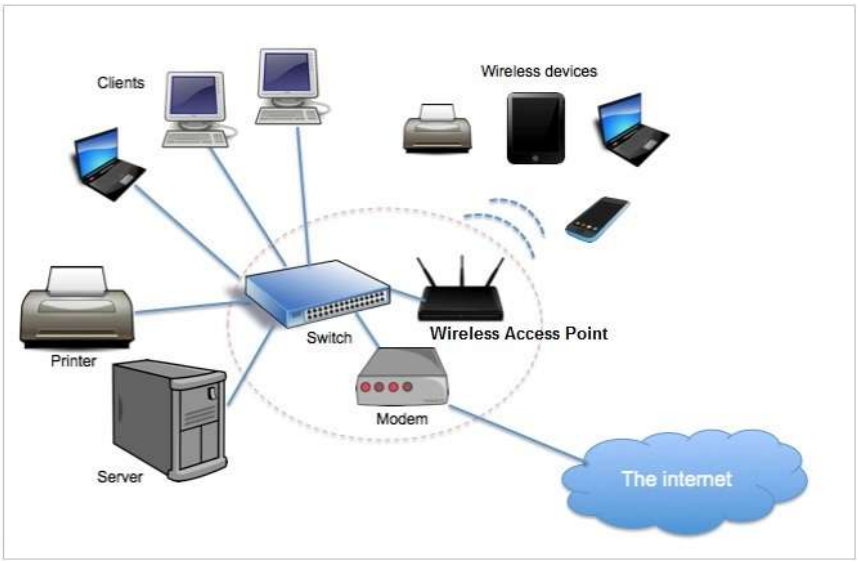
perangkat keras jaringan komputer yang berfungsi sebagai pusat transmisi nirkabel, memungkinkan perangkat berkemampuan nirkabel (seperti laptop, smartphone, tablet) untuk terhubung ke jaringan kabel atau jaringan nirkabel lainnya menggunakan teknologi Wi-Fi.

Gambar 3.9. Access

Latihan 1

1. Jelaskan apa yang di maksud dengan jaringan komputer?
2. Sebutkan 7 perangkat keras (hardware) jaringan komputer lokal!
3. Jelaskan perbedaan komputer server dan komputer client!
4. Jelaskan perbedaan router dan switch!
5. Lebih cepat mana kecepatan transfer data antara kabel fiber optic dengan kabel twisted pairs? Berikan alasanmu!

2. Jaringan Internet



Gambar 3.10. Jaringan Internet

Internet merupakan singkatan dari Interconnected Network. Internet adalah jaringan komputer global yang menghubungkan jutaan perangkat komputer di seluruh dunia. Sejarah internet dimulai pada tahun 1960-an sebagai proyek penelitian militer di Amerika Serikat yang bertujuan untuk mengembangkan jaringan komputer yang tahan terhadap serangan nuklir. Dikenal sebagai ARPANET (Advanced Research Projects Agency Network), jaringan ini dibangun oleh

Advanced Research Projects Agency (ARPA), yang saat itu merupakan divisi Departemen Pertahanan Amerika Serikat.

Pada tahun 1969, ARPANET berhasil menghubungkan empat universitas di Amerika Serikat :

a. University of California, Los Angeles (UCLA).
b. Stanford Research Institute (SRI).
c. University of California, Santa Barbara (UCSB).
d. University of Utah.

Ini merupakan tonggak sejarah penting karena merupakan pembentukan jaringan komputer pertama yang menggunakan protokol paket switching.

Pengertian internet itu sendiri mungkin dapat kita rumuskan sebagai suatu jaringan komunikasi yang menghubungkan satu media elektonik dan media yang lainnya atau kumpulan dari beberapa komputer atau ponsel, yang saling berhubungan serta saling terkoneksi satu sama lainnya. Internet sendiri adalah jaringan WAN yang terbesar dan paling luas yang menghubungkan jutaan jaringan dan komputer di seluruh dunia. Ini memungkinkan pengguna untuk mengakses informasi, layanan, dan sumber daya lainnya seperti email, situs web, media sosial, streaming video, dan banyak lagi.

Bagaimana data dapat terkirim ke internet? Pengiriman data di internet adalah proses yang kompleks namun terstruktur, yang pada dasarnya bekerja dengan memecah informasi menjadi potongan-potongan kecil, mengirimkannya melalui berbagai jaringan, dan menyatukannya kembali di tujuan akhir. Proses ini diatur oleh seperangkat aturan yang disebut protokol TCP/IP.

Berikut adalah rincian konsep utama pengiriman data di internet :

1. Model Paket Switching (Packet Switching)

Ini adalah tulang punggung pengiriman data internet. Data tidak dikirim sebagai satu aliran tunggal yang berkelanjutan. Sebaliknya, data dipecah menjadi unit-unit kecil yang disebut paket (packets).

Setiap paket berisi data asli ditambah header dan trailer (informasi tambahan) yang mencakup :

- Alamat IP sumber (pengirim).
- Alamat IP tujuan (penerima).
- Nomor urut paket (agar bisa disusun kembali dengan benar).
- Data untuk pengecekan kesalahan (checksum).

2. Peran Protokol TCP/IP

Protokol adalah bahasa dan aturan komunikasi. TCP/IP adalah standar universal internet :

- TCP (Transmission Control Protocol) : Bertanggung jawab untuk memastikan data terkirim dengan andal. TCP membagi data menjadi paket di sisi pengirim dan menyusunnya kembali di sisi penerima. Jika ada paket yang hilang, TCP meminta pengiriman ulang.
- IP (Internet Protocol): Bertanggung jawab untuk pengalamatan dan perutean. IP memberikan alamat unik (alamat IP) untuk setiap perangkat dan menentukan jalur terbaik yang harus diambil setiap paket untuk mencapai tujuannya.

3. Proses Pengiriman Data

Saat Anda mengirim email atau mengakses situs web, inilah yang terjadi :

- Enkapsulasi (Pengemasan) : Data dibuat di aplikasi Anda, lalu protokol TCP memecahnya menjadi paket-paket. Setiap paket diberi informasi IP dan informasi lain yang diperlukan.
- Perutean (Routing) : Paket-paket ini mulai melakukan perjalanan melalui jaringan lokal (router rumah/kantor Anda) dan diteruskan ke Penyedia Layanan Internet (ISP) Anda.
- Transit Jaringan : Router di sepanjang jalur (dari ISP Anda, melalui kabel serat optik bawah laut atau darat, hingga ke server tujuan) memeriksa alamat IP tujuan pada setiap paket. Setiap router memutuskan jalur terbaik berikutnya untuk paket tersebut agar lebih dekat ke tujuan. Paket dari satu pengiriman yang sama bisa saja menempuh jalur yang berbeda-beda.

- Perakitan Kembali (Reassembly) : Saat paket-paket tiba di tujuan (misalnya, server situs web atau komputer teman Anda), protokol TCP di sisi penerima menggunakan nomor urut paket untuk menyusun kembali data ke bentuk aslinya.
- Konfirmasi : Pihak penerima mengirimkan konfirmasi (acknowledgement) kembali ke pengirim bahwa paket telah diterima dengan benar. Jika ada paket yang tidak sampai atau rusak, pengirim akan mengirimkannya kembali.

Analogi Sederhana :

Bayangkan Anda mengirimkan sebuah buku tebal ke luar negeri.

- Buku : Data yang ingin dikirim.
- Halaman Buku : Paket-paket data.
- Alamat/Prangko di Setiap Halaman : Header dan IP address.
- Kantor Pos & Kurir : Router dan ISP yang merutekan paket.
- Penerima Menyusun Ulang Halaman: Proses perakitan kembali TCP.

Intinya, pengiriman data internet adalah proses kolaboratif, terdesentralisasi, dan sangat efisien yang memastikan data dalam bentuk paket-paket kecil dapat melakukan perjalanan dengan cepat dan andal melintasi jaringan global menggunakan aturan standar TCP/IP.

B. Transmisi Data pada Jaringan Komputer

Transmisi data adalah proses pengiriman dan penerimaan data dari satu perangkat ke perangkat lain melalui media jaringan. Transmisi ini memungkinkan komputer saling bertukar informasi, baik dalam jaringan lokal (LAN) maupun jaringan luas (WAN).

Transmisi data berdasarkan media yang digunakan, dibagi menjadi 2 :

1. Transmisi Kabel (Wired).

Transmisi data yang menggunakan kabel sebagai media penghantar data, diantaranya :

a. Kabel Twisted Pair (UTP (Unshielded Twisted Pairs)/STP (Shielded Twisted Pairs))
   - Digunakan pada jaringan LAN.
   - Terdiri dari pasangan kabel yang dipilin.
   - Kelebihan : Murah, mudah dipasang.
   - Kekurangan : Rentan *interferensi* (gangguan sinyal eksternal atau internal yang mencampuri sinyal data yang sedang dikirim melalui kabel tembaga, menyebabkan penurunan kualitas sinyal, kesalahan transmisi, atau bahkan hilangnya koneksi. Secara sederhana, interferensi seperti suara berisik yang mengganggu pembicaraan telepon, membuat sulit memahami apa yang dikatakan.) terutama kabel UTP.

b. Kabel Coaxial
   - Memiliki pelindung yang kuat.
   - Dahulu banyak dipakai pada jaringan bus topology.
   - Kelebihan : Stabil dan tahan gangguan.
   - Kekurangan : Kurang fleksibel, mulai jarang digunakan.

c. Kabel Fiber Optic
   - Menggunakan cahaya sebagai media transmisi.
   - Kelebihan : Sangat cepat, tahan interferensi, jarak jauh.
   - Kekurangan : Pemasangan lebih rumit.

2. Transmisi Nirkabel (Wireless)

Transmisi data yang menggunakan gelombang elektromagnetik tanpa kabel, diantaranya :

a. Wi-Fi (Wireless Fidelity)
   - Digunakan untuk jaringan lokal tanpa kabel.
   - Cocok untuk laptop, HP, dan perangkat IoT (Internet of Think).

b. Bluetooth
   - Komunikasi jarak dekat (short range).
   - Cocok untuk headset, keyboard, transfer file.

c. Radio dan Microwave Link
   - Digunakan untuk komunikasi jarak jauh seperti menara BTS.

d. Infrared
   - Terbatas jarak dekat dan harus tanpa halangan.
   - Contoh: Remote TV, beberapa sensor.

