PENULIS:

DEVIE RAHMAWATI • MILA VIENDYASARI
RIZKY AMELIAH • RANGGA ADI NEGARA
INDRIANI RAHMAWATI • GIRI LUMAKTO
RIENZY K. R.

EDITOR :

RIENZY KHOLIFATUR

DESAIN:

DESHADI TRI AGUNG S.

MODUL STRATEGI HIDUP DI DUNIA DIGITAL

Devie Rahmawati • Mila Viendyasari • Rizki Ameliah
Rangga Adi Negara • Indriani Rahmawati
Giri Lumakto • Rienzy K. R.

Diterbitkan oleh:
Program Vokasi Humas - Universitas Indonesia

DAFTAR ISI

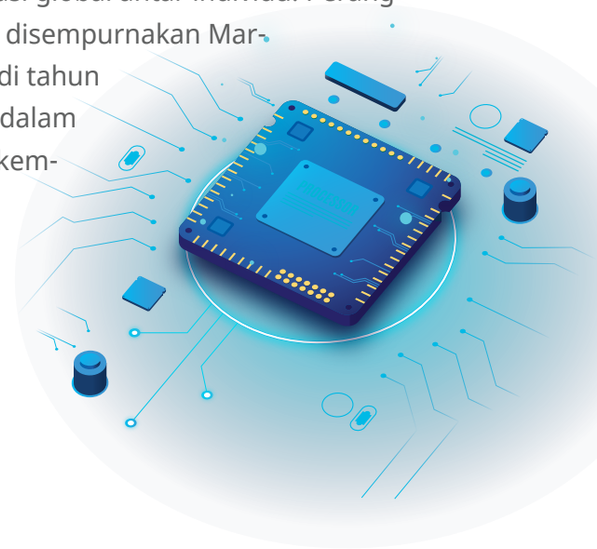
01 LANSKAP DIGITAL

Telepon pintar kerap dikaitkan dengan penggunaan internet. Sebuah lembaga riset *internetlivestats* (2016) menyebutkan bahwa Indonesia menduduki peringkat ke 12 pengguna internet terbanyak. Lembaga ini mengestimasi bahwa lebih dari 53 juta penduduk Indonesia sudah mengakses internet, angka ini menunjukkan peningkatan pengguna internet sebanyak 6,5% dari tahun 2014. Penetrasi internet Indonesia juga meningkat, di tahun 2014 hanya 17% meningkat menjadi 20% di tahun 2016.

Yuk baca sejarah tentang internet di bawah ini:

Internet dan Komputer

Di awal abad ke-20, teknologi komunikasi telah mengalami loncatan signifikan. Dunia kini berada dalam genggaman berkat Internet. Komersialisasi Internet di awal 1960-an memungkinkan komunikasi global antar individu. Perangkat telepon nirkabel yang disempurnakan Martin Cooper dari Motorola di tahun 1973 membawa dunia ke dalam genggaman. Namun, perkembangan Internet yang cukup cepat saat ini tidak lepas dari perangkat utama yang menjadi medium pertama kali, yaitu komputer.



Evolusi Internet

Periode Waktu	Perkembangan yang Terjadi
1960 - 1985	Penemuan digital-packet switching dan standar protokol.
1985 - 1995	• Dimulainya institusi pengelola internet mandiri. • Perkembangan NSFNET dan berbarengan dengan infrastruktur swasta. • Tumbuhnya minat akan PC dan sambungan LAN
1995 - sekarang	• Difusi dari WWW *(World Wide Web)*. • Munculnya jaringan internet yang terprivatisasi dan komersialisasi konten Internet.

Secara historis, dan sampai komputer dibagi menjadi 2 klasifikasi. Yang pertama adalah komputer analog dan yang kedua digital. Kedua klasifikasi komputer ini berkembang seiring zaman. Dan yang kita temui sampai saat ini adalah komputer digital. Kedua jenis komputer ini berbeda baik secara fungsi, fitur dan ukuran. Sedang komputer yang kita gunakan saat ini adalah komputer digital yang pada tahun 1960-an sudah mulai terkoneksi dengan internet.

Internet: Dimulai di Empat Titik

IMP pertama yang beroperasi di awal September 1969 adalah di UCLA *(University of California Los Angeles)*. Pada bulan Oktober disusul IMP di SRI *(Stanford Research Institute)*. Bulan berikutnya, IMP di UCSB *(University of California at Santa Barbara)* beroperasi. Dan IMP keempat yang beroperasi tepat di bulan Desember 1969 adalah di *University of Utah*. Selama 2 bulan, ke 4 komputer saling bertukar dan berkirim pesan dengan baik. Ke 4 komputer yang menjadi node dalam jejaring ARPANET tersebut digambarkan dalam jejaring ARPANET seperti digambarkan dengan grafik di atas.

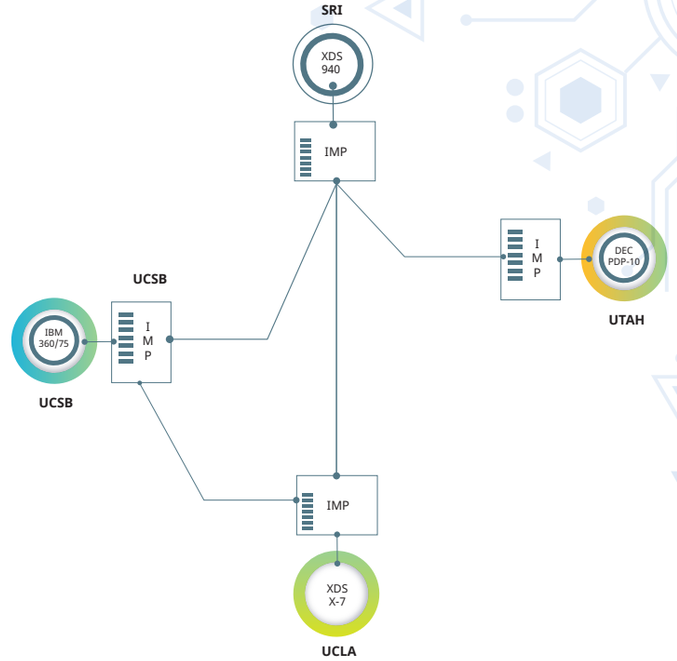


Figure 2. The Initial Four-node ARPANET (1969)

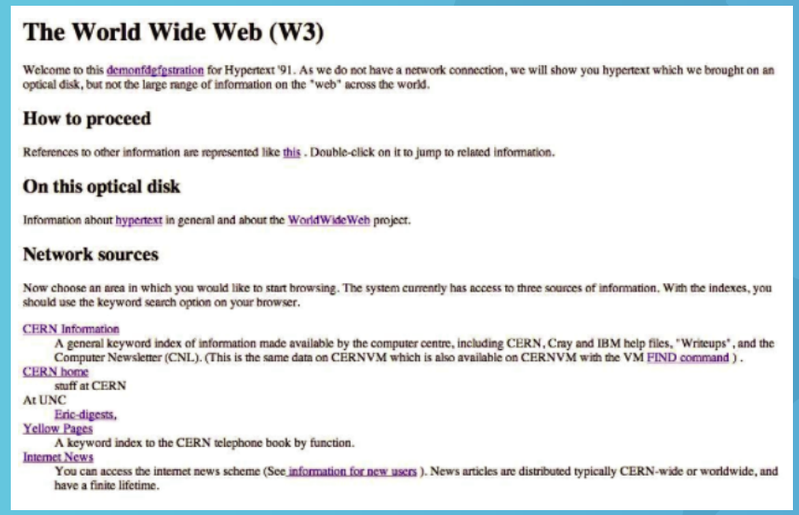
Di akhir tahun 1975, sudah ada 57 node yang beroperasi. Dan pada tahun 1977, sudah ada 111 node yang beroperasi. Gambar dibawah menunjukkan perkembangan ARPANET di A.S sampai tahun 1977. Namun pada tahun 1988, ARPANET akhirnya dinonaktifkan atau dimatikan.

Yuk Tengok Web Pertama di Dunia

Sejak awal tahun 1990-an, *World Wide Web (Web, atau WWW)* tumbuh dengan pesat. Walau pada masa awal pertumbuhan eksponensial ini, masih diwakili dan eksklusif digunakan oleh sektor akademik. Konferensi *World Wide Web* dilangsungkan di CERN *(Conseil Européen pour la Recherche Nucléaire)* di bulan Mei tahun 1994. Konferensi yang diadakan di Genewa

ini dihadiri oleh tokoh dan akademisi yang memiliki pengaruh dalam membangun Web. Konferensi ini juga menjadi pertemuan akbar pertama terkait Web. Dibawah ini adalah penampakan web atau situs internet pertama yang masih ada sampai saat ini. Walau cukup sederhana, namun canggih pada masanya.

Figur penting dalam pengembanan konsep dan implementasi WWW adalah Tim Berners-Lee. Beliaulah yang merancang prototipe awal Web di akhir tahun 1990. Berners-Lee terus mengembangkan Web saat ia bekerja di CERN. Beliau juga yang menetapkan prinsip dasar dari Web yang sampai hari ini masih dianut secara global.



The World Wide Web (W3)

Welcome to this demonfdgfgstration for Hypertext '91. As we do not have a network connection, we will show you hypertext which we brought on an optical disk, but not the large range of information on the "web" across the world.

How to proceed

References to other information are represented like this . Double-click on it to jump to related information.

On this optical disk

Information about hypertext in general and about the WorldWideWeb project.

Network sources

Now choose an area in which you would like to start browsing. The system currently has access to three sources of information. With the indexes, you should use the keyword search option on your browser.

CERN Information
A general keyword index of information made available by the computer centre, including CERN, Cray and IBM help files, "Writeups", and the Computer Newsletter (CNL). (This is the same data on CERNVM which is also available on CERNVM with the VM FIND command) .
CERN home
stuff at CERN
At UNC
Eric-digests,
Yellow Pages
A keyword index to the CERN telephone book by function.
Internet News
You can access the internet news scheme (See information for new users). News articles are distributed typically CERN-wide or worldwide, and have a finite lifetime.

Pertumbuhan Eksponensial Internet

Pada tahun 1999, negara China menempati urutan ke 8. Tetapi Pada tahun 2020 di kuartal ke 1 telah menempati urutan pertama. Disusul dengan negara-negara berkembang lain selain Amerika Serikat. Jika dibandingkan dengan popu-

lasinya tiap negara. Maka persentase paling kecil dari top 15 negara di atas adalah Jepang. Dan perbandingan populasi terbanyak dipegang oleh Bangladesh (94.199%).

Seiring perkembangan internet, implementasinya pun turut tumbuh. Pertumbuhan eksponensial yang disaksikan selama tahun 1990-an menunjukkan potensi yang lebih banyak pada kehidupan manusia. Berbagai area tersebut seperti bisnis, inisiatif sosial, dan fitur aplikasi terus tumbuh mulai saat itu. Walaupun dalam perkembangannya akan menjadi tidak terbatas. Seperti saat ini perkembangan Internet yang diaplikasikan dalam *Internet of Things (IoT)*. Selama perkembangannya, beberapa dari area implementasi dari teknologi Web antara lain:

- Industri pariwisata (pemesanan tiket dan hotel, akomodasi, dsb)
- *E-marketing* (via web, aplikasi dan sosial media)
- *E-commerce* atau on-line shopping (Amazon, Alibaba, dll)
- Situs portal sites (seperti Google, Yahoo, Bing, dll)
- Layanan rekrutmen pekerjaan (Craigslist, LinkedIn, dsb)
- *Internet banking*
- Pelelangan online (eBay)
- Portal berita dan surat kabar digital
- *Platform* sosial media (Facebook dan Twitter)

02 MESIN PENCARIAN INFORMASI, CARA PENGGUNAAN DAN PEMILAHAN DATA

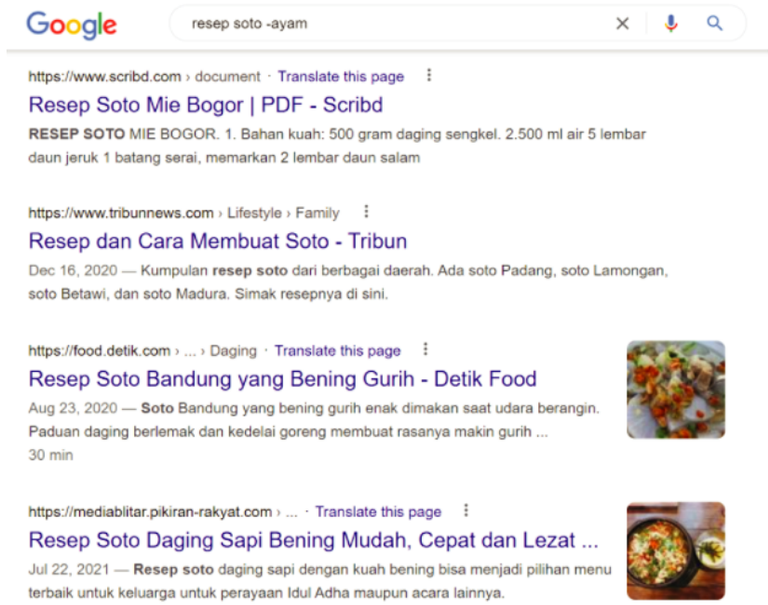
Cara penggunaan mesin pencarian informasi dapat dilakukan dengan mengetik kata kunci *(keyword)* di kolom pencarian, kata kunci dapat berupa satu kata atau lebih. Kemudian klik *enter,* maka berbagai hasil pencarian yang relevan akan muncul. Jika belum menemukan informasi yang dibutuhkan, maka kita dapat kembali ke laman pencarian dan mengubah kata kunci yang lebih sesuai. Mesin pencarian informasi juga menyediakan saran pencarian yang membantu kita menemukan informasi yang dibutuhkan.

