



PROGRAM PENDIDIKAN
VOKASI

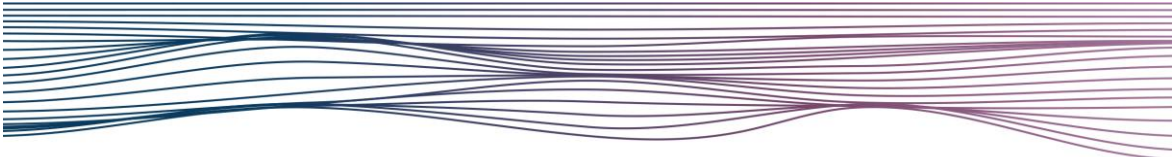


MODUL KEAMANAN DIGITAL

Penulis:

Devie Rahmawati,
Mila Viendyasari,
Rizky Ameliah,
Rangga Adi Negara,
Indriani Rahmawati,
Giri Lumakto





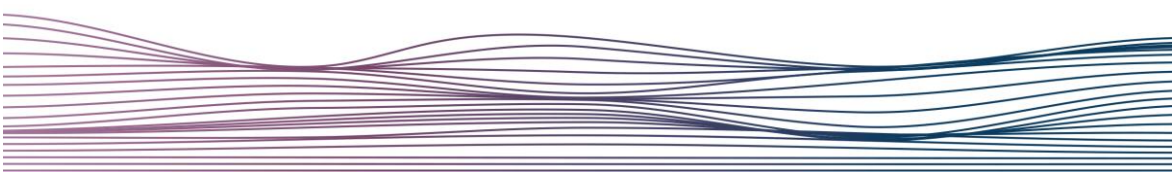
MODUL KEAMANAN DIGITAL

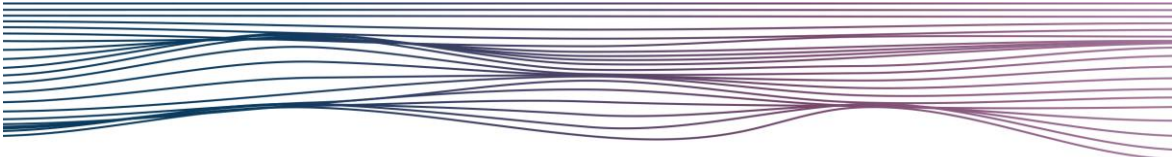
Penulis:

Devie Rahmawati,
Mila Viendyasari,
Rizky Ameliah,
Rangga Adi Negara,
Indriani Rahmawati,
Giri Lumakto

Penerbit:

Program Studi Hubungan Masyarakat
Program Vokasi Universitas Indonesia





Modul Keamanan Digital

Penulis:

Devie Rahmawati, Mila Viendyasari, Rizky Ameliah,
Rangga Adi Negara, Indriani Rahmawati,
Giri Lumakto

Editor :

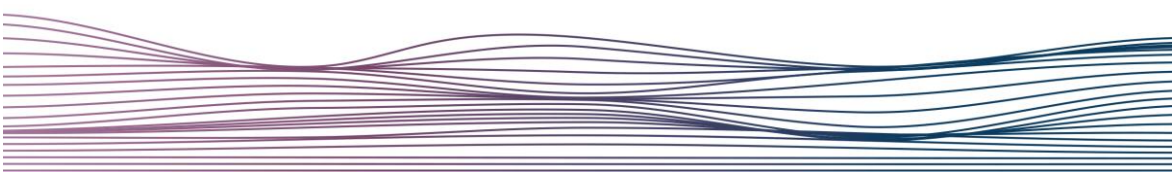
Rienzy K. R.

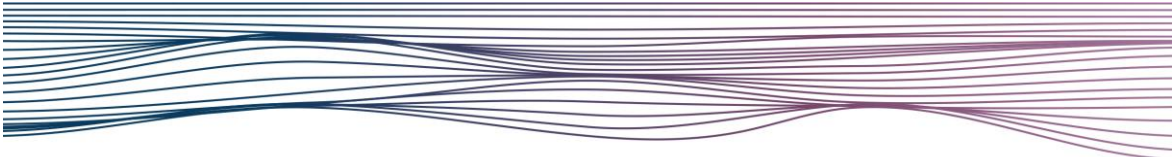
Desain:

Gina A. R.

Penerbit:

Program Studi Hubungan Masyarakat
Program Vokasi Universitas Indonesia
Jl. Akses Vokasi Ui, Kukusan, Kecamatan Beji, Kota Depok, Jawa Barat
Kampus Ui Depok Gedung A Depok





Modul Keamanan Digital

Penulis

Devie Rahmawati

Mila Viendyasari

Dedy Permadi

Rizky Ameliah

Rangga Adi Negara

Indriani Rahmawati

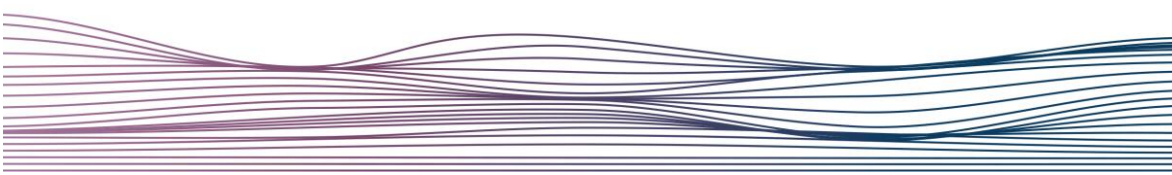
Giri Lumakto

Editor

Rienzy K. R.

Desain

Gina A. R.



Diterbitkan oleh:

Program Studi Hubungan Masyarakat Program Vokasi Universitas Indonesia, Jakarta 2021.

Dilarang mengutip atau memperbanyak sebagian atau seluruh isi buku ini dalam bentuk apa pun (seperti cetak, fotokopi, mikrofilm, CD-ROM, dan rekaman suara) tanpa izin tertulis dari penerbit.

Sanksi Pelanggaran Pasal 113

Undang-undang Nomor 28 Tahun 2014 tentang Hak Cipta

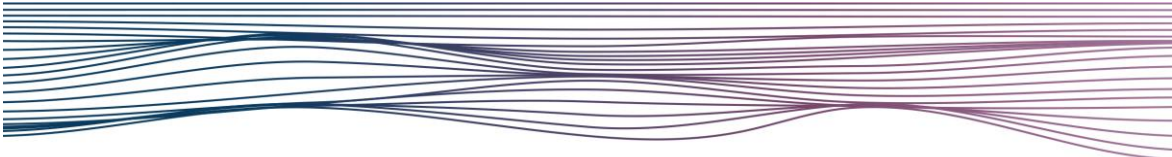
(1) Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000,00 (seratus juta rupiah).

2) Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/ atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).

(3) Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/ atau pidana denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

(4) Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/ atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

Isi di luar tanggung jawab Percetakan



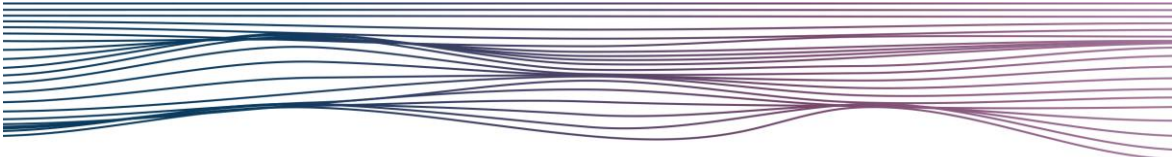
Daftar Isi	4
Media Sosial	19
Keamanan Akun	35
Masalah Data Pribadi	44
Tips Aman Bersosial Media	
Daftar Pustaka	56



PROGRAM PENDIDIKAN
VOKASI



MEDIA SOSIAL



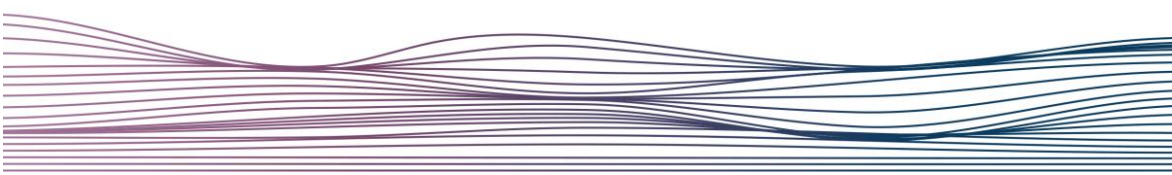
MEDIA SOSIAL

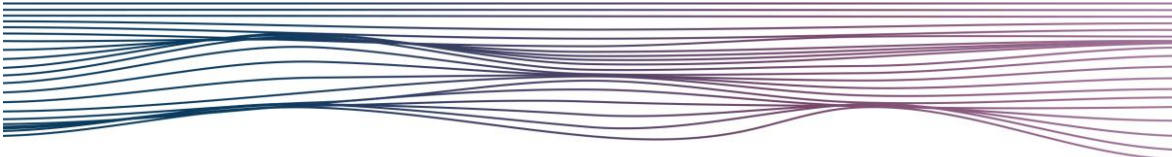
Teknologi berkembang begitu cepat dan telah mengubah cara kita hidup, bekerja, dan bersosialisasi dengan sesama. Teknologi dan sosial media adalah dua hal yang tidak terpisahkan. Sosial media bukan hanya sebagai tempat berkomunikasi, namun juga menjadi tempat berekspresi, tempat meluapkan perasaan bahkan pikiran. Perkembangan sosial media tidak bisa lepas dari perkembangan teknologi. Teknologi digital menghadirkan ruang komunikasi dan media informasi yang tidak lagi terbatas oleh jarak dan waktu. Di media sosial kita bisa bebas berpendapat dan berekspresi, namun perlu ditegaskan bahwa kebebasan tersebut bukanlah kebebasan mutlak tanpa batas dan etika.

Social media merupakan media yang paling ampuh untuk tetap terhubung dengan teman, keluarga, bahkan dunia, bukan hanya itu saja, media social merupakan wadah untuk up to date pada berita terbaru.

Kembali pada tahun 2005, ketika media sosial masih dalam masa pertumbuhan, hanya sekitar 5 persen pengguna di Amerika Serikat yang terlibat dalam media sosial. Pada 2019, jumlah itu tumbuh menjadi sekitar 70 persen (Frances Dalomba, LICSW, 2020)

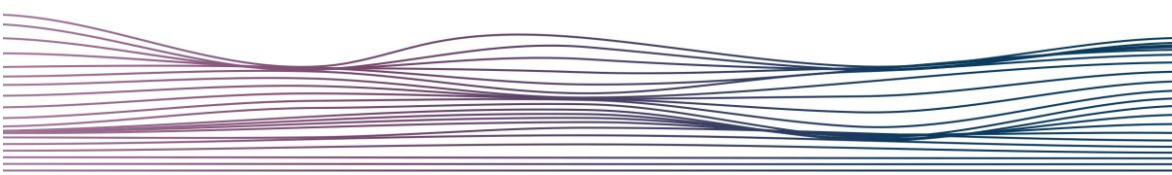
Pew Research Center mensurvei penggunaan dan popularitas media sosial di kalangan orang dewasa AS pada awal 2019. Survei tersebut menemukan bahwa platform sosial yang paling banyak digunakan untuk orang dewasa adalah YouTube dan Facebook; remaja lebih suka SnapChat dan Instagram, sementara TikTok dilaporkan merupakan jejaring sosial yang tumbuh paling cepat di antara pengguna yang lebih muda.





Penggunaan media sosial hampir universal di kalangan remaja saat ini. Pew Research Center melaporkan 97 persen anak berusia 13 hingga 17 tahun menggunakan setidaknya satu dari tujuh platform online utama.

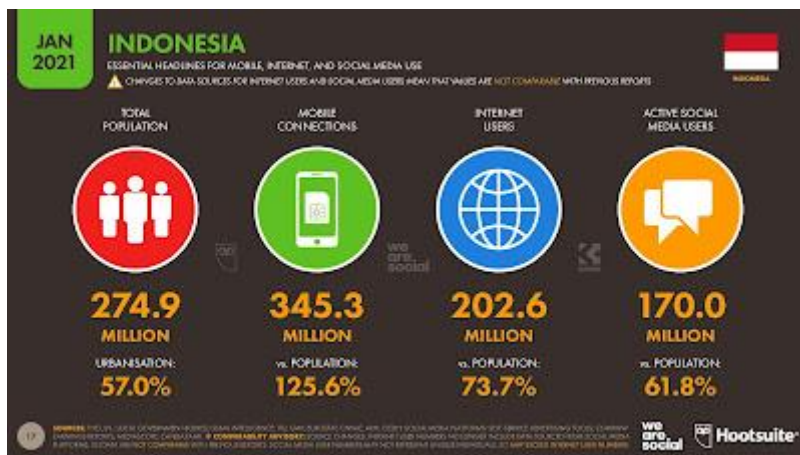
Jumlah waktu yang dihabiskan di situs sosial sangat mencengangkan. Satu laporan menunjukkan rata-rata remaja usia 13 hingga 18 menghabiskan sekitar sembilan jam di media sosial setiap hari; remaja usia 8 hingga 12 tahun aktif selama sekitar enam jam sehari.



PENGGUNA INTERNET DI INDONESIA

Penggunaan Internet di Indonesia pada tahun 2021 mencapai 202,6 juta, dimana jumlah seluler (*mobile*) yang terkoneksi sebanyak 345,3 juta dari 274,9 juta penduduk Indonesia.

Masyarakat Indonesia yang aktif di social media mencapai 170 juta orang (*We Are Social*, 2021).



Gambar 1.1 Penggunaan Internet Indonesia

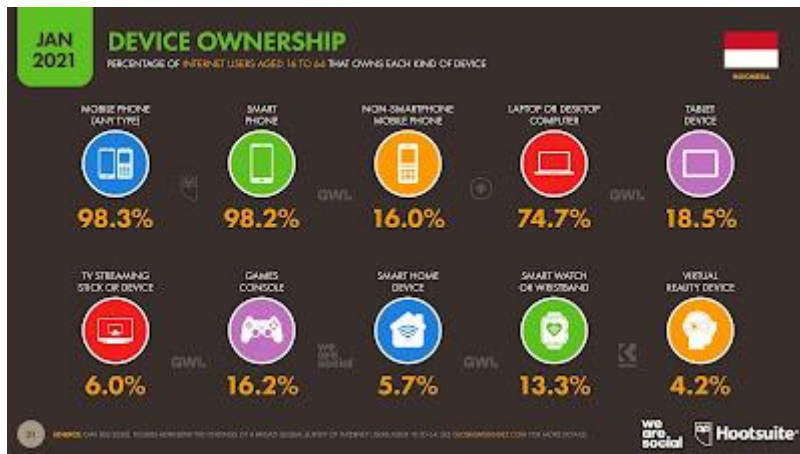
Pertumbuhan populasi (Januari 2021 vs Januari 2020): +1,1% (+2,9 juta), dimana terdapat pertumbuhan koneksi seluler (*mobile*): +1,2% (+4 juta), penambahan pengguna

internet: +15,5% (27 juta), dan penambahan pengguna media sosial aktif: +6,3% (10 juta) (*We Are Social*, 2021).