Faktor-Faktor yang mempengaruhi kualitas transmisi data, diantaranya :

1. Bandwidth
   Bandwidth adalah lebar pita atau kapasitas maksimum suatu jalur komunikasi untuk mengirim data. Semakin besar bandwidth, semakin banyak data yang dapat dikirim pada satu waktu. Contoh: Fiber optik memiliki bandwidth lebih besar dibanding kabel UTP.
2. Jarak (Distance)
   Semakin jauh jarak pengiriman data, semakin besar kemungkinan sinyal melemah. Pada kabel tembaga, jarak panjang dapat menyebabkan data hilang atau salah. Solusinya adalah menggunakan repeater, switch, atau media fiber optik untuk jarak jauh.
3. Media Transmisi
   Jenis media sangat mempengaruhi kualitas transmisi.
   a. Kabel Tembaga (UTP, STP, Koaksial) mudah terpengaruh gangguan elektromagnetik dan Jarak efektif terbatas (biasanya 100 meter untuk UTP).
   b. Fiber Optik menggunakan cahaya sangat cepat dan tidak terpengaruh interferensi. Cocok untuk transmisi jarak jauh.
   c. Wireless (Wi-Fi, Bluetooth, Microwave) terpengaruh kondisi cuaca, penghalang fisik, dan gelombang lain. Mudah terjadi interferensi jika banyak perangkat menggunakan frekuensi sama.
4. Noise / Interferensi. Noise adalah gangguan yang memengaruhi kualitas sinyal dalam jalur transmisi. Sumber noise : Peralatan listrik (mesin, motor, AC), Perangkat yang memancarkan gelombang radio, Kabel listrik yang berdekatan dengan kabel jaringan. Dampaknya Data rusak, lambat, atau tidak sampai.

Latihan 2

1. Apa yang dimaksud jaringan internet?Jelaskan menurut pendapatmu!
2. Mengapa internet di rumah bisa lancar, tetapi di sekolah atau tempat ramai sering terasa lambat? Faktor apa saja yang memengaruhi kecepatan dan kualitas internet?
3. Apa yang dimaksud paket switching dalam proses pengiriman data di internet?
4. Jelaskan pengertian transmisi data dalam jaringan komputer!
5. Sebutkan faktor-faktor yang mempengaruhi kualitas transmisi data dalam jaringan komputer!

UJI KOMPETENSI BAB III

I. Berilah tanda silang (X) pada huruf a, b, c, atau d pada jawaban yang tepat!

1. LAN adalah singkatan dari…
   A. Local Area Network
   B. Large Access Network
   C. Line Area Network
   D. Local Access Node
2. Berikut ini manakah yang bukan merupakan tempat atau wilayah jaringan lokal komputer ….
   A. Sekolah
   B. Gedung kantor
   C. Antar benua
   D. Rumah
3. Jika ingin menghubungkan lebih dari dua perangkat dalam jaringan yang sama, dibutuhkan perangkat tambahan, yaitu ...
   A. Komputer
   B. Access Point
   C. Switch
   D. Repeater
4. Kabel yang paling umum digunakan dalam jaringan komputer lokal (LAN) adalah…
   A. Kabel HDMI
   B. Kabel USB
   C. Kabel UTP
   D. Kabel VGA
5. Nama perangkat jaringkan komputer berikut ini adalah ….

   A. Switch
   B. Twisted Pairs
   C. Mikrotik
   D. Access Point
6. Dalam sebuah jaringan komputer, apa yang bisa dilakukan oleh client ….
   A. Mentransfer data
   B. Menginstall aplikasi
   C. Menghapus aplikasi
   D. Merubah sistem operasi
7. Fungsi utama dari alamat IP dalam jaringan LAN adalah…
   A. Menyimpan file pada komputer
   B. Memberi identitas setiap perangkat
   C. Menghapus data pada jaringan
   D. Mempercepat akses internet
8. Komponen yang menghubungkan komputer ke jaringan melalui kabel atau sinyal nirkabel adalah ...
   A. Switch
   B. Access Point
   C. Kabel UTP
   D. NIC
9. Perangkat yang menghubungkan beberapa jaringan komputer yang berbeda dan mengarahkan lalu lintas data di antara jaringan tersebut untuk memastikan paket data sampai ke tujuan yang benar adalah ...
   A. Switch
   B. Access Point
   C. Router
   D. NIC
10. Menggunakan serat kaca atau plastik tipis untuk mentransmisikan data dalam bentuk cahaya. Kabel ini menawarkan kecepatan transfer data yang sangat tinggi dan jangkauan yang lebih jauh, sering digunakan untuk koneksi internet berkecepatan tinggi atau jaringan perusahaan besar. Adalah ciri – ciri kabel jaringan komputer ...
    A. Twisted pair
    B. Coaxial
    C. Fiber optic
    D. Wifi
11. Kabel coaxial adalah ...
    A. Terdiri dari beberapa pasang kabel tembaga yang dililit satu sama lain untuk mengurangi interferensi.
    B. Jenis kabel yang lebih tua, dulu populer untuk jaringan komputer dan TV kabel. Terdiri dari inti tembaga padat yang dikelilingi oleh lapisan isolasi dan pelindung logam.
    C. Menggunakan serat kaca atau plastik tipis untuk mentransmisikan data dalam bentuk cahaya.

D. media untuk menyalurkan energi listrik yang terdiri dari konduktor (seperti tembaga atau aluminium) yang dilapisi dengan isolator (pembungkus dari bahan thermoplastik atau thermosetting) untuk menghantarkan arus listrik dengan aman.

12. Internet adalah singkatan dari ….
    A. Interconnected Network
    B. International Networking
    C. Intraconnected Network
    D. Inter Network
13. Nama proyek dari departemen pertahanan Amerika Serikat yang mengembangkan jaringan komputer adalah ....
    A. APRA
    B. ARPANET
    C. UCLA
    D. WAN
14. Tahun lahirnya internet sering dikaitkan dengan keberhasilan ARPANET menghubungkan empat universitas pada tahun…
    A. 1945
    B. 1969
    C. 1975
    D. 1983
15. IP adalah singkatan dari ...
    A. Internet Protocol
    B. Internet Posting
    C. Intranet Protocol
    D. Intranet Posting
16. Data dibuat di aplikasi Anda, lalu protokol TCP memecahnya menjadi paket-paket. Setiap paket diberi informasi IP dan informasi lain yang diperlukan adalah ...
    A. Perutean (Routing)
    B. Enkapsulasi (Pengemasan)
    C. Transit Jaringan
    D. Konfirmasi
17. Perakitan Kembali (Reassembly) pada proses pengiriman data di internet adalah ...
    A. Pihak penerima mengirimkan konfirmasi (acknowledgement) kembali ke pengirim bahwa paket telah diterima dengan benar. Jika ada paket yang tidak sampai atau rusak, pengirim akan mengirimkannya kembali.
    B. Router di sepanjang jalur (dari ISP Anda, melalui kabel serat optik bawah laut atau darat, hingga ke server tujuan) memeriksa alamat IP tujuan pada setiap paket. Setiap router memutuskan jalur terbaik berikutnya untuk paket tersebut agar lebih dekat ke tujuan. Paket dari satu pengiriman yang sama bisa saja menempuh jalur yang berbeda-beda.
    C. Saat paket-paket tiba di tujuan (misalnya, server situs web atau komputer teman Anda), protokol TCP di sisi penerima menggunakan nomor urut paket untuk menyusun kembali data ke bentuk aslinya.
    D. Paket-paket ini mulai melakukan perjalanan melalui jaringan lokal (router rumah/kantor Anda) dan diteruskan ke Penyedia Layanan Internet (ISP) Anda.
18. Proses pengiriman dan penerimaan data dari satu perangkat ke perangkat lain melalui media jaringan disebut ...
    A. Transmisi Data
    B. Transmisi Nirkabel
    C. Bandwitdh
    D. Media Transmisi
19. Kecepatan transfer data biasanya diukur dengan satuan…
    A. Hertz
    B. Decibel
    C. Mbps
    D. Watt
20. Kabel fiber optic mentransmisikan data menggunakan…
    A. Gelombang radio
    B. Sinyal cahaya
    C. Sinyal listrik
    D. Gelombang mikro

II. Jawablah pertanyaan-pertanyaan di bawah dengan singkat dan jelas!

1. Jelaskan perbedaan jaringan komputer lokal dan jaringan internet!
2. Sebutkan dan jelaskan 3 jenis kabel jaringan komputer!
3. Mengapa dalam jaringan komputer setiap komputer harus memiliki alamat IP?
4. Bagaimana proses pengiriman data di internet?
5. Sebutkan dan jelaskan transmisi data dalam jaringan komputer berdasarkan media yang digunakan!

BAB IV
CYBERBULLYING

Tujuan Pembelajaran

Setelah mempelajari bab ini murid mampu memahami :

1. Pengertian cyberbullying.
2. Bentuk – bentuk cyberbullying.
3. Dampak yang ditimbulkan dari cyberbullying
4. Penyebab adanya cyberbullying.
5. Cara mengatasi cyberbullying.

Pertanyaan Pemantik

1. Pernahkah kalian melihat komentar negatif atau kasar di media sosial? Apa yang kalian rasakan saat melihatnya?
2. Bagaimana menurut kalian perasaan seseorang yang menjadi korban cyberbullying meskipun tidak bertemu langsung dengan pelaku?
3. Apakah membagikan ulang foto seseorang tanpa izin termasuk cyberbullying?
4. Mengapa orang lebih berani melakukan perundungan di internet dibandingkan di dunia nyata?
5. Apa yang bisa kalian lakukan jika melihat teman menjadi korban cyberbullying?

MATERI

Cyberbullying adalah tindakan perundungan atau penindasan yang dilakukan melalui media digital seperti media sosial, aplikasi pesan, game online, email, atau platform digital lainnya. Tindakan ini dapat berupa komentar kasar, penyebaran rumor, ancaman, penghinaan, atau penyebaran foto/video tanpa izin yang bertujuan menyakiti, mempermalukan, atau merendahkan orang lain. Cyberbullying berlangsung secara daring sehingga dapat terjadi kapan saja, bersifat anonim, dan menyebar dengan cepat sehingga dampaknya lebih luas daripada perundungan langsung.

