

# Digital Safety

## “Aman, nyaman, dan kreatif di Internet”

**KEAMANAN & BENTUK KEJAHATAN DI DUNIA DIGITAL**

**Bhayu Rhama, ST., MBA., Ph.D**

**Literasi Digital Netizen Fair 2021**

**Rabu, 24 November 2021**



# BHAYU RHAMA, PH.D

## Pendidikan Terakhir:

S3 Kebijakan Pariwisata, University of Central Lancashire, United Kingdom

## Pekerjaan:

2020 – sekarang: Wakil Dekan Bidang Umum & Keuangan, FISIP Universitas Palangka Raya

2019 – sekarang: Staf Ahli Rektor Bidang Kebijakan Publik, Universitas Palangka Raya

2004 – sekarang: Komisaris PT. Barama Intercity Tour & Travel

2010 – sekarang: Dosen Kebijakan Pariwisata, FISIP Universitas Palangka Raya

## Organisasi:

2021 – 2026: Dewan Pengarah Generasi Digital Indonesia (GRADASI) DPC Kota Palangka Raya

2020 – 2025: Ketua DPC Komite Seni Budaya Nusantara (KSBN) Kota Palangka Raya

2020 – 2024: Penentu Kebijakan Badan Promosi Pariwisata Daerah Kota Palangka Raya

2018 – 2023: Ketua DPD Association of Indonesian Tours & Travel Agencies (ASITA) Kalimantan Tengah

2018 – 2023: Bidang Departemen Konferensi Indonesia Association of Public Administration

## Website:

[www.bhayurhama.com](http://www.bhayurhama.com)