Gambar 1.2 Pertumbuhan Penggunaan Digital Indonesia

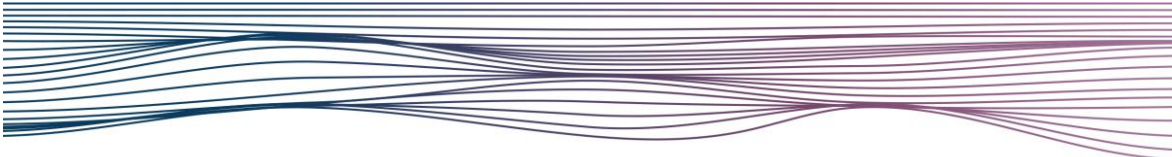
Jumlah penggunaan *smartphone* di era digital juga semakin meningkat. Menurut data *we are social*, 2021 menyebutkan bahwa jumlah telepon seluler (jenis apa pun): 98,3%, *Smartphone*: 98,2%, telepon seluler bukan *smartphone*: 16%, komputer *laptop* atau *desktop*: 74,7%, perangkat tablet: 18,5%, perangkat TV *streaming*: 6%, Game: 16,2%, perangkat *smart home*: 5,7%, perangkat *smart watch* atau *wristband*: 13,3%, dan perangkat *virtual reality*: 4,2%.



Gambar 1.3 Kepemilikan *Device*

Waktu rata-rata harian pengguna internet:

- Menggunakan internet (dari perangkat apa pun): 8 jam 52 menit
- Menonton siaran TV maupun *streaming* TV: 2 jam 50 menit
- Menggunakan media sosial: 3 jam 14 menit
- Membaca berita *online* dan koran: 1 jam 38 menit
- Mendengarkan layanan *music streaming*: 1 jam 30 menit
- Mendengarkan siaran radio: 33 menit
- Mendengarkan layanan *podcasts*: 44 menit
- Bermain *video games* menggunakan konsol *games*: 1 jam 16 menit



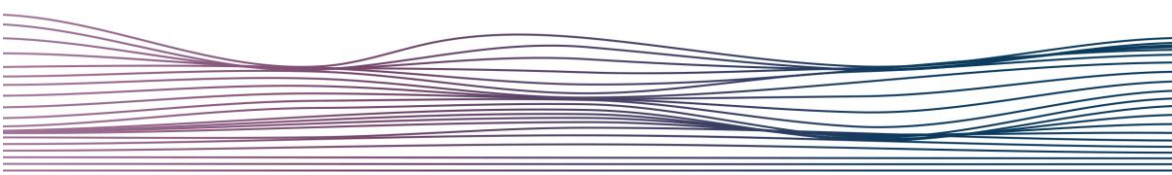
PRO KONTRA SOSIAL MEDIA

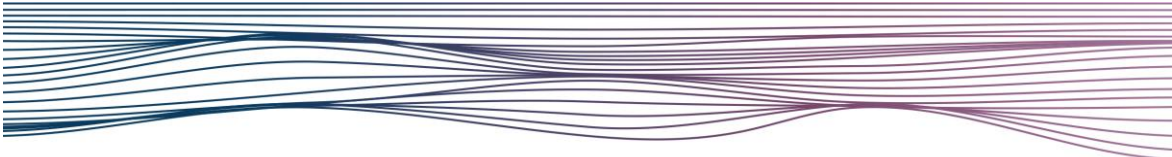
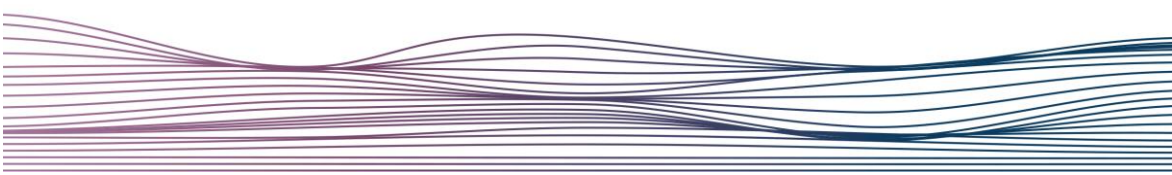
(Frances Dalomba, LICSW, 2020)

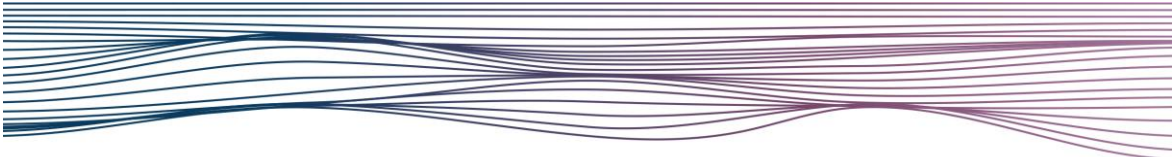
Sisi Positif Sosial Media

- Media sosial menawarkan kenyamanan
- Media sosial mampu menghubungkan semua orang dalam skala besar, mampu menghubungkan dengan keluarga, teman, bahkan seluruh pengguna internet
- Sosial media sebagai wadah pencari informasi dan mampu memberikan akses cepat ke informasi dan penelitian
- Youtube sebagai media pembelajaran online, menambah keterampilan kerja, tutorial dan lain-lain
- Media di bidang sosial(penggalangan dana, bantuan bencana dll)
- Media penghubung antara pencari kerja dan perusahaan
- Media transaksi
- Media marketing

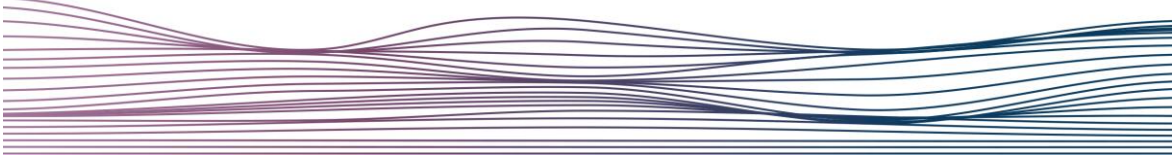
Sisi Negatif Sosial Media

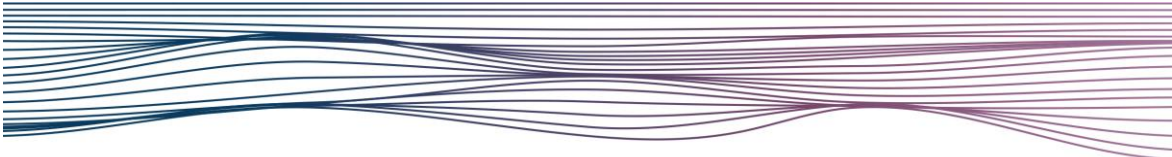
- Online vs Realitas. Media sosial itu sendiri tidak masalah. Ini adalah cara orang menggunakannya sebagai pengganti komunikasi aktual dan sosialisasi langsung. “Teman” di media sosial mungkin sebenarnya bukan teman, dan bahkan mungkin orang asing.
- 

- 
- Peningkatan penggunaan. Semakin banyak waktu yang dihabiskan di media sosial dapat menyebabkan cyberbullying, kecemasan sosial, depresi, dan paparan konten yang tidak sesuai usia.
 - Media Sosial membuat ketagihan. Saat Kamu bermain game atau menyelesaikan tugas, Kamu berusaha melakukannya sebaik mungkin. Setelah Kamu berhasil, otak Kamu akan memberi Kamu dosis dopamin dan hormon kebahagiaan lainnya, membuat Kamu bahagia. Mekanisme yang sama berfungsi saat Kamu memposting gambar ke Instagram atau Facebook. Setelah Kamu melihat semua notifikasi yang “like” suka dan komentar positif muncul di layar Kamu, Kamu secara tidak sadar akan menjadikannya sebagai hadiah. Tapi bukan itu saja, media sosial penuh dengan pengalaman yang mengubah suasana hati.
 - Takut Ketinggalan. FOMO telah menjadi tema umum, dan sering mengarah pada kegiatan “cek dan cek” media sosial. Gagasan bahwa Kamu mungkin kehilangan sesuatu jika Kamu tidak online dapat memengaruhi kesehatan mental Kamu.
 - Masalah citra diri. Situs media sosial menyediakan alat yang memungkinkan orang untuk mendapatkan persetujuan orang lain atas penampilan mereka dan kemungkinan untuk membandingkan diri mereka dengan orang lain. Ini dapat dikaitkan dengan masalah citra tubuh.
- 



"Selfieholics" dan orang-orang yang menghabiskan sebagian besar waktu mereka memposting.



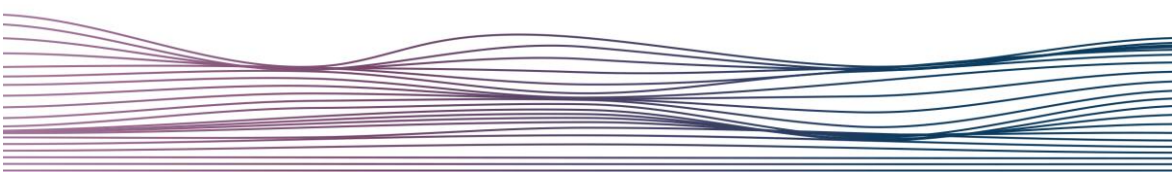


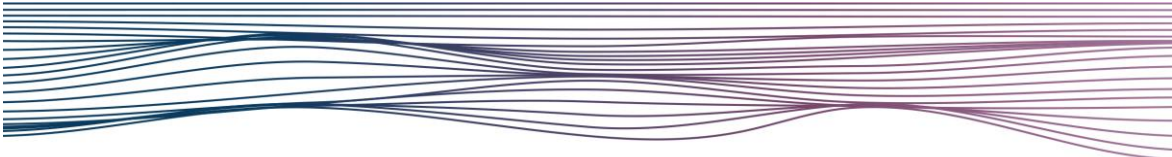
Sosial Media dan Bully

Di balik perkembangan teknologi, sayangnya ada sisi buruk yang ditawarkan teknologi, misalnya kasus bully. Kasus bully di sosial media seringkali disebut cyberbullying. Cyberbullying mampu menyebabkan trauma yang mendalam baik secara fisik maupun psikis. Korban bully sering mengalami ketakutan dan yang paling parah sering kali menjadikan hal-hal bully sebagai suatu hal yang “wajar”, jadi jika mereka tidak mengalami bully, maka mereka menjadi aneh (Frances Dalomba, LICSW, 2020)

Tahukah kamu?

- Setiap 7 menit, anak Amerika mengalami tindakan cyberbullying. Sayangnya tindakan tersebut jarang mendapatkan intervensi bantuan dari orang dewasa. Hanya 4 % kasus bully yang diselesaikan oleh orang dewasa, 11 % diselesaikan bersama teman sebaya dan 85% kasus bully tidak ditangani.
- Satu dari empat remaja di Amerika Serikat (25 %) menjadi korban bully, dan 43% mengalami bully saat online.
- Kasus bully di sosial media sangat maraj, namun 58% korban bully justru tidak memberi tahu orang tua atau bahkan ke teman dekatnya.

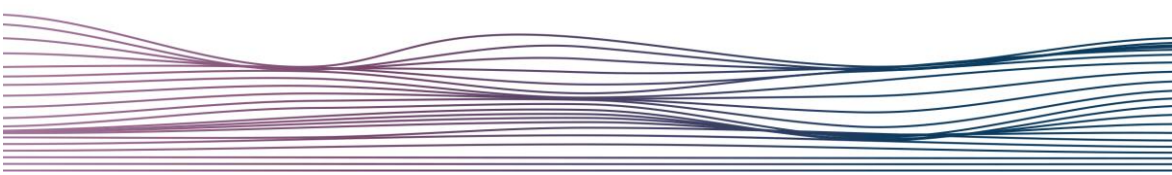




Sosial Media dan Kasus Bunuh Diri

FOMO “*Fear of Missing Out*” fenomena tidak mau ketinggalan dan haus mengikuti trend sosial media. Salah satu dampak FOMO yaitu meningkatnya kasus bunuh diri (Frances Dalomba, LICSW, 2020). Menurut American Foundation for Suicide Prevention, bunuh diri menjadi salah satu penyebab utama kematian anak-anak di bawah usia 14 tahun. Mayoritas mereka meninggal akibat gantung diri.

Tingkat bunuh diri di antara anak berusia 10 hingga 14 tahun telah tumbuh lebih dari 50 persen selama tiga dekade terakhir, menurut American Association of Suicidology. Menurut American Foundation for Suicide Prevention tingkat bunuh diri di antara anak-anak antara usia 10 dan 14 tahun sangat rendah, tetapi merangkak naik.





PROGRAM PENYUJUKAN
VOKASI



KEAMANAN AKUN

PASSWORD

Password itu diibaratkan sebagai kunci media sosial kita, sebagai perlindungan pertama. Layaknya sebuah rumah yang memiliki kunci untuk melindungi isi rumah, sosial media juga harus dilindungi, agar tidak semua orang bisa masuk dan mengatur konten kita. Urusan password bukan urusan yang enteng, walaupun kenyataannya banyak yang masih menganggap remeh, bahkan untuk anak remaja yang sedang dimabuk cinta, atas nama kepercayaan, mereka rela saling menukar password mereka. Tidak ada yang salah, asal dilakukan dalam kondisi sadar, namun tidak bisa dipungkiri bahwa semua orang berpotensi menghancurkan kita, jadi jangan mudah percaya.

Be Social, Be Secure

Masalah password:

1. Mudah memberikan password ke orang lain

Password itu ibarat celana dalam, dimana untuk menjaga kebersihan, kita tidak elok bergantian celana dalam dengan orang lain. Mengapa kita tidak dianjurkan membagi password kita ke orang lain, karena kita tidak bisa menjamin apakah orang tersebut bisa dipercaya atau justru dia yang akan membagikan rahasia kita. Informasi pribadi harus kita sendiri yang akses, jangan memberikan kesempatan orang lain untuk mengakses sosial media kita, jangan sampai akun kita jatuh pada tangan yang salah.