Ada kemungkinan kita tidak menemukan informasi yang diharapkan. Hal ini mengindikasikan adanya kemungkinan informasi tersebut memang tidak tersedia atau kata kunci yang kita gunakan kurang sesuai.

Tips Agar Mudah Mendapatkan Informasi Yang Lebih Sesuai

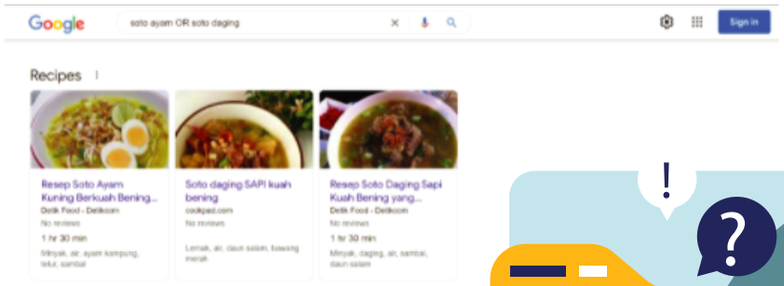
(Gibbs, 2016 & Goodwill Community Foundation, n.d.):

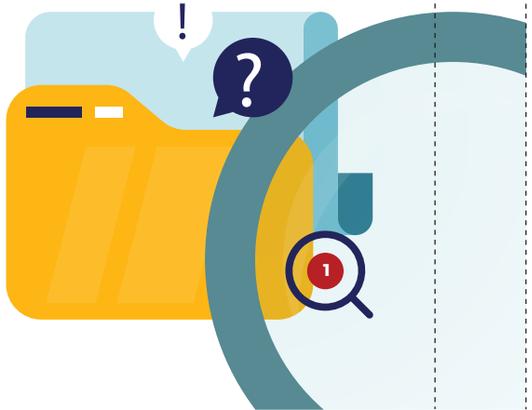
1. Menggunakan karakter tanda hubung (-) untuk menghilangkan kata khusus yang tidak diinginkan, misalnya kita ingin mencari informasi resep masakan selain ayam. Maka setelah mengetik ‘resep masakan -ayam’, seluruh resep selain masakan berbahan ayam akan muncul.



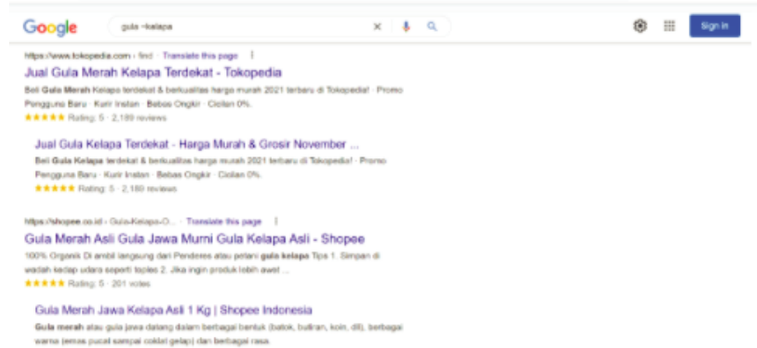
2. Menggunakan karakter tanda petik (“ ”) untuk mencari kata atau frasa yang lebih spesifik. Misalnya, kita ingin mencari informasi resep masakan soto ayam. Maka setelah mengetik ‘resep “soto ayam”’, seluruh resep berbaga i soto ayam akan muncul, bukan seluruh masakan yang mengandung kata ‘soto’ maupun ‘ayam’ saja.

3. Menggunakan istilah OR untuk menemukan salah satu informasi yang dibutuhkan. Misalnya, kita mengetik ‘soto ayam OR soto daging’, maka resep yang muncul adalah soto ayam dan soto daging.

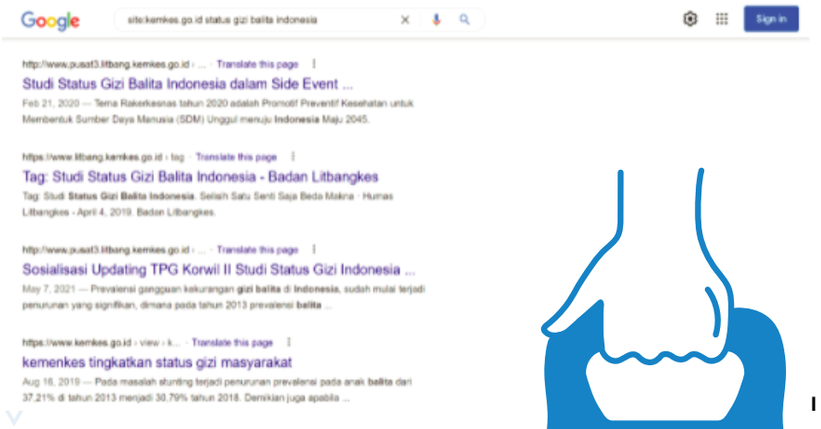




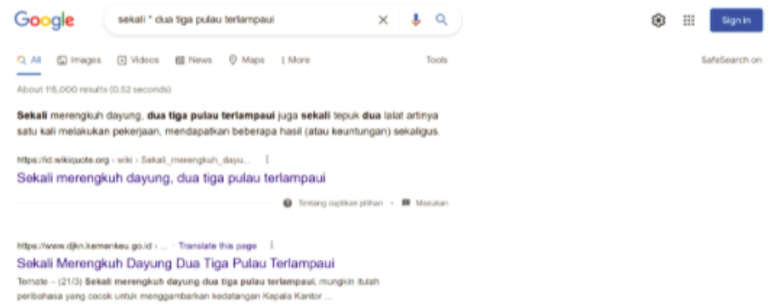
4. Menggunakan sinonim dari kata kunci. Ketika kita masih ragu dengan istilah yang digunakan, kita dapat menggunakan sinonim dari kata tersebut dengan diawali tanda baca *tilde* (~). Misalnya, kita ingin mencari gula merah namun tidak yakin apakah harus mencari gula merah atau gula kelapa, maka dapat menuliskan ‘gula ~kelapa’, maka hasil yang muncul juga akan menampilkan sinonim kata tersebut.



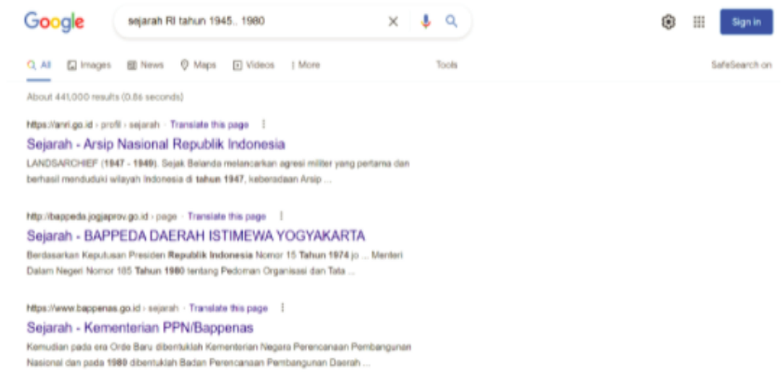
5. Mencari dalam sebuah situs. Misalnya kita ingin mencari informasi mengenai status gizi balita Indonesia, agar data tersebut valid maka kita ingin mencari dari Kementerian Kesehatan RI, maka kita dapat mengetik ‘*site*:kemkes.go.id status gizi balita indonesia’ dan seluruh data yang relevan dari situs Kemenkes RI akan muncul.



6. Menggunakan tanda bintang (*) untuk informasi yang tidak lengkap. Sebagai contoh, kita lupa bagian dari sebuah pribahasa, maka kita dapat mencarinya dengan mengetik ‘sekali * dua tiga pulau terlampaui’



7. Mencari informasi diantara dua nilai menggunakan simbol dua titik (..) dan diakhiri dengan spasi. Contohnya, ketika ingin mencari sejarah Indonesia dari tahun 1945 hingga 1980 maka kita dapat menuliskan ‘sejarah RI tahun 1945.. 1980’ dan hasilnya akan menunjukkan berbagai peristiwa sejarah Republik Indonesia dalam periode tersebut.



Pahami Kelayakan Usia untuk Sebuah Situs dan Aplikasi

Mungkin banyak orang abai terkait fitur pembatasan usia dalam situs atau aplikasi. Hanya karena sebuah situs atau aplikasi populer, mereka sembrono masuk ke situs atau mengunduh aplikasi. Sejatinya, fitur keamanan seperti batasan usia dapat dapat melindungi kita atau anggota keluarga di dunia digital.

Perlu diingat bahwa sebuah situs atau aplikasi untuk remaja mungkin tidak cocok untuk anak berusia lebih muda. Hal ini karena banyak konten di sebuah situs atau aplikasi yang kita tidak sesuai untuk anak-anak. Seperti contohnya anak menonton konten dewasa atau tidak relevan secara di sebuah situs.

Sebaiknya obrolkan dengan anak, anggota keluarga atau teman tentang situs, aplikasi sampai platform media sosial digunakan. Seperti misalnya apa saja yang menarik dalam sebuah platform media sosial. Dan paling penting tentu dengan siapa mereka berinteraksi.

Yang terpenting adalah pemahaman tentang nilai dan tata krama pada interaksi online. Karena hal ini terkait kedewasaan. Sehingga, baik anak, anggota keluarga, atau teman dapat memahami batasan usia pada sebuah situs atau aplikasi.

03 ETIKA BERINTERNET *(NETTIQUETTE)*

Apa Sih Netiket?

Internet bukanlah satu jaringan belaka. Sebaliknya, Internet adalah sekelompok ribuan jaringan individu yang telah memilih untuk memungkinkan lalu lintas melintas di antara mereka. Lalu lintas yang dikirim ke Internet mungkin benar-benar melintasi beberapa jaringan yang berbeda sebelum mencapai tujuannya. Oleh karena itu, pengguna yang terlibat dalam internetworking ini harus menyadari beban yang ditempatkan pada jaringan lain yang berpartisipasi. Sehingga dengan dasar ini, muncullah **netiket *(netiquette).***

Netiket hadir untuk membantu users berkomunikasi lebih efektif saat online. Tentunya juga untuk menghindari kesalahpahaman yang tidak perlu dan potensi konflik. Tanpa pemahaman yang baik tentang *netiquette* kita berisiko menampilkan perilaku negatif. Walau banyak sekali jenis aturan dalam netiket, beberapa aturan umum dalam netiket adalah:

- Hormati privasi orang – Jika seseorang tidak nyaman berbagi informasi dengan kita, cobalah untuk tidak memaksa atau menekan mereka untuk melakukannya. Juga, jangan pernah berbagi informasi pribadi orang lain seperti alamat, nomor telepon atau email tanpa izin karena ini dapat dianggap *doxing.*

- Gunakan bahasa yang baik. Meskipun kita mungkin menganggapnya sebuah kata lucu atau tidak berbahaya, orang lain mungkin dapat tersinggung atau merasa menjengkelkan di dunia nyata yang tak berbatas.

- Jangan suka sarkastik! Sarkasme seringkali tidak dipahami dengan baik di internet!

- Pilih emoji dengan hati-hati - Emoji atau *emoticon* telah menjadi bahasa yang diakui dengan berbagai pemahaman!

- Pastikan bahwa jika kita menggunakan *emoticon* yang sesuai untuk emosi yang disampaikan. Karena salah emoji dapat dengan mudah mengubah konteks seluruh percakapan.

- Menghormati pandangan orang lain. Internet akan menjadi lebih indah jika kita menghargai berbagai pendapat dan keyakinan yang beragam.

Tips Terlindungi Dari Berita Hoaks

Sumber: ***LibGuides at University of West Florida (2021)***

a. Evaluasi, Evaluasi, Evaluasi

Gunakan kriteria berikut ini untuk mengevaluasi sumber:

***1. Currency (*keterbaruan informasi):** Apakah informasi terkini? Bisa saja, misalnya, di Facebook, kita akan mengklik sebuah cerita dan melihat bahwa tanggalnya berasal dari beberapa bulan atau

tahun yang lalu, tetapi teman kita memberikan komentar emosional seolah-olah itu baru saja terjadi.

2. *Relevance* (relevansi): Kriteria ini berlaku jika kita mencari informasi. Apakah informasi yang kita temukan sesuai dengan apa yang dibutuhkan? Sudahkah kita melihat berbagai sumber sebelum memilih informasi ini?

3. *Authority* (Penulis): Siapa penulis/penerbit/sponsor berita? Apakah penulis memiliki maksud tertentu di balik tulisannya?

4. *Accuracy* (Akurasi/Ketepatan): Apakah informasi didukung oleh bukti? Apakah penulis mengutip sumber yang kredibel?

5. Apakah informasi tersebut dapat diverifikasi di tempat lain?

6. *Purpose* (Tujuan): Apa tujuan dari berita tersebut? Provokasi? Untuk menginformasikan? Untuk menjual? Ini dapat memberi kita petunjuk tentang bias yang mungkin terjadi.

b. Google It!