# Digital Safety

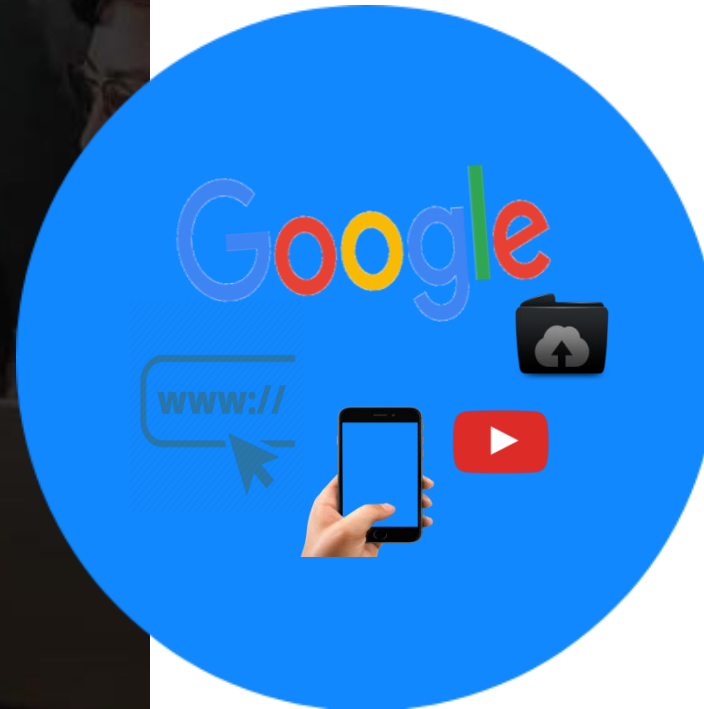
---



Pentingnya Menjaga Keamanan  
Agar Tetap Nyaman Dalam  
Menggunakan Internet



Bentuk-bentuk Kejahatan Yang  
Perlu Diwaspadai Di Dunia Digital

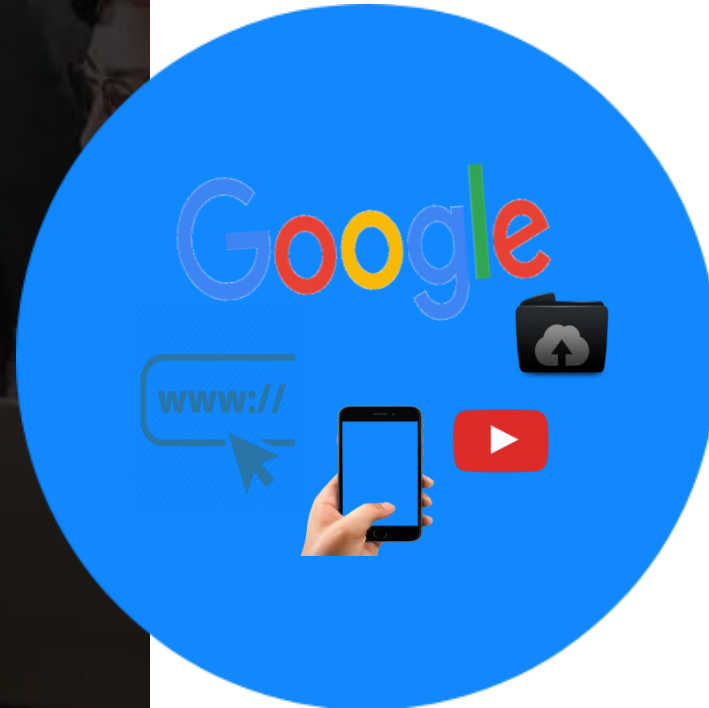


# Digital Safety

---



PENTINGNYA MENJAGA  
KEAMANAN AGAR TETAP  
NYAMAN DALAM  
MENGUNAKAN  
INTERNET

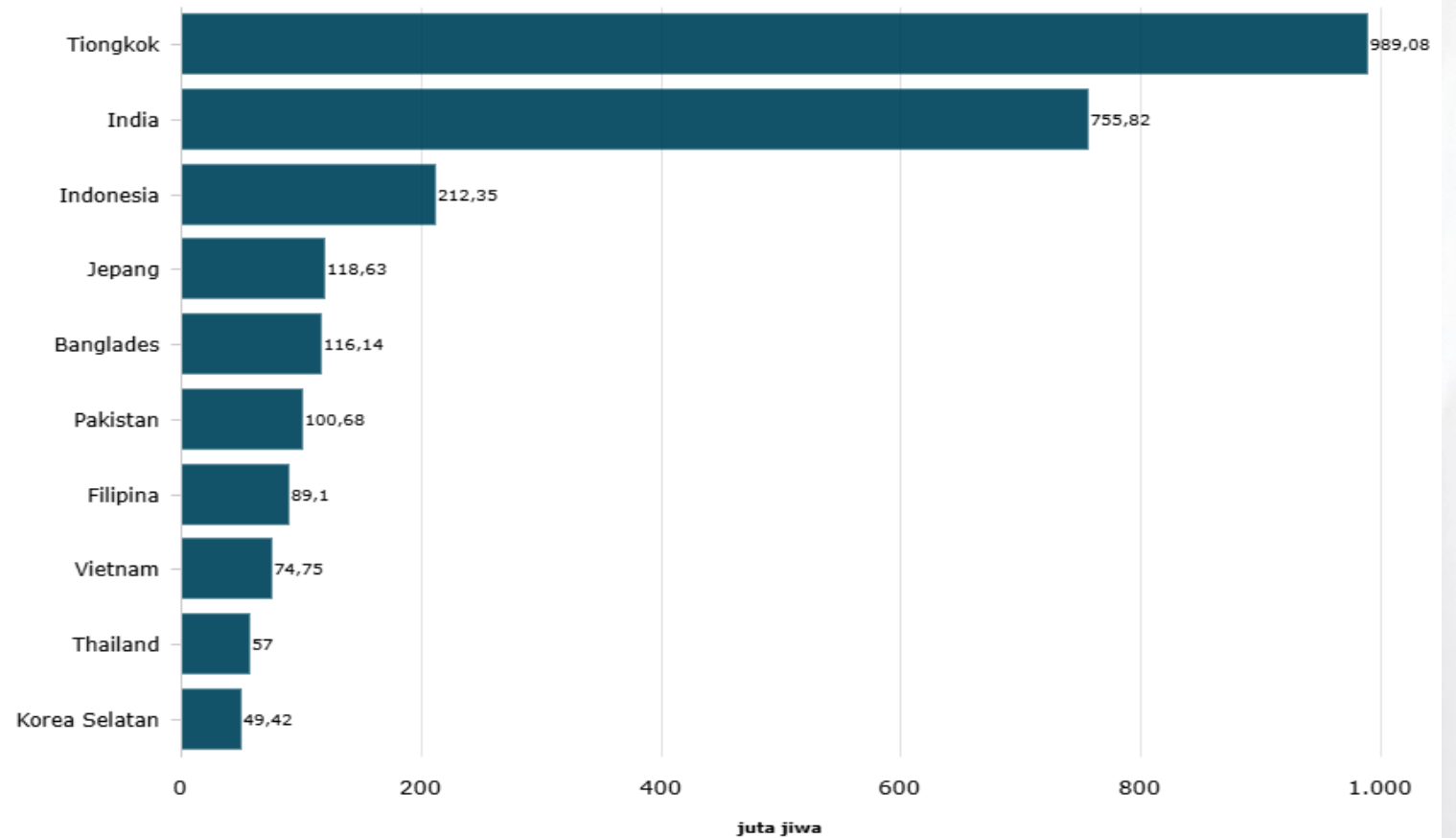




# Pengguna Internet Terbanyak di ASIA



10 Negara Asia dengan Jumlah Pengguna Internet Terbanyak (Mar 2021)





Menurut laporan We Are Social, jumlah pengguna internet di Indonesia pada Januari 2021, mencapai 202,6 juta pengguna atau sekitar 73,3 persen dari populasi. Secara tahunan, jumlah pengguna bertambah 15,5 persen atau sekitar 27 juta pengguna.

HootSuite melaporkan bahwa pengguna internet berusia 16 hingga 64 tahun diketahui memiliki beberapa perangkat elektronik berbeda, termasuk telepon genggam (baik smartphone maupun non-smartphone), laptop/PC, tablet, smartwatch, dan sebagainya.

Peningkatan tersebut perlu diimbangi pemahaman beraktivitas di ruang digital yang baik



# INTERNET



*Pemanfaatan internet pada masa ini, tidak terbatas pada pencarian informasi saja namun sudah meluas dalam bentuk pemanfaatan teknologi dalam kehidupan sehari-hari seperti penggunaan email, sosial media, toko online, transaksi perbankan, sampai dengan alat rumah tangga (Rini, 2015)*

*Tapi kemudahan yang diciptakan dari pemanfaatan internet tersebut datang dengan konsekuensi: KEAMANAN*