2. Membuat password yang mudah diingat dan umum

Passwordnya yang umum cenderung digunakan oleh banyak orang. Hasil riset yang dilakukan oleh National Cyber Security Centre, Inggris mengurutkan penggunaan password terbanyak di dunia, hasilnya:

- Password 12345 digunakan oleh 23,3 juta di dunia
- Password 123456789 digunakan oleh 3,8 juta di Dunia

- Password dengan kata “password” digunakan sebanyak 3,6 juta di dunia

Ketiga password tersebut merupakan password yang sering dipakai di dunia, bukan hanya di Indonesia. Password umum akan mudah juga dihack/dijebol/diretas. Ibarat gembok, para maling selalu memiliki seribu cara untuk membobol gembok. Sama halnya dengan maling, jika kita tidak memperhatikan keamanan dan kekuatan password kita, maka akun kita bisa dengan mudah dihack/dibobol/diretas oleh para penjahat digital.

AUTENTIKASI DUA FAKTOR/LANGKAH

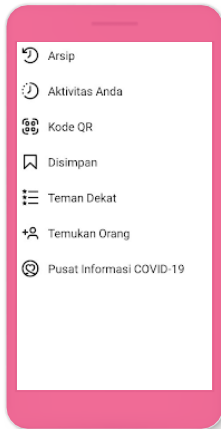
Password saja ternyata tidak cukup kuat untuk melindungi sosial media kita. Perlindungan ekstra/tambahan bisa menggunakan autentikasi dua faktor. Autentifikasi dua faktor ibarat kita memiliki kunci gembok gkamu, gembok yang pertama menggunakan kunci, gembok yang kedua menggunakan *finger print* dan sensor muka. Sehingga bisa dipastikan yang bisa masuk ke dalam hanya sang pemilik.

Cara mengaktifkan autentikasi dua faktor:

Facebook



Instagram



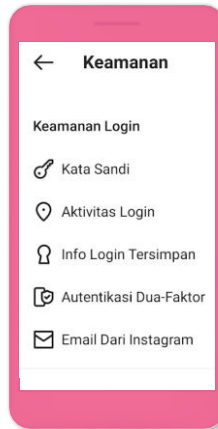
Masuk ke Profil dan klik

Setting/Pengaturan



Pilih 2 metode ini:

- Kode SMS dari handphone kita
- Kode login dan



Klik keamanan dan masuk ke

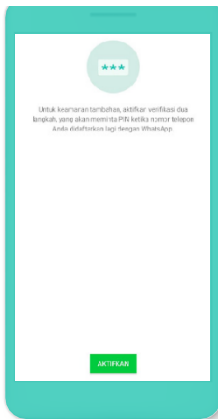


Setelah autentifikasi dua factor diaktifkan, kita harus memasukkan kode yang dikirim Instagram kalau kita

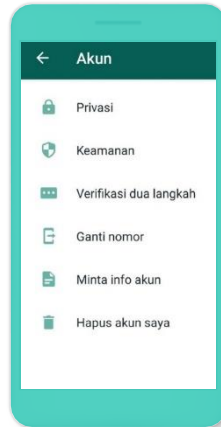
Whatsapp



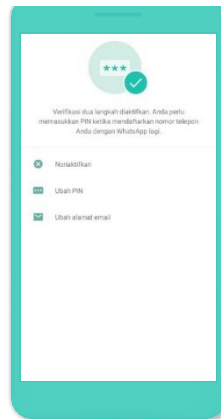
Masuk ke profil dan klik



Aktifkan verifikasi dua langkah dengan memasukkan kode



Klik akun dan pilih verifikasi dua langkah

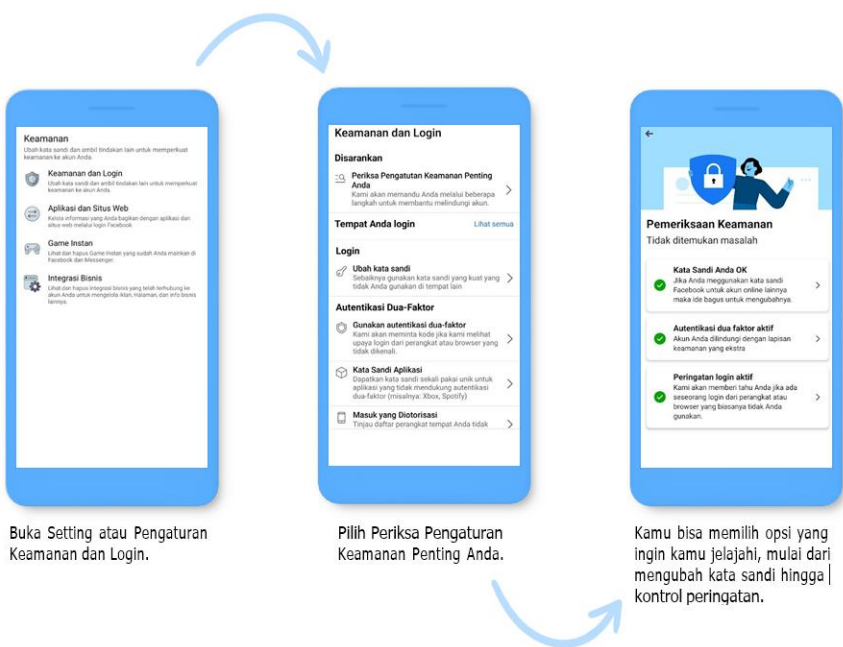


Setelah verifikasi dua langkah diaktifkan, kita harus memasukkan kode PIN yang kita buat



Cek Keamanan Facebookmu!

Langkah-langkah memastikan apakah akun Facebook kita sudah aman atau masih butuh keamanan tambahan



Buka Setting atau Pengaturan Keamanan dan Login.

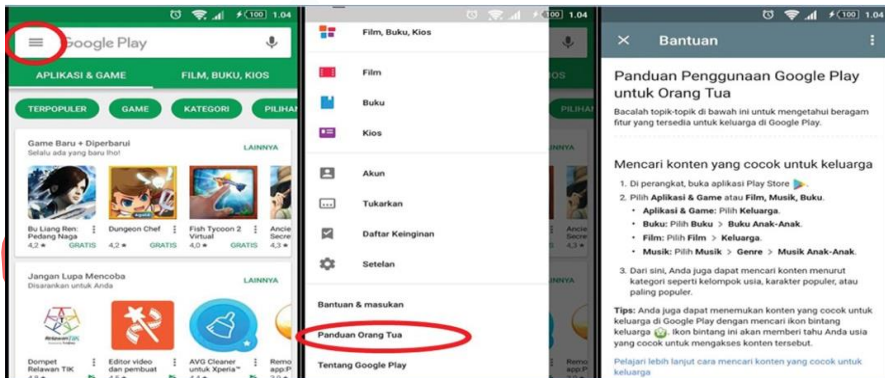
Pilih Periksa Pengaturan Keamanan Penting Anda.

Kamu bisa memilih opsi yang ingin kamu jelajahi, mulai dari mengubah kata sandi hingga kontrol peringatan.

Perlindungan pada Anak

Panduan google play bagi Orang Tua

Google Play menyediakan fitur Panduan Orang Tua pada aplikasinya. Oleh karena itu, setiap orang tua yang memberikan anaknya gawai atau akses terhadap gawai yang menggunakan sistem operasi Android wajib untuk membaca panduan ini terlebih dahulu sebelum menyerahkannya pada anak.



Panduan Cara:

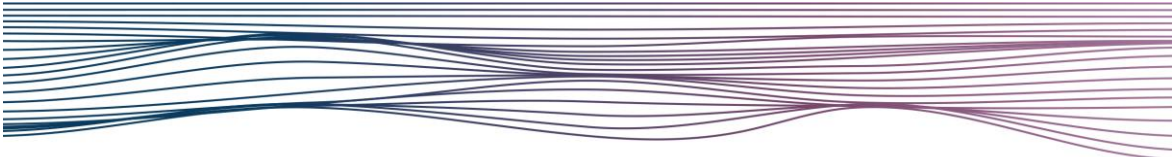
1. Buka Aplikasi Google Play pada gawai
2. Tap bagian menu di bagian kiri atas
3. Pilih menu panduan orang tua



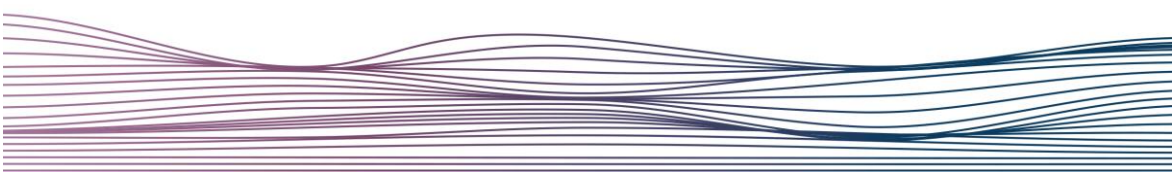
PROGRAM PENDIDIKAN
VOKASI



MASALAH DATA PRIBADI



Rekap masalah pribadi yang terjadi di Indonesia

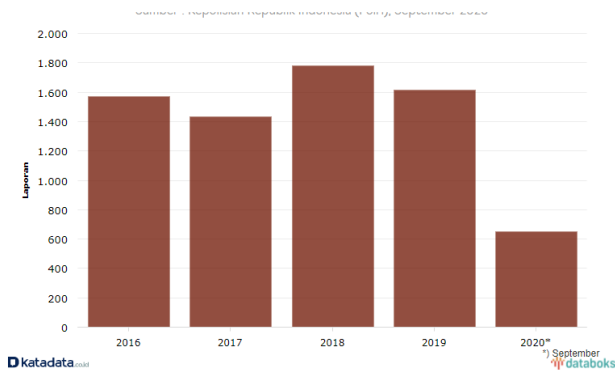
- Direktorat Tindak Pidana Siber Bareskrim Polri mencatat pada periode Januari hingga November 2020 terjadi sebanyak 4.250 laporan kejahatan siber.
 - Dari ribuan kasus, 1.158 kasus di antaranya merupakan kasus penipuan dan 267 kasus akses ilegal.
 - Sementara dari tahun ke tahun jumlah tindak pidana siber juga mengalami peningkatan (CNN, 2020).
 - Tim *Threat Protection Intelligence* Microsoft memperingatkan bahwa penjahat dunia maya mengambil keuntungan dari pandemi COVID-19 dengan mengadaptasi dan memperbarui metode serangan
 - Temuan ini berasal dari analisis dari beragam sumber data Microsoft, termasuk 8 triliun sinyal ancaman yang diterima dan dianalisis oleh Microsoft setiap hari, mencakup periode 12 bulan, dari Januari hingga Desember 2019.
- 

Jumlah Laporan Penipuan Daring Per Tahun

Sumber : Kepolisian Republik Indonesia, September 2020

Pada data lima tahun terakhir, Kepolisian Republik Indonesia menyebutkan sejak 2016 sampai dengan September 2020 ribuan kasus penipuan daring telah dilaporkan.

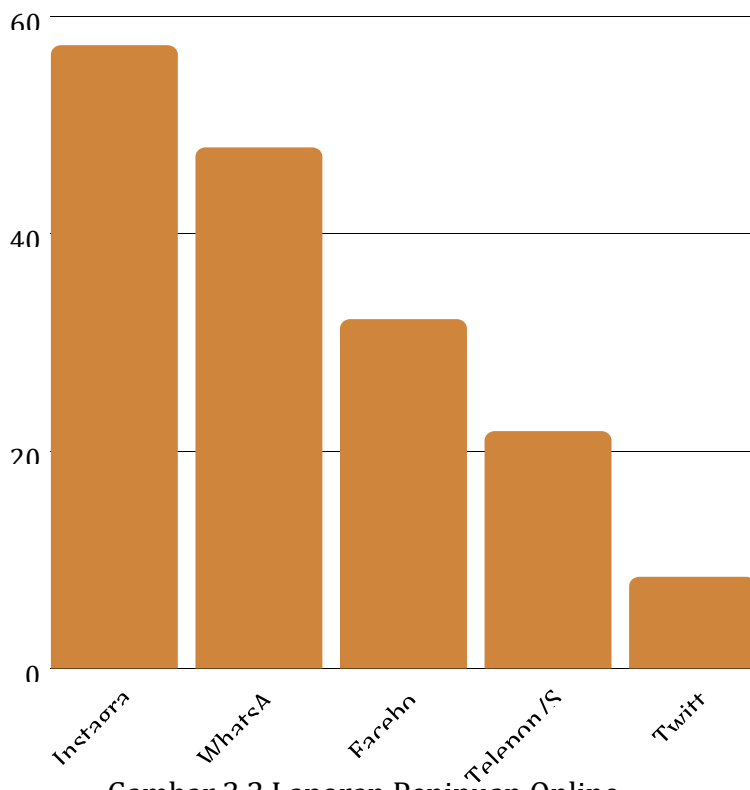
Pada 2016 terjadi laporan kasus penipuan daring sebanyak 1.570 kasus; tahun 2018 sebanyak 1.430; tahun 2019 sebanyak 1.781; dan tahun 2019 sebanyak 1.617 kasus; dan sampai dengan September 2020 telah ada 649 kasus yang dilaporkan. Seluruh kasus dalam 5 tahun terakhir berkisar 7.047 kasus.



Gambar 3.1 Jumlah Laporan Kasus Penipuan Daring

Laporan penipuan Online Januari 2019-2020

1.617 laporan



Gambar 3.2 Laporan Penipuan Online

Instagram: 573

WhatsApp: 479

Facebook: 321

Telepon/SMS: 218

Twitter: 84

JENIS-JENIS MASALAH DATA PRIBADI

1. SCAM

Strateginya dengan memanfaatkan empati dan kelengahan pengguna. Metodenya beragam, bisa menggunakan telepon, SMS, WhatsApp, email, maupun surat berantai.

Yuk cek ciri-ciri Scam yang beredar di sekitar kita

01

Kerabat sakit dan segera membutuhkan

02

Mengirimkan bahan kepada korban dan beralasan tertahan di imigrasi dan meminta

03

Keluarga dari pelaku tiba-tiba hilang dan pelaku

04

Para korban biasanya dimintakan sejumlah uang

05

Perbaikan kendaraan dan sedang berada di

Gangguan Spam di Indonesia (2019)

Sumber: Modul Aman dalam Bermedia Digital

Telepon 28 kali rata-rata
telpon perbulan nomor 3
dunia

SMS 46 kali rata-rata SMS
perbulan, nomor 10 dunia

Scam berbentuk Website

Scam bisa juga berbentuk website. Para pelaku Scam membuat website yang semirip mungkin dengan website asli, hingga masyarakat tidak menyadari bahwa yang diklik merupakan website palsu.