A. Jenis – Jenis Cyberbullying

1. Harassment (Pelecehan)

harassment cyberbullying adalah tindakan melecehkan, mengancam, atau mempermalukan seseorang secara berulang-ulang melalui teknologi digital seperti media sosial, email, atau pesan teks. Ini termasuk mengirim pesan yang kasar, menyebarkan rumor, membagikan informasi pribadi atau foto memalukan secara online, serta membuat akun palsu untuk menyebarkan kebohongan.

2. Flaming (Pertengkaran Daring)

Flaming dalam cyberbullying adalah tindakan mengirimkan pesan-pesan berisi kata-kata kasar, marah, atau hinaan yang bertujuan untuk memprovokasi atau menyakiti orang lain secara daring. Ini bisa berupa unggahan komentar di media sosial, pesan teks, atau email, dan sering kali memicu pertengkaran daring antar individu atau kelompok.

3. Denigration (Pencemaran Nama Baik)

Denigration adalah jenis cyberbullying yang berfokus pada pencemaran nama baik dengan menyebarkan informasi negatif atau kejelekan seseorang di internet untuk merusak reputasi dan harga dirinya. Tindakan ini bisa dilakukan dengan menyebarkan kebohongan, mengunggah foto atau video yang sudah diubah secara tidak benar, atau menceritakan aib seseorang agar orang lain memandang buruk terhadapnya.

4. **Impersonation (Penyamaran)**
   Impersonation adalah indakan berbahaya di mana seseorang berpura-pura menjadi orang lain di dunia maya untuk menyebarkan informasi atau pesan yang memfitnah, mempermalukan, atau mencemarkan nama baik korban. Pelaku biasanya membuat akun palsu atau meretas akun orang lain untuk mengirimkan pesan yang merusak reputasi dan hubungan korban.
5. **Outing**
   Outing adalah bentuk cyberbullying yang melibatkan penyebaran informasi pribadi seseorang secara daring tanpa izin untuk mempermalukan atau menyakiti mereka. Pelaku membagikan rahasia, pesan pribadi, foto, atau data sensitif lainnya, yang bisa merusak reputasi korban dan menimbulkan dampak emosional yang parah.
6. **Exclusion (Pengucilan)**
   Exclusion dalam cyberbullying adalah pengucilan yang disengaja terhadap seseorang dari grup daring, aktivitas, atau grup pertemanan. Bentuknya bisa berupa tidak memasukkan seseorang ke dalam grup obrolan, tidak mengajak untuk bergabung dalam permainan daring, atau sengaja mengabaikan seseorang secara daring.
7. **Trickery (Menipu untuk Mendapatkan Informasi Pribadi)**
   Trickery dalam cyberbullying adalah tindakan menipu atau membujuk korban secara daring agar membagikan informasi pribadi atau gambar sensitif, yang kemudian akan disalahgunakan dan disebarkan kepada orang lain. Pelaku akan membangun kepercayaan dengan berpura-pura menjadi teman atau orang terdekat sebelum menyebarkan rahasia korban, yang bisa berakibat pada rasa malu, perusakan reputasi, dan dampak psikologis serius bagi korban.
8. **Cyberstalking (Penguntitan Siber)**
   Cyberstalking adalah tindakan menguntit, mengawasi, atau mengganggu seseorang secara terus-menerus melalui media digital seperti media sosial, email, pesan instan, atau platform online lainnya. Pelaku biasanya melakukan pemantauan secara berlebihan, mengirim pesan atau ancaman berulang, mencari informasi pribadi korban, hingga mencoba mengontrol aktivitas online korban.

B. Penyebab terjadinya cyberbulyling

1. Anonymity (Anonimitas) adalah kondisi di mana identitas seseorang tidak diketahui atau tidak teridentifikasi. Istilah ini merujuk pada keadaan "tanpa nama" dan sering digunakan dalam konteks privasi digital, penelitian, dan hukum untuk menjaga kerahasiaan individu. Anonimitas dapat tercipta secara sengaja atau tidak sengaja, dan berfungsi untuk melindungi privasi, menjaga kebebasan berekspresi, atau menyembunyikan identitas untuk alasan tertentu.
2. Kurangnya empati dalam cyberbullying adalah ketidakmampuan pelaku untuk memahami atau merasakan penderitaan korban, yang memungkinkan mereka untuk bertindak agresif dan menyakiti orang lain secara daring tanpa merasa bersalah. Ini sering kali terjadi karena pelaku tidak dapat melihat dampak langsung dari tindakan mereka, ditambah lagi kurangnya isyarat nonverbal di dunia maya.
3. Lelucon yang berlebihan dalam cyberbullying adalah bentuk perundungan digital yang dilakukan dengan cara menggunakan humor, candaan, atau olok-olok secara berlebihan sehingga menyakiti, merendahkan, atau mempermalukan seseorang di dunia maya. Pada awalnya mungkin terlihat seperti canda, tetapi ketika : dilakukan berulang-ulang, menyinggung fisik, keluarga, atau kondisi pribadi, mengandung ejekan atau penghinaan, atau membuat korban merasa malu, tertekan, atau takut, maka lelucon tersebut sudah berubah menjadi cyberbullying, bukan lagi candaan biasa.
   Contoh :
   - Mengunggah meme tentang teman lalu menertawakan kekurangannya.
   - Melontarkan komentar "cuma bercanda kok" setelah mengolok-olok seseorang.

- Membuat grup chat untuk meledek seseorang secara terus-menerus.
- Edit foto seseorang untuk dijadikan bahan lelucon yang merendahkan.

4. Lingkungan digital tanpa aturan dalam cyberbullying adalah kondisi ketika ruang online tidak memiliki pengawasan, pedoman, atau batasan yang jelas sehingga perilaku negatif—termasuk perundungan digital—dapat terjadi dengan mudah.
5. Balas dendam atau konflik pribadi dalam cyberbullying adalah jenis tindakan perundungan digital yang dilakukan seseorang untuk membalas sakit hati, dendam, atau masalah pribadi terhadap orang lain melalui media online. Biasanya pelaku merasa pernah disakiti — baik secara langsung maupun tidak langsung — kemudian menggunakan media digital untuk membalas, seperti :
   - Mengirim pesan kasar atau menghina
   - Menyebarkan aib atau fitnah
   - Mengunggah konten yang mempermalukan korban
   - Menghasut orang lain untuk membenci korban
   - Membocorkan data pribadi (doxxing)
6. Pengaruh teman sebaya dalam cyberbullying yang paling umum terjadi, terutama pada remaja :
   - Tekanan untuk Ikut-Ikutan (Peer Pressure)
     Remaja sering merasa perlu menyesuaikan diri dengan kelompoknya. Ketika teman sebaya melakukan perundungan di dunia digital, seseorang bisa terdorong untuk ikut terlibat agar dianggap "keren" atau diterima dalam kelompok.
   - Normalisasi Perilaku Negatif
     Jika dalam suatu kelompok perilaku mengejek atau menghina di media sosial dianggap biasa, maka anggota kelompok akan menganggap cyberbullying sebagai hal normal. Akibatnya, batas benar–salah menjadi kabur.
   - Penguatan Perilaku Pelaku
     Dukungan, atau komentar positif dari teman sebaya terhadap aksi perundungan dapat memperkuat perilaku pelaku. Mereka merasa mendapat dukungan sehingga cyberbullying terus berlanjut.
   - Rasa Takut Keluar dari Kelompok
     Sebagian remaja tidak ingin dikucilkan. Mereka memilih diam atau tidak membela korban karena takut menjadi sasaran berikutnya. Sikap pasif ini secara tidak langsung mendukung terjadinya cyberbullying.
   - Kurangnya pemahaman tentang etika digital
     Kondisi ketika seseorang tidak memahami aturan, norma, dan perilaku yang seharusnya dilakukan saat berinteraksi di dunia digital, sehingga dapat menyebabkan tindakan menyakiti, merendahkan, atau merugikan orang lain secara online.
     Berikut beberapa bentuk kurangnya pemahaman etika digital yang sering memicu cyberbullying :
     a. Tidak memahami batasan privasi digital.
        - Menganggap wajar menyebarkan foto, video, atau informasi pribadi orang lain tanpa izin.
        - Tidak menyadari bahwa tindakan tersebut bisa berdampak besar pada korban.
     b. Menganggap dunia maya sebagai tempat bebas tanpa aturan
        - Berpikir bahwa komentar kasar, ejekan, atau hinaan di internet tidak memiliki konsekuensi.
        - Merasa aman karena bersembunyi di balik identitas anonim.
     c. Tidak memahami pentingnya komunikasi yang sopan
        - Mengirim pesan bernada marah, mengejek, atau memprovokasi tanpa mempertimbangkan perasaan orang lain.
        - Tidak tahu cara menyampaikan kritik secara santun di ruang digital.
     d. Kurang memahami jejak digital (digital footprint)

- Tidak sadar bahwa setiap aktivitas online terekam dan dapat ditelusuri.
- Menganggap bahwa postingan yang sudah dihapus benar-benar hilang.

e. Tidak mengenal konsekuensi hukum
   - Banyak pelaku cyberbullying tidak tahu bahwa tindakan mereka bisa berujung pada pelanggaran hukum seperti UU ITE.

f. Minimnya empati dalam komunikasi online
   - Tidak bisa merasakan dampak emosional pada korban karena tidak melihat reaksi langsung.
   - Menganggap bahwa menyakiti lewat teks atau komentar bukanlah hal serius.

