

## Ciri-Ciri Sumber Informasi Digital yang Kredibel

1. Informasi didukung oleh sumber data  
Informasi yang kredibel tidak muncul dari ruang hampa atau sekadar opini pribadi. Pernyataan di dalam situs web harus didukung oleh angka, statistik, atau hasil penelitian yang nyata.
2. Domain dan situs web yang resmi  
Alamat situs (*URL*) adalah identitas pertama yang harus diperiksa. Domain resmi biasanya dikelola oleh institusi yang memiliki akuntabilitas hukum dan akademik.

Jenis Domain	Keterangan	Tingkat Kepercayaan
.go.id	Situs resmi Pemerintah Indonesia	Sangat tinggi
ac.id / .edu	Institusi Pendidikan/Universitas	Sangat tinggi
.sch.id	Situs resmi Sekolah	Tinggi
.or.id / .org	Organisasi resmi (non-profit)	Tinggi
.com / .net	Komersial (perlu dicek reputasi mediana)	Sedang
.blogspot / .wordpress	Blog pribadi (gratisan)	Rendah (umumnya berupa opini)

3. Tanggal publikasi yang terbaru  
Dunia digital bergerak sangat cepat, terutama di bidang teknologi dan kesehatan. Informasi yang benar 5 tahun lalu mungkin sudah tidak relevan atau sudah dikoreksi hari ini.
4. Informasi bersifat netral dan objektif  
Situs yang kredibel bertujuan untuk **mengedukasi**, bukan menghasut atau memicu emosi pembaca.
  - **Ciri-ciri tidak kredibel:** Menggunakan judul bombastis (*clickbait*), banyak menggunakan tanda seru (!!!), atau kata-kata yang menyudutkan pihak tertentu secara subjektif.
  - **Ciri-ciri kredibel:** Menggunakan bahasa formal, memaparkan fakta dari dua sisi, dan tetap tenang dalam penyampaiannya.
5. Data penulis  
Siapa yang bicara menentukan kualitas pembicaraan. Situs yang bertanggung jawab akan mencantumkan nama penulis secara jelas, seringkali disertai dengan profil singkat atau latar belakang keahliannya.
6. Referensi sumber data  
Poin ini berkaitan dengan poin pertama. Penulis yang jujur akan menunjukkan dari mana mereka mendapatkan informasi tersebut melalui **tautan (link) sumber** atau daftar pustaka di akhir tulisan.  
Ini memudahkan pembaca untuk melakukan *cross-check* (verifikasi silang) ke sumber aslinya. Jika sebuah situs mengklaim sesuatu tanpa memberi tahu asalnya, itu adalah "lampu merah" bagi kebenaran informasi tersebut.

## Aktivitas 1 - Investigasi Informasi Digital

**Topik** : Kredibilitas Sumber Informasi Digital

**Media** : Microsoft Word dan Sumber Informasi Web

**Nama** :

**Kelas** :

**Tanggal** :

### Petunjuk kerja!

1. Buka aplikasi microsoft word
2. Buat tabel dengan kolom seperti di bawah ini!
3. Kunjungi aplikasi pencari data (google) dengan kata pencarian "Dampak nyata jejak digital (digital footprint) bagi masa depan karir."
4. Temukan 2 situs yang membahas topik tersebut dengan ketentuan:
  - a. Situs A : berasal dari domain yang memiliki kredibilitas baik (situs resmi)
  - b. Situs B : berasal dari domain yang memiliki kredibilitas kurang baik (blog / forum diskusi)
5. Analisis perbedaan dari kedua situs tersebut!

Tabel aktivitas kerja!

No	Kriteria Kredibilitas	Situs A	Situs B
1	Judul artikel & tautan URL		
2	Ekstensi domain		
3	Identitas penulis		
4	Tanggal penulisan		
5	Tampilan dan iklan		
6	Referensi		
7	Objektivitas		
8	Hasil analisis / kesimpulan		

## Risiko Menggunakan Sumber Informasi Digital yang Tidak Kredibel

Beberapa risiko menggunakan sumber informasi digital yang tidak kredibel:

### A. Penyebaran Informasi yang Salah (Hoaks)

Hoaks adalah informasi yang salah, menyesatkan, atau palsu yang sengaja disebarluaskan untuk tujuan antara lain, menciptakan konflik sosial, membuat orang panik dan resah, memicu perselisihan antar kelompok, atau merusak reputasi seseorang dengan opini yang menjatuhkan.