Ciri-ciri Scam Website:

- Memiliki nama dan domain website yang mirip dengan yang asli. Contoh:

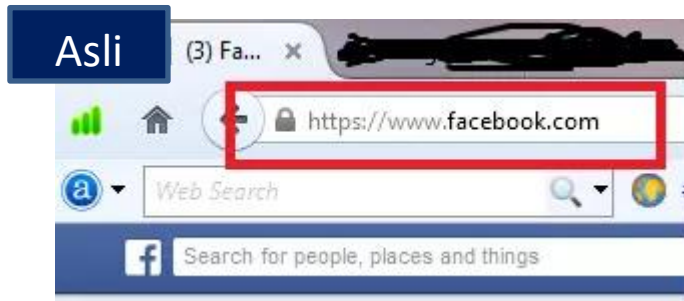
Asli

KlikBCA

Pals

KlickBCA

- Tampilan 100% sama



2. SPAM

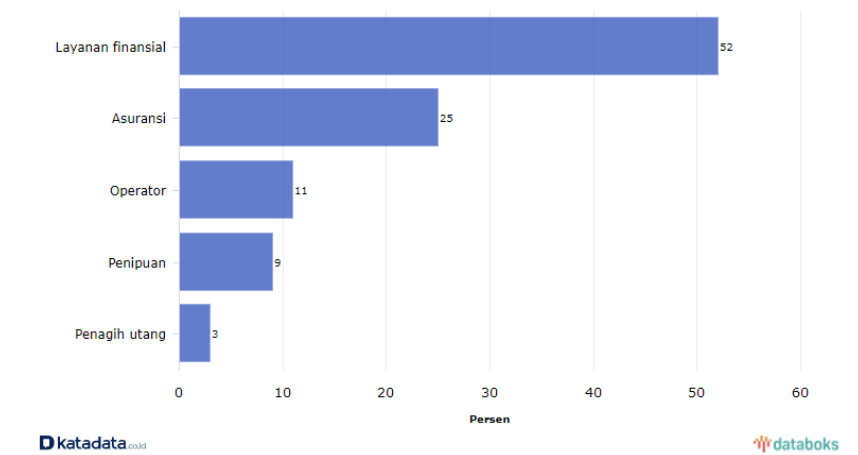
Spam merupakan perilaku yang dilakukan secara **terus-menerus dan berulang**.

Tahapan spam dimulai dengan mengganggu para korban dan berlanjut menjadi penipuan dan pencurian data

(Alazab dan Broadhurst, 2015).

Jenis-jenis pesan spam sebagai berikut:

Berdasarkan survey yang dilakukan oleh Katadata, **52% spam berbentuk sebagai layanan finansial, disusul oleh asuransi sebesar 25%.**



Gambar 3.3 Kasus-kasus Spam

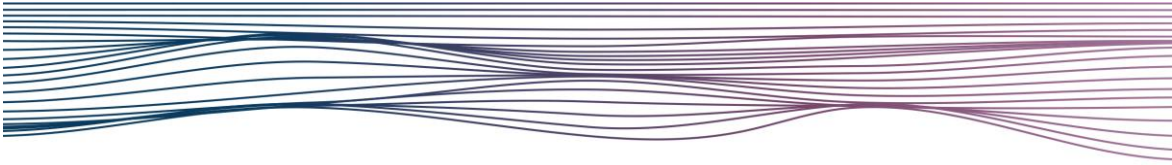
Kasus Spam yang sempat menghebohkan

Pada tahun 2016, pelanggan selular di Indonesia dihebohkan dengan adanya panggilan tak terjawab (missed call) dari nomor prefix +77 yang berasal dari Rusia.

Dilansir dari Techwelkin, modus seperti ini sudah terjadi sejak tahun 2000 dan biasanya dilakukan oleh perusahaan telepon dari negara-negara Afrika dan Rusia. Para pelaku biasanya menggunakan international premium rate number (IPRN) dan bekerjasama dengan perusahaan telpon tersebut.

Para pelaku akan mendapat komisi dari operator asal yang IPRN-nya dipakai untuk melakukan panggilan. Komisi yang didapat biasanya \$1 untuk setiap panggilan masuk. Biasanya ratusan ribu orang yang tertipu oleh panggilan ini, jadi bisa dibayangkan berapa besar uang yang mereka terima.



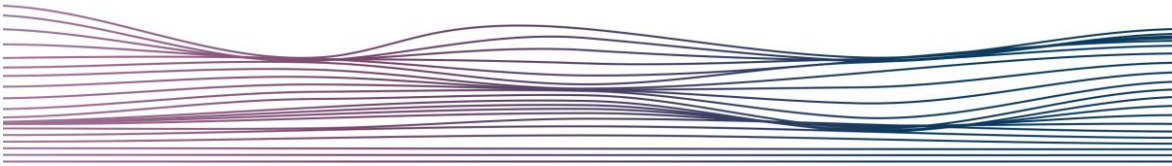


Panggilan Spam

Sumber : Tirto.id (2020)

Ada 17.983 laporan tentang nomor-nomor tidak dikenal yang melakukan panggilan sepanjang tahun 2018 (Data Tellows Indonesia).

Dari 17.983 laporan, jenis panggilan yang tidak dikenal berupa:

- **Telemarketing** →sebanyak
1.002 laporan
 - **Perusahaan Penagih Hutang** →sebanyak
557 laporan
 - **Penipuan Uang** →sebanyak
234 laporan
 - **Iklan Agresif** →sebanyak
172 lapor
- 

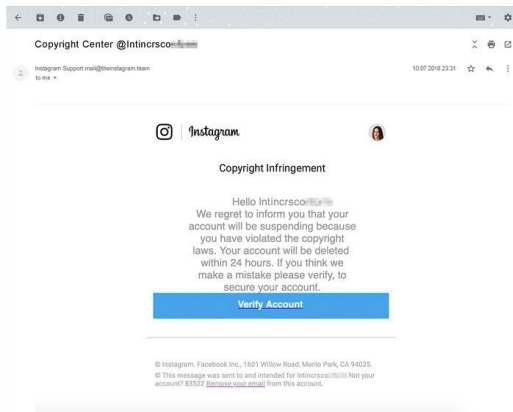
3. PHISHING

Phishing adalah istilah penipuan yang menjebak korban dengan target menyasar kepada orang-orang yang percaya bahwa informasi yang diberikannya jatuh ke orang yang tepat.



- *Phishing* dilakukan dengan menduplikat situs web atau aplikasi bank atau *provider*. Ketika kita memasukkan informasi rahasia, uang kita akan langsung dikuras oleh *cracker* tadi.
- Kejahatan *phishing* ini dilakukan oleh oknum dengan menghubungi kita sebagai calon korbannya melalui email, telepon, atau pesan teks dengan mengaku dari lembaga sah. Biasanya oknum-oknum yang melakukan *phishing* akan menanyakan beberapa data sensitive seperti identitas pribadi, detail perbankan, kartu kredit, dan juga kata sandi.

Jenis-jenis Phishing



Gambar 3.4 Phishing melalui email



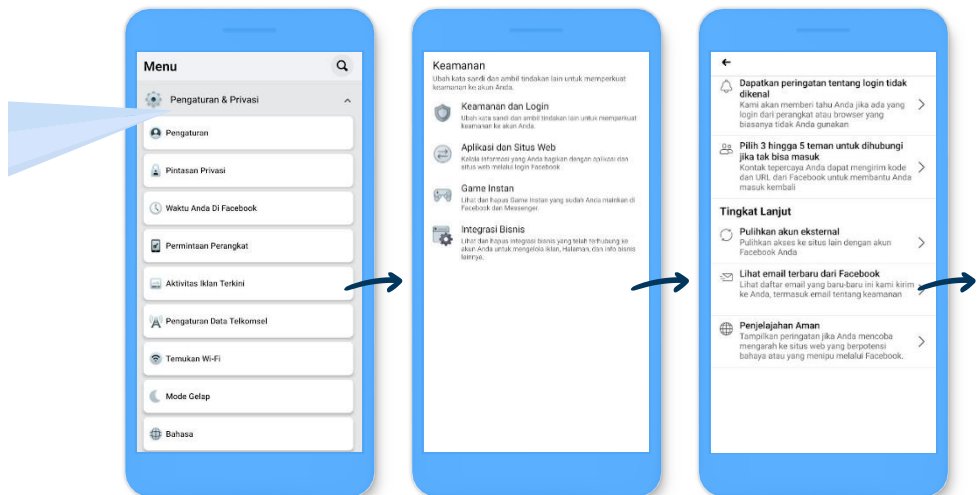
Gambar 3.5 Phishing melalui WA (share link)

Pelaku phishing selalu memiliki seribu cara dan alasan agar korban memberikan informasi pribadi mereka. Misal yang sering terjadi yaitu teknik phishing yang seolah-olah mengirimkan pesan melalui email atas nama Facebook, Instagram, Twitter, WhatsApp, bahkan Youtube. Narasi yang pelaku mainkan adalah akan menghapus akun korban. Jika korban tidak mengikuti arahan yang diberikan.

Disinilah dibutuhkan ketelitian, sebab email yang mereka pakai akan sangat mirip dengan email aslinya, pelaku

bukan hanya menggunakan nama saja, namun juga menyantumkan logo, agar korban merasa yakin.

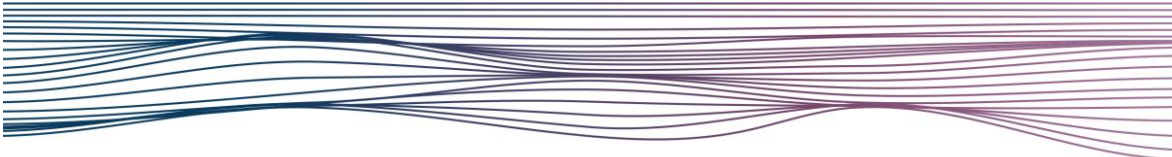
Tips mengecek pesan, apakah pesan tersebut benar dari facebook:



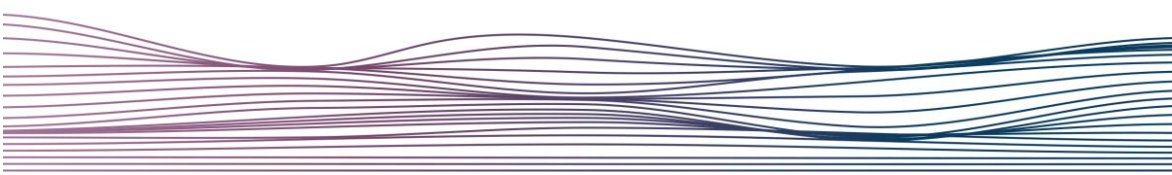
Buka Setting/Pengaturan Keamanan dan Login dengan mengklik di kananatas Facebook.

Klik Pengaturan & Privasi, lalu klik Keamanan dan Login.

Scroll turun ke Lihat email terbaru dari Facebook, lalu klik Lihat.



TIPS TERHINDAR DARI PHISHING

1. Jangan sekali-kali memberikan detail email bahkan password ke siapapun
 2. Jangan pernah menerima permintaan pertemanan dari orang yang tak dikenal. Pelaku penipuan sering menggunakan akun palsu dan memenuhi timeline atau linimasa korban dengan konten spam, dan yang berbahaya korban mengklik link tersebut dan phishing pun terjadi.
 3. Ganti passwordmu secara rutin. Mengganti password sama halnya dengan mengganti sikat gigi. Layaknya sikat gigi, jika kita tidak mengganti sikat gigi, maka fungsi dari sikat gigi sudah tidak seperti di awal, karena bagian sikat sudah mulai melebar, dan justru menyakiti gusi kita.
 4. Cek aktivitas akun kita. Cek secara rutin, history akun kita, apa yang kita akses dan aplikasi apa saja yang kita download. Pastikan kamu mengetahui apa yang kamu lakukan. Jika kamu merasa tidak pernah membuka/mengaksesnya, maka kamu perlu waspada.
 5. Jika kamu mendapatkan pesan yang aneh, jangan takut untuk segera melaporkan.
- 

4. HACKING

Cara kerja para *hacker* adalah dengan melakukan pembobolan/peretasan sampai dengan percobaan keamanan situs situs web dan komputer.



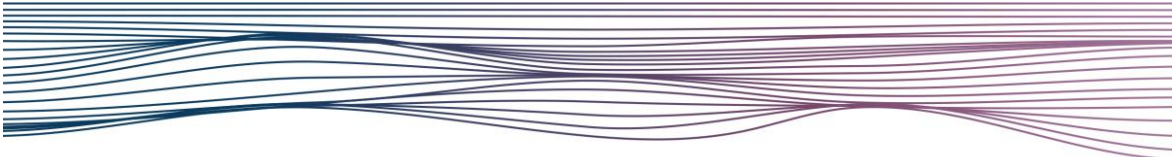
Gambar 3.5 Virus Hacking

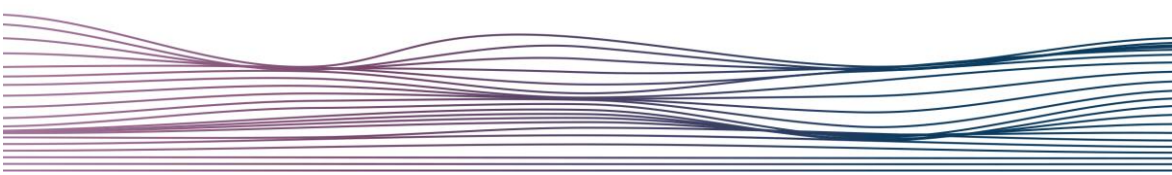
Sumber : Modul Literasi Digital Kominfo

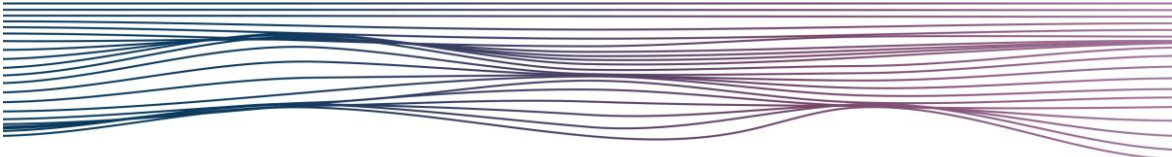
Gambar 3.6 Realtime
Hacker Serang Situs v

Sumber: Jogja.tribun

Jika akun Facebookmu dihack, ikuti cara berikut untuk mengembalikan akunmu

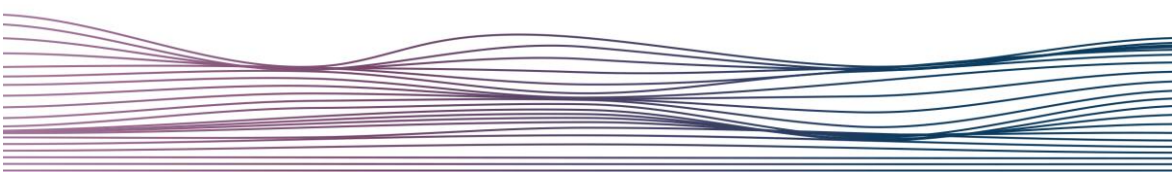
- 
- Laporkan! <http://www.facebook.com/hacked>.
Lengkapi laporan dengan menyertakan alamat email dan nomor HP saat mendaftar akun.
 - Jika tidak ada akses, kamu cukup mengisi data-data yang diminta misal email dan no hp.
 - Pihak facebook akan menerima laporan dan akan segera memproses verifikasi akun. Tahap selanjutnya kamu harus menyiapkan foto identitas seperti KTP atau SIM.
 - Tunggu akunmu balik dengan selamat.