# DUA MATA PISAU INTERNET

## 1 Menimbulkan Permasalahan

Berurusan dengan hukum karena komentar dan status di jejaring sosial yang menyinggung perasaan atau melecehkan orang lain.

1

3

## 3 Manfaat Internet Sehat

Mampu memanfaatkan secara baik dan tepat guna serta dengan etika dan norma yang berlaku

## 2 Masyarakat Cerdas

Membangun budaya internet sehat dan aman. Hal itu dapat dilakukan jika masyarakat cukup cerdas.

2

4

## 4 Memberi Nilai Tambah

Kreatif dengan menciptakan karya baru yang berpotensi memberikan manfaat dan nilai tambah





Gawai kita adalah pintu ke dunia digital,  
Seperti di dunia nyata, kita tidak akan  
keluar pintu tanpa persiapan.



# Digital Safety

Digital Safety atau keamanan digital adalah sebuah proses untuk memastikan penggunaan layanan digital dapat dilakukan secara aman dan nyaman.  
(Sammons & Cross 2017)



- Diibaratkan juga sebagai bentuk pertahanan diri perangkat yang berhubungan dengan akses digital, baik perangkat lunak maupun keras karena akan selalu ada celah yang dapat dimanfaatkan pihak tidak bertanggung jawab.
- Internet menghubungkan secara luas, identitas digital pengguna internet bisa sama dengan identitas di dunia nyata, bisa juga tidak.
- Kita menjadi rentan berinteraksi dengan orang yang tidak kita kenal dengan tujuan yang tidak kita ketahui



# PENTINGNYA MENJAGA KEAMANAN AGAR TETAP NYAMAN DALAM MENGUNAKAN INTERNET ?

Menjaga dan mencegah penyalahgunaan akses data dalam system teknologi informasi dari seseorang yang tidak memiliki hak untuk mengakses maupun memanfaatkan data sistem sebagai berikut:

Ada 3 alasan kenapa keamanan data itu penting:

1. Mencegah potensi kerugian material
2. Mengurangi resiko penyalahgunaan informasi
3. Memperkecil peluang tindakan kriminal





## Privasi & Data yang perlu dijaga

1. **Kartu identitas**
2. **Kartu Elektronik/ Perbankan**
3. **Kode atau barcode**
4. **Atribut sekolah anak**
5. **Atribut keamanan tempat kerja**
6. **Permasalahan keluarga**
7. **Foto rumah dan isi rumah secara keseluruhan atau video yang memperlihatkan akses rumah dll.**



# Landasan Hukum Keamanan Digital

## Peraturan Menteri No. 20 Tahun 2018 tentang perlindungan data pribadi (PDP)

PERMEN ini dibuat dengan tujuan perlindungan data pribadi yang disimpan, dirawat, dan dijaga kerahasiaannya

## UU No.82 Tahun 2012 tentang Penyelenggaraan sistem & transaksi elektronik

Undang-undang ini dibuat guna sebagai landasan hukum terhadap transaksi digital maupun online di seluruh Indonesia. Undang-undang ini dapat dijadikan sebagai bahan acuan yang berkaitan dengan penggunaan alat bukti elektronik dalam sebuah perjanjian

## UU Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE)

Selain mengatur mengenai digital identity dan pelaksanaan transaksi elektronik maupun digital di Indonesia. Pada dasarnya UU ITE ini mengatur pula tentang perbuatannya dilarang di dalam transaksi elektronik maupun digital yang masuk keadaan cyber crimes, contohnya konten ilegal yang terdiri antara lain:

1. Kesusilaan, perjudian, penghinaan / pencemaran nama baik, pengancaman dan pemerasan (Pasal 27, 28 dan Pasal 29 UU ITE)
2. Akses ilegal (Pasal 30)
3. Intersepsi ilegal (Pasal 30)
4. Gangguan terhadap data (data interference, Pasal 32 UU ITE)
5. Gangguan terhadap sistem (system interferencem Pasal 33 UU ITE)
6. Penyalahgunaan alat dan perangkat (misuse of device, Pasal 34 UU ITE)

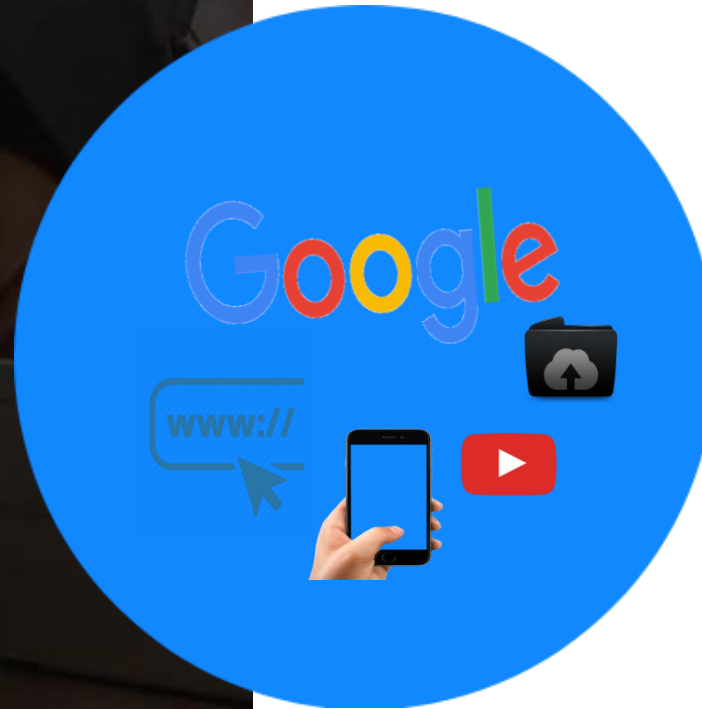
Keamanan Digital.