Ciri-ciri informasi hoaks:

1. Tidak ada sumber yang kredibel atau terpercaya yang mendukung informasi tersebut
2. Menggunakan kata-kata atau bahasa yang berlebihan dan emosional
3. Menggunakan judul yang menarik perhatian, tetapi tidak sesuai dengan isi berita
4. Hanya menyajikan sebagian informasi saja sehingga menimbulkan kesimpulan yang salah
5. Berita hoaks cenderung menyebar dengan sangat cepat melalui media sosial

Cara menghindari berita hoaks:

1. Pastikan kebenaran informasi dengan mencari sumber yang terpercaya sebelum menyebarkannya
2. Waspada judul yang sensasional
3. Perhatikan bahasa yang digunakan, apakah provokatif atau emosional
4. Percayakan informasi pada sumber terpercaya yang memiliki reputasi publik yang baik dan selalu mengutamakan akurasi
5. Cek berita menggunakan situs **cekfakta.com**, **turnbackhoax.id**, atau situs-situs pemerintah seperti **kominfo.go.id**

Dampak negatif dari informasi hoaks:

1. Kehilangan uang karena tertipu informasi yang salah
2. Nama baik seseorang atau lembaga dapat rusak akibat berita bohong
3. Dapat memicu perselisihan dan perpecahan di masyarakat
4. Berita bohong tentang bencana atau wabah dapat menyebabkan kepanikan dan kekacauan

### B. Kejahatan Siber

Kejahatan siber merupakan suatu tindakan kriminal yang memanfaatkan teknologi komputer dan jaringan internet. Contoh: peretasan, penipuan, penyebaran *malware* (virus komputer) yang bertujuan untuk merugikan masyarakat, individu, organisasi, bahkan lembaga negara.

Contoh kejahatan siber yang umum dilakukan:

1. Peretasan berupa penembusan sistem komputer secara ilegal untuk mencuri data sensitif, merusak sistem, atau mendapatkan akses tanpa izin.
2. Phising yaitu mengelabui pengguna internet untuk memberikan informasi pribadi, seperti kata sandi atau nomor kartu kredit dengan cara menyamar sebagai lembaga terpercaya atau meminta untuk mengunjungi link situs yang sudah disiapkan
3. *W malware* berupa penyebaran lunak berbahaya yang dapat merusak komputer, mencuri data, atau mengontrol komputer dari jarak jauh
4. Cyberbullying yaitu tindakan mengganggu, mengintimidasi atau melecehkan orang lain melalui dunia digital

Cara melindungi diri dari kejahatan siber:

1. Menggunakan kata sandi yang kuat (kombinasi huruf besar, huruf kecil, angka, dan simbol)
2. Menggunakan fitur MFA (*Multi-Factor Authentication* atau Autentikasi Multi-Faktor) adalah metode keamanan yang mengharuskan pengguna memberikan dua atau lebih bukti identitas (faktor verifikasi) untuk mengakses akun atau sistem, melampaui sekadar kata sandi.
3. Berhati-hati dengan tautan atau lampiran atau aplikasi yang mencurigakan
4. Melakukan pembaruan perangkat lunak secara teratur
5. Menggunakan perangkat lunak antivirus atau firewall untuk melindungi komputer

### C. Merusak Reputasi Pribadi

Menggunakan atau menyebarkan informasi yang salah bisa merusak reputasi seseorang. Menyebarkan informasi palsu (hoaks) merusak reputasi karena memanipulasi persepsi publik, menciptakan fitnah, dan mengubah opini negatif secara cepat. Hoaks bertindak sebagai pembunuhan karakter yang memicu ketidakpercayaan, merusak kredibilitas, memecah belah, serta seringkali menyebabkan dampak sosial, emosional, dan hukum serius bagi korban.

Berikut adalah alasan rinci mengapa informasi palsu merusak reputasi:

1. Manipulasi Persepsi dan Citra: Informasi palsu dirancang untuk merekam fakta agar publik melihat seseorang secara negatif, menodai citra, dan menurunkan kredibilitas yang telah dibangun.