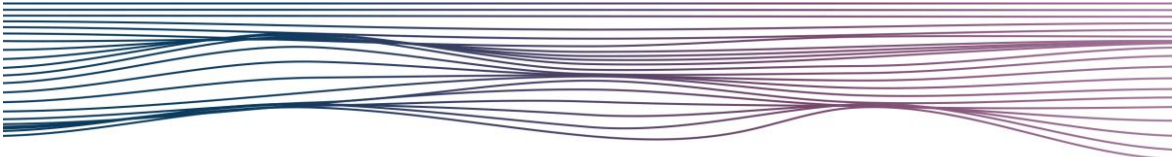




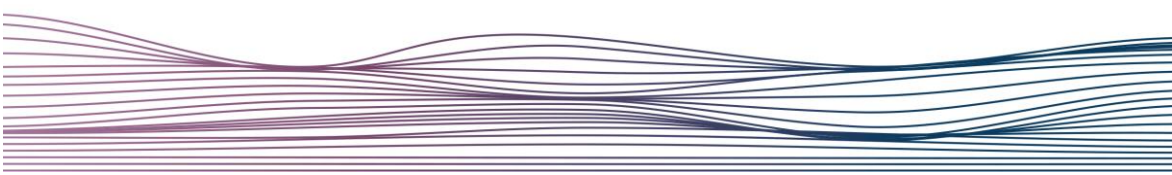
Jika akun Instagrammu dihack, ikuti cara berikut untuk mengembalikan akunmu

- Laporkan! [Help.instagram.com](https://help.instagram.com).
- Pilih menu privasi dan keamanan → melaporkan sesuatu → sepertinya akun saya diretas
- Instagram akan menghilangkan akunmu sementara, jadi jangan panik ya
- Instagram akan mengirimkan informasi lebih lanjut melalui email
- Isi formulir yang dikirimkan oleh Instagram dan kirimkan data pribadi seperti foto dan KTP kita
- Proses pemulihan akun berlangsung selama 4-7 hari.





Jika WhatsAppmu dihack, ikuti cara berikut untuk mengembalikan akunmu

- Verifikasi nomor kamu segera, cek disini <http://faq.whatsapp.com/android/verification/verifying-your-number>
 - Masukkan kode SMS 6 digit angka
 - Verifikasi dua langkah. Jika kamu diminta untuk verifikasi dua langkah, yakni memasukkan kode, maka kamu harus memasukkan kode lanjutan
 - Jika kamu tidak mendapatkan kode, maka kamu hacker sudah mendapatkan kode tersebut.
 - Tenang, kamu harus menunggu selama 7 hari untuk bisa masuk ke whatsapp tanpa kode verifikasi dua langkah.
 - Di hari ke-7, kamu akan otomatis bisa masuk ke whatsapp pribadimu.
- 

5. Ghosting

Istilah “ghosting” saat ini populer di kalangan anak muda. Ghosting berasal dari kata “Ghost”, kegiatannya sering diartikan sebagai cara baru untuk memutus komunikasi dengan lawan jenis. Kegiatan ini erat hubungannya dengan hubungan percintaan.

Ibaratnya pas udah baper, pas lagi sayang-sayangnya, eh sumber kebahagiaannya hilang. Ghosting dan sosial media memiliki hubungan yang erat. Seringkali pelaku ghosting menjalankan aksinya di sosial media. Ghosting bukan hanya terjadi di Indonesia.

Kasus ghosting di Amerika Serikat berada di posisi 13-23% remaja Amerika mengaku pernah menjadi korban ghosting. Di Spanyol, sekitar 19,3% remaja pernah mengalami ghosting di tahun 2020 (Navarro, 2020)

Tahukah kamu?

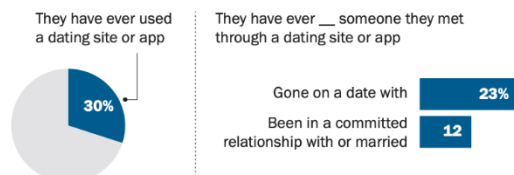
30% orang dewasa di Amerika Serikat mengaku pernah menjadi pengguna aplikasi kencan “*online dating*”. Tidak ada yang salah dengan *online dating*, namun mayoritas wanita yang menggunakan aplikasi tersebut mengaku pernah menjadi korban pelecehan atau mendapatkan pesan eksplisit berbau seks melalui platform tersebut (Pew Research, 2020).

Berdasarkan riset yang dilakukan oleh Pew Research Center pada tahun 2020, 3 dari 10 remaja di Amerika mengaku pernah menggunakan aplikasi online dating.

12% diantaranya memutuskan untuk menikah atau melanjutkan komitmen, sedang 23% mngakhiri hubungan bahkan tidak merasa memiliki hubungan yang spesial (ghosting)

Three-in-ten Americans have used a dating site or app; 12% have married or been in a committed relationship with someone they met through online dating

% of U.S. adults who say ...



Note: Those who did not give an answer are not shown.
Source: Survey of U.S. adults conducted Oct. 16-28, 2019.
"The Virtues and Downsides of Online Dating"

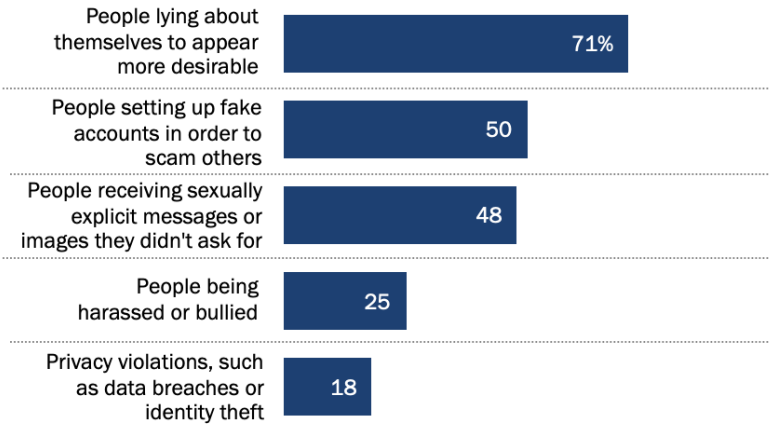
PEW RESEARCH CENTER

Gambar 3.6. Riset Ghosting

Mayoritas para pengguna online dating menganggap bahwa pasangan mereka di dunia online merupakan orang yang paling mudah dibohongi. 71% merahasiakan identitas mereka, 50% menggunakan akun palsu dan menggunakan sarana scam ke pasangan, 48% menerima pesan berbau seks dan pesan yang menjurus ke arah pornografi, 25% mengalami bully, dan 18% mengalami kekerasan (Pew Research, 2020)

A majority of online daters think it is very common for users to lie to appear more desirable

*% of online dating users who say ___ on dating sites and apps is **very common***



Note: Online dating users refers to respondents who say they have ever used an online dating site or app. Those who did not give an answer or who gave other responses are not shown.

Source: Survey of U.S. adults conducted Oct. 16-28, 2019.

"The Virtues and Downsides of Online Dating"

PEW RESEARCH CENTER

Gambar 3.7. Pengalaman Pengguna Online Dating

6. Breadcrumbs

Berbeda dengan ghosting, fenomena Breadcrumbs nyatanya jauh lebih meyakinkan. Breadcrumbs merupakan fenomena dimana seseorang yang tidak saling memiliki hubungan namun saling dekat dan tiba-tiba hilang kontak (ghosting), namun salah satu pihak melakukan komunikasi sporadik tanpa komitmen. Gampangnya adalah kamu dekat dengan orang, lalu orang itu tiba-tiba menghilang tanpa alasan, beberapa bulan kemudian dia datang dengan cara membalas story kamu, dm, atau bahkan WA hanya sekedar menanyakan kabar.

Ibaratnya nih, cewek lagi pas sayang-sayangnya ditinggal, pas udah move on si cowok dateng lagi. Jadi breadcrumbs lebih menyakitkan dibandingkan ghosting. Kalau ghosting cukup sekali, kalau breadcrumbs bisa berkali, layaknya serpihan roto yang disebar-sebarin.

Breadcrumbs dikenal juga sebagai perilaku menghantui, dimana seseorang tidak siap berkomitmen, namun dia juga tidak siap mengucapkan selamat tinggal kepada pasangannya. Jadi si pasangan ibaratnya menjadi cadangan dan hanya sebagai “cadangan”.

7. Catfishing

Istilah *catfish* mulai muncul dari sebuah tayangan dokumenter asal Amerika Serikat berjudul sama yang diproduksi oleh Henri Joost dan Ariel Schulman pada 2010 tentang para korban yang memiliki hubungan dengan seseorang yang memiliki identitas fiktif - identitas yang tidak pernah ada di dunia nyata (Van Dijck, 2013). Kemunculan *catfish* sendiri biasanya disebabkan oleh kebebasan individu untuk membuat akun pribadi sebagai cerminan identitas yang mereka ingin tampilkan.

Selain itu, pengguna SNS juga bisa memiliki lebih dari satu akun. Istilah catfishing sendiri digunakan untuk menggambarkan terhadap orang lain terutama pasangannya yang sebelumnya tidak pernah bertemu (Adama, 2017). Catfishing juga bisa diartikan sebagai seseorang yang menggunakan profil personal palsu pada SNS untuk melakukan kecurangan atau melakukan penipuan (Catfish Definition, n d).

Pada awalnya, *catfish* secara apabla diartikan k e dalam bahasa Indonesia secara langsung berarti ‘ikan lele’. Namun, istilah ini kemudian bergeser di masyarakat modern menjadi seorang yang berpura-pura menjadi orang lain dengan menciptakan identitas baru di internet, terutama di SNS. Adapun tujuan untuk melakukan *catfishing* adalah untuk menjalin hubungan romantik via media daring (Prastyphylia, 2014).

Pada dasarnya walaupun sama-sama berada dalam kategori menggunakan informasi palsu, catfishing sendiri berbeda dengan impersonation dan juga poser karena catfish lebih condong kepada online dating scams (Ahmad et al., 2017).

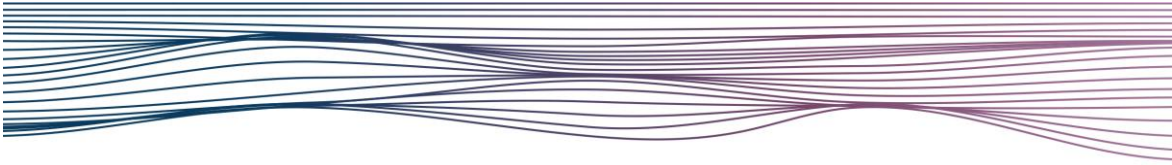
Bayu Skak Punya Lagu Galau Karena Pernah Jadi Korban Catfish!

Novita Caesaria - Sabtu, 30 Oktober 2021 | 15:00 WIB

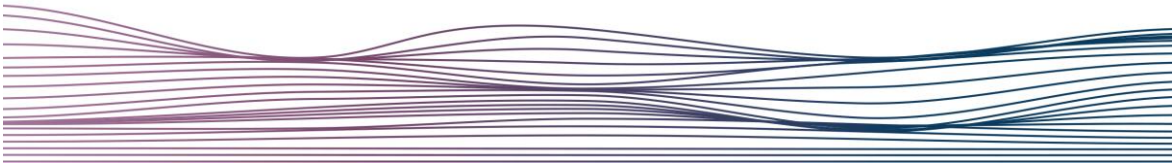


Gambar 3.8 Kasus Bayu Skak

Salah satu korban yang mengalami tindakan catfish adalah Bayu Eko Moektito, atau biasa dikenal sebagai YouTuber Bayu Skak. Dalam video unggahan nya di platform Youtube, dia menjelaskan mengenai penipuan identitas yang dialaminya. Kedekatannya dengan seseorang bernama Dara Fleisher Cohen atau dikenal Dara, berawal dari DM Instagram yang dikirimkan oleh Dara, yang mengaku sebagai calon dokter yang sedang melakukan



Pendidikan di Singapura. Perkenalan tersebut berlanjut menjadi hubungan yang lebih serius “pacarana”. Namun ternyata sosok Dara ternyata tidak ada, ternyata foto dan video yang disebar merupakan milik artis India bernama Dipshika ([cewekbanget.grid.id](https://www.cewekbanget.grid.id))

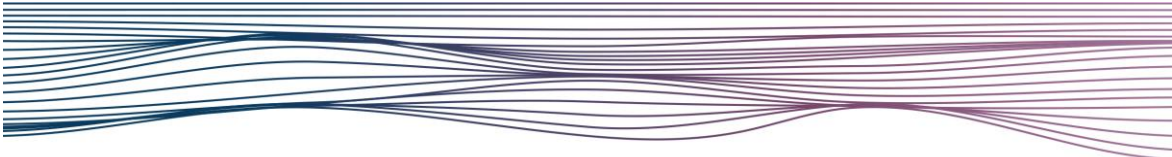




PROGRAM PENDIDIKAN
VOKASI

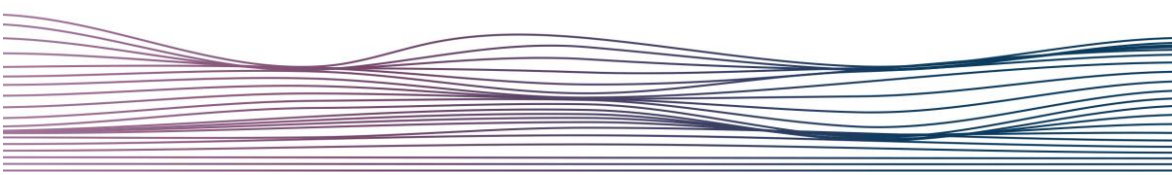


TIPS AMAN DAN NYAMAN BERMEDIA SOSIAL



Tips Aman dan Nyaman Bermedia Sosial bagi Orang Tua untuk Anak

(Frances Dalomba, LICSW, 2020)

- Menjadi model percontohan yang baik bagi anak, baik di dunia nyata maupun dunia maya
 - Atur batasan namun tetap ajak anak berdiskusi. Orang tua sering kali tidak membolehkan anak untuk bermain gadget begitu saja tanpa mengajak anak berdiskusi atau sekedar memberikan alasan yang rasional mengapa tidak boleh bermain gadget lama-lama. Batasi bukan berarti meniadakan waktu bermain gadget
 - Ajak anak berdiskusi tentang apa yang anak temukan di sosial media. Luangkan waktu untuk mendengarkan cerita anak, apresiasi tentang apa yang dia dapat,anggapi dengan bijak, dan jangan buru-buru menghakimi anak
 - Tetap waspada tentang privasi anak. Ajari anak perlahan-lahan, bahwa ada hal yang tidak bisa dengan mudah disebarakan kepada orang lain melalui sosial media.
- 

Tips aman Bersosial Media

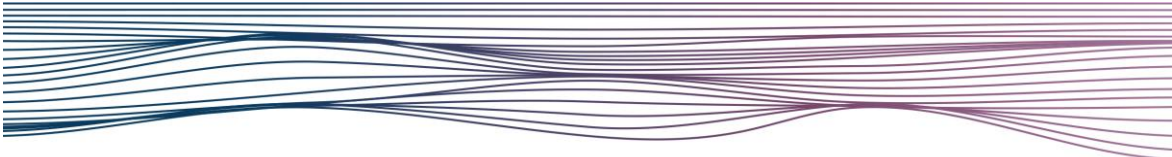
(Cyber Security, 2021)

Sosial media merupakan platform yang sudah menjadi bagian dari kehidupan online manusia. Jaringan sosial media menjadi media untuk tetap menjadikan manusia untuk selalu terhubung dengan yang lain, namun kita juga harus peduli dan waspada dengan informasi pribadi yang seringkali kita post.