C. Dampak Cyberbullying

Cyberbullying memiliki dampak yang luas dan merusak bagi korbannya, mencakup aspek fisik, mental, sosial, dan akademik. Konsekuensi ini bisa bersifat jangka pendek maupun jangka panjang yang serius, termasuk kasus ekstrem seperti bunuh diri. :

1. Dampak bagi Korban

a. Dampak Psikologis dan Emosional

Ini adalah dampak yang paling umum dan parah. Korban sering mengalami :

- Depresi dan Kecemasan
  Perasaan sedih yang mendalam, putus asa, dan kekhawatiran berlebihan adalah hal yang umum terjadi.
- Kehilangan Harga Diri
  Hinaan dan ejekan terus-menerus dapat membuat korban merasa tidak berharga dan kurang percaya diri.
- Perasaan Terisolasi
  Korban mungkin merasa sendirian dan terasing secara sosial, seolah-olah tidak ada yang bisa dimintai bantuan.
- Trauma
  Pengalaman traumatis dari cyberbullying yang berkelanjutan dapat menyebabkan trauma psikologis jangka panjang.
- Pikiran untuk Bunuh Diri
  Dalam kasus yang parah, korban mungkin melihat bunuh diri sebagai satu-satunya jalan keluar dari penderitaan mereka.

b. Dampak Fisik

Stres dan kecemasan intens akibat cyberbullying dapat bermanifestasi sebagai masalah fisik, seperti :

- Sakit Kepala dan Nyeri Otot
  Ketegangan akibat stres dapat menyebabkan sakit kepala tegang dan nyeri di area leher atau otot lainnya.
- Gangguan Tidur
  Kesulitan tidur atau mengalami mimpi buruk adalah hal yang sering dialami oleh korban.
- Masalah Pencernaan
  Stres kronis dapat mengganggu fungsi pencernaan.
- Penurunan Kekebalan Tubuh
  Stres yang berkepanjangan dapat melemahkan sistem kekebalan tubuh, membuat korban lebih rentan terhadap penyakit.

c. Dampak Sosial dan Akademik

- Penarikan Diri dari Lingkungan Sosial
  Korban mungkin menghindari interaksi sosial atau pertemanan karena rasa takut dan tidak aman.
- Penurunan Prestasi Akademik

Sulit berkonsentrasi dan belajar dapat menyebabkan penurunan motivasi dan nilai akademik. Korban bahkan bisa kehilangan minat pada sekolah atau sering absen.

- Kerusakan Reputasi
  Konten daring yang merugikan dapat merusak reputasi korban secara permanen.

2. Dampak bagi pelaku

a. Konsekuensi Hukum dan Kriminal
   Di Indonesia, cyberbullying bukanlah sekadar kenakalan remaja, melainkan tindak pidana yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Pelaku dapat menghadapi :
   - Tuntutan Pidana
     Jika korban atau orang tua korban melaporkan insiden tersebut kepada pihak berwajib, pelaku dapat dikenakan sanksi pidana, termasuk denda besar atau hukuman penjara, tergantung pada sifat dan tingkat keparahan tindakan (misalnya, pencemaran nama baik, penyebaran konten asusila, atau ancaman kekerasan).
   - Catatan Kriminal
     Hukuman ini dapat meninggalkan catatan kriminal permanen yang berdampak besar pada peluang kerja atau pendidikan di masa depan.

b. Konsekuensi Sosial dan Reputasi
   Tindakan cyberbullying yang dilakukan pelaku seringkali bersifat publik dan dapat dengan mudah didokumentasikan serta disebarluaskan, yang menyebabkan :
   - Kerusakan Reputasi Digital
     Reputasi online yang tercoreng akibat perilaku negatif sulit dipulihkan. Konten atau laporan tentang tindakan mereka dapat muncul saat pencarian nama mereka di internet, memengaruhi citra diri mereka di mata teman, keluarga, dan calon pemberi kerja.
   - Penolakan Sosial
     Pelaku seringkali dikucilkan oleh rekan sebaya, teman sekolah, atau komunitas mereka. Mereka mungkin kehilangan teman dan kesulitan membangun hubungan sosial yang sehat.
   - Masalah dalam Hubungan Interpersonal
     Kurangnya empati dan kecenderungan untuk menyakiti orang lain secara daring dapat menghambat kemampuan pelaku untuk menjalin hubungan pribadi yang mendalam dan bermakna.

c. Konsekuensi Akademik dan Profesional
   Perilaku bullying dapat memiliki dampak jangka panjang pada jenjang pendidikan dan karier :
   - Disiplin Sekolah/Universitas
     Pelaku dapat menghadapi tindakan disipliner dari institusi pendidikan, termasuk skorsing atau bahkan drop out.
   - Kesulitan Mencari Pekerjaan
     Banyak perusahaan modern melakukan pemeriksaan latar belakang media sosial (social media background checks). Sejarah perilaku cyberbullying dapat menjadi penghalang serius dalam mendapatkan pekerjaan atau beasiswa.
   - Kehilangan Kepercayaan
     Kehilangan kepercayaan dari figur otoritas (guru, mentor, atasan) akibat perilaku tidak etis.

d. Konsekuensi Psikologis Jangka Panjang
   Meskipun pelaku mungkin merasa berkuasa sesaat, perilaku ini sering kali berakar pada isu psikologis pribadi yang belum terselesaikan (seperti kurangnya rasa aman, atau trauma masa lalu).

- Siklus Kekerasan
  Pelaku yang tidak mendapatkan bantuan untuk mengubah perilakunya cenderung tumbuh menjadi individu yang rentan terlibat dalam perilaku antisosial atau kriminalitas di masa dewasa.
- Kurangnya Empati
  Terus-menerus melakukan tindakan tanpa memikirkan perasaan orang lain dapat mengikis empati, keterampilan sosial fundamental untuk kehidupan bermasyarakat yang sehat.

3. Dampak bagi lingkungan

a. Merusak Iklim Sosial dan Rasa Aman
   Cyberbullying menciptakan lingkungan yang penuh ketakutan, kecemasan, dan ketidakamanan.
   - Hilangnya Rasa Aman
     Baik di sekolah, tempat kerja, atau komunitas daring, insiden cyberbullying membuat individu merasa tidak aman untuk berinteraksi secara terbuka.
   - Peningkatan Stres Kolektif
     Tingkat stres dan kecemasan tidak hanya dialami oleh korban, tetapi juga menyebar ke orang-orang di sekitar yang mengetahui atau menyaksikan insiden tersebut, termasuk para saksi (bystanders).
   - Ketidakpercayaan
     Kepercayaan antarindividu menurun. Orang menjadi lebih curiga dan enggan membuka diri atau menjalin pertemanan baru karena takut menjadi target berikutnya.

b. Memutus Dinamika Interaksi Sosial yang Sehat
   Perilaku intimidasi online mengganggu cara orang berinteraksi satu sama lain.
   - Isolasi Sosial
     Korban seringkali menarik diri dari lingkungan sosialnya, yang menyebabkan hilangnya keragaman interaksi dalam grup atau kelas.
   - Normalisasi Perilaku Agresif
     Ketika cyberbullying tidak ditangani secara efektif, perilaku tersebut dapat dianggap sebagai hal yang "normal" atau "biasa" oleh lingkungan sekitar. Ini mendorong siklus kekerasan di mana perilaku agresif menjadi cara yang diterima untuk menyelesaikan konflik atau mencari perhatian.
   - Ketidakpedulian (Bystander Effect)
     Saksi yang sering melihat cyberbullying tanpa intervensi bisa menjadi apatis atau takut untuk campur tangan, sehingga masalah menjadi semakin parah.

c. Penurunan Produktivitas dan Kesejahteraan Lingkungan
   Dampak negatif ini berimbas pada fungsi lingkungan secara keseluruhan.
   - Penurunan Kinerja Akademik/Profesional
     Di lingkungan sekolah atau kantor, suasana yang tidak kondusif akibat bullying mengganggu konsentrasi dan motivasi, yang menyebabkan penurunan produktivitas dan hasil kerja atau akademik secara keseluruhan.
   - Peningkatan Ketidakhadiran
     Korban mungkin sering absen dari sekolah atau pekerjaan untuk menghindari interaksi sosial yang menyakitkan, yang mengganggu stabilitas lingkungan tersebut.
   - Beban Sumber Daya
     Lingkungan (sekolah, komunitas, atau perusahaan) harus mengalokasikan sumber daya ekstra untuk menangani, menyelidiki, dan memediasi konflik, serta memberikan dukungan kesehatan mental, yang dapat menguras waktu dan energi yang seharusnya digunakan untuk aktivitas positif.

D. Cara Mencegah dan Menghindari Cyberbullying

Mencegah dan menghindari cyberbullying membutuhkan pendekatan proaktif, baik dalam perilaku online pribadi maupun dalam pengelolaan lingkungan digital. Strategi yang efektif melibatkan kombinasi antara perlindungan diri, etika digital, dan pengetahuan tentang cara bertindak ketika insiden terjadi. Berikut adalah langkah-langkah utama untuk mencegah dan menghindari cyberbullying :

1. Perlindungan Diri dan Pengaturan Privasi

a. Jaga Kerahasiaan Informasi Pribadi
   Jangan pernah membagikan detail pribadi seperti alamat rumah, nomor telepon, atau lokasi sekolah kepada orang yang tidak dikenal secara daring.
b. Perkuat Pengaturan Privasi
   Manfaatkan pengaturan privasi yang tersedia di semua platform media sosial dan aplikasi. Batasi siapa saja yang dapat melihat unggahan Anda, mengirim pesan, atau menambahkan Anda sebagai teman hanya pada orang yang Anda kenal dan percayai.
c. Tolak Permintaan dari Orang Asing
   Jangan menerima permintaan pertemanan atau mengikuti dari akun yang tidak Anda kenal. Banyak pelaku cyberbullying menggunakan akun palsu atau anonim.
d. Blokir Akun Pelaku
   Segera blokir pengguna yang mengirim pesan menjengkelkan atau menyakitkan. Hal ini akan menghentikan komunikasi langsung dan mengurangi stres.

2. Etika Digital dan Perilaku Online yang Sehat

a. Pikir Sebelum Mengunggah/Komentar
   Ingatlah bahwa apa yang Anda unggah secara online dapat dilihat oleh banyak orang dan bertahan lama. Hindari komentar negatif, menghakimi, atau menyakitkan.
b. Tumbuhkan Empati
   Perlakukan orang lain secara online sama seperti Anda ingin diperlakukan di kehidupan nyata.
c. Jangan Terpancing
   Jika menjadi target, jangan membalas pesan atau komentar yang memprovokasi. Pelaku seringkali mencari reaksi emosional, dan membalas hanya akan memperburuk situasi.
d. Jadilah Teladan Positif
   Tunjukkan perilaku online yang positif dan suportif. Dukung teman atau kenalan yang menjadi korban cyberbullying.