Jika kita menemukan sesuatu melalui media sosial, cobalah untuk mencari di mesin pencari informasi, seperti google, terlebih dahulu! Cobalah telusuri apakah mesin pencari menunjukkan tiga hal berikut:

1. Ada/tidaknya situs berita terkemuka lainnya melaporkan hal yang sama.
2. Ada/tidaknya situs web cek fakta telah membantah klaim tersebut
3. Jika hanya oknum tertentu yang melaporkan klaim tersebut, maka dalam kasus ini, mungkin diperlukan lebih banyak penggalian.

b. Dapatkan Berita dari Sumber Berita

Salah satu cara termudah untuk menghindari jebakan berita palsu adalah dengan membuka langsung situs web berita yang kredibel mengenai berita tersebut. Mengandalkan media sosial untuk melihat apa yang sedang tren semakin mewajibkan kita untuk memverifikasi setiap meme atau artikel berita yang ditemui.

c. Bedakan Opini dengan Fakta

Opini sekarang banyak gunakan dalam sumber berita. Kita mungkin setuju dengan pendapat yang disajikan atau penulis mungkin hanya mengkontekstualisasikan fakta. Namun, kita harus memahami bahwa penulis menyajikan fakta dengan cara yang sesuai dengan agenda mereka dan pikirkan mereka sendiri untuk menarik perhatian pembaca sebanyak mungkin.

Citra Diri di Dunia Digital

Sejatinya pencitraan diri telah lama menjadi kajian. Goffman, seorang sosiolog sekaligus psikolog abad 20 menganalisis interaksi antar-pribadi dan cara orang memposisikan diri dalam proses menampilkan gambaran kepribadian *front*

stage yang sesuai. Maka mereka mendapatkan panggung atau sebuah aksi teatrikal untuk menunjukkan karakteristik personal di hadapan orang. Selama interaksi, orang ini akan mengambil bagian sebagai seorang aktor.

Ketika berada di panggung, seorang aktor tentu akan menyadari cara-cara memahami dari target penonton. Mereka juga menganalisis cara-cara melihat aturan atau norma tertentu dan konvensi sosial agar tidak gagal untuk mencapai tujuan. Seorang aktor pun dapat menggunakan properti (kostum, dekorasi), petanda (karakter atau peranan), dan cerita (narasi) saat mereka tampil. Sehingga cara tersebut tidak menjatuhkan citra atau kepribadian yang ingin mereka ciptakan. Tingkah laku aktor dapat berubah 180 derajat saat dalam ranah pribadi atau di belakang layar *(backstage).*

Dengan kata seseorang dapat menampilkan diri di dunia nyata dan digital secara berbeda. Walau representasi diri secara online juga dibatasi fitur. Namun batasan penggunaan teknologi ini malah memungkinkan fleksibilitas yang terbatas guna mempresentasikan diri pribadi secara online. Banyak orang dapat membuat jenis presentasi online pribadi yang berbeda-beda baik model *front stage* atau *back stage*. Semua tergantung situasi dan kondisi. Walau pada beberapa kasus, representasi diri dapat merugikan orang lain.

Kita Kenal Diri dengan *Digital Presence*

Pengaburan batas antara kehidupan pribadi online dan *offline* telah menghasilkan banyak identitas yang terlihat atau tidak terlihat. Seperti contohnya fungsi kepakaran hingga peran sederhana seseorang. Prosesnya ini secara konstan membentuk rangkaian jejak digital yang didasarkan pada feedback dan input sosial. Seringkali hal ini disebut sebagai digital presence, atau juga jejak digital *(digital footprint).*

Konsep digital *presence* dibagi menjadi dua dimensi.

Para pengguna Internet meninggalkan jejak digital sebagai:

1) *Digital identity.*
2) *Digital self.*

Dimensi pertama mengacu kembali ke korpus atau database jejak digital yang sedang dibangun dengan bantuan platform dan struktur media sosial di dunia digital. Sedang dimensi kedua menyatakan 'saya' di jejaring sosial dan fakta dengan memiliki konteks, refleksi diri, ekspresi diri dan manipulasi diri ideal secara virtual. Namun kedua dimensi ini sering tumpang tindih. Tinggal bagaimana kita mengelola dua dimensi tersebut agar bermanfaat.

Pondasi Dasar Nilai dan Etika di Internet

Kemajuan teknologi seperti internet telah memunculkan apa yang dapat disebut sebagai paradoks teknologi. Di satu sisi, individu dan institusi dalam masyarakat kontemporer sangat bergantung pada inovasi teknologi untuk kemajuan dan

peluang untuk meningkatkan kehidupan manusia dan masyarakat dalam ekonomi, di sisi lain teknologi dapat memiliki konsekuensi anti-manusia terhadap individu mana yang harus membela dan melindungi diri mereka sendiri.

Munculnya Internet menghadirkan peluang dan tantangan yang sangat besar bagi kemanusiaan. Jika kita bekerja untuk melestarikan keterbukaan dan keragamannya, kita dapat memastikan bahwa Net akan digunakan untuk mengubah kondisi manusia menjadi lebih baik, dan dapat mencegah atau mengurangi konsekuensi yang kurang diinginkan.

Dan secara umum, internet sendiri memiliki nilai-nilai sebagai berikut:

- Net menghubungkan kita semua bersama-sama.
- Net harus terbuka dan tersedia untuk semua.
- Pengguna net memiliki hak untuk berkomunikasi.
- Pengguna bersih memiliki hak privasi.
- Orang-orang adalah pengurus Net, bukan pemiliknya.
- Tata kelola Net harus terbuka dan inklusif.
- Jaring harus mencerminkan keragaman manusia, bukan homogenisasi itu.

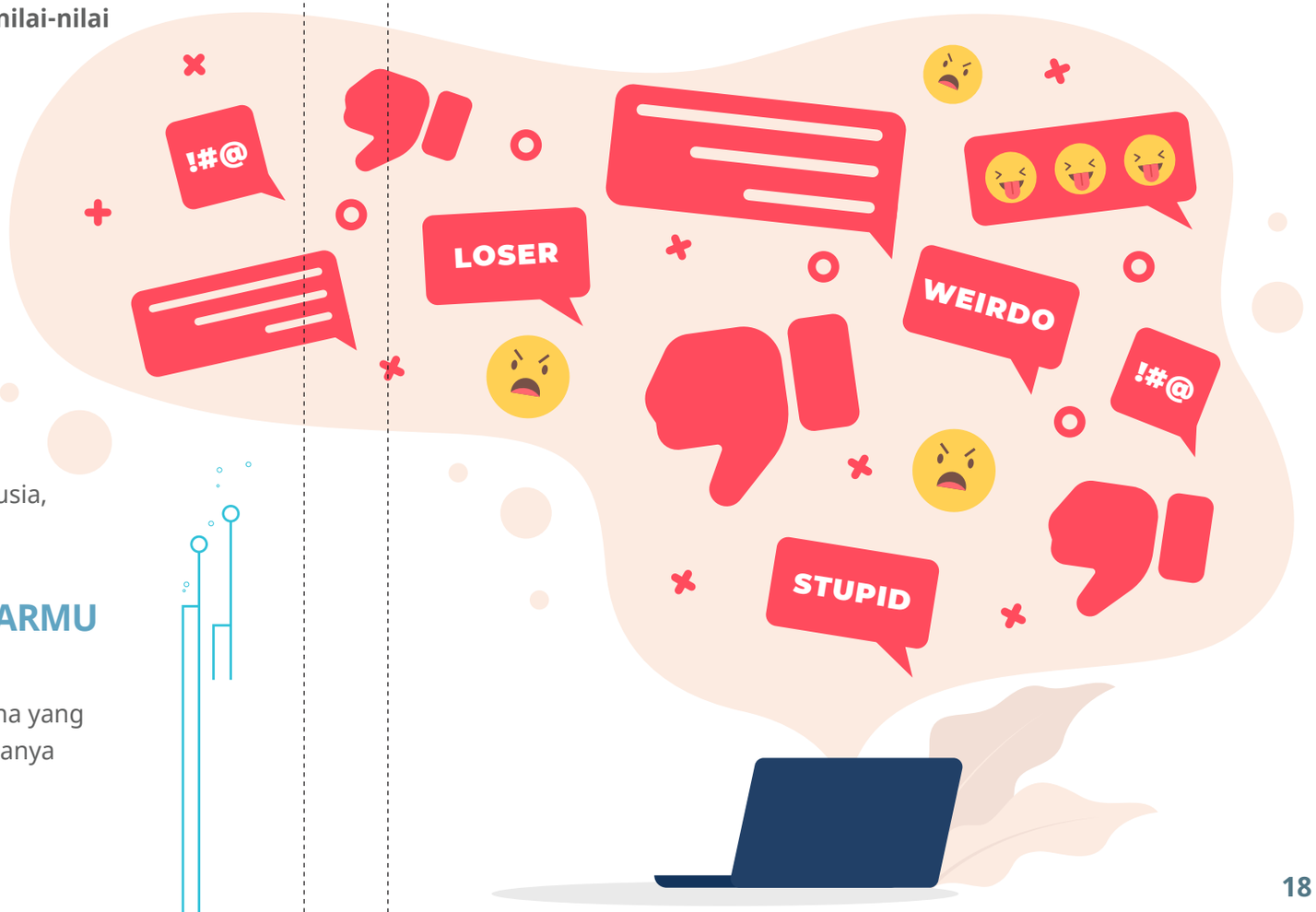
04 KENALI *CYBERBULLYING* DI SEKITARMU

Kita mungkin kesulitan untuk membedakan mana yang disebut sebagai perundungan dan mana yang hanya

candaan tersebut telah melewati batas. Ketika kita meminta lawan bicara untuk berhenti namun mereka tetap mengutarakan candaan tersebut kita merasa tidak nyaman, artinya ini tergolong bullying. Sementara jika hal tersebut terjadi di dunia maya, maka disebut sebagai ***cyberbullying.***

Jika kita mengalami perundungan terjadi di media sosial, maka kita hal yang dapat kamu lakukan adalah:

1. Melaporkan postingan tersebut di sosial media karena seluruh media sosial berkewajiban menjaga penggunanya tetap nyaman berinteraksi.



2. Jika perundungan tersebut membahayakan, segeralah menghubungi polisi.
3. Cobalah mengambil gambar *(screen capture)* bukti perundungan jika sewaktu-waktu dibutuhkan saat melapor.

Waspada Cyberbullying (Perundungan Siber) dan Jenisnya

Cyberbullying merupakan perilaku merisak orang lain dalam komunikasi dunia digital. Aktivitas ini didasari ketimpangan kekuatan dan pengaruh *(power & influence)* yang nyata. Perilaku ini pada umumnya diulang dari waktu ke waktu. Konsekuensinya, tercipta situasi yang sulit bagi korban untuk dapat menghindar.

Contoh *cyberbullying* yang umum dilakukan antara lain:

- Mengirim pesan yang mendiskreditkan secara individual atau dalam grup.
- Mendorong orang untuk melukai diri sendiri di media sosial.
- Secara verbal memaki pengguna lain secara online.
- Menggunakan teknologi digital untuk mengucilkan atau menyudutkan orang lain.

Tanda-tanda dari orang yang terkena *cyberbullying* antara lain:

- Menyembunyikan atau mematikan layar *smartphone*/laptop/PC dengan cepat saat orang lain hadir.
- Menjadi orang yang ragu-ragu untuk menjelaskan apa dilakukan di *platform* media sosial atau *game online.*
- Sangat jarang menggunakan gawai atau malah enggan menggunakannya sama sekali.

Perundungan siber bisa saja menimpa kita. Semua orang pasti membuat kesalahan. Aktivitas berikut dapat menjadi menjadi solusi bagi korban *cyberbullying.* Dan yang lebih penting membuat kita waspada.

- Diskusikan pentingnya reputasi atau jejak digital dan sopan santun (netiket) dengan anggota keluarga, saudara, atau teman.
- Tinjaulah kembali peraturan terkait penggunaan perangkat dan pertimbangkan konsekuensi yang lebih ketat terkait akses gawai dan internet.
- Atur kembali fitur fitur keamanan perangkat dan pan taulah secara teliti orang terdekat kita agar tidak menyalahi netiket.

Waspada Online Grooming?

Bukan tidak mungkin kita, anggota keluarga, atau teman bertemu orang lain secara *online*. Sayangnya mereka urung mengatakan kepada kita hal ini. Tak disangka, mereka mengalami online grooming.

Online grooming adalah aktivitas pertemanan dengan orang lain demi keuntungan finansial bahkan tujuan seksual. Para pelaku grooming (*groomer*) kadang tidak hanya menggunakan media sosial untuk menjalankan aksinya. Mereka juga merambah aplikasi chat, komunitas online bahkan *game online.*

Para *groomer online* ini terkadang orang yang tidak selalu asing bagi kita. Kadang para pelaku sudah pernah bertemu dengan kita. Modus groomer pada umumnya menggunakan internet untuk membangun hubungan personal. Mereka membuat korban seolah-olah sebagai kekasih atau pacar mereka.

Para *groomer online* umumnya menggunakan profil palsu. Dengan ini mereka mencoba untuk mendapatkan kepercayaan. Mereka juga berpura-pura memiliki minat yang sama, menawarkan hadiah dan mengatakan hal-hal baik, walau berpura-pura belaka.

Begitu *groomer* mendapat kepercayaan, mereka akan mengarahkan percakapan ke arah perilaku dan pengalaman seksual. Mereka akan meminta untuk mengirim foto atau video asusila. Lalu kadang mereka ingin bertemu langsung. Tak jarang juga mereka akan memeras dengan mengancam untuk berbagi gambar atau video asusila korban dengan keluarga dan teman-teman anak di medsos.

Yuk kita lebih waspada pada online grooming. Obrolkan dengan anggota keluarga, saudara, dan teman isu ini. Sehingga kita dan mereka dapat terhindar dari perilaku menyimpang ini di dunia digital.