Berikut tips aman bersosial media, gimana caranya tetap eksis tapi tidak membahayakan diri sendiri:

- Privasi dan keamanan sosial media.
Pelajari lebih mendalam apa itu privasi dan keamanan sosial. Keduanya sangat penting agar kamu mengetahui sebenarnya siapa sih yang melihat postingan kamu, apa sih yang kamu posting, dan menjaga pengalaman online kamu tetap positif.
- “Sekali ngepost, selalu ngepost”.
Reputasi kita bukan hanya berlaku di dunia nyata, di dunia maya pun reputasi akan tetap melekat. Lindungi reputasimu di sosial media. Apapun yang kamu posting akan menjadi rekam jejakmu dan tersimpan rapi disana. Berpikir dua kali sebelum kamu memposting foto pribadimu. Coba pikirkan, apakah ini aman untuk masa depanmu. Riset menunjukkan hampir 70% perusahaan menolak calon kandidat berdasarkan informasi yang mereka temukan di online. Jadi hati-hati ya!

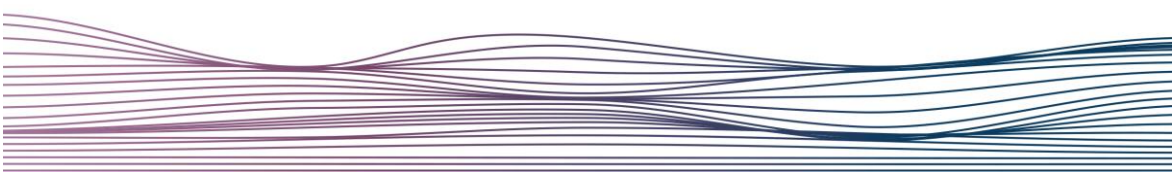
- Reputasi online aman, masa depan cerah.
Riset menunjukkan bahwa banyak orang yang mendapatkan pekerjaan karena memiliki branding yang positif di sosial media.
- Jaga data pribadi kamu.
Terkadang orang tidak menyadari bahwa tanpa sadar dia menyebarkan informais pribadinya ke sosial media. Misal sertifikat vaksin, foto ktp, no hp, nama lengkap, tanggal lahir, pekerjaan, rutinitas, bahkan sudut rumah. Semakin banyak informasi yang kamu posting di sosial media, semakin tinggi risiko para hacker atau orang jahat yang bisa menggunakan informai pribadi untuk hal-hal kriminal, seperti pencurian identitas, mengakses data kita, hingga pinjaman online.
- Ketahui siapa teman kamu di sosial media.
Seringkali informasi pribadi kita justru disebarakan oleh teman online kita. Jika kamu ingin menyebarkan informasi umum, karya, tutorial dll kamu bisa share untuk umum, semua teman-teman online kamu bisa melihat. Namun jika kamu share informasi pribadi misal kegiatan sehari-hari yang tidak bisa dishare, disarankan share ke terdekat kamu atau sering dikenal dengan sebutan “close friends”.
- Pilah dan Pilih Teman Online.
Tidak semua akun di sosial media harus kita ikuti “follow”. Ketahui tujuan kalian mengapa harus mengikuti mereka. Jika ada akun yang dirasa membuat tidak nyaman, kamu bisa unfollow, hide



akun atau bahkan block jika ada kejadian yang membahayakan

- Pakai security software.

Cara ini masih dirasa efektif untuk melindungi virus, malware, dan kerugian yang lain.



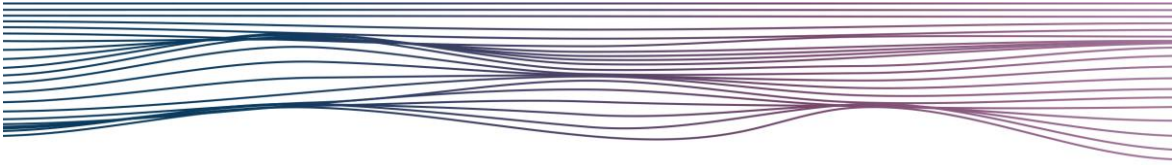
Tips Menjaga Rekam Jejak di Dunia Digital

Setiap tindakan online yang kita lakukan akan meninggalkan jejak digital. Tidak ada yang salah dengan jejak digital, justru darisanalah kita mengetahui informasi apa saja yang sudah kita akses selama di internet atau biasa disebut “history”.

Semua tindakan yang kita lakukan di dunia digital terekam, tercatat, dan terorganisir dengan rapi, mulai dari apa yang kita akses, jam hingga detik, dll. Itu termasuk kegiatan kita seperti komentar di sosial media teman, upload foto, like postingan teman, riwayat login, dll.

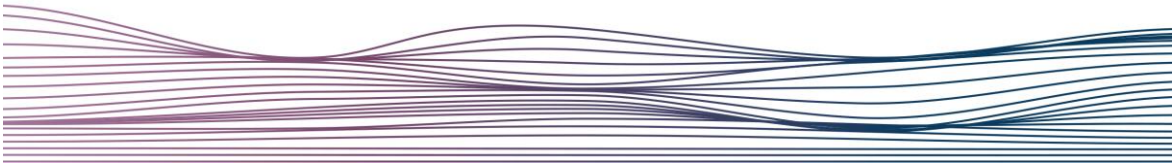
Oleh karena itu kita harus tetap berhati-hati dengan tindakan yang kita lakukan, bukan berarti menganggap dunia digital bebas dan tidak ada orang yang tahu, justru segala aktivitas terekam, tercatat, dan terorganisir dengan rapi. Yuk ikuti tips berikut ini (:

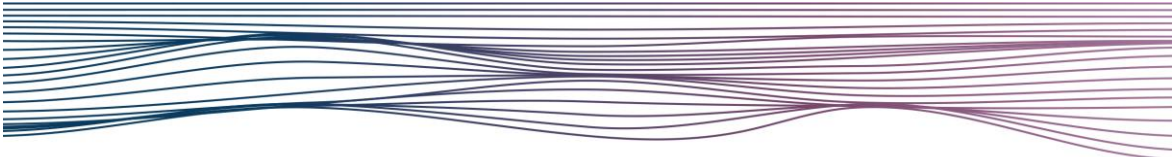
1. Pikirkan dahulu sebelum klik. Semua yang kita klik di internet juga terekam dan tercatat
2. Jaga reputasimu. Jangan komentar negatif, posting foto yang tidak layak, forward informasi tidak jelas cenderung hoaks dll
3. Lindungi informasi pribadi. Perkuat password, jangan malas ganti password secara berkala dan hindari password dengan tanggal lahir
4. Lihatlah dirimu selayaknya kamu ingin dilihat. Pencitraan, ciptakan citra yang bagus, bukan hanya seolah-olah bagus atau bahkan berpura-pura



menjadi orang baik. Tetaplah menjadi pribadimu dengan gayamu. Bebas bukan berarti tanpa aturan

5. Ciptakan konten positif di setiap postinganmu. Konten positif dan yang bermanfaat
6. Jadikan dirimu sebagai role model minimal bagi dirimu dan keluargamu.
7. Ingat rekam jejak tidak akan pernah hilang dan akan tetap melekat pada diri kita.

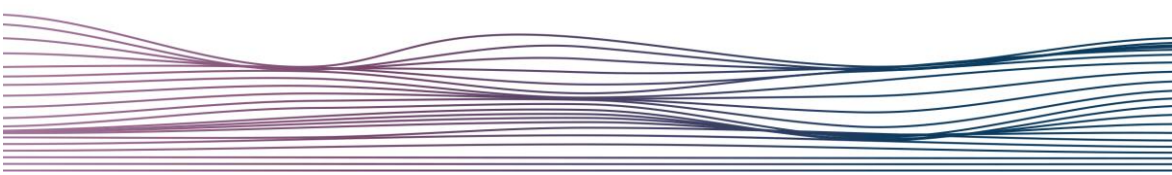




Mengapa Keamanan Digital Itu Penting?

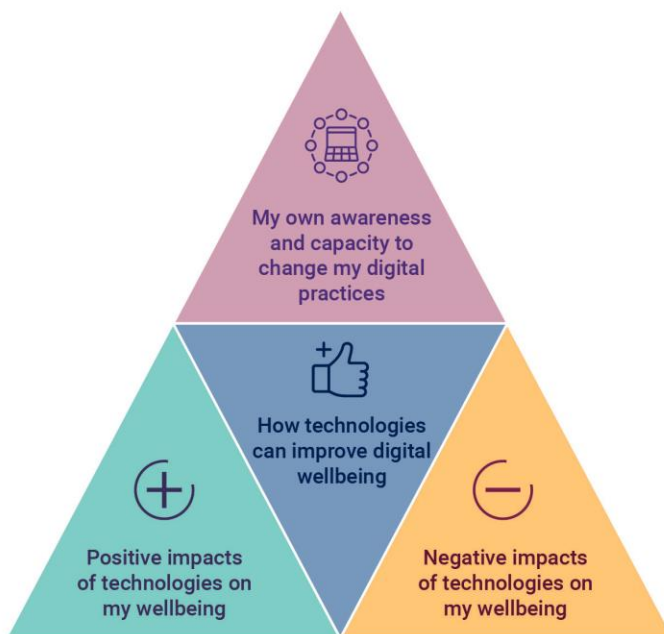
Akun sosial media kita itu ibaratnya seperti rumah, layaknya sebuah rumah pasti memiliki perabotan-perabotan rumah tangga hingga aset penting yang selalu terjaga di dalam rumah. Sama halnya dengan akun sosial media kita, didalamnya juga mengandung identitas pribadi kita, username atau nama online kita, foto-foto kita, video kita, pesan kita dengan teman kita, kontak telpon, info pembayaran yang kita pakai, bahkan yang tanpa kita sadari yakni di dalam akun kita juga bisa mendeteksi titik lokasi kita.

Nah layaknya sebuah rumah, untuk melindungi rumah kita dari pencuri, kita juga harus melengkapi rumah kita dengan gerbang yang kokoh, kunci rumah yang canggih, bahkan sampai meminta bantuan satpam untuk melindungi rumah kita. Sama halnya dengan akun kita, akun kita juga penting, dan banyak pihak yang berusaha untuk masuk dan mencuri identitas penting kita. Nah untuk mencegah tindakan pencurian, kita membutuhkan digital safety atau keamanan dalam bermedia digital.

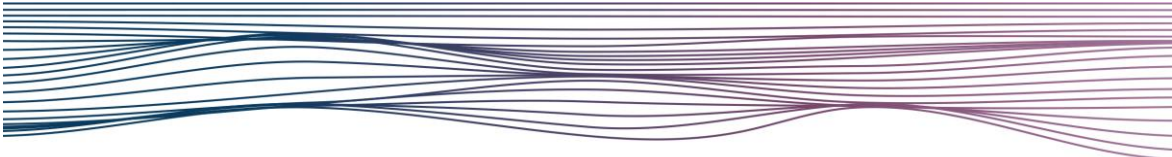




Gambar 4.1 Pentingnya Keamanan Digital
Sumber: Facebook

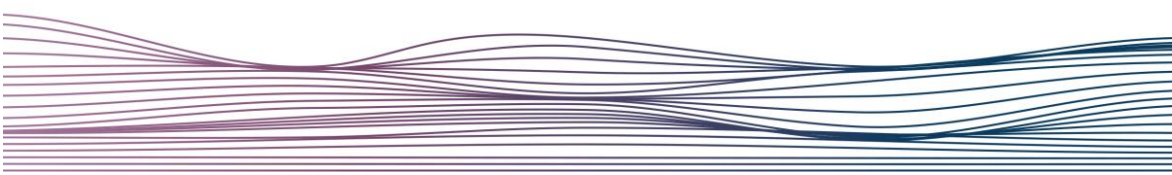


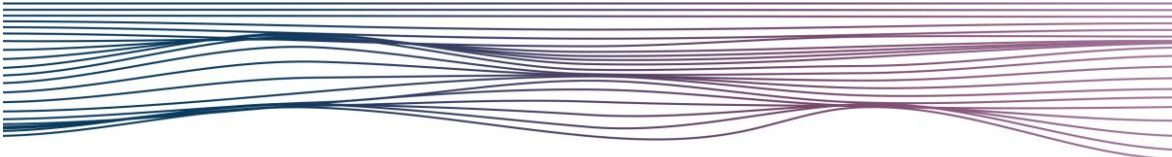
Gambar 4.2 framework Digital wellbeing 2019



Tahukah kamu bahwa menjaga kesehatan bukan hanya untuk kesehatan fisik semata, kesehatan digital juga penting loh. Apa itu kesehatan digital?