# Digital Safety

---



BENTUK-BENTUK  
KEJAHATAN YANG  
PERLU DIWASPADAI DI  
DUNIA DIGITAL



# Cyber Crime

- *Cyber Crime atau kejahatan dunia maya*
- *Cyber crime adalah tindakan ilegal yang dilakukan pelaku kejahatan dengan menggunakan teknologi komputer dan jaringan internet untuk menyerang sistem informasi korban*



# Cyber Crime



*Cyber crime* Indonesia diatur dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah menjadi UU Nomor 19 Tahun 2016. Jadi, belum ada UU *cyber crime* secara khusus.

*Cyber crime* termasuk dalam kategori perbuatan yang dilarang dalam UU ITE.

1. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain dengan cara apapun
2. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi elektronik dan/atau dokumen Elektronik
3. Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.





# Bentuk-bentuk Cyber Crime



**Social Engineering**

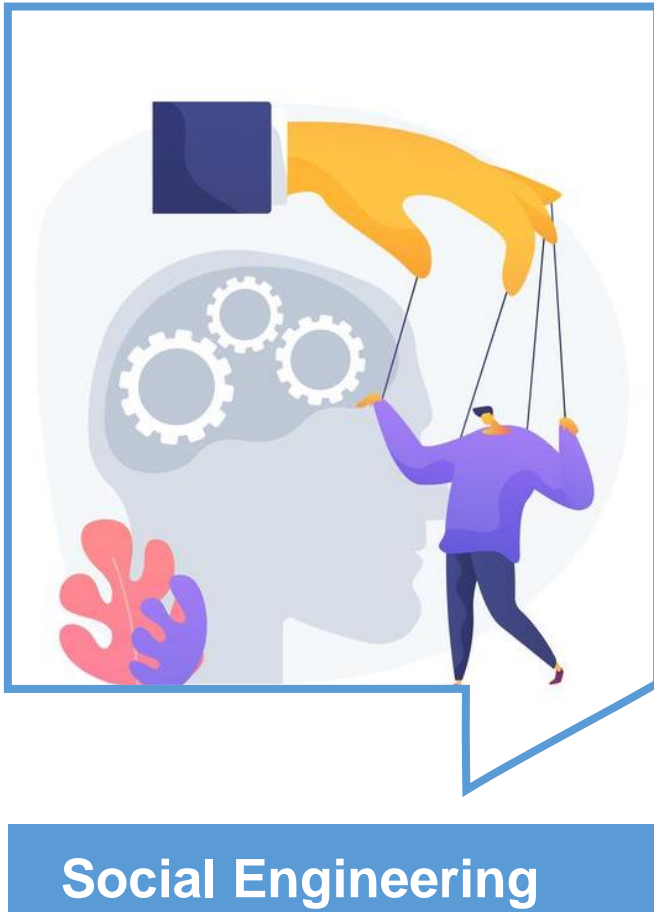


**Hacking**

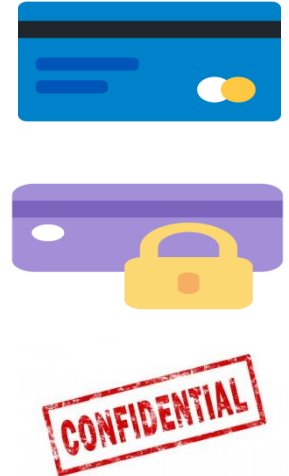


**Malware**

# Bentuk-bentuk Cyber Crime



*Social engineering* atau rekayasa sosial, adalah sebuah teknik manipulasi psikologis yang memanfaatkan kesalahan manusia agar secara sadar memberikan data seperti nomor kartu kredit, password dan informasi penting lainnya.



*Social engineering yang paling umum ialah:*

1. *PHISHING*
2. *SPOOFING*
3. *SCAM CALL*



*Biasanya hal ini dilakukan melalui email atau telepon dimana kriminal akan mengatasnamakan perusahaan atau lembaga tertentu supaya anda dengan kemauan sendiri memberikan informasi yang diminta*

# Bentuk-bentuk Cyber Crime



Hacking

*Hacking* adalah serangan digital dimana seseorang mengakses atau membajak akun atau file anda tanpa sepengetahuan anda untuk mencuri atau mengubah data atau aset tertentu.