3. Edukasi dan Komunikasi

a. Diskusi Terbuka
   Bicarakan secara rutin tentang pengalaman dan tantangan di dunia maya dengan orang tua, guru, atau orang dewasa tepercaya lainnya.
b. Libatkan Orang Tua/Wali
   Bagi remaja, melibatkan orang tua dalam proses pencegahan sangat penting. Orang tua dapat memantau aktivitas online dan memastikan anak merasa aman untuk melaporkan masalah.
c. Pahami Kebijakan Platform
   Kenali cara kerja fitur bantuan dan pelaporan di platform media sosial yang Anda gunakan. Perusahaan media sosial memiliki kewajiban untuk menjaga keamanan pengguna.

4. Tindakan Ketika Terjadi Cyberbullying

a. Simpan Bukti
   Ambil tangkapan layar (screenshot) dari pesan, komentar, atau unggahan yang bersifat bullying. Bukti ini sangat diperlukan jika Anda memutuskan untuk melaporkan insiden tersebut.
b. Beri Tahu Orang Dewasa Terpercaya
   Jangan mencoba menghadapi pelaku sendirian. Cari dukungan dari orang tua, guru, konselor profesional, atau pihak berwajib.
c. Laporkan ke Pihak Berwenang
   Jika ancaman bersifat serius, laporkan ke pihak sekolah, platform media sosial terkait, atau kepolisian. Di Indonesia, pelaporan dapat dilakukan melalui TePSA (Telepon Pelayanan Sosial Anak) di nomor 1500771 atau melalui Unit Siber Polri jika diperlukan.

E. Sanksi Pidana dari Tindakan Cyberbullying

1. Pencemaran Na ma Baik dan Penghinaan

a. Pasal 27A UU No. 1 Tahun 2024 (sebelumnya Pasal 27 ayat (3) UU ITE): Setiap orang dilarang menyerang kehormatan atau nama baik seseorang dengan cara menuduhkan sesuatu hal melalui media elektronik, kecuali jika pelaku mampu membuktikan kebenaran tuduhannya.
b. Sanksi (Pasal 45 ayat (4) UU No. 1 Tahun 2024): Pelaku dapat dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp400.000.000,00 (empat ratus juta rupiah).

2. Ancaman Kekerasan atau Menakut-nakuti

a. Pasal 29 UU ITE: Setiap Orang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi.
b. Sanksi (Pasal 45B UU ITE): Pelaku dapat dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

3. Penyebaran Konten Asusila

a. Pasal 27 ayat (1) UU ITE: Melarang distribusi/transmisi/akses konten yang melanggar kesusilaan.
b. Sanksi (Pasal 45 UU ITE): Ancaman pidana penjara hingga 6 (enam) tahun dan/atau denda hingga Rp1.000.000.000,00 (satu miliar rupiah).

Penting untuk dicatat bahwa jika pelaku cyberbullying adalah anak di bawah umur, proses hukumnya menggunakan Undang-Undang Sistem Peradilan Pidana Anak (UU SPPA), yang lebih mengedepankan pendekatan keadilan restoratif dan diversi (penyelesaian di luar pengadilan) daripada hukuman penjara formal.

Tugas 1

Studi Kasus Cyberbullying "Lelucon yang Kebablasan"

Kasus: "Meme dan Batasan Humor Digital"

Latar Belakang Kasus

Tomi adalah siswa kelas 8 yang dikenal pandai, tetapi sering gugup saat presentasi di depan kelas. Saat presentasi mata pelajaran Sejarah, Tomi melakukan kesalahan kecil, salah menyebutkan tahun penting, dan wajahnya memerah karena malu.

Risa, seorang siswa yang mahir mengedit gambar dan sangat aktif di media sosial, diam-diam merekam momen tersebut dengan ponselnya.

Pemicu Cyberbullying (Lelucon Kebablasan)

Setelah jam sekolah, Risa mengedit rekaman Tomi. Ia menambahkan efek filter yang lucu dan membesarkan wajah Tomi saat panik, lalu menyematkan teks lucu, mengubahnya menjadi sebuah Meme yang ia beri judul: *"Wajah Kawan Kita saat Otaknya Eror!"*

Risa kemudian mengunggah Meme tersebut ke fitur InstaStory pribadinya dengan tujuan "hanya untuk lucu-lucuan" dan menandai beberapa teman terdekatnya.

Penyebaran dan Salah Paham Konteks

Tanpa sepengetahuan Risa, salah satu temannya, Joko, tidak hanya melihat, tetapi juga menyimpan Meme itu. Joko kemudian menyebarkannya ke grup *chat* kelas yang lebih besar, dan bahkan membagikannya lagi ke grup *fans page* sekolah.

Dalam hitungan jam, Meme Tomi menjadi viral di kalangan siswa. Banyak komentar bermunculan, sebagian besar berisi tawa dan *emoticon* lucu, tetapi ada juga yang mulai menambahkan komentar pribadi tentang kepribadian Tomi.

Dampak

Tomi yang melihat Meme-nya beredar luas merasa bukan hanya dipermalukan, tetapi juga dikhianati. Ia merasa malu dan tertekan, bahkan sampai mematikan notifikasi dan tidak berani membuka media sosialnya lagi. Ia mulai menghindari Risa dan Joko, serta enggan berpartisipasi dalam diskusi kelas karena takut direkam dan dijadikan bahan lelucon lagi.

pertanyaan

1. Jelaskan, bentuk konten digital apa yang digunakan Risa untuk melakukan perundungan siber ini, mengapa tindakan tersebut meskipun awalnya dianggap "lelucon", dikategorikan sebagai *cyberbullying*?
2. Hak apa dari Tomi yang telah dilanggar oleh Risa dan Joko terkait pengeditan dan penyebaran konten pribadinya?
3. Mengapa konten yang dianggap "hanya bercanda" di media sosial dapat berisiko terhadap reputasi Risa sendiri di masa depan, meskipun ia menghapusnya?
4. Risa berdalih, "Saya cuma mau lucu-lucuan." Jelaskan mengapa, dalam dunia digital, niat awal tidak selalu membatalkan tanggung jawab atas dampak yang ditimbulkan oleh konten yang kita buat dan sebarkan?
5. Seandainya kamu sebagai ketua kelas, solusi apa yang paling cepat dan efektif yang harus kamu ambil untuk menghentikan penyebaran Meme Tomi di dalam jaringan komunikasi sekolah? Sebutkan minimal dua (2) tindakan.

UJI KOMPETENSI BAB IV

I. Berilah tanda silang (X) pada huruf a, b, c, atau d pada jawaban yang tepat!

1. Perundungan yang menggunakan teknologi digital, seperti ponsel, komputer, dan internet, disebut sebagai...
   A. Bullying Verbal
   B. Bullying Fisik
   C. Cyberstalking
   D. Cyberbullying
2. Mengirim pesan teks atau komentar yang isinya kasar, penuh amarah, dan memprovokasi pertengkaran secara online dikenal dengan istilah...
   A. Outing
   B. Flaming
   C. Exclusion
   D. Impersonation
3. Dampak psikologis yang paling umum dialami oleh korban cyberbullying adalah...
   A. Peningkatan prestasi akademik
   B. Meningkatnya interaksi sosial
   C. Depresi dan kecemasan
   D. Peningkatan rasa percaya diri
4. Salah satu cara pencegahan cyberbullying yang paling efektif terkait privasi akun media sosial adalah...
   A. Menerima semua permintaan pertemanan dari siapapun.
   B. Memposting semua informasi pribadi secara detail.
   C. Mengatur akun media sosial menjadi mode privat.
   D. Selalu membiarkan akun dalam mode publik.
5. Jika Anda menjadi korban cyberbullying, langkah pertama dan terpenting yang harus Anda lakukan adalah...
   A. Membalas perundungan tersebut dengan kata-kata yang lebih kasar.
   B. Mencari pelaku untuk diselesaikan secara fisik di dunia nyata.
   C. Mendokumentasikan (mengambil tangkapan layar) dan menyimpan semua bukti.
   D. Menghapus semua bukti perundungan dan akun media sosial.
6. Tindakan sengaja mempublikasikan rahasia atau informasi pribadi seseorang yang memalukan di media sosial tanpa izin, disebut sebagai...
   A. Denigration
   B. Harassment
   C. Cyberstalking
   D. Outing
7. Perbedaan utama antara cyberbullying dan bullying tradisional (tatap muka) adalah...
   A. Bullying tradisional tidak dapat didokumentasikan, sedangkan cyberbullying dapat didokumentasikan.
   B. Cyberbullying tidak memiliki dampak psikologis yang serius, sedangkan bullying tradisional memiliki.
   C. Cyberbullying dilakukan secara anonim atau semi-anonim, dan jangkauannya lebih luas.
   D. Cyberbullying hanya melibatkan kata-kata, sedangkan bullying tradisional melibatkan fisik.
8. Peran siswa yang hanya melihat atau membaca perundungan online tanpa melakukan tindakan apapun disebut sebagai...
   A. Defender (Pembela)
   B. Victim (Korban)
   C. Perpetrator (Pelaku)
   D. Bystander (Saksi Pasif)
9. Dalam konteks etika digital, tindakan yang seharusnya dilakukan jika Anda melihat unggahan yang memicu kebencian atau perundungan adalah...
   A. Menyimpan unggahan tersebut untuk lucu-lucuan.
   B. Ikut berkomentar untuk meredakan suasana.
   C. Melaporkan konten tersebut kepada administrator platform.
   D. Langsung memblokir semua akun tanpa mencatat bukti.
10. Mengapa penting bagi korban cyberbullying untuk tidak menghapus pesan atau komentar ancaman yang mereka terima?

A. Agar pesan tersebut tetap dapat dilihat oleh teman-teman korban.
B. Untuk membuat koleksi pesan-pesan unik.
C. Karena itu adalah satu-satunya cara untuk membuktikan terjadinya perundungan.
D. Agar pelaku merasa bersalah dan menghentikan aksinya.