Kesehatan digital menurut digital wellbeing 2019 yakni bagaimana seseorang mampu mengendalikan dampak teknologi dan layanan digital terhadap kesehatan mental, fisik. Dan emosional masyarakat. (JISC, 2019)





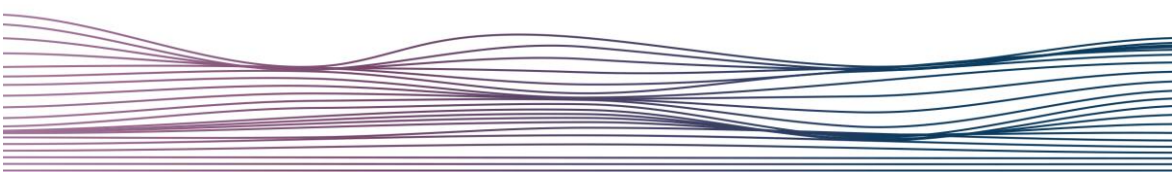
DAMPAK DIGITAL PADA KEHIDUPAN PRIBADI

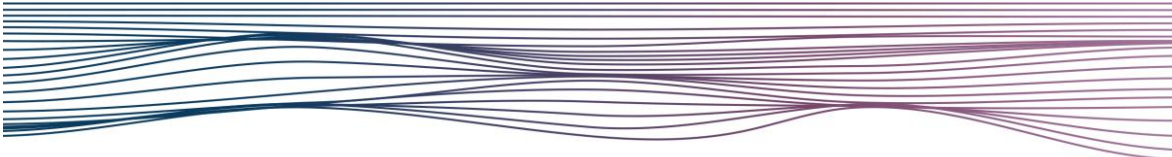
(Sumber: JISC, 2019)

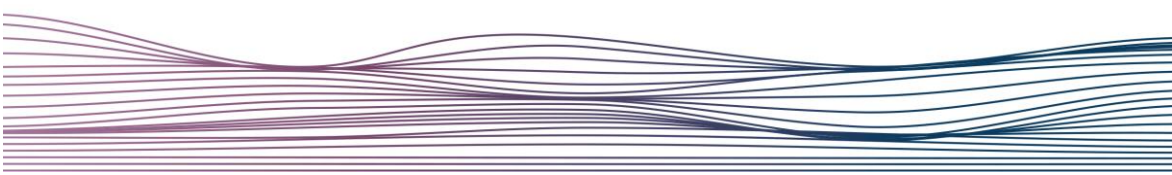
DAMPAK POSITIF

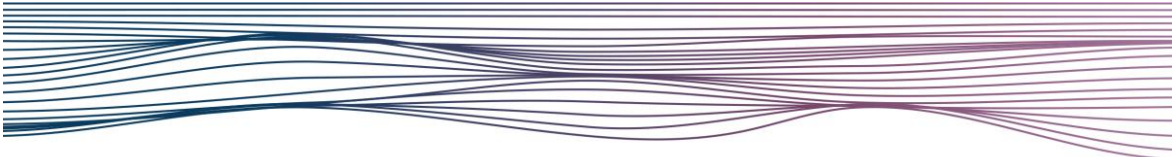
- Menciptakan identitas pribadi yang positif
- Membangun harga diri atau reputasi diri di dunia digital
- Hiburan (misalnya permainan, kesenangan interaksi, musik)
- Kenyamanan/time saving (misalnya belanja)
- Akses ke ide/inspirasi baru
- Media untuk menjaga kesehatan fisik (misal video work out, zumba dari youtube)

DAMPAK NEGATIF

- Membandingkan diri kita dengan orang lain, terutama tentang pencapaian orang. Sosial media menjadi media bagi banyak orang untuk share tentang keberhasilannya, ada yang menyikapi sebagai motivasi namun banyak juga yang justru dengan konten tersebut membuat orang merasa insecure dan terpuruk.
 - Kecanduan perilaku online (misalnya perjudian, porno)
 - Konsumsi pasif
- 

- 
- Akses ke aktivitas/ materi ilegal
 - Pelanggaran data pribadi
 - Kurangnya akses dan/atau tertinggal
 - Kurang tidur
 - Dampak pada kesehatan fisik (misalnya ketegangan mata, postur tubuh, kurangnya Latihan)





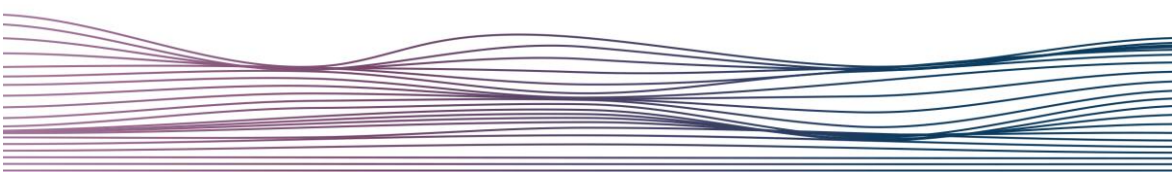
DAMPAK DIGITAL PADA KEHIDUPAN SOSIAL

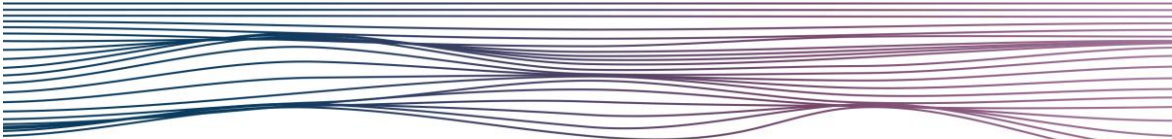
(Sumber: JISC, 2019)

DAMPAK POSITIF:

- Mencegah isolasi
- Membangun dan memelihara hubungan
- Mengurangi kesepian
- Partisipasi penuh dan koneksi dengan keluarga, teman dan komunitas yang lebih luas
- Meningkatkan kesempatan untuk para difabel

DAMPAK NEGATIF:

- Perundungan siber
 - *Online Grooming* (misalnya jenis kelamin, radikalisasi, grooming pada anak)
 - Eksklusif dan/atau tingkat aksesibilitas (misalnya jenis kelamin, usia, kemiskinan)
- 



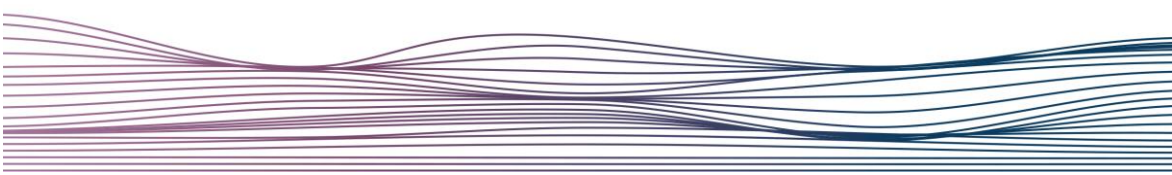
DAMPAK DIGITAL PADA PENDIDIKAN

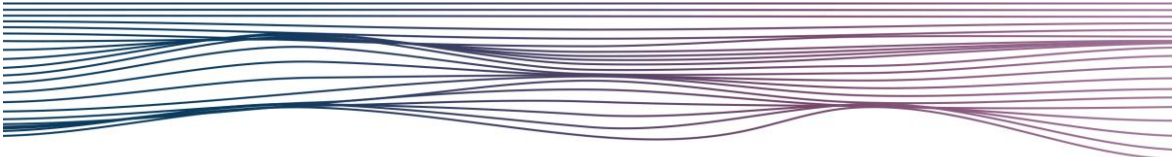
(Sumber: JISC, 2019)

DAMPAK POSITIF

- Cara alternatif untuk belajar
- Kolaborasi online dan mampu membuka kesempatan belajar
- Pembelajaran yang menarik
- Praktek keterampilan digital untuk melamar pekerjaan
- Pelajari keterampilan digital untuk karir baru
- Peningkatan akses untuk belajar
- Lebih menarik

DAMPAK NEGATIF

- Kurangnya keterampilan digital
 - Kelebihan beban digital
 - Penggunaan teknologi yang tidak tepat
- 



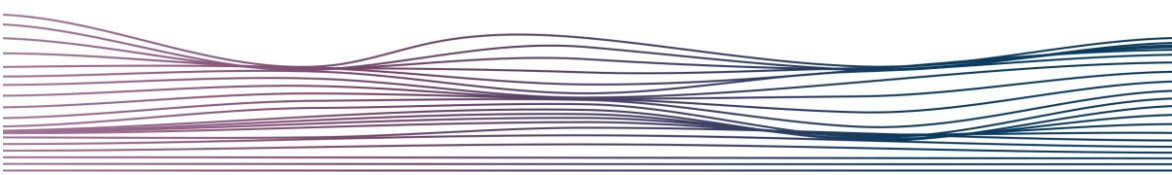
DAMPAK DIGITAL PADA DUNIA KERJA

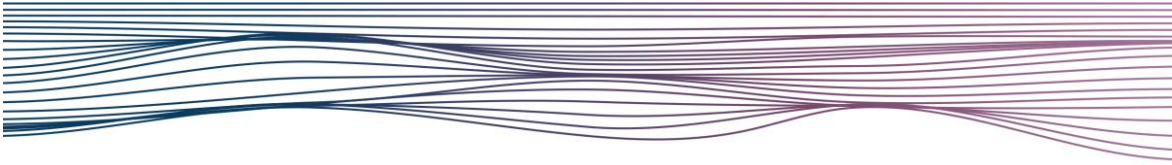
(Sumber: JISC, 2019)

DAMPAK POSITIF

- Meningkatkan komunikasi
- Kolaborasi global
- Kerja fleksibel
- Alat untuk mengelola beban kerja
- Alat untuk membuat segalanya lebih mudah
- Menciptakan positif profesional identitas online
- Tautan ke profesional lain/ jaringan subjek

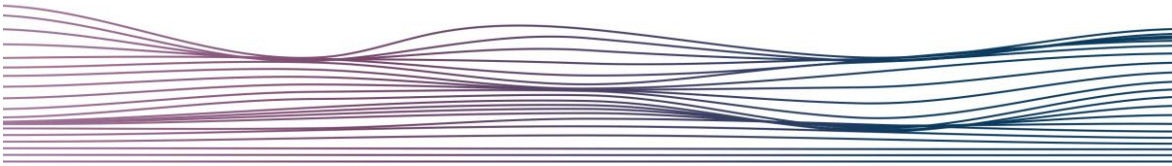
DAMPAK NEGATIF

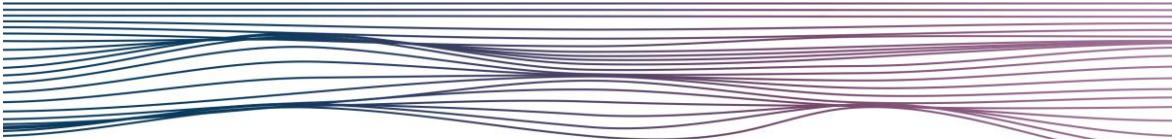
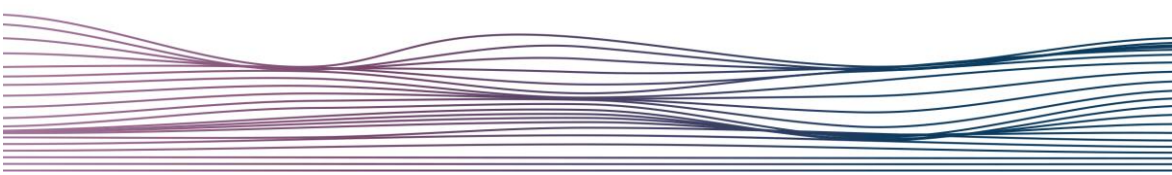
- Kelebihan beban digital
 - Selalu aktif (akses 24 jam)
 - Perubahan peran/ aktivitas pekerjaan
 - Otomatisasi tugas (misalnya redundansi)
 - Ergonomi yang buruk sehingga mempengaruhi kesehatan fisik
- 

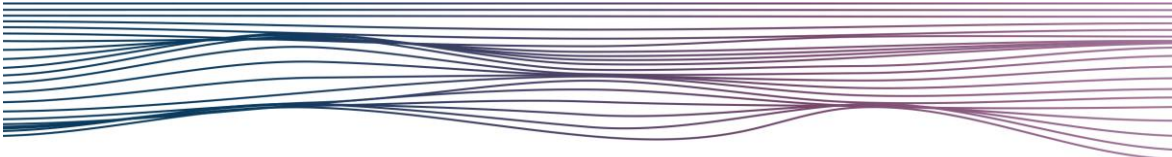


KELOLA KEHIDUPAN ONLINEMU SEKARANG JUGA!

(Sumber: JISC, 2019)

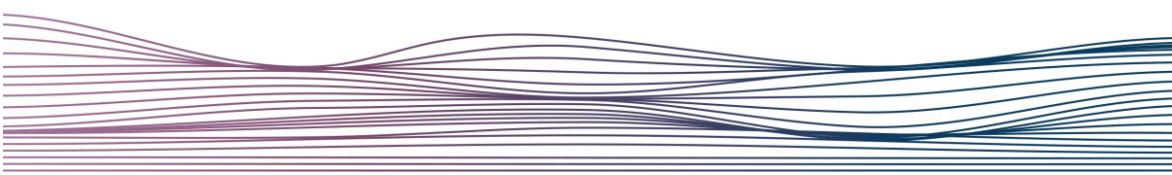


- 
1. Gunakan akses digital yang relevan dengan pembelajaran dan pekerjaan anda
 2. Luangkan waktumu untuk menjelajahi dan memahami oreferensi kebutuhan digital anda
 3. Pertimbangkan dampak aktivitas digital bagi anda sendiri dan orang lain. Tips mengurangi dampak negatif digital pada tubuh anda:
 - a. Perhatikan postur tubuh yang baik (agronomi), jarak antara mata dengan layar, posisi duduk, kecerahan monitor, dan memastikan jam tidur cukup
 - b. Hindari hal-hal negatif, jika anda menjadi korban, pastikan anda mengetahui tatacara peloporannya
 - c. Menggunakan fitur keamanan digital seperti password dan two step aunthetication proses
 - d. Mengambil peran positif dan mampu mengidentifikasi potensial masalah digital
 4. Kelola beban kerja digital anda. Walaupun teknologi terbukti mampu meningkatkan efisiensi pekerjaan, hal tersebut dibarengi juga dengan menciptakan harapan yang tidak realistis sehingga seseorang dipaksa untuk menyelesaikan tugas dalam waktu 24/7 sehingga mampu menyebabkan stress akibat kurang istirahat.
 5. Pastikan anda mengetahui cara penggunaan setiap peralatan digital, alat, layanan, hingga konten digital
 6. Ciptakan dan kelola identitas anda menjadi reputasi yang membanggakan di dunia digital
- 



“Secara umum, hanya anak yang merasa aman, yang bisa bergerak maju dengan sehat. Mereka perlu diberikan rasa aman. Mereka tidak bisa didorong ke depan, jika kebutuhan mereka untuk merasa aman tetap ada untuk dipenuhi.”