Mengapa Harus ada Ujaran Kebencian?

Ketika kita menemukan konten yang mengandung ujaran kebencian terhadap seseorang/organisasi/kelompok tertentu, Damar Juniarto dari Forum Demokrasi Digital yang dilansir dalam BBC.com (2015) menyampaikan bahwa kita dapat berperan aktif untuk menyampaikan kepada pengunggah bahwa konten yang disebarkan mengandung ujaran kebencian yang akan menyulut emosi banyak pihak dan tidak menyelesaikan masalah yang dimaksud. Selanjutnya kita juga dapat mengingatkan bahwa ia bisa dijerat UU ITE, UU No. 40 Tahun 2008 tentang Diskriminasi Rasial, dan aturan lain yang relevan. Jika tidak digubris juga, maka kita dapat melaporkan dan memastikan bahwa orang lain mengetahui bahwa akun tersebut merupakan akun penyebar ujaran kebencian (bisa dengan mengambil gambar bukti *(screenshot)* dan menginfokan pada orang lain).

Medsos Sebagai Cermin Diri

Banyak orang menggunakan media sosial karena beberapa alasan. Pertama, untuk terhubung ke lingkungan kekerabatannya sendiri. Kedua untuk menjadi bagian dari sebuah jaringan pertemanan besar. Ketiga untuk mendapatkan dukungan sosial atau bahkan untuk memperkuat reputasi kepakaran. Selain itu users juga menggunakan platform media, seperti Facebook, Twitter, Google, dll sosial nyaris tanpa biaya. Namun, users secara sukarela memberikan data pribadi mereka untuk mengikuti pola periklanan dan pemasaran para penyedia *platform*. Dan dalam konteks ini menjaga data pribadi dan privasi patut menjadi perhatian.

Walau pada hakikatnya situs web komunitas sosial atau platform sosmed merupakan contoh umum yang telah meningkatkan konektivitas antar manusia sebagai gaya hidup aktual dan juga membantu jejaring sosial luas dari ikatan yang rentan *(weak ties)*. Ikatan rentan ini seperti ikatan pertemanan antar rekan kerja atau seorang kenalan.

Tak jarang dalam *weak ties* ini kita menjadi bermacam-macam pribadi. Karena bagi banyak users, pembentukan antara

karakter khusus dan berbeda semata-mata ditujukan untuk rekan kerja dan menarik minat pemberi kerja. Sehingga hal ini menjadi simbol pertukaran verbal diri seseorang terhadap 'teman online'. Sehingga, ada baiknya bentuk-bentuk kepribadian cermin diri di sosmed ini tidak tumpang tindih di dunia nyata.

05 MARI BIJAK BERTRANSAKSI

Di balik kemudahan bertransaksi daring, terdapat bahaya yang mengintai, misalnya . Oleh sebab itu, kita sebagai pengguna harus lebih bijak dalam menggunakan transaksi ini dengan menjalankan tips dari **Young Americans : Centre for Financial Education (n.d) dan Goodwill Foundation (n.d) berikut ini:**

a. Periksalah koneksi https, artinya situs web menggunakan koneksi yang aman bagi data pribadi yang kita masukkan
b. Meneliti akun penjual. Kita dapat meneliti dari nomor telepon yang mungkin dapat dihubungi jika kita mengalami kendala saat bertransaksi. Selain itu, kita juga dapat menelitinya dari ulasan pembeli sebelumnya
c. Menggunakan metode pembayaran yang aman. Sebaiknya hindari pembayaran transfer langsung ke rekening penjual.
d. Kartu kredit dapat menjadi pilihan yang paling aman, jika kita tidak mau membagikan nomor kartu ke banyak penjual, maka kita bisa menggunakan jasa pembayaran seperti Paypal, Google Wallet, dan sebagainya.
e. Simpan riwayat transaksi, termasuk diantaranya tanggal, nomor transaksi, deskripsi, harga produk, hingga riwayat surel transaksi. Hal ini mungkin berguna saat terjadi kendala.
f. Hindari memberikan password, kode OTP, dan data penting lainnya kepada siapapun.
g. Jangan gunakan tanggal lahir, nomor ponsel, nama teman/hewan/saudara sebagai kata sandi.
h. Berhati-hati dengan pesan scam melalui surel (yang terkadang disertai tautan tertentu) dan situs web yang mencurigakan.
i. Berhati-hati menggunakan komputer umum yang digunakan

untuk transaksi online. Pastikan tidak meninggalkan komputer tanpa pengawasan saat transaksi dan segera logout akun setelah bertransaksi.

Identitas Online Palsu untuk Menipu, Waspadalah

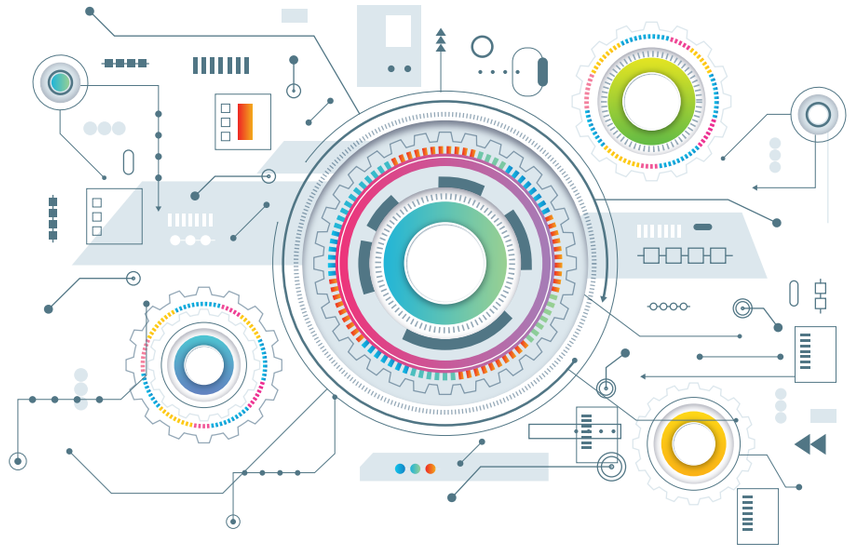
Penipuan identitas adalah penggunaan informasi yang dicuri dari orang secara sengaja dan terencana. Kejahatan ini mempengaruhi individu yang identitasnya telah dicuri dan bisnis di mana identitas yang dicuri telah digunakan untuk melakukan transaksi penipuan. Selain itu, identitas palsu yang digunakan tidak harus dari seseorang yang hidup, atau bahkan nyata. Pencuri sering berasumsi identitas almarhum atau membuat identitas palsu orang-orang yang tidak pernah ada untuk melakukan kejahatan. **Beberapa contoh penipuan dengan identitas online palsu yaitu:**

- Penipuan kartu kredit: Menggunakan kartu kredit atau nomor kartu kredit orang lain untuk melakukan pembelian penipuan
- Pekerjaan atau penipuan terkait pajak: Menggunakan nomor Jaminan Sosial orang lain dan informasi pribadi lainnya untuk mendapatkan pekerjaan atau mengajukan pengembalian pajak penghasilan
- Penipuan telepon atau utilitas: Menggunakan informasi pribadi orang lain untuk membuka ponsel atau akun utilitas
- Penipuan bank: Menggunakan informasi pribadi orang lain untuk mengambil alih akun keuangan yang ada atau untuk membuka akun baru atas nama orang lain
- Penipuan pinjaman atau sewa: Menggunakan informasi pribadi orang lain untuk mendapatkan pinjaman atau sewa
- Dokumen pemerintah atau penipuan manfaat: Mengguna kan informasi pribadi orang lain untuk mendapatkan man faat pemerintah

06 FITUR PROTEKSI PERANGKAT KERAS

Kita tahu bahwa sebuah sistem komputer berisi perangkat keras seperti prosesor, monitor, RAM dan banyak lagi, dan satu hal yang sistem operasi memastikan bahwa perangkat tersebut tidak dapat diakses langsung oleh pengguna. Pada dasarnya, perlindungan perangkat keras dibagi menjadi 3 kategori: perlindungan CPU, Perlindungan Memori, dan perlindungan I/O.

Hal-hal tersebut dijelaskan sebagai berikut di bawah ini.



1. CPU Protection

Perlindungan CPU harus diperhatikan karena kita tidak dapat memberikan CPU ke suatu proses selamanya, itu harus untuk beberapa waktu yang terbatas jika tidak, proses lain tidak akan mendapatkan kesempatan untuk menjalankan proses. Maka untuk itu, timer digunakan untuk mengatasi situasi ini. yang pada dasarnya memberikan waktu tertentu untuk suatu proses dan setelah timer dieksekusi, sebuah sinyal akan dikirim ke proses untuk meninggalkan CPU. maka proses tidak akan menahan CPU lebih lama.

Kita harus memastikan bahwa sistem operasi mempertahan-kan kendali. Kita harus mencegah program pengguna terjebak dalam infinite loop atau tidak memanggil layanan sistem, dan tidak pernah mengembalikan kontrol ke sistem.

operasi. Untuk mencapai tujuan ini, kita dapat menggunakan

timer. Timer dapat diatur untuk menginterupsi komputer setelah jangka waktu tertentu. Periodenya bisa tetap atau berubah-ubah. Pengatur waktu variabel umumnya diimplementasikan oleh jam tingkat tetap dan penghitung. Sistem operasi mengatur penghitung. Setiap kali jam berdetak, penghitung dikurangi. Ketika penghitung mencapai 0, interupsi terjadi.

Sebelum menyerahkan kendali kepada pengguna, sistem operasi memastikan bahwa pengatur waktu diatur untuk menyela. Jika penghitung waktu menyela, kontrol ditransfer secara otomatis ke sistem operasi, yang dapat memperlakukan interupsi sebagai kesalahan fatal atau dapat memberi program lebih banyak waktu. Jelas, instruksi yang mengubah operasi timer adalah hak istimewa. Dengan demikian, kita dapat menggunakan timer untuk mencegah program pengguna berjalan terlalu lama. Teknik sederhana adalah menginisialisasi penghitung dengan jumlah waktu yang diizinkan untuk dijalankan oleh suatu program.

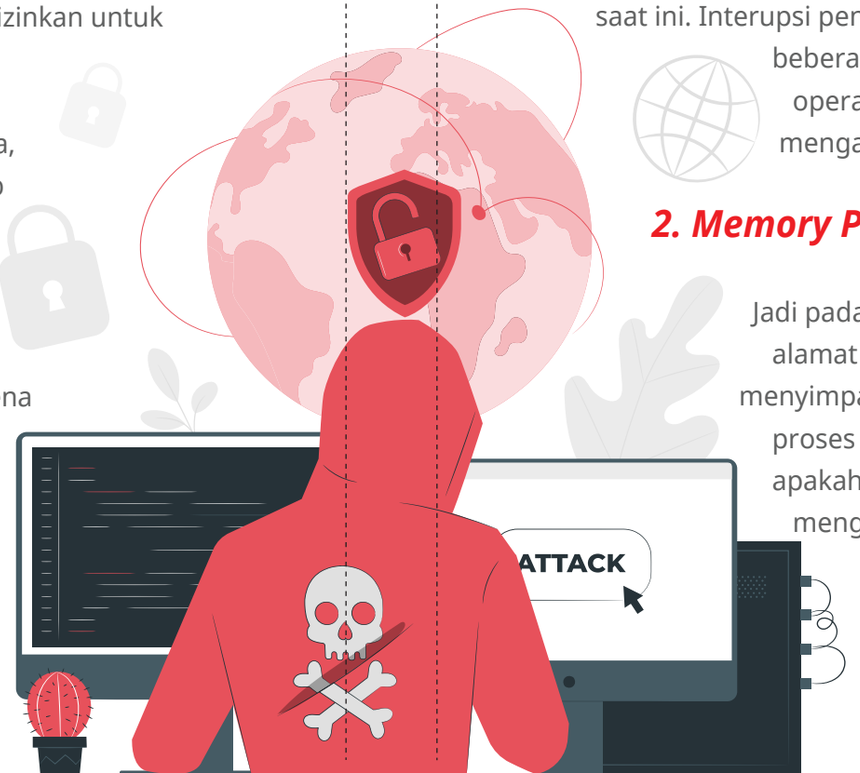
Program dengan batas waktu 7 menit, misalnya, penghitungnya akan diinisialisasi ke 420. Setiap detik, penghitung waktu terputus dan penghitung dikurangi 1. Selama penghitung positif, kontrol dikembalikan ke program pengguna . Ketika penghitung menjadi negatif, sistem operasi menghentikan program karena melebihi batas waktu yang ditentukan.

Penggunaan timer yang lebih umum adalah untuk mengimplementasikan pembagian waktu. Dalam kasus yang paling sederhana, pengatur waktu dapat diatur untuk

menginterupsi setiap N milidetik, di mana N adalah irisan waktu yang diizinkan untuk dieksekusi oleh setiap pengguna sebelum pengguna berikutnya mendapatkan kendali atas CPU.

Sistem operasi dipanggil pada akhir setiap irisan waktu untuk melakukan berbagai tugas pemeliharaan, seperti menambahkan nilai N ke catatan yang menentukan (untuk tujuan akuntansi) jumlah waktu yang telah dijalankan oleh program pengguna sejauh ini. Sistem operasi juga menyimpan register, variabel internal, dan buffer, dan mengubah beberapa parameter lain untuk mempersiapkan program berikutnya untuk dijalankan. Prosedur ini dikenal sebagai saklar konteks. Mengikuti saklar konteks, program berikutnya melanjutkan eksekusinya dari titik di mana ia tinggalkan (ketika irisan waktu sebelumnya habis).