11. Perundungan yang melibatkan pembuatan dan penyebaran rumor atau fitnah melalui media sosial atau email, dengan tujuan merusak reputasi korban, disebut...
A. Denigration
B. Trickery
C. Harassment
D. Exclusion

12. Undang-Undang di Indonesia yang dapat menjerat pelaku cyberbullying, terutama yang berkaitan dengan pencemaran nama baik dan penyebaran konten ilegal, adalah...
A. UU Lalu Lintas dan Angkutan Jalan
B. UU Informasi dan Transaksi Elektronik (ITE)
C. UU Perlindungan Anak
D. UU Hak Cipta

13. Mengapa tindakan *Impersonation* (berpura-pura menjadi orang lain) sangat berbahaya dalam cyberbullying?
A. Sangat mudah untuk dibuktikan dan dilaporkan.
B. Pelaku dapat merusak reputasi korban dengan memposting konten yang tidak pantas atas nama korban.
C. Karena membuat akun korban terlihat lebih keren.
D. Hanya membingungkan teman-teman korban sesaat.

14. Salah satu ciri khas *jejak digital* (digital footprint) terkait kasus cyberbullying adalah...
A. Bersifat permanen dan dapat menjadi bukti kuat atas tindakan pelaku.
B. Hanya diketahui oleh korban dan pelaku.
C. Sulit dilacak karena internet tidak menyimpan data apapun.
D. Hanya berlaku selama 24 jam dan akan otomatis terhapus.

15. Jika seorang teman dikeluarkan dari grup *chat* kelas hanya karena ia berbeda pendapat atau memiliki minat yang berbeda, ini termasuk bentuk cyberbullying...
A. Exclusion
B. Trickery
C. Impersonation
D. Flaming

16. Mana yang merupakan contoh dari tindakan *cyberstalking*?
A. Mengirimkan ancaman berulang dan memantau aktivitas korban secara intens dan menakutkan.
B. Mengirim satu komentar menghina di Instagram.
C. Membuat *polling* tentang siapa siswa terburuk di kelas.
D. Mengedit foto guru menjadi lucu.

17. Ketika seorang korban *cyberbullying* memilih untuk menutup diri dan jarang berinteraksi dengan teman-temannya di sekolah, ini menunjukkan dampak pada aspek...
A. Sosial
B. Ekonomi
C. Fisik
D. Akademik

18. Prinsip 'Think Before You Post' dalam etika digital sangat penting untuk mencegah cyberbullying karena...
A. Mempercepat proses unggahan gambar dan video.
B. Semua yang diposting akan selalu disukai orang lain.
C. Membantu memastikan konten yang diunggah tidak mengandung unsur merugikan atau menyinggung orang lain.
D. Hanya berlaku untuk konten yang bersifat rahasia.

19. Jika Anda tahu siapa pelaku cyberbullying, tindakan paling tepat yang harus dilakukan setelah mendokumentasikan bukti adalah...
A. Mencoba berbicara secara langsung dengan pelaku tanpa bantuan orang dewasa.
B. Mengancam pelaku untuk segera menghapus unggahannya.
C. Menerbitkan informasi pribadi pelaku di media sosial.

D. Melaporkan kasus tersebut kepada pihak yang berwenang (orang tua, guru BK, atau administrator platform).

20. Mengapa cyberbullying seringkali lebih menyakitkan daripada bullying tradisional?
    A. Konten perundungan dapat dilihat oleh audiens yang luas dan bertahan selamanya (permanen).
    B. Karena pelaku cyberbullying selalu dikenal dan mudah ditangkap.
    C. Karena korbannya hanya satu orang dan tidak ada yang tahu.
    D. Karena hanya terjadi di malam hari saat korban sendirian.

II. Jawablah pertanyaan-pertanyaan di bawah dengan singkat dan jelas!

1. Jelaskan apa yang dimaksud dengan cyberbullying?
2. Jelaskan 3 penyebab terjadinya cyberbullying!
3. Jelaskan minimal tiga dampak negatif yang dapat dialami oleh seorang remaja yang menjadi korban cyberbullying!
4. Sebutkan langkah-langkah yang dapat dilakukan siswa jika menjadi korban cyberbullying!
5. Mengapa etika digital penting untuk mencegah cyberbullying?

BAB V
INFORMASI PRIVAT DAN PUBLIK

Tujuan Pembelajaran

Setelah mempelajari bab ini murid mampu memahami :

1. Pengertian informasi privat dan publik.
2. Perbedaan informasi privat dan publik.
3. Jenis – jenis informasi privat dan publik.
4. Ancaman dan resiko terhadap informasi privat dan cara melindunginya.
5. Peran Informasi Publik dalam Masyarakat Digital.
6. Etika dan Tanggung Jawab Digital dalam Menggunakan Informasi Publik.

Pertanyaan Pemantik

1. Mengapa kita perlu memahami perbedaan Informasi Privat dan Informasi Publik di era digital?
2. Mengapa nama lengkap dan tanggal lahir termasuk Informasi Privat dan apa risikonya jika disalahgunakan?
3. Apakah Informasi Publik bisa berbahaya jika diubah atau disalahgunakan? Mengapa kita tetap harus berhati-hati?
4. Saat mengunggah foto liburan yang menampilkan alamat rumah, informasi apa yang termasuk Privat dan apa yang termasuk Publik?
5. Apa tanggung jawab kita sebagai warga digital dalam menjaga Informasi Privat orang lain di media sosial?

MATERI

Informasi adalah data yang telah diolah, diproses, atau dikelola sedemikian rupa sehingga memiliki arti, nilai, dan makna bagi penerimanya, seperti keterangan, kabar, atau berita. Secara umum, informasi merujuk pada :

- Pesan atau berita
  Apa yang disampaikan atau diterima melalui komunikasi.
- Pengetahuan yang diperoleh
  Fakta, data, atau instruksi yang didapatkan dari pembelajaran, pengalaman, atau penelitian
- Hasil pengolahan data
  Data mentah (fakta, angka, simbol) yang diproses menjadi sesuatu yang memberikan wawasan atau pemahaman

Informasi diklasifikasikan menjadi dua kategori utama, yaitu Informasi Privat dan Informasi Publik.

A. Informasi Privat

Informasi Privat atau Data Pribadi adalah segala informasi yang berkaitan dengan seseorang yang dapat digunakan untuk mengidentifikasi individu tersebut, baik secara langsung maupun tidak langsung.

Jenis – jenis informasi privat :

1. Identitas Dasar
   Contohnya : Nama lengkap, Tanggal lahir, Alamat rumah, Alamat email, Nomor telepon, nomor KTP, nomor SIM, nomor paspor, dan nomor pokok wajib pajak (NPWP), Foto KTP, SIM, paspor, akta kelahiran, ijazah, dan sertifikat tanah.

2. Identitas Keuangan
   Contohnya : Nomor rekening bank, Nomor kartu ATM/Kredit, PIN.
3. Data Khusus
   Contohnya : Kata sandi (password), Foto atau video pribadi, Catatan kesehatan, Lokasi saat ini (GPS).
4. Informasi medis
   Contohnya : Riwayat penyakit, alergi, dan foto rontgen
5. Jejak Digital
   Contohnya : Riwayat pencarian (browsing history), Like dan komentar di media sosial, Pola belanja online, Foto profil di media sosial, data biometrik seperti sidik jari, dan data yang dikumpulkan oleh aplikasi atau situs web.

Melindungi data privat sama pentingnya dengan mengunci pintu rumahmu. Jika dibiarkan terbuka, orang yang tidak bertanggung jawab bisa masuk dan melakukan hal yang merugikan. Ada **beberapa alasan utama mengapa informasi privat perlu dilindungi :**

1. Mencegah Penipuan Identitas (Identity Theft)
   Jika data pribadi Anda (misalnya: KTP, nomor HP, alamat) dicuri, orang lain dapat menggunakannya untuk membuka akun, meminjam uang, atau melakukan kejahatan atas nama Anda.
2. Menghindari Cyberbullying dan Pelecehan
   Foto atau chat pribadi yang bocor dapat menjadi bahan ejekan atau perundungan siber oleh teman sebaya atau orang asing.
3. Menjaga Keamanan Finansial
   Kebocoran data keuangan (meskipun hanya PIN e-wallet Anda) dapat mengakibatkan kerugian uang.
4. Menjaga Kebebasan Berekspresi
   Jika Anda merasa terus diawasi atau data Anda tidak aman, Anda akan takut untuk berpendapat atau berekspresi secara jujur di dunia maya.

Ancaman adalah tindakan jahat yang dilakukan oleh individu atau kelompok untuk mendapatkan datamu secara ilegal. Ancaman pelanggaran privasi di dunia digital seringkali datang dalam bentuk :

1. Phishing
   Upaya untuk mendapatkan data sensitif (seperti username dan password) dengan menyamar sebagai institusi tepercaya (bank, media sosial, atau sekolah). Biasanya pelaku mengirim email/pesan yang isinya mendesak Anda untuk mengklik tautan palsu dan memasukkan data login Anda.
2. Malware (Perangkat Lunak Jahat)
   Program jahat ini bisa masuk ke HP atau laptopmu melalui aplikasi bajakan atau file yang kamu unduh sembarangan. Malware ini disembunyikan dalam aplikasi/file gratis yang diunduh ilegal. Setelah terinstal, ia bisa mencuri data Anda.
3. Pembobolan Akun (Account Takeover)
   Jika kamu menggunakan password yang sama untuk banyak akun, pelaku yang berhasil mendapatkan satu password (misalnya dari akun game) akan mencoba menggunakannya untuk membobol akunmu yang lain (seperti email utama atau media sosial).
4. Oversharing
   Berbagi terlalu banyak detail tentang kehidupan pribadi secara sukarela di media sosial, seperti lokasi terkini (live location), rencana liburan, atau foto kartu identitas. Hal ini bisa dimanfaatkan oleh stalker atau perampok yang memantau kapan rumah Anda kosong.
5. Pelacakan (Tracking)

Situs web atau aplikasi melacak aktivitas online Anda untuk tujuan iklan atau analisis data. Cara kerja dari pelanggaran privasi ini adalah menggunakan cookies atau fitur GPS pada ponsel Anda tanpa Anda sadari.