Psikolog asal Amerika, Abraham Maslow,



Daftar Pustaka

- Abdulah, A., Samadi, B., & Gharleghi, B. (2014). A Study on the Negative Effects of Social Networking Sites Such as Facebook among Asia Pacific University Scholars in Malaysia Sustainable entrepreneurs: who they are? View project E Commerce Implementation on Iranian SMEs View project A Study on the Nega. *International Journal of Business and Social Science*, 5(10), 133–145.
- Adam, A. (2017). Catfishing: Tipu Muslihat Gebetan Khayalan. Tirto.Id. Alshenqeeti, H. (2014). Interviewing as a Data Collection Method: A Critical Review. *English Linguistics Research*, 3(1). <https://doi.org/10.5430/elr.v3n1p39>
- Anwar, F. (2017). Perubahan dan Permasalahan Media Sosial. *Jurnal Muara Ilmu Sosial, Humaniora Dan Seni*, 1(1), 137–144.
- APJII (2020). Laporan survei internet APJII 2019-2020 (Q2). Didapat dari <https://apjii.or.id/survei2019x>.
- Badan Pusat Statistik (BPS). (2019). Indeks pembangunan teknologi, informasi, dan komunikasi/ict development index 2018. Jakarta: Badan Pusat Statistik.
- Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Business and Management*, 1–23. <https://doi.org/https://doi.org/10.9790/487X-0124852>
- Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime and Law*, 20(3), 261–283. <https://doi.org/10.1080/1068316X.2013.772180> Burke, P.

J., & Stets, J. E. (2009). *Identity Theory* (1st ed.). Oxford University Press. Catfish Definition. (n.d.). Mirriam Webster.

CNN (2020, Desember 1). Polri tangani 4.250 kejahatan siber saat pandemi. Diperoleh dari <https://www.cnnindonesia.com/nasional/20201201141213-12-576592/polritangani-4250-kejahatan-siber-saat-pandemi>

Denzin, N. K., & Lincoln, Y. S. (2018). *The SAGE Handbook of Qualitative Research*. In Synthese (Vol. 195, Issue 5). <https://doi.org/10.1007/s11229-017-1319-x> Diandra.

(2017). Pemerintah ingin media sosial dimanfaatkan untuk hal produktif

Duhita, S. (2018). Pengakuan 'Faker' Online, Sanggup Memperdaya Orang Agar Mau Pacaran Tanpa Ketemuan. Vice Indonesia.

Ellison, N., Heino, R., & Gibbs, J. (2006). Managing Impressions Online: Self-Presentation Processes in the Online Dating Environment. *Journal of Computer-Mediated Communication*, 11(2), 415–441. <https://doi.org/10.1111/j.1083-6101.2006.00020.x> Federal Trade Commission. (n.d.). Online Dating Scams Infographic.

Facebook. 2020. Panduan Anti Ribet #NyamanBersosmed. Kominfo

Finkel, E. J., Eastwick, P. W., Karney, B. R., Reis, H. T., & Sprecher, S. (2012). Online Dating: A Critical Analysis From the Perspective of Psychological Science. In

Psychological Science in the Public Interest, Supplement (Vol. 13, Issue 1).

<https://doi.org/10.1177/1529100612436522>

Frost-Arnold, K. (2016). Social Media, Trust, and the Epistemology of Prejudice. *Social Epistemology*, 30(5–6), 513–531.

<https://doi.org/10.1080/02691728.2016.1213326>

Gibbs, J. L., Ellison, N. B., & Lai, C. H. (2011). First comes love, then comes google: An investigation of uncertainty reduction strategies and self-disclosure in online dating. *Communication Research*, 38(1), 70–100.
<https://doi.org/10.1177/0093650210377091>

Goffman, E. (1959). *The Presentation of Self in Everyday Life* (Issue 1). Anchor Books.
<https://doi.org/10.5465/amr.1989.4279016>

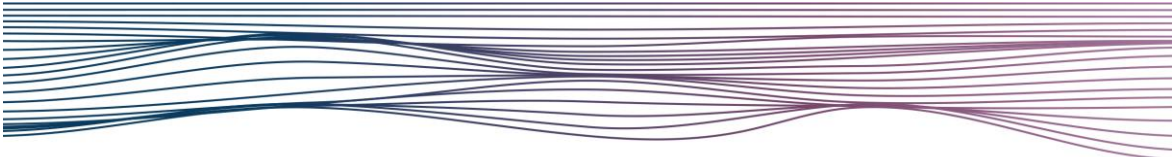
Google Support. (2021). Do an Advanced Search on Google. Diperoleh dari
<https://support.google.com/websearch/answer/35890?co=GENIE.Platform%3DAndroid&hl=en>

Google, Temasek, Bain & Company (2020). At full velocity: Resilient and racing ahead. Diperoleh dari
<https://economysea.withgoogle.com/>
<https://news.microsoft.com/wpcontent/uploads/prod/sites/421/2020/02/Digital-Civility-2020-Global-Report.pdf>

Jayani, D. H. (2020). Pembangunan teknologi Indonesia tertinggal di negara G20. *Katadata*. Diperoleh dari
[https://databoks.katadata.co.id/datapublish/2020/02/28/pembangunan-teknologiindonesiatertinggaldinegarag20#:~:text=ICT%20Development%20Index%202017&text=Angka%20ini%20berada%20di%20posisi,terendah%20di%20G20%20setelah%20India.&text=Pada%2010%20Februari%2020%2C%20Indonesia,prinsip%20Countervailing%20Duty%20\(CVD\).&text=Pada%202020%2C%20PDB%20per%20kapita,atau%20terendah%20kedua%20di%20G20](https://databoks.katadata.co.id/datapublish/2020/02/28/pembangunan-teknologiindonesiatertinggaldinegarag20#:~:text=ICT%20Development%20Index%202017&text=Angka%20ini%20berada%20di%20posisi,terendah%20di%20G20%20setelah%20India.&text=Pada%2010%20Februari%2020%2C%20Indonesia,prinsip%20Countervailing%20Duty%20(CVD).&text=Pada%202020%2C%20PDB%20per%20kapita,atau%20terendah%20kedua%20di%20G20)

Katadata Insight Center & Kominfo. (2020). Status literasi digital Indonesia 2020: Hasil survei di 34 provinsi. Jakarta: Katadata Insight Center & Kominfo.

Kominfo, Siberkreasi, & Deloitte. (2020). *Roadmap literasi digital 2021-2024*. Jakarta: Kominfo, Siberkreasi, & Deloitte.



Microsoft TRG. (2021) Civility, Safety & Interaction Online February 2020 [PowerPoint slides].

Goodwill Community Foundation. (n.d.). *Internet Basic:*

Using Search Engine. GCFLearnFree. Retrieved November

Tuesday, 2021, from

<https://edu.gcfglobal.org/en/internetbasics/using-search-engines/1/>

Gibbs, S. (2016, January Friday). *How to use search like a pro:*

10 tips and tricks for Google and beyond. TheGuardian.com.

Retrieved November Tuesday, 2021, from

<https://www.theguardian.com/technology/2016/jan/15/how-to-use-search-like-a-pro-10-tips-and-tricks-for-google-and-beyond>

internetlivestats. (2016). *Internet Users By Country (2016)*.

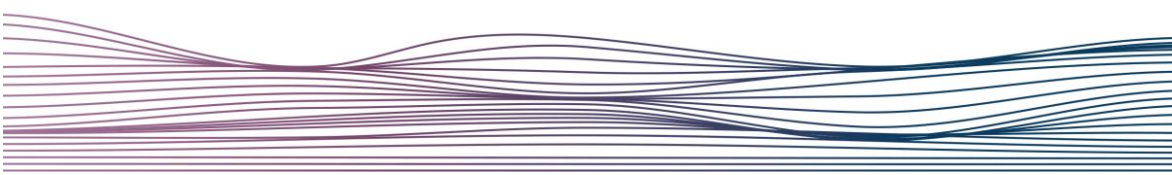
<https://www.internetlivestats.com/internet-users-by-country/>

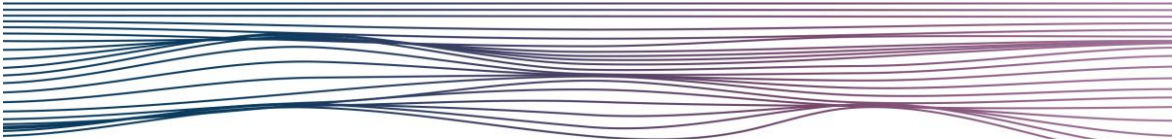
LibGuides at University of West Florida Libraries. (2021,

August). *Tips for Avoiding Fake News*. University Library of

University of West Florida. Retrieved November, 2021, from

<https://libguides.uwf.edu/c.php?g=609513&p=4274530>





BBC.com. (2015, Agustus). #TrenSosial: Bagaimana menghadapi para penebar kebencian di medsos? *BBC.com*.

https://www.bbc.com/indonesia/majalah/2015/08/150826_trensosial_hatespeech

Goodwill Foundation. (n.d.). *Belanja online dengan aman*.

edu.gcfglobal.org. https://edu.gcfglobal.org/en/tr_id-internet-safety/belanja-online-dengan-aman/1/

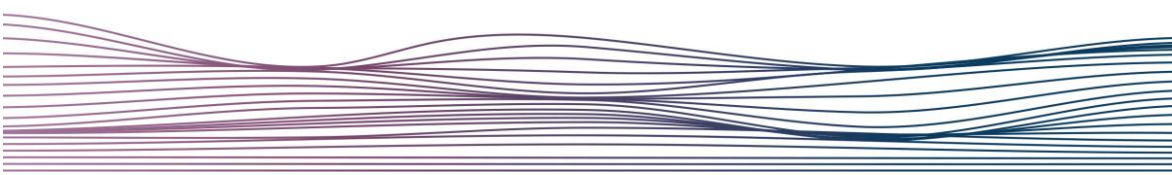
Young Americans : Centre for Financial Education. (n.d.).

Benefits and Risk of Online Banking. Young Americans : Centre for Financial Education. <https://yacenter.org/young-americans-bank/internet-banking/benefits-risk-online-banking/>

State of California Department of Justice. (n.d.). *Protect Your Computer From Viruses, Hackers, and Spies*. Office of The Attorney General: State of California Department of Justice. <https://oag.ca.gov/privacy/facts/online-privacy/protect-your-computer>

Australian Digital Health Agency. (2020, September).

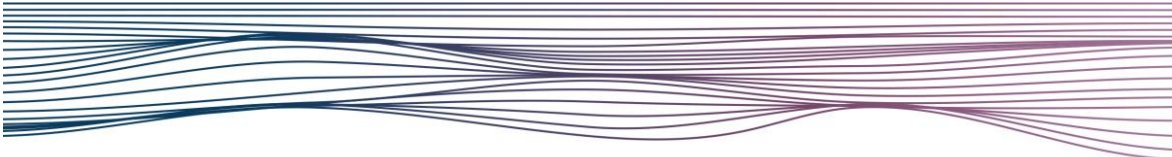
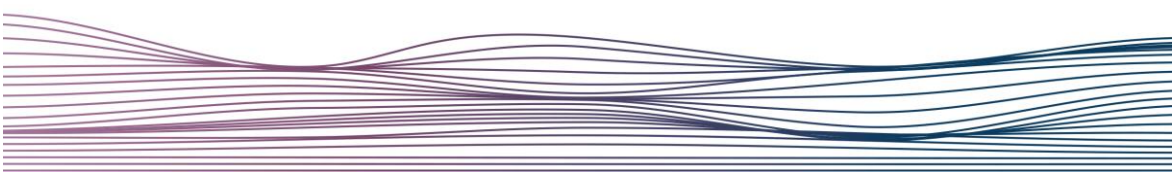
Supporting a Positive Security Culture: MANAGING YOUR DIGITAL FOOTPRINT. Australian Digital Health Agency.



https://www.digitalhealth.gov.au/sites/default/files/2020-11/Manage_your_digital_footprint.pdf

Daftar Pustaka Link

1. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7037474/>
2. <https://www.pewresearch.org/internet/2020/02/06/the-virtues-and-downsides-of-online-dating/>
3. <https://www.pewresearch.org/fact-tank/2020/02/06/10-facts-about-americans-and-online-dating/>
4. <https://www.lifespan.org/lifespan-living/social-media-good-bad-and-ugly> (bab 1 sosial media dan tips aman)
5. <https://socialmediacub.org/blog/from-the-clubhouse/teenagers-why-you-should-care-about-your-digital-footprint/> (tips rekam jejak)
6. <https://www.digitalcitizenship.nsw.edu.au/articles/leaving-a-digital-footprint> (rekam jejak)
7. <https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/social-media/>
8. <https://www.nidirect.gov.uk/articles/social-media-online-gaming-and-keeping-children-safe-online#toc-7> (staying safe while playing online)
9. <https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely> (basic privacy social media)
10. <https://www.cybersmile.org/what-we-do/advice-help/catfishing> (catfishing)

- 
11. <https://www.facebook.com/help/325807937506242/>
 12. https://www.researchgate.net/publication/347786555_Development_and_Validation_of_Breadcrumbs_in_Affective-Sexual_Relationships_BREAD-ASR_Questionnaire_Introducing_a_New_Online_Dating_Perpetration
 13. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6352099/>
 14. <https://www.esafety.gov.au/about-us/tech-trends-and-challenges/doxing>
 15. <https://www.cybersmile.org/advice-help/doxing>
(contoh kasus doxing)
 16. [Digital wellbeing | Building digital capability \(jisc.ac.uk\)](#)
 17. [The Psychology of FOMO | Fear of Missing Out | King University Online](#)
 18. <https://datareportal.com/reports/digital-2021-indonesia>
 19. [https://www.kominfo.go.id/content/detail/8600/waspada-panggilan-spam-dari-77/0/sorotan media](https://www.kominfo.go.id/content/detail/8600/waspada-panggilan-spam-dari-77/0/sorotan-media)
 20. <https://www.digitalcapability.jisc.ac.uk/what-is-digital-capability/digital-wellbeing/>
- 



PROGRAM PENDIDIKAN
VOKASI



KOMINFO | SIBERKREASI

VOKASI HUMAS UI | KLINIK DIGITAL | DIGITAL MAKARA PROJECT

2021