# Bentuk-bentuk Cyber Crime



**Malware**

*Malware (Malicious Software) merupakan cyber attack yang bertujuan untuk mencuri data, uang atau merusak program atau device.*

*Malware memiliki beberapa jenis:*

- 1. SPYWARE: yang memungkinkan kriminal melakukan pengintaian terhadap data atau aktivitas online anda dan mencuri informasi penting seperti password, pin dan sebagainya.*
- 2. RANSOMWARE: Jenis malware yang bisa mengunci atau menyembunyikan file atau akun anda dan mengharuskan anda membayar online terlebih dahulu untuk dapat membukanya kembali*
- 3. ADWARE: Malware yang bersembunyi dalam device anda dan mengawasi aktivitas online anda dan terus memberikan spam atau advertisements yang sesuai*





## **Apa saja kerugian yang ditimbulkan dari Cyber Crime?**

### **1. Reputasi online bisa terancam**

Jika menggunakan aktivitas online untuk berbisnis. Jika menjadi korban, bisa jadi bisnis online anda akan kehilangan kepercayaan pelanggan

### **2. Kehilangan data penting**

Hal ini bisa terjadi baik pada akun pribadi maupun website yang menyimpan data pribadi pelanggan

### **3. Kerusakan software dan sistem komputer**

Hal ini sering terjadi pada sistem operasi yang rentan, baik yang sudah lawas maupun yang versi bajakan

### **4. Kehilangan sejumlah uang**

Tak hanya dialami oleh individu, maupun perusahaan, kehilangan sejumlah uang akibat tindak cyber crime juga dialami oleh negara.



# Aman Bermedia Digital

## 1. Pengamanan Perangkat Digital

Pemahaman tentang proteksi perangkat digital harus dimiliki oleh semua pengguna perangkat seperti telepon pintar, computer dan tablet karena terdapat resiko yang mungkin dapat terjadi jika tidak diproteksi dengan baik. Misalnyakebocoran data, *social engineering*, serangan *Cryptojacking*.

## 2. Pengamanan Identitas Digital

Hindari menggunakan identitas digital yang menampilkan informasi penting seperti nama ibu kandung dan tanggal lahir. Melindungi keamanan surat elektronik (email) dengan memperbaharui pasword secara rutin

## 3. Memahami Rekam Jejak

Dalam kondisi yang lebih terbuka pada dunia maya, identitas digital harus dikelola dengan baik agar dapat meninggalkan jejak digital yang baik pula.

## 4. Mewaspada Penipuan Digital

Perlu pemahaman dan peningkatan literasi digital dalam kerangka ketahanan keamanan digital dengan minimal kompetensi yang dimiliki : kemampuan analisis, kemampuan verifikasi dan kemampuan evaluasi.



# Tips Aman Menggunakan Internet



***6 Tips yang bisa dilakukan untuk menjadikan internet sebagai tempat yang aman (UNICEF Indonesia):***

- 1. Tunjukkan perilaku baik di dunia maya***
- 2. Periksa pengaturan akun dan kata sandi***
- 3. Jangan menyebarkan rumor***
- 4. Tidak sembarang menerima permintaan pertemanan***
- 5. Pikirkan dahulu sebelum mengirim sesuatu***
- 6. Verifikasi berita sebelum dibagikan***





# Tips Menjaga Keamanan Facebook dan Instagram



- **Jangan gunakan password yang sama**

Gunakan kata sandi dengan minimal 6 karakter yang sulit diterka oleh pihak eksternal. Masing2 akun online ideqalnya memiliki kata kunci sendiri yang berbeda dari password akun lain.



- **Hindari kata kunci yang umum atau menggunakan nama sendiri sebagai kata kunci.**

Agar password lebih kuat, kombinasikan karakter dengan huruf, angka, dan simbol. Paling [enting, jangan pernah membagikan password akun anda ke orang lain.