Penggunaan lain dari timer adalah untuk menghitung waktu saat ini. Interupsi pengatur waktu memberi sinyal berlalunya beberapa periode, memungkinkan sistem operasi menghitung waktu saat ini dengan mengacu pada beberapa waktu awal.



2. Memory Protection

Jadi pada dasarnya Bare register menyimpan alamat awal program dan membatasi register menyimpan ukuran proses, sehingga ketika suatu proses ingin mengakses memori maka diperiksa apakah dapat mengakses atau tidak dapat mengakses memori.

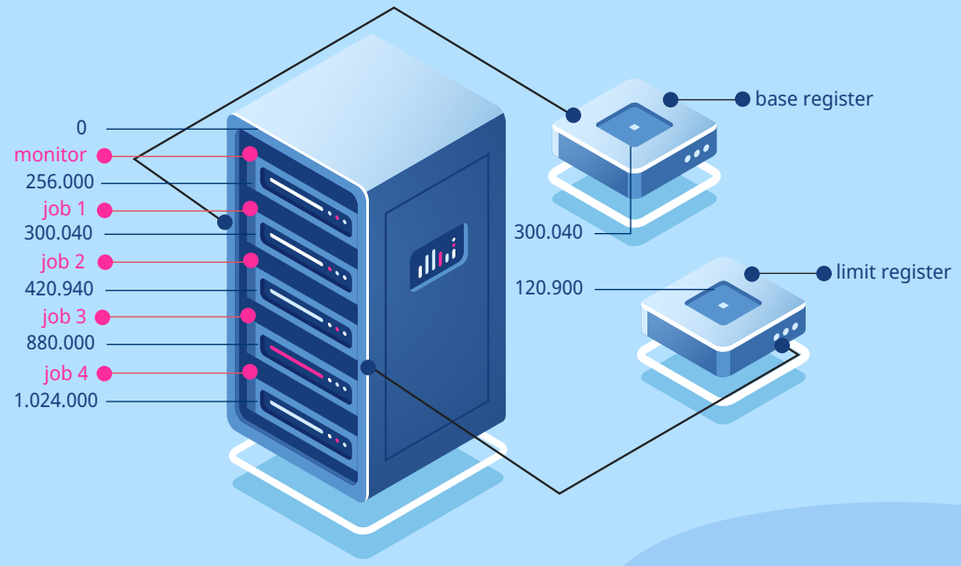
Untuk memastikan operasi yang benar, kita harus melindungi vektor interupsi dari modifikasi oleh program pengguna. Selain itu, kita juga harus melindungi rutin layanan interupsi di sistem operasi dari modifikasi. Bahkan jika pengguna tidak mendapatkan kontrol yang tidak sah dari komputer, memodifikasi rutinitas layanan interupsi mungkin akan mengganggu operasi yang tepat dari sistem komputer dan spooling dan bufferingnya.

Kita kemudian melihat bahwa kita harus memberikan perlindungan memori setidaknya untuk vektor interupsi dan rutinitas layanan interupsi dari sistem operasi. Secara umum, kami ingin melindungi sistem operasi dari akses oleh program pengguna, dan, di samping itu, untuk melindungi program pengguna dari satu sama lain. Perlindungan ini harus disediakan oleh perangkat keras.

Untuk memisahkan ruang memori setiap program, kita memerlukan kemampuan untuk menentukan kisaran alamat resmi yang dapat diakses oleh program, dan untuk melindungi memori di luar ruang tersebut. Kita dapat memberikan perlindungan ini dengan menggunakan dua register,

Dalam perlindungan memori, kita berbicara tentang situasi itu ketika dua atau lebih proses berada dalam memori dan satu proses dapat mengakses memori proses lainnya dan untuk mencegah situasi ini kami menggunakan dua register sebagai:

a. Bare Register
b. Limit Register



Basis dan register batas menentukan ruang alamat logis

(Sumber: https://qu.edu.iq/cm/wp-content/uploads/2014/12/lec7.pdf)

Register dasar menyimpan alamat memori fisik legal terkecil; register batas berisi ukuran rentang. Misalnya, jika register dasar menampung 300040 dan register batas adalah 120900, maka program dapat secara legal mengakses semua alamat dari 300040 hingga 420940 inklusif.

Perlindungan ini dilakukan oleh perangkat keras CPU yang membandingkan setiap alamat yang dihasilkan dalam mode pengguna dengan register. Upaya apapun oleh program yang mengeksekusi dalam mode pengguna untuk mengakses memori monitor atau memori pengguna lain menghasilkan jebakan ke monitor, yang memperlakukan upaya tersebut sebagai kesalahan fatal. Skema ini mencegah program pengguna memodifikasi kode atau struktur data baik sistem operasi atau pengguna lain.

Register dasar dan batas dapat dimuat hanya oleh sistem operasi, yang menggunakan instruksi istimewa khusus. Karena instruksi yang diistimewakan dapat dieksekusi hanya dalam mode monitor, dan karena hanya sistem operasi yang mengeksekusi dalam mode monitor, hanya sistem operasi yang dapat memuat register dasar dan batas. Skema ini memungkinkan monitor untuk mengubah nilai register, tetapi mencegah program pengguna mengubah isi register.

Sistem operasi, yang dijalankan dalam mode monitor, diberikan akses tak terbatas ke monitor dan memori pengguna. Ketentuan ini memungkinkan sistem operasi untuk memuat program pengguna ke dalam memori pengguna, membuang program terse-but jika terjadi kesalahan, untuk mengakses dan mengubah parameter panggilan sistem, dan seterusnya.

3. I/O Protection

Jadi ketika kita memastikan perlindungan I/O maka beberapa kasus tidak akan pernah terjadi di sistem seperti:
Terminasi I/O dari proses lain
Lihat I/O dari proses lain
Memberikan prioritas pada proses tertentu I/O

Program pengguna dapat mengganggu operasi normal sistem dengan mengeluarkan instruksi I/O ilegal, dengan mengakses lokasi

memori di dalam sistem operasi itu sendiri,atau dengan menolak melepaskan CPU. Kami dapat menggunakan berbagai mekanisme untuk memastikan bahwa gangguan tersebut tidak dapat terjadi di sistem.

Untuk mencegah pengguna melakukan I/O ilegal, kami mendefinisikan semua instruksi I/O sebagai instruksi yang diistimewakan. Dengan demikian, pengguna tidak dapat mengeluarkan instruksi I/O secara langsung; mereka harus melakukannya melalui sistem operasi. Agar perlindungan I/O menjadi lengkap, kita harus yakin bahwa program pengguna tidak akan pernah bisa mengendalikan komputer dalam mode monitor. Jika bisa, proteksi I/O bisa dikompromikan.

Pertimbangkan komputer yang mengeksekusi dalam mode pengguna. Ini akan beralih ke mode monitor setiap kali interupsi atau jebakan terjadi, melompat ke alamat yang ditentukan dari vektor interupsi. Jika program pengguna, sebagai bagian dari eksekusinya, menyimpan alamat baru dalam vektor interupsi, alamat baru ini dapat menimpa alamat sebelumnya dengan alamat dalam program pengguna.

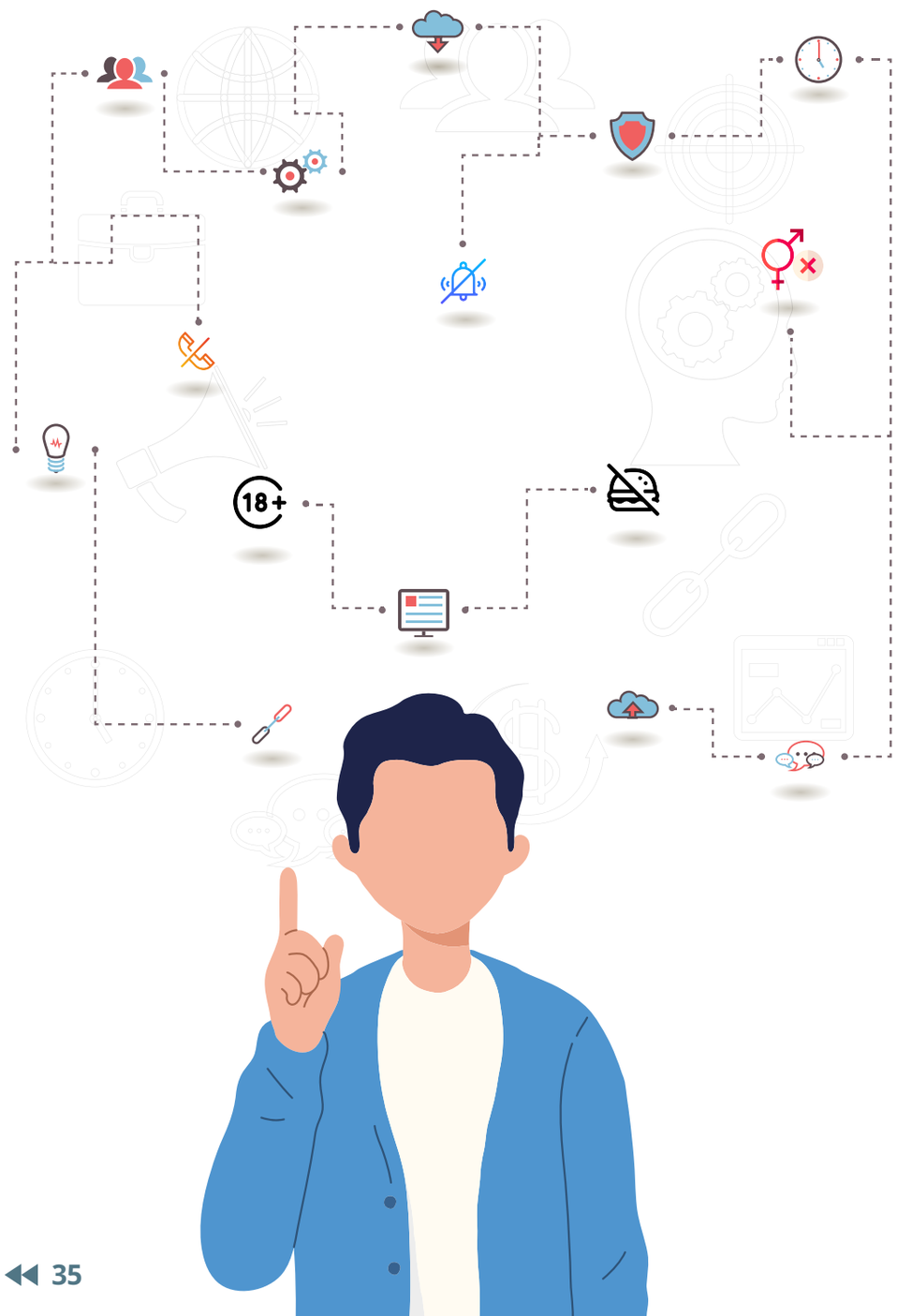
Kemudian, ketika jebakan atau interupsi yang sesuai terjadi, perangkat keras akan beralih ke mode monitor, dan akan mentransfer kontrol melalui vektor interupsi (dimodifikasi) ke program pengguna! Program pengguna dapat mengontrol komputer dalam mode monitor. Bahkan, program pengguna dapat mengontrol komputer dalam mode monitor dengan banyak cara lain. Sistem operasi, mengeksekusi dalam mode monitor, memeriksa apakah permintaan itu valid dan (jika permintaan itu valid) melakukan I/O yang diminta. Sistem operasi kemudian kembali ke pengguna.

Ini Aturan Terbaik Terkait Perangkat dan Penggunaannya

Sebaiknya kita tak perlu ragu dalam menetapkan batasan dan aturan pada perangkat digital. Baik pada diri kita atau anggota keluarga misalnya. Penggunaan perangkat digital sebaiknya memiliki batas yang wajar. Screentime atau durasi saat menatap layar menjadi kunci pembatasan ini.

Batasi *screentime* pada aktivitas dan kebiasaan berikut ini:

- Pertama, tidak ada yang menggunakan perangkat saat makan.



- Hindari menggunakan *smartphone* sebelum tidur.
- Tetapkan hukuman bila terjadi pelanggaran jika terkait anggota keluarga, misalnya tidak mendapatkan jatah uang mingguan.
- Perlu sifat tegas terkait tentang sanksi yang akan didapat baik untuk diri sendiri atau orang lain.

Perangkat aturan secara lisan atau tertulis ini sejatinya dapat mendukung hubungan saling percaya. Batasan ini juga dapat membantu menjaga fokus dan aktivitas yang kita lakukan. Dan juga penting, aturan ini memastikan waktu tidur mereka tidak terganggu notifikasi perangkat. Atau malah begadang menjelajah internet tanpa kejelasan.

Pahami Kelayakan Usia untuk Sebuah Situs dan Aplikasi

Mungkin banyak orang abai terkait fitur pembatasan usia dalam situs atau aplikasi. Hanya karena sebuah situs atau aplikasi populer, mereka sembrono masuk ke situs atau mengunduh aplikasi. Sejatinya, fitur keamanan seperti batasan usia dapat dapat melindungi kita atau anggota keluarga di dunia digital.

Perlu diingat bahwa sebuah situs atau aplikasi untuk remaja mungkin tidak cocok untuk anak berusia lebih muda. Hal ini karena banyak konten di sebuah situs atau aplikasi yang kita tidak sesuai untuk anak-anak. Seperti contohnya anak menonton konten dewasa atau tidak relevan secara di sebuah situs.