Risiko adalah konsekuensi atau kerugian yang akan kamu alami jika ancaman di atas berhasil. Berikut adalah dampak nyata yang harus kamu waspadai :

1. Kerugian Finansial (Uang Hilang)
   Jika data-data bank yang kamu miliki bocor melalui phishing di HP-mu, uang di rekening bisa hilang. Bahkan untuk kamu sendiri, data yang digunakan untuk pinjaman online ilegal bisa menyebabkan tagihan hutang yang tidak pernah kamu buat.
2. Kerusakan Reputasi dan Mental (Cyberbullying & Doxing)
   Doxing adalah praktik menyebarkan informasi pribadi seseorang ke publik tanpa izin (alamat rumah, nomor HP, nama orang tua, foto pribadi) dengan tujuan untuk mempermalukan atau melecehkan korban. Data yang disalahgunakan tidak hanya merugikan secara uang, tapi juga secara sosial dan mental. Kamu bisa menjadi korban cyberbullying yang parah, merasa malu, stres, atau bahkan takut untuk pergi ke sekolah atau bertemu teman.
3. Kehilangan Kontrol Akun (Di-hack)
   Jika email utama atau akun media sosialmu diretas, kamu akan kehilangan akses ke akun tersebut. Pelaku bisa menggunakan akunmu untuk menipu teman-temanmu, menyebarkan hoax atas namamu, atau bahkan mengunggah konten yang tidak pantas, merusak hubungan pertemanan dan citramu di sekolah.
4. Diskriminasi
   Meskipun jarang terjadi di usia SMP, data sensitif tentang kesehatan atau keyakinan bisa digunakan untuk mendiskriminasimu di masa depan (misalnya, saat melamar pekerjaan atau mendaftar beasiswa).

Untuk melindungi data privat kalian, Terapkan langkah-langkah berikut untuk mengamankannya :

1. Kelola Kata Sandi (Password Management)
   - Gunakan Kata Sandi Kuat
     Kombinasi minimal 8-12 karakter, termasuk huruf besar, huruf kecil, angka, dan simbol ($%@!).
   - Jangan Gunakan Kata Sandi yang Sama
     Gunakan kata sandi yang berbeda untuk setiap akun penting (email, e-wallet, media sosial).
   - Aktifkan Otentikasi Dua Faktor (2FA)
     Fitur keamanan tambahan yang memerlukan kode verifikasi dari perangkat lain (misalnya SMS atau aplikasi Authenticator) selain kata sandi saat Anda login.
2. Etika Digital (Netiket) dan Berbagi Informasi
   - Pikirkan Sebelum Mengunggah (Think Before You Post)
     Jangan pernah memposting foto tiket pesawat atau kartu identitas, foto yang memperlihatkan lokasi rumah atau sekolah Anda secara detail, keluhan atau chat pribadi orang lain tanpa izin.
   - Hormati Privasi Orang Lain
     Selalu minta izin sebelum mengunggah foto atau video teman Anda.

3. Pengaturan Akun dan Aplikasi
   - Atur Akun Menjadi Privat
     Ubah pengaturan privasi di media sosial Anda menjadi Privat (Private Account) agar hanya teman yang Anda setujui yang dapat melihat unggahan Anda.

- Batasi Izin Aplikasi
  Periksa secara rutin izin yang diminta oleh aplikasi di ponsel Anda. Misalnya, apakah aplikasi game perlu izin mengakses mikrofon atau lokasi Anda? Matikan izin yang tidak perlu.
- Nonaktifkan Lokasi
  Matikan fitur layanan lokasi (GPS) pada aplikasi media sosial (misalnya Instagram dan TikTok) saat tidak diperlukan.

4. Waspadai Tautan dan Unduhan
   - Jangan Klik Tautan Sembarangan
     Jangan pernah mengklik tautan atau mengunduh lampiran dari email, SMS, atau chat dari sumber yang tidak dikenal, meskipun mengatasnamakan hadiah atau kejutan.
   - Cek URL
     Selalu periksa alamat situs web (URL) sebelum memasukkan username atau password Anda. Pastikan diawali dengan https:// (menandakan koneksi aman).

B. Informasi Publik

informasi publik adalah data atau keterangan yang pada dasarnya dapat diakses oleh setiap orang. Tujuannya adalah untuk menjamin hak warga negara untuk tahu, mendorong partisipasi masyarakat, serta mewujudkan penyelenggaraan negara yang transparan, efisien, dan akuntabel. Di Indonesia, hak masyarakat untuk memperoleh Informasi Publik dijamin oleh Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (UU KIP). Hal ini menegaskan bahwa keterbukaan informasi adalah ciri penting dari negara yang demokratis.

Meskipun disebut "Publik", tidak semua informasi yang dimiliki oleh Badan Publik boleh dibuka. Ada dua kategori utama Informasi Publik :

1. Informasi Terbuka
   Informasi yang wajib disediakan dan dapat diakses oleh semua orang tanpa perlu alasan atau izin khusus.
   Contoh : Anggaran sekolah, Hasil Ujian Nasional/Sekolah (umumnya), Peraturan dan kebijakan pemerintah, Jadwal layanan publik.
2. Informasi Dikecualikan
   Informasi yang tidak boleh diakses oleh publik karena dapat membahayakan keamanan negara, menghambat proses hukum, atau melanggar hak privasi seseorang.
   Contoh : Data pribadi seseorang (KTP, rekam medis), Strategi pertahanan negara, Hasil penyelidikan kriminal yang sedang berlangsung, Rahasia jabatan/bisnis.

Di era digital, akses terhadap Informasi Publik semakin mudah melalui website resmi, portal data terbuka, dan media sosial lembaga. Peran informasi publik dalam masyarakat digital diantaranya :

1. Mendorong Transparansi
   Masyarakat dapat mengawasi bagaimana uang negara digunakan (misalnya: anggaran pembangunan sekolah atau jalan).
2. Meningkatkan Partisipasi Publik
   Masyarakat dapat memberikan masukan atau kritik yang didasarkan pada data dan fakta yang akurat.
3. Memerangi Berita Palsu (Hoaks)
   Informasi publik resmi dapat dijadikan
4. Sarana Belajar dan Penelitian
   Siswa dapat menggunakan data publik (misalnya data statistik penduduk, data iklim) untuk tugas-tugas penelitian Informatika atau mata pelajaran lain.

Sebagai warga digital yang cerdas dan beretika, Anda memiliki tanggung jawab saat menggunakan dan berbagi Informasi Publik.

1. Verifikasi (Mengecek Kebenaran)
   - Waspada Sumber: Jangan mudah percaya pada Informasi Publik yang disebarkan melalui grup chat tanpa sumber yang jelas.
   - Cek Sumber Asli: Selalu verifikasi informasi dengan mengunjungi website resmi Badan Publik terkait (misalnya, website Kementerian, Badan Pusat Statistik, atau website sekolah).
   - Cross-Check: Bandingkan informasi dari satu sumber dengan sumber kredibel lainnya (misalnya, berita di media massa nasional).
     Penggunaan yang Bertanggung Jawab
   - Gunakan Sesuai Tujuan
     Gunakan Informasi Publik untuk kepentingan yang positif, seperti belajar, berpendapat, atau berpartisipasi dalam diskusi publik.
   - Hindari Memanipulasi
     Jangan mengubah, memotong, atau memanipulasi Informasi Publik untuk tujuan negatif (misalnya, membuat hoaks atau memfitnah).
   - Berikan Kredit (Citation)
     Saat menggunakan data atau dokumen dari Badan Publik dalam tugas atau presentasi, wajib mencantumkan sumbernya dengan jelas (misalnya: "Data bersumber dari BPS, 2024").
2. Jaga Informasi Publik yang Dikecualikan
   - Hargai Batasan Privasi
     Jika Anda menemukan data yang seharusnya bersifat Informasi Dikecualikan (seperti data pribadi teman atau guru), Anda tidak boleh menyebarkannya.
   - Laporkan
     Jika Anda melihat ada kebocoran Informasi Dikecualikan di platform publik, segera laporkan kepada pihak yang bertanggung jawab (admin atau guru).

C. Perbedaan Informasi Privat dan Informasi Publik

Dalam dunia digital, membedakan antara informasi yang harus dirahasiakan (privat) dan yang boleh diketahui umum (publik) adalah keterampilan penting dalam beretika digital (Netiket) dan menjaga keamanan diri.

Perbandingan informasi privat dan informasi publik

Kriteria Pembeda	***Informasi Privat (Data Pribadi)***	***Informasi Publik***
Definisi Dasar	Data atau fakta yang berkaitan langsung dengan individu dan digunakan untuk mengidentifikasi orang tersebut.	Data atau fakta yang dihasilkan oleh Badan Publik (pemerintah/lembaga) yang berkaitan dengan kepentingan umum dan wajib diketahui masyarakat.
Tujuan Utama	Perlindungan dan keamanan individu dari penipuan, peretasan, atau penyalahgunaan.	Transparansi, akuntabilitas, dan partisipasi masyarakat dalam pemerintahan.
Kepemilikan	Dimiliki oleh Individu (perseorangan).	Dimiliki oleh Badan Publik (lembaga/organisasi) atas nama negara/masyarakat.
Akses Dasar	Dibatasi dan Rahasia. Hanya boleh diakses oleh pemiliknya atau pihak yang diberi izin.	Terbuka untuk Umum (kecuali ada pengecualian).

Kriteria Pembeda	***Informasi Privat (Data Pribadi)***	***Informasi Publik***
Risiko Utama Jika Bocor	Penipuan Identitas (*Identity Theft*), *Cyberbullying*, Kerugian Finansial.	Penyalahgunaan Wewenang (Korupsi), Ketidakpercayaan Publik, *Hoaks* (jika disalahgunakan).
Landasan Hukum di Indonesia	Perlindungan Data Pribadi (UU PDP).	Keterbukaan Informasi Publik (UU KIP).