2. Pembunuhan Karakter (Fitnah): Hoaks sering kali berupa fitnah atau tuduhan palsu yang keji, bertujuan langsung menghancurkan nama baik seseorang di mata publik.
3. Kecepatan Penyebaran di Media Sosial: Informasi palsu menyebar sangat cepat, membuat narasi negatif tertanam kuat di ingatan masyarakat sebelum klarifikasi dilakukan.
4. Memicu Opini Negatif dan Kebencian: Hoaks menysar emosi, memicu kemarahan, kepanikan, dan kebencian sosial yang berakibat pada pengucilan atau perundungan terhadap korban.
5. Dampak Jangka Panjang: Meskipun terbukti salah, jejak digital dari informasi palsu sering kali sulit dihilangkan sepenuhnya, menyebabkan kerugian reputasi yang permanen.

#### D. Risiko Keamanan Data

Berikut risiko yang mungkin terjadi jika menggunakan sumber informasi digital yang tidak kredibel:

1. Pencurian identitas seperti nama lengkap, alamat rumah, nomor telepon, bahkan kartu kredit atau email pribadi bisa disalahgunakan
2. Terkena *malware* dan virus seperti saat membuka link atau file yang dibagikan dari sumber yang tidak tepercaya
3. Sumber yang tidak kredibel seringkali digunakan sebagai sarana melakukan phishing yang diarahkan ke situs web palsu dan dirancang untuk mencuri informasi
4. Sumber yang tidak kredibel bisa menjadi alat untuk menjalankan berbagai jenis penipuan seperti penipuan investasi atau penipuan online lainnya
5. Informasi atau data yang dibagikan di platform yang tidak aman atau tidak kredibel berisiko mudah bocor dan jatuh ke pihak yang tidak bertanggung jawab.

## Aktivitas 2 - Analisa dan Investigasi Berita Hoaks

**Topik** : Risiko Menggunakan Sumber Informasi Digital yang tidak Kredibel

**Media** : Microsoft Word dan Sumber Informasi Web

**Nama** :

**Kelas** :

**Tanggal** :

### Petunjuk kerja!

1. Buka aplikasi microsoft word
2. Buat tabel dengan kolom seperti di bawah ini!
3. Kunjungi aplikasi pencari data (google) dengan topik sebagai berikut:

Nomor Absen	Topik
1, 7, 13, 19, dan 25	Investigasi bencana alam
2, 8, 14, 20, dan 26	Investigasi masalah wabah penyakit atau kesehatan remaja
3, 9, 15, 21, dan 27	Investigasi penipuan online
4, 10, 16, 22, dan 28	Investigasi konflik sosial
5, 11, 17, 23, dan 29	Investigasi isu penutupan atau aturan baru media sosial
6, 12, 18, dan 24	Investigasi merusak reputasi / citra dari seorang tokoh

4. Temukan 2 situs / berita online yang membahas topik tersebut dengan ketentuan:
  - c. Situs A : berita yang diragukan atau palsu tentang topik yang dibahas
  - d. Situs B : berita yang tepercaya dari topik yang sedang dibahas
5. Analisis dan investigasi perbedaan dari kedua situs tersebut!

### Tabel aktivitas kerja!

No	Komponen Analisis	Situs A	Situs B
1	Judul berita		
2	Tangkapan layar berita		
3	Nama penulis		
4	Domain situs	(Contoh: .go.id / .com)	(Contoh: .blogspot / anonim)
5	Gaya bahasa	(Objektif / Informatif)	(Menakut-nakuti / Huruf Kapital)
6	Tanggal publikasi	(Ada / Tidak) - sebutkan	(Ada / Tidak) - sebutkan
7	Sumber data	(Ada / Tidak) - sebutkan	(Ada / Tidak) - sebutkan
8	Risiko Jika Dipercaya	Apa bahaya yang timbul jika masyarakat lebih percaya pada Berita B daripada Berita A terkait isu yang dipilih	Apa bahaya yang timbul jika masyarakat lebih percaya pada Berita B daripada Berita A terkait isu yang dipilih
9	Dampak perasaan	Jika dipercaya, akan ....	Jika dipercaya, akan ....
10	Verifikasi (buka situs cekfakta.com, turnbackhoax.id, atau web resmi pemerintah	Hasil verifikasi ...	Hasil verifikasi ...
11	Kesimpulan		