Sebaiknya obrolkan dengan anak, anggota keluarga atau teman tentang situs, aplikasi sampai platform media sosial

digunakan. Seperti misalnya apa saja yang menarik dalam sebuah platform media sosial. Dan paling penting tentu dengan siapa mereka berinteraksi.

Yang terpenting adalah pemahaman tentang nilai dan tata krama pada interaksi online. Karena hal ini terkait kedewasaan. Sehingga, baik anak, anggota keluarga, atau teman dapat memahami batasan usia pada sebuah situs atau aplikasi.

Proteksi Perangkat Digitalmu Sekarang!

Setiap perangkat lunak umumnya memiliki cara melindungi penggunanya masing-masing sesuai kebijakan perusahaan pengembangnya. Sistem operasi dalam gawai yang kita gunakan pun memiliki kebijakan masing-masing. Berikut ini merupakan tips untuk melindungi gawai kita dari virus, peretas, maupun pengintai ***(State of California Department of Justice, n.d):***

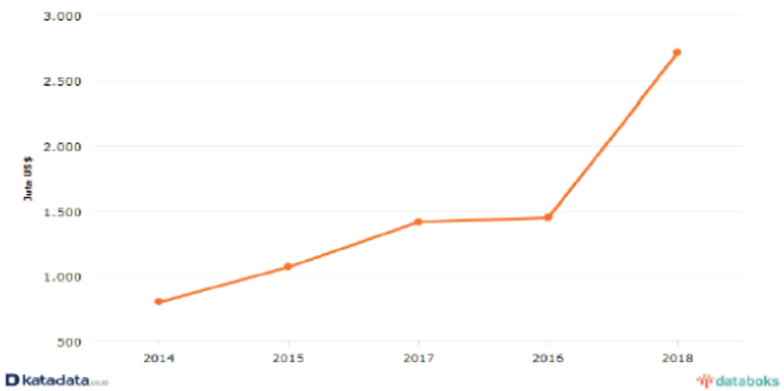
a. Perbarui sistem operasi dan aplikasi penting secara berkala, kegiatan ini dapat meminimalisir kecacatan aplikasi yang mempermudah peretas mencuri data kita.
b. Gunakan *antivirus* secara rutin untuk menelusuri seluruh file dalam gawai kita dan memeriksa apakah ada dokumen yang mencurigakan
c. Gunakan *antispyware* untuk melindungi

aktivitas gawai kita. Beberapa antivirus sudah memasukkan fitur ini. Tanda bahwa gawai kita terkena *spyware* yakni, tiba-tiba gawai kita dipenuhi banyak iklan, terpindah ke websita yang tidak kita inginkan, dan kecepatan beroperasi gawai yang semakin melambat.
d. Gunakan *firewall* untuk memutuskan komunikasi ke dan dari sumber yang tidak kita setujui (misalnya telepon iseng).
e. Gunakan kata sandi yang kuat, misalnya menggunakan huruf pertama dari sebuah frase yang mudah kita ingat, contoh It@tTd--Indonesia tanah airku tanah tumpah darahku.
f. Gunakan kata sandi yang unik khususnya untuk transaksi, sosial media, dan surel.
g. Gunakan verifikasi tambahan, misalnya pemindai sidik jari dan wajah
h. Berhati-hati dengan apa yang kita klik. Misalnya, jika kita mendapat surel yang menyatakan bahwa akun perbankan kita terkunci dan mem-
in- ta kita memasukkan kata sandi, segera pikir ulang untuk mengikuti perintah surel tersebut. Hubungi bank melalui nomor resmi dan pastikan kebenaran surel tersebut karena, umumnya, bank tidak pernah meminta kata sandi maupun data pribadi secara langsung.
i. Berhati-hati saat belanja *daring*, pastikan
situs belanja tersebut aman dan terpercaya sebelum memasukkan data pribadi dan nomor kartu kredit.
j. Berhati-hati dengan apa yang kita publikasikan. Bisa saja saat mengunggah sebuah konten, kita tidak sengaja mempublikasikan informa-

si personal.

Merespon informasi data bocor. Data kita bisa jadi bocor ke pihak yang tidak bertanggung jawab. Misalnya, jika kita mendapatkan informasi kebocoran data yang mengandung nomor kartu kredit kita, segera bekukan akun untuk menghindari peretas menggunakan kartu kredit kita.

07 WASPADA PENIPUAN DIGITAL



Kerugian dari Kejahatan Dunia Maya yang Dilaporkan IC3 2014-2018

Sumber: Statista, 9 Juli 2019

Kominfo meminta masyarakat untuk mewaspadai ragam modus penipuan online yang biasanya terjadi di ruang digital, seperti *phising, pharming, sniffing, money mule,* dan *social engineering.*

Bagaimana cara mereka bekerja? Yuk simak penjelasan singkat berikut ini:

1. Modus penipuan berupa ***phising*** dilakukan oleh oknum yang mengaku dari lembaga resmi dengan menggunakan telepon, email atau pesan teks.

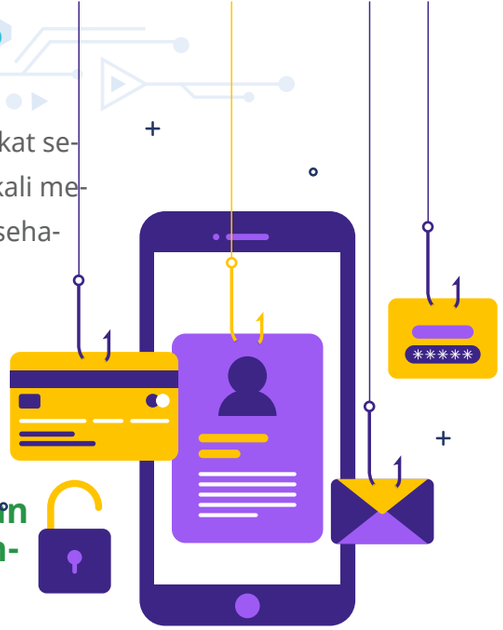
2. Phraming *hand-phone,* yakni penipuan dengan modus mengarahkan mangsanya kepada situs web palsu dimana entri domain *name system* yang ditekan/di-*click* korban akan tersimpan dalam bentuk *cache.*

3. Sniffing, yakni oknum pelaku akan meretas untuk mengumpulkan informasi secara illegal lewat jaringan yang ada pada perangkat korbannya dan mengakses aplikasi yang menyimpan data penting pengguna.

4. Money Mule, yakni penipuan jenis ini misalnya ada oknum yang meminta korbannya untuk menerima sejumlah uang ke rekening untuk nantinya ditransfer ke rekening orang lain. Money mule ini biasanya ditanyakan pelaku dengan calon korban, maukah dapat hadiah atau pajaknya dikirim dulu. Jadi, sekarang itu masyarakat perlu berhati-hati karena money mule ini digunakan untuk money laundry atau pencucian uang. “Kamu akan saya kirim uang, tapi harus transfer balik ke rekening ini”. Penipuan ini sering terjadi di masyarakat dan banyak yang tertipu karena sudah bahagia dulu sehingga tidak memiliki waktu untuk berpikir jernih.

5. Social engineering, yakni pelaku memanipulasi psikologis korban hingga tidak sadar memberikan informasi penting dan sensitif yang kita miliki. Pelaku mengambil kode OTP atau *password* karena sudah memahami behavior targetnya.

Dengan kata lain, masyarakat seringkali tidak sadar seringkali membagikan data-data yang seharusnya perlu dijaga



Aktivitas transaksi di ruang digital dapat menimbulkan seseorang melakukan tindak kejahatan berupa penipuan online (Kominfo, 2021)

Saat ini terdapat 202,6 juta pengguna internet di Indonesia. Ini angka yang sangat besar, yang aktif di sosial media ada 170 juta jiwa atau 87% menggunakan aplikasi jejaring pesan Whatsapp, 85% mengakses Instagram dan Facebook, dengan rerata penggunaan 8 jam 52 menit sehari. Jadi, ini melebihi batas waktu masyarakat kita berkomunikasi di ruang digital sehingga dapat memicu seseorang melakukan tindak kejahatan penipuan dengan memanfaatkan situasi untuk mendapatkan keuntungan.

Ragam Penipuan Digital Apa Saja Sih?

Dalam berbagai kasus serangan siber di atas, penipuan digital menjadi salah satu bentuk kejahatan digital yang cukup rentan dan banyak dialami oleh masyarakat. Setidaknya ada empat bentuk penipuan digital, yaitu *scam, spam, phising*, dan *hacking*. Secara teknis, penipuan dapat bersifat social engineering dengan ragam bentuk yang kita terima mulai dari SMS, telepon, email bahkan dalam bentuk virus

serta pembajakan/peretasan akun dan cloning platform yang kita miliki.

1. Scam

Merupakan permainan atau tindakan untuk menipu kepercayaan seseorang yang bertujuan untuk mendapatkan keuntungan dengan cepat. Beberapa tipe dari *scam* yaitu:

a. Upaya mendapatkan informasi pribadi

Upaya dalam mendapatkan informasi pribadi dengan cara:

1. Hacking

Peretasan terjadi ketika scammer memperoleh akses ke informasi pribadi kita dengan menggunakan teknologi untuk membobol komputer, perangkat seluler, atau jaringan kita. Mereka akan menggunakan informasi yang mereka peroleh untuk melakukan aktivitas penipuan, seperti pencurian identitas atau mereka dapat memper oleh akses langsung ke detail perbankan dan kartu kredit kita.

2. Identity Theft

Pencurian identitas adalah jenis penipuan yang melibat kan penggunaan identitas orang lain untuk mencuri uang atau mendapatkan keuntungan lain.

3. Phishing

Penipuan phishing adalah upaya penipu untuk mengelabui kita agar memberikan informasi pribadi seperti nomor rekening bank, kata sandi, dan nomor kartu kredit kita. Penipu menghubungi kita dengan berpura-pura dari bisnis yang sah, dan pesan phishing dirancang agar terlihat asli, dan sering kali menyalin format yang diguna kan oleh organisasi yang berpura-pura diwakili oleh

kan oleh organisasi yang berpura-pura diwakili oleh scammer, termasuk merek dan logo mereka.

4. Remote Access Scams.

Penipuan akses jarak jauh mencoba meyakinkan kita bahwa kita memiliki masalah komputer atau internet dan kita perlu membeli perangkat lunak baru untuk memper baiki masalah tersebut. Penipu berpura - pura menjadi penyedia jasa layanan service, dan membuat kita berpikir bahwa benar ada virus, sehingga meminta akses jarak jauh ke komputer kita.

b. Buying or Selling

1. Classified Scams

Penipuan rahasia menipu pembeli online di situs web rahasia untuk berpikir bahwa mereka berurusan dengan kontak yang sah tetapi sebenarnya itu adalah scammer.

2. False Billing

Penipuan penagihan palsu meminta kita atau bisnis kita untuk membayar faktur palsu untuk daftar direktori, iklan, pembaruan nama domain, atau perlengkapan kantor yang tidak kita pesan.

3. Health & Medical Products

Penipuan produk kesehatan dan medis dapat menjual produk perawatan kesehatan kepada kita dengan harga rendah yang tidak pernah kita terima, atau membuat janji palsu tentang produk, obat-obatan, dan perawatan mereka.

4. Mobile Premium Service

Scammers membuat kompetisi SMS atau penipuan trivia

untuk menipu kita agar membayar tarif panggilan atau teks yang sangat tinggi saat membalas pesan teks yang tidak diminta di ponsel atau ponsel pintar kita.

5. Online Shopping Scams

Penipuan belanja online melibatkan scammer yang berpura-pura menjadi penjual *online* yang sah, baik dengan situs web palsu atau iklan palsu di situs pengecer asli.

6. Overpayment Scams

Penipuan kelebihan pembayaran bekerja dengan membuat kita 'mengembalikan' *scammer* yang telah mengirimi kita terlalu banyak uang untuk barang yang kita jual

7. Psychic & Clairvoyant

Penipuan psikis dan peramal dirancang untuk menipu kita agar memberikan uang anda, biasanya menawarkan 'bantuan' dengan imbalan biaya.

3. Health & Medical Products

Penipuan produk kesehatan dan medis dapat menjual produk perawatan kesehatan kepada kita dengan harga rendah yang tidak pernah kita terima, atau membuat janji palsu tentang produk, obat-obatan, dan perawatan mereka.

c. Dating/Romance

Penipu memanfaatkan orang yang mencari pasangan, seringkali melalui situs kencan, aplikasi, atau media sosial dengan berpura-pura menjadi calon teman. Mereka memainkan pemicu emosional untuk membuat kita memberikan uang, hadiah, atau detail pribadi.

d. Fake Charities

Scammers menyamar sebagai badan amal asli dan meminta sumbangan atau menghubungi kita dan mengaku sedang mengumpulkan uang/dana setelah bencana alam atau peristiwa besar.

e. Investasi

1. Betting & Sports Investments Scam

Penipuan taruhan dan investasi olahraga mencoba meyakinkan kita untuk berinvestasi dalam sistem dan perangkat lunak yang di klaim 'sangat mudah' yang dapat 'menjamin' kita mendapat untung dari acara olahraga.

2. Investment Scam

Penipuan investasi melibatkan janji pembayaran besar, uang cepat atau pengembalian yang dijamin. Selalu curiga terhadap setiap peluang investasi yang menjanjikan pengembalian tinggi dengan sedikit atau tanpa risiko – jika tampaknya terlalu bagus untuk menjadi kenyataan, mungkin memang demikian dan kemungkinan besar adalah penipuan.

f. Jobs

1. Jobs & Employment Scams

Pekerjaan dan penipuan pekerjaan menipu kita untuk menyerahkan uang kita dengan menawarkan cara 'terjamin' untuk menghasilkan uang cepat atau pekerjaan bergaji tinggi dengan sedikit usaha.