Memahami perbedaan ini sangat penting saat Anda berinteraksi dengan teknologi di sekolah atau di rumah. Berikut adalah contoh konkret dalam kehidupan siswa :

Situasi	***Informasi Privat***	***Informasi Publik***
Di Sekolah	Nilai rapor Anda, Catatan kesehatan Anda, Foto pribadi di galeri ponsel.	Anggaran pembangunan kelas baru, Jadwal pelajaran kelas, Struktur organisasi kelas, Struktur organisasi OSIS.
Di Media Sosial	Kata sandi akun Anda, Lokasi rumah Anda saat ini (via GPS), Percakapan *chat* pribadi dengan teman.	Postingan resmi dari akun sekolah, Pengumuman lomba terbuka, Informasi jadwal *live streaming* umum.
Dokumen Resmi	Nomor Induk Siswa (NIS), Nomor Induk Siswa Nasional (NISN), Nomor Induk Kependudukan (NIK) Anda, Tanda tangan digital Anda.	Peraturan sekolah tentang seragam, Daftar nama guru dan mata pelajaran, Peta atau denah umum sekolah.

Sebagai warga digital yang cerdas (Literasi Digital), Anda harus memiliki sikap yang berbeda terhadap kedua jenis informasi ini :

1. Sikap Terhadap Informasi Privat
   Tindakan yang harus dilakukan untuk melindungi (Protektif) data adalah gunakan kata sandi kuat, aktifkan 2FA, dan jangan pernah membagikan data ini kepada orang asing atau di form online yang tidak tepercaya. Hormati privasi orang lain, jangan pernah mengambil atau menyebarkan data pribadi teman tanpa izin, meskipun itu "hanya bercanda."
2. Sikap Terhadap Informasi Publik
   Tugas utama Anda adalah menganalisis dan memanfaatkan data ini untuk kebaikan bersama. Tindakan yang harus dilakukan adalah lakukan verifikasi (cek kebenaran) terhadap Informasi Publik yang Anda temukan di internet. Jangan memanipulasi Informasi Publik. Jika Anda mengutipnya, wajib mencantumkan sumber untuk menghargai pembuat informasi dan menjaga akurasi.

Kapan Data Pribadi Menjadi Publik? Sebuah Informasi Privat dapat berubah menjadi bersifat publik melalui tindakan Anda sendiri, yang sering disebut Oversharing.

Kondisi	***Deskripsi***	***Status Data***
Foto di Galeri HP	Foto *selfie* di dalam kamar Anda.	Privat
Foto Diunggah ke Akun Publik	Foto yang sama Anda unggah ke Instagram dengan *setting* akun Publik.	Semi-Publik. Anda telah memilih untuk mempublikasikannya, dan siapa pun dapat melihat/mengambilnya.
Foto Dijadikan Meme	Foto tersebut diambil, diedit, dan disebarkan ke grup *chat* tanpa izin Anda.	Publikasi Melanggar Hukum. Data Anda disalahgunakan untuk publikasi negatif (cyberbullying).

UJI KOMPETENSI BAB V

I. Berilah tanda silang (X) pada huruf a, b, c, atau d pada jawaban yang tepat!

1. Manakah di antara berikut ini yang merupakan definisi paling tepat dari informasi privat?
   A. Data statistik jumlah penduduk suatu negara.
   B. Informasi yang tersedia secara bebas untuk siapa saja dan boleh disebarluaskan.
   C. Berita yang disiarkan di televisi nasional.
   D. Informasi yang berhubungan dengan pribadi seseorang dan identitasnya yang wajib dilindungi.
2. Manakah dari data berikut ini yang tergolong sebagai informasi publik?
   A. Jadwal keberangkatan kereta api
   B. Nomor Induk Kependudukan (NIK)
   C. Password akun media sosial
   D. Riwayat penyakit seseorang
3. Mengapa nama gadis ibu kandung sering dijadikan pertanyaan keamanan oleh bank dan harus dijaga kerahasiaannya?
   A. Karena digunakan sebagai verifikasi identitas untuk mereset password atau akses rekening.
   B. Karena nama ibu sulit diingat oleh orang lain.
   C. Karena merupakan tradisi lama yang tidak memiliki fungsi keamanan.
   D. Agar orang tua menjadi terkenal.
4. Tindakan penipuan online yang mencoba memancing korban untuk memberikan data pribadi seperti password atau nomor kartu kredit disebut...
   A. Hacking C. Browsing
   B. Phishing D. Spamming
5. Fitur apa pada media sosial yang memungkinkan kamu membatasi siapa saja yang bisa melihat foto dan statusmu?
   A. Tombol Like C. Notifikasi
   B. Pengaturan Privasi (Privacy Settings) D. Kolom Komentar
6. Apa risiko utama jika kamu membagikan foto tiket pesawat atau boarding pass secara lengkap di media sosial?
   A. Barcode/kode QR pada tiket dapat dipindai untuk mencuri data pribadi dan membatalkan penerbangan.
   B. Tidak ada risiko sama sekali.
   C. Orang lain jadi tahu kamu sedang liburan.
   D. Teman-teman akan merasa iri.
7. Manakah kombinasi password yang paling kuat untuk melindungi informasi privat?
   A. tanggal123 C. K4mB!ng_Gunun9$24
   B. passwordku D. namasayaadalahbudi
8. Apa yang dimaksud dengan 'Jejak Digital' (Digital Footprint)?
   A. Sejarah penemuan komputer.
   B. Rekam jejak aktivitas seseorang yang tertinggal saat menggunakan internet.
   C. Aplikasi untuk melacak lokasi lari pagi.
   D. Bekas jari pada layar sentuh smartphone.
9. Dalam konteks sekolah, manakah yang biasanya bukan merupakan informasi publik?
   A. Visi dan Misi sekolah
   B. Alamat dan nomor telepon kantor sekolah
   C. Daftar kegiatan ekstrakurikuler
   D. Nilai ulangan harian siswa secara spesifik dengan nama lengkap

10. Apa fungsi fitur Two-Factor Authentication (2FA) dalam melindungi informasi privat?
    A. Membuat password menjadi terlihat oleh publik.
    B. Menghapus semua data lama secara otomatis.
    C. Mempercepat koneksi internet saat login.
    D. Menambahkan lapisan keamanan kedua selain password, biasanya berupa kode OTP.
11. Mengapa kita sebaiknya tidak menyalakan fitur 'Lokasi' (GPS) secara terus-menerus pada setiap postingan media sosial?
    A. Orang lain tidak akan peduli.
    B. Dapat memberikan pola kebiasaan dan lokasi terkini kita kepada orang jahat.
    C. Sinyal internet akan terganggu.
    D. Akan membuat baterai HP cepat habis saja.
12. Apa yang dimaksud dengan 'Oversharing'?
    A. Membagikan tautan berita hoax.
    B. Terlalu banyak membagikan informasi pribadi secara detail di internet.
    C. Membagikan file berukuran besar.
    D. Berbagi koneksi internet dengan teman.
13. Manakah yang termasuk etika baik dalam menjaga privasi orang lain?
    A. Memposting foto teman yang sedang tidur tanpa izin.
    B. Menyebarkan nomor telepon guru ke grup publik.
    C. Meminta izin terlebih dahulu sebelum mengunggah foto atau video yang memuat wajah orang lain.
    D. Membaca pesan pribadi di HP teman yang tertinggal.
14. Ketika mendaftar aplikasi baru, kita sering diminta menyetujui 'Kebijakan Privasi' (Privacy Policy). Apa fungsinya?
    A. Hanya formalitas agar terlihat keren.
    B. Menjelaskan bagaimana data kita akan diambil, digunakan, dan dilindungi oleh pembuat aplikasi.
    C. Memberikan bonus poin kepada pengguna.
    D. Agar aplikasi tidak berbayar.
15. Apa yang dimaksud dengan enkripsi (encryption) pada aplikasi pesan instan (seperti WhatsApp)?
    A. Mengirim pesan tanpa kuota internet.
    B. Menghapus pesan secara otomatis setelah dibaca.
    C. Membuat pesan bisa dibaca oleh semua orang.
    D. Mengubah pesan menjadi kode acak sehingga hanya pengirim dan penerima yang bisa membacanya.
16. Jika kamu menggunakan komputer di warnet atau laboratorium sekolah, apa langkah terakhir yang WAJIB dilakukan sebelum pergi?
    A. Mematikan monitor.
    B. Menghapus icon aplikasi di desktop.
    C. Melakukan 'Log Out' atau 'Sign Out' dari semua akun yang dibuka.
    D. Langsung pergi begitu saja.
17. Manakah yang merupakan contoh data biometrik yang bersifat privat?
    A. Nama hewan peliharaan.
    B. Ukuran sepatu.
    C. Warna kesukaan.
    D. Sidik jari dan pemindaian wajah (Face ID).
18. Apa itu 'Pencurian Identitas' (Identity Theft)?
    A. Memiliki nama yang sama dengan orang lain.
    B. Mencuri dompet seseorang di jalan.
    C. Lupa nama sendiri.
    D. Menggunakan data pribadi orang lain (seperti nama, NIK, foto) untuk menyamar menjadi orang tersebut demi keuntungan.

19. Tanda gembok (padlock) di sebelah kiri alamat website (URL) pada browser menandakan bahwa...
    A. Website tersebut tidak bisa dibuka.
    B. Website tersebut milik pemerintah.
    C. Website tersebut berbayar.
    D. Koneksi ke website tersebut aman terenkripsi (HTTPS).
20. Sikap yang paling tepat sebelum membagikan (share) informasi yang kita terima dari grup chat adalah...
    A. Memeriksa kebenaran informasi (saring) dan mempertimbangkan privasi sebelum sharing.
    B. Membagikan hanya kepada orang yang kita tidak suka.
    C. Mengubah isinya agar lebih seru.
    D. Langsung bagikan agar menjadi yang pertama tahu.

II. Jawablah pertanyaan-pertanyaan di bawah dengan singkat dan jelas!

1. Jelaskan perbedaan mendasar antara informasi privat dan informasi publik!
2. Sebutkan minimal tiga (3) contoh data yang termasuk dalam kategori informasi privat (data pribadi) yang harus dilindungi!
3. Mengapa kita dilarang membagikan nama ibu kandung secara sembarangan di media sosial atau kepada orang yang tidak dikenal?
4. Jelaskan risiko atau bahaya yang mungkin terjadi jika seseorang melakukan oversharing (terlalu banyak berbagi) informasi privat, seperti lokasi terkini (live location) atau foto tiket pesawat di media sosial!
5. Berikan contoh situasi di mana sebuah informasi bisa berubah dari privat menjadi publik, dan jelaskan mengapa kita harus berhati-hati dalam situasi tersebut!