- **Hindari "Phising".**

Sebelum memasukkan informasi log in anda di mana pun, sebaiknya pastikan lebih dulu bahwa laman tersebut benar-benar yang resmi dan asli



Aman Bermedia Sosial







# Tips Menjaga Keamanan Facebook dan Instagram

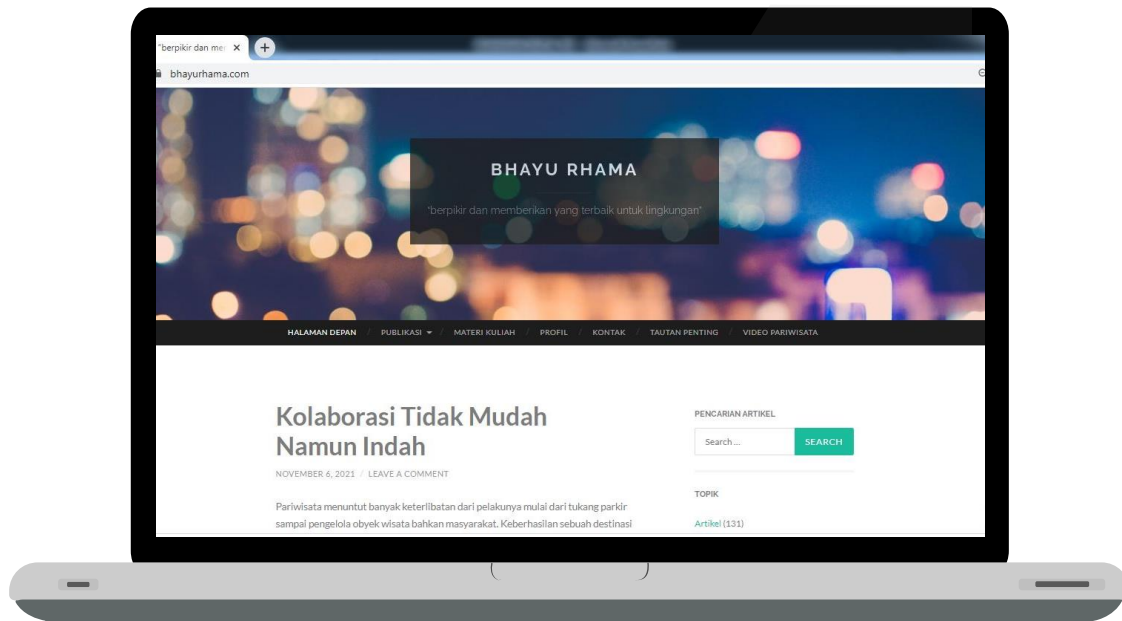


- **Jangan lupa log out jika menggunakan perangkat publik**  
Jangan lupa untuk keluar dari akun (log out) jika menggunakan perangkat umum atau bukan perangkat milik pribadi.
- **Jangan asal klik URL**  
Apabila menerima tautan, teliti lagi apakah tautan tersebut aman untuk dibuka atau tidak. Termasuk jika menemukan URL yang tidak jelas atau informasi clickbait di posting Facebook atau Instagram
- **Aktifkan peringatan log in mencurigakan**  
Untuk meningkatkan keamanan, pengguna bisa mengaktifkan notifikasi apabila ada log in mencurigakan.
- **Nyalakan verifikasi dua langkah.**  
Ini menjadi salah satu fitur keamanan yang ditekankan FB & IG untuk melindungi privasi.



Aman Bermedia Sosial





[www.bhayurhama.com](http://www.bhayurhama.com)

## Menjaga Konsistensi Menulis di Media

Tips paling dasar agar bisa konsisten menulis bahkan sampai bisa *bikin* buku ialah dengan cara terus melakukan praktik menulis, setiap hari atau setiap saat, apa pun kondisinya. Berusahalah untuk memiliki jadwal menulis yang *ajeg* (tetap) setiap harinya. Jangan lupa, iringi dengan memperbanyak referensi beragam bacaan, dan jangan sekali-kali melakukan tindakan plagiasi (menjiplak karya orang lain).

Kegiatan menulis ini adalah salah satu kegiatan positif dalam pemanfaatan media digital.

Sumber: <https://himmahonline.id/analisis/menulis-butuh-konsistensi/>



# THANK YOU

**Bhayu Rhama, ST., MBA., Ph.D**

[www.bhayurhama.com](http://www.bhayurhama.com)