2. Pyramid Scams

Skema piramida adalah skema 'cepat kaya' yang ilegal dan sangat berisiko yang pada akhirnya dapat mengha biskan banyak uang.

g. Ancaman & Pemerasan

1.Malware & Ransomware

Malware menipu kita untuk menginstal perangkat lunak yang memungkinkan scammers mengakses file dan melacak apa yang kita lakukan, sementara *ransomware* menuntut pembayaran untuk 'membuka kunci' komputer atau file kita.

2. Threats to Life, Arrest or Other

Ancaman terhadap nyawa, penangkapan, atau lainnya melibatkan tuntutan scammers untuk membayar uang yang seharusnya anda bayar dan ancaman jika kita tidak bekerja sama.

h. Unexpected money

1. Inheritance Scams

Penipuan ini menawarkan janji warisan palsu untuk menipu kita agar berpisah dengan uang kita atau membagikan detail bank atau kartu kredit kita sendiri.

2. Unexpected Money Scams

Penipuan uang tak terduga melibatkan seseorang di luar negeri yang menawarkan kita bagian dalam jumlah besar uang atau pembayaran dengan syarat kita harus

membantu mereka mentransfer uang ke luar negara mereka.

3. Rebate Scams

Penipuan rabat mencoba meyakinkan kita bahwa kita berhak atas rabat atau penggantian biaya dari pemerin tah, bank, atau organisasi tepercaya.

i.Unexpected winnings

1. Scratchie Scams

Scratchie scam berbentuk kartu scratchie palsu yang menjanjikan semacam hadiah, dengan syarat 'pemenang' membayar biaya penagihan.

2. Travel Prize Scams

Penipuan hadiah perjalanan adalah upaya untuk menipu kita agar berpisah dengan uang kita untuk mengklaim 'hadiah' seperti liburan gratis atau diskon.

3.Unexpected Price & Lottery Scams

Penipuan hadiah dan lotere yang tidak terduga bekerja dengan meminta kita membayar semacam biaya untuk mengklaim hadiah atau kemenangan kita dari kompetisi atau lotre yang tidak pernah kita ikuti.

2. Spam

Spam adalah segala jenis komunikasi digital yang tidak diinginkan dan tidak diminta yang dikirim secara massal. Seringkali spam dikirim melalui email, tetapi juga dapat didistribusikan melalui pesan teks, panggilan telepon, atau media sosial. Spammer menggunakan banyak bentuk komunikasi untuk mengirim pesan yang tidak diinginkan secara massal. Beberapa di antaranya adalah:

a. Phising Email

Email phishing adalah jenis spam yang dikirim oleh penjahat dunia maya ke banyak orang, berharap untuk "mengaitkan" beberapa orang. Email phishing menipu korban agar memberikan informasi sensitif seperti login situs web atau informasi kartu kredit

b. Email Spoofing

Email palsu meniru, atau menipu, email dari pengirim yang sah, dan meminta anda untuk mengambil tindakan. Spoof yang dijalankan dengan baik akan berisi branding dan konten yang sudah dikenal, seringkali dari perusahaan besar yang terkenal seperti PayPal atau Apple.

c. Tech Support Scam

Dalam penipuan dukungan teknis, pesan spam menunjukkan bahwa kita memiliki masalah teknis dan kita harus menghubungi dukungan teknis dengan menghubungi nomor telepon atau mengklik tautan dalam pesan.

d. Current Event

Topik hangat dalam berita dapat digunakan dalam pesan spam untuk menarik perhatian kita. Pada tahun 2020 ketika dunia menghadapi pandemi Covid-19 dan ada peningkatan pekerjaan dari rumah, beberapa scammer mengirim pesan spam yang menjanjikan pekerjaan jarak jauh yang dibayar dalam Bitcoin.

e. Advance - Fee

Jenis spam ini menjanjikan hadiah finansial jika kita pertama kali memberikan uang muka. Pengirim biasanya menunjukkan bahwa uang muka ini adalah semacam biaya pemrosesan atau uang yang sungguh-sungguh untuk membuka jumlah yang lebih besar, tetapi begitu anda membayar, uang itu meng-hilang.

f. Malspam

Malspam adalah pesan spam yang mengirimkan malware ke perangkat kita. Pembaca yang tidak curiga yang mengklik tautan atau membuka lampiran email berakhir dengan beber-apa jenis malware termasuk ransomware, Trojan, bot, pencuri info, *cryptominers, spyware,* dan *keyloggers.*

g. Call & Text

Apakah anda pernah menerima robocall? Itu panggilan spam. Pesan teks dari pengirim yang tidak dikenal yang mendesak kita untuk mengklik tautan yang tidak dikenal? Itu disebut sebagai spam pesan teks atau "smishing", kombinasi SMS dan *phishing.*

3. Phising

Phising adalah salah satu ancaman yang paling membuat frustasi yang kita hadapi. Sebagian besar tahu apa itu dan bagaimana cara kerjanya, tapi kita masih terjebak. Penipuan, yang melibatkan penjahat mengirim pesan yang menyamar sebagai organisasi yang sah, menargetkan ratusan juta organ-isasi setiap hari. Pesan mengarahkan penerima ke situs web palsu yang menangkap informasi pribadi mereka atau berisi

lampiran berbahaya. Diantaranya:.

a. Email Phising

Sebagian besar serangan phishing dikirim melalui email. Penjahat akan mendaftarkan domain palsu yang meniru organisasi asli dan mengirimkan ribuan permintaan umum. Ada banyak cara untuk menemukan email phishing, tetapi sebagai aturan umum, kita harus selalu memeriksa alamat email dari pesan yang meminta kita untuk mengklik link atau mendownload lampiran

b. Spear Phising

Ada dua jenis phishing lain yang lebih canggih yang melibat-kan email. Yang pertama, spear phishing, menjelaskan email berbahaya yang dikirim ke orang tertentu. Penjahat yang melakukan ini sudah memiliki beberapa atau semua informasi tentang korban.

c. Whaling

Serangan perburuan paus bahkan lebih bertarget, membidik para eksekutif senior. Meskipun tujuan akhir penangkapan “ikan paus” sama dengan jenis serangan phishing lainnya, tekniknya cenderung jauh lebih halus. Penipuan yang melibat-kan pengembalian pajak palsu adalah jenis perburuan “paus” yang semakin umum. Formulir pajak sangat dihargai oleh penjahat karena berisi sejumlah informasi yang berguna: nama, alamat, nomor Jaminan Sosial dan informasi rekening bank.

d. Smishing & Vishing

Smishing melibatkan penjahat mengirim pesan teks (yang isinya hampir sama dengan email phishing), dan vishing melibatkan percakapan telepon. Penipuan vishing umum melibatkan penjahat yang menyamar sebagai penyelidik penipuan (baik dari perusahaan kartu atau bank) memberi tahu korban bahwa akun mereka telah dilanggar. Penjahat kemudian akan meminta korban untuk memberikan rincian kartu pembayaran untuk memverifikasi identitas mereka atau untuk mentransfer uang ke rekening 'aman' – yang mereka maksud adalah rekening penjahat.

e. Angler Phising

Sebagai vektor serangan yang relatif baru, media sosial menawarkan sejumlah cara bagi penjahat untuk mengelabui orang. URL palsu; situs web kloning, posting, dan tweet; dan pesan instan (yang pada dasarnya sama dengan smishing) semuanya dapat digunakan untuk membujuk orang agar membocorkan informasi sensitif atau mengunduh malware.

c. Whaling

Serangan perburuan paus bahkan lebih bertarget, membidik para eksekutif senior. Meskipun tujuan akhir penangkapan "ikan paus" sama dengan jenis serangan phishing lainnya, tekniknya cenderung jauh lebih halus. Penipuan yang melibatkan pengembalian pajak palsu adalah jenis perburuan "paus" yang semakin umum. Formulir pajak sangat dihargai oleh penjahat karena berisi sejumlah informasi yang berguna: nama, alamat, nomor Jaminan Sosial dan informasi rekening bank.

4. Hacking

Peretasan tidak selalu merupakan tindakan jahat, tetapi paling sering dikaitkan dengan aktivitas ilegal dan pencurian data oleh penjahat dunia maya. Peretasan mengacu pada penyalahgunaan perangkat seperti komputer, ponsel cerdas, tablet, dan jaringan untuk menyebabkan kerusakan atau sistem yang rusak, mengumpulkan informasi tentang pengguna, mencuri data dan dokumen, atau mengganggu aktivitas terkait data.

Biasanya ada empat pendorong utama yang menyebabkan pelaku jahat meretas situs web atau sistem: (1) keuntungan finansial melalui pencurian rincian kartu kredit atau dengan menipu layanan keuangan, (2) spionase perusahaan, (3) untuk mendapatkan ketenaran atau rasa hormat terhadap mereka. bakat peretasan, dan (4) peretasan yang disponsori negara yang bertujuan untuk mencuri informasi bisnis dan intelijen nasional. Selain itu, ada peretas bermotivasi politik—atau peretas—yang bertujuan menarik perhatian publik dengan membocorkan informasi sensitif, seperti Anonymous, LulzSec, dan WikiLeaks. Beberapa jenis peretas paling umum yang melakukan aktivitas ini meliputi:

a. Black Hat Hackers

Peretas topi hitam adalah "orang jahat" dari adegan peretasan. Mereka berusaha keras untuk menemukan kerentanan dalam sistem komputer dan perangkat lunak untuk mengeksploitasinya untuk keuntungan finansial atau untuk tujuan yang lebih jahat, seperti untuk mendapatkan reputasi, melakukan spionase perusahaan, atau sebagai bagian dari kampanye peretasan negara-bangsa. Tindakan individu ini dapat menim-

bulkan kerusakan serius pada pengguna komputer dan organisasi tempat mereka bekerja. Mereka dapat mencuri informasi pribadi yang sensitif, membahayakan komputer dan sistem keuangan, dan mengubah atau menghapus fungsionalitas situs web dan jaringan penting

b. White Hat Hackers

Peretas topi putih dapat dilihat sebagai "orang baik" yang berusaha mencegah keberhasilan peretas topi hitam melalui peretasan proaktif. Mereka menggunakan keterampilan teknis mereka untuk membobol sistem untuk menilai dan menguji tingkat keamanan jaringan, yang juga dikenal sebagai peretasan etis. Ini membantu mengekspos kerentanan dalam sistem sebelum peretas topi hitam dapat mendeteksi dan mengeksploitasinya. Teknik yang digunakan peretas topi putih mirip atau bahkan identik dengan peretas topi hitam, tetapi orang-orang ini disewa oleh organisasi untuk menguji dan menemukan lubang potensial dalam pertahanan keamanan mereka.

c. Grey Hat Hackers

Peretas topi abu-abu duduk di suatu tempat antara orang baik dan orang jahat. Tidak seperti peretas topi hitam, mereka berusaha melanggar standar dan prinsip tetapi tanpa bermaksud merugikan atau mendapatkan keuntungan finansial. Tindakan mereka biasanya dilakukan untuk kebaikan bersama. Misalnya, mereka mungkin mengeksploitasi kerentanan untuk meningkatkan kesadaran bahwa kerentanan itu ada, tetapi tidak seperti peretas topi putih, mereka melakukannya secara publik. Ini memperingatkan aktor jahat tentang

keberadaan kerentanan.

Berikut ini merupakan upaya yang dapat dilakukan untuk melindungi diri dari scam, spam, phising, maupun hacking:

a. Jangan pernah membagikan ataupun mengunggah alamat email ke publik. Hal ini bertujuan untuk mengurangi risiko pengiriman email spam maupun peretasan apabila kata sandinya lemah dan mudah ditebak.
b. Berpikir sebelum meng-klik tautan link maupun mengunduh dokumen dari sumber yang tidak jelas.
c. Jangan membalas pesan spam karena pengirim pesan dapat mengetahui bahwa alamat surel tersebut aktif dan meningkatkan risiko surel tersebut menjadi target penipuan lainnya.
d. Gunakan aplikasi penyaring spam dan antivirus untuk menurunkan risiko.
e. Hindari penggunaan email pribadi maupun perusahaan untuk mendaftar aplikasi yang tidak terlalu penting.

Tips Terhindar Penipuan Digital

1. Budayakan menjaga data privasi;
2. Untuk organisasi perlu membuat standart operational procedure yang ketat. Meski kadang merepotkan hal itu perlu dilakukan. Selain menyiapkan teknologi dan pengamanan data, juga perlu memperkuat sumberdaya manusia yang ada dalam organisasi agar bisa menerapkan budaya data privacy;
3. Kita harus membuat password akun yang yang benar-benar tidak mudah ditebak. Kemudian sering-sering mengganti

password, Serta selalu melakukan update karena update software itu ada dua biasanya untuk meningkatkan fitur-fiturnya tapi juga untuk menutup lubang (keamanan) yang bisa menjadi peluang masuknya para penjahat untuk mengambil data;
4. Tambah literasi digitalmu dengan mengikuti webinar-webinar tentang literasi digital, seperti yang diselenggarakan oleh Kominfo;
5. Berpikir dahulu sebelum bertindak dan jangan panik.

Obrolin Isu-Isu Dunia Digital

Pernahkah kita membahas isu di dunia digital sebagai bagian dari percakapan sehari-hari? Mungkin banyak yang belum terbiasa melakukannya. Kasus seperti *cyberbullying*, sexting dan pelanggaran hak cipta ada baiknya kita obrolkan. Isu ini sama pentingnya dengan isu di dunia nyata seperti kriminalitas di jalan raya, misalnya.

Isu lain seperti hoaks atau *phising* dan *scam* juga perlu dibahas. Sebaiknya jangan memproses semua yang dilihat di dunia digital dengan nilai nominal. Seperti banyaknya jumlah *follow-*

ers, like, comments dan *share*. Pastikan kita dapat memverifikasi apakah informasi itu benar dan akurat.

Ini juga penting, pahami dan gunakan fitur keamanan yang diinstal pada komputer, tablet dan smartphone kita. Walau pengaturan pada platform media sosial dan situs berbeda-beda, sebaiknya kita lebih dahulu memahami fitur keamanan yang disediakan.

Nah, jangan ragu obrolin isu-isu di dunia digital. Selain dapat membuat kita waspada, orang lain pun mendapat informasi bermanfaat. Sehingga baik kita maupun orang lain dapat terhindar dari hal-hal yang tidak diinginkan di dunia digital

08 REKAM JEJAK DIGITAL DI MEDIA

Yuk Pahami Jejak Digital!

Jejak digital tidak akan dapat dihapus sepenuhnya. Aturlah setting privasi perangkat kita. Perlu kita ingat bahwa penipu, atau pelaku tindak asusila di dunia digital menghubungi dan mengeksploitasi orang karena jejak digital yang tidak baik atau renta.

Apa saja yang telah beredar secara online, bisa tetap online selamanya. Obrolkan bersama tentang konsekuensi potensial dari berbagi foto atau video yang diposting. Kita perlu pertanyakan apakah hal-hal yang diposting berkontribusi baik pada jejak digital kita sendiri.

Salah satu alat pengontrol privasi yang paling baik adalah pribadi kuat dan bijak dalam menggunakan perangkat digital. Komunikasi di dunia nyata, dengan anggota keluarga juga sebaiknya dibangun atas kondisi yang harmonis dan transparan. Sehingga jejak digital dapat memberikan reputasi online yang baik untuk kita dan orang di sekitar.

Selain itu, dikenal pula manajemen jejak digital yang membantu kita lebih mengontrol apa yang kita bagikan di dunia maya. Berikut ini beberapa tips manajemen jejak digital yang bisa kita lakukan menurut ***Australian Digital Health Agency (2020):***

a. Mengidentifikasi jejak digital. Cari nama kita di mesin pencarian informasi dan identifikasi apa saja informasi yang terlihat secara publik
b. Perbarui informasi. Pastikan data personal dan data mengenai pekerjaan kita sudah menunjukkan informasi terkini. Kita bisa menelusuri mana informasi yang ingin kita tampilkan dan mana yang tidak. Pada tahap ini, mungkin kita membutuhkan bantuan admin untuk mengubah informasi tertentu.
c. Pikirkan sebelum mengunggah konten. Sebelum membagikan data personal dan pekerjaan secara daring, pastikan kita memahami apakah yang kita bagikan penting dan apakah akan membahayakan kita sendiri atau orang lain di masa depan?
d. Pelajari aturan privasi. Pahami data apa saja data yang dikumpulkan oleh platform yang kita gunakan.
e. Cek pengaturan konfigurasi di gawai yang kita gunakan dan pelajari apakah aplikasi tertentu dapat mengakses informasi seperti foto, lokasi, kalender, dan kontak.

f. Gunakan kata sandi yang unik dan kuat di setiap gawai, aplikasi, dan akun daring. Pertimbangkan pula untuk menggunakan verifikasi lain seperti pemindai sidik jari dan wajah.
g. Bersihkan histori pencarian setelah digunakan.
Ingat bahwa orang lain, termasuk keluarga, teman, organisasi profesional, dapat mengunggah informasi mengenai kita secara daring. Jelaskan sejauh mana kita mau orang lain mengunggah data kita.
h. Rencana masa depan. Pertimbangkan untuk membagikan daftar akun media sosial yang kita gunakan dan bagikan kepada orang yang kita percaya apabila terjadi sesuatu yang tidak diinginkan di masa depan.
i. Tinjau secara berkala untuk memperbarui seluruh informasi dan pengaturan privasi akun media sosial kita.

Dinamika Privasi di Dunia Digital

Dunia digital seperti kita ketahui memiliki dinamika yang

positif dan negatif. Banyak aplikasi atau situs yang sangat berguna bagi kita. Namun banyak juga aplikasi atau situs yang malah berbahaya dan negatif.

Sisi negatif dunia digital dapat menimpa ketika kita gunakan teknologi sebagai wadah pelampiasan emosi. Ada baiknya kita mampu mengidentifikasi dan menangani emosi negatif. Lakukan aktivitas untuk mencegah kebosanan atau BT. Bisa juga kita praktekkan pernapasan meditatif atau yoga.

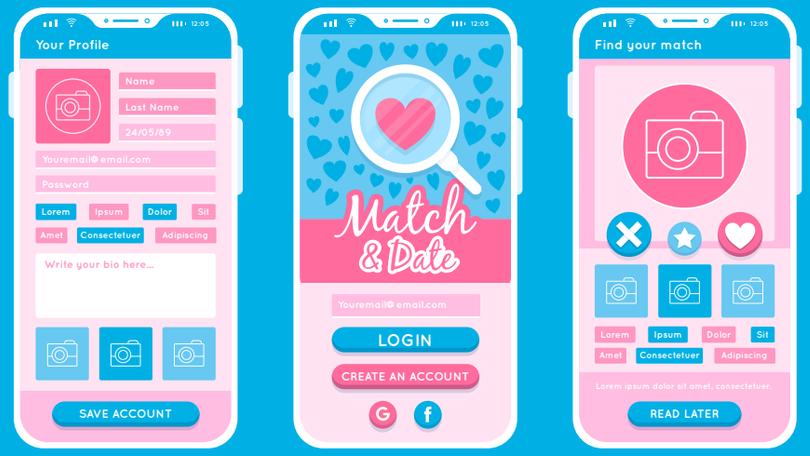
Di sisi lain platform digital seperti media sosial dapat mendukung kita untuk mengeksplorasi dan menemukan lebih banyak tentang diri kita sendiri. Selain itu dunia digital mampu mendukung aktivitas dan keperluan pekerjaan, sekolah, bisnis, sampai personal.

Namun perlu kita pastikan bahwa berperilaku baik dan benar kita lakukan saat online. Karena banyak orang salah dalam mengatur privasi mereka. Mereka salah dalam berbagi hal-hal yang sangat personal seperti foto, opini, dan perilaku. Dampaknya, jejak digital yang cenderung buruk ini abadi.

09 MINOR SAFETY (CATFISHING)

Istilah catfish mulai muncul dari sebuah tayangan dokumenter asal Amerika Serikat berjudul sama yang diproduseri 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 catfish sendiri digunakan untuk menggambarkan seseorang yang melakukan penipuan identitas diri terhadap orang lain terutama pasangannya yang sebelumnya tidak pernah bertemu (Adam, 2017). Catfish juga memiliki arti sebagai seseorang yang menggunakan profil personal palsu pada SNS untuk melakukan kecurangan atau melakukan penipuan (Catfish Definition, n.d.).

Pada awalnya, catfish secara apabila diartikan ke 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, catfish sendiri berbeda dengan impersonation dan juga poser karena catfish lebih condong kepada online dating scams (Ahmad et al., 2017).

Catfish muncul dan berusaha menarik perhatian individu lain dengan identitas palsu yang digunakannya. Identitas palsu ini digunakan untuk kepentingan menjalin hubungan dengan orang lain. 'Kebebasan untuk menjadi apa di SNS merupakan salah satu penyebab dari munculnya catfish. Kebebasan inilah yang digunakan oleh para pelaku catfish untuk mengonstruksi identitas digital yang akan mereka gunakan (Magdy et al., 2017).

Konstruksi identitas merupakan sebuah komponen integral dalam kehidupan manusia yang telah diteliti dan diperiksa dengan berbagai sudut pandang. Identitas dikonstruksi sesuai dengan keinginan apa yang ingin ditampilkan di publik

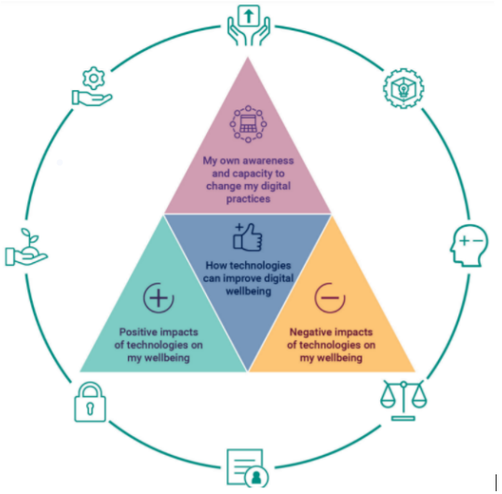
(Dowling, 2011). Identitas pun sering dikonstruksikan di SNS. Catfish masuk ke kategori pelanggaran di dalam SNS karena menipu dengan cara berpura–pura menjadi orang lain dengan menciptakan identitas baru secara virtual. Hal ini berarti orang tersebut melakukan penipuan identitas (Smith et al., 2017).

Penipuan sendiri merupakan suatu tindakan seseorang ataupun sekelompok orang dengan membuat kesan bahwa sesuatu itu benar adanya dan tidak palsu sehingga mengakibatkan orang lain memberikan kepercayaan pada realitas tersebut. Penipuan juga dapat didefinisikan sebagai sebuah bujukan kepada orang lain dengan menipu, merangkai kata–kata bohong, menggunakan nama palsu, dan keadaan palsu sehingga keadaan tersebut memaksa korban untuk memberikan sesuatu sebagai umpan balik atas tindakan yang dilakukan oleh pelaku. Dampaknya bagi korban sendiri adalah berupa kerugian, baik dari sisi psikologis, finansial, maupun fisik (Rusmana, 2015).

Salah satu korban yang mengalami tindakan catfish adalah Bayu Eko Moekti- to, atau biasa dikenal sebagai YouTuber Bayu Skak. Dalam video

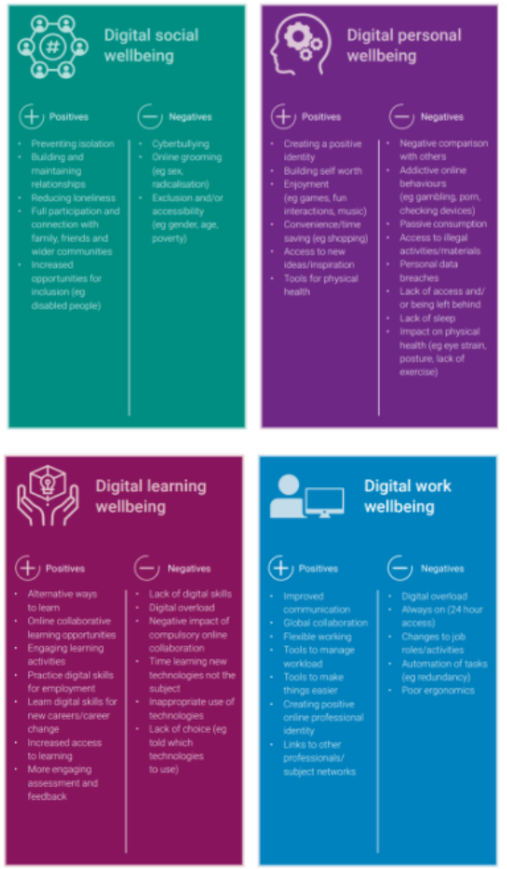
unggahannya di platform Youtube, dia menjelaskan mengenai penipuan identitas yang dialaminya. Kedekatannya dengan seseorang bernama Dara Fleisher Cohen atau biasa disebut Dara, berawal dari direct message Instagram yang dikirimkan oleh Dara, yang mengaku sebagai seorang calon dokter yang sedang melakukan Pendidikan di Singapura. Perkenalan tersebut berlanjut ke ikatan yang lebih serius yaitu pacaran. Namun, tanpa dia sadari bahwa sosok yang dia kenal sebagai Dara itu tidak pernah ada. Foto maupun video yang diunggah di SNS milik Dara ternyata merupakan foto dan video milik artis India bernama Dipshika (Rizka, 2018).

10 DIGITAL RIGHTS (HAK DIGITAL WARGA NEGARA)



Empat Aspek Kesejahteraan Digital Individu yang Dikelilingi oleh Delapan Prinsip Praktik Digital yang Baik

Sumber: Jisc, n.d



Hak dan kewajiban digital dapat memengaruhi kesejahteraan digital setiap pengguna. Kesejahteraan digital merupakan istilah yang merujuk pada dampak dari layanan teknologi dan digital terhadap kesehatan mental, fisik, dan emosi seseorang. Siapa yang bertanggung jawab untuk menciptakan kesejahteraan digital? jawabannya adalah setiap individu. Terdapat empat aspek kesejahteraan individu yang digambarkan dalam piramida dan delapan prinsip praktik digital yang baik yang digambarkan pada lingkaran (Jisc, n.d).

Sementara delapan prinsip praktik digital yang baik diantaranya (Jisc, n.d),

a. Menyediakan pelayanan inklusif dan responsif yang mendorong pekerjaan digital maupun aktivitas pembelajaran.
b. Menyertakan aspek kesejahteraan digital dalam kebija kan yang sudah ada, khususnya yang berkaitan dengan kebijakan aksesibilitas dan inklusi
c. Menyediakan lingkungan fisik dan daring yang aman. Prinsip ini termasuk penyediaan pencahayaan ruangan yang memadai, akses WiFi, dsb dan memastikan setiap individu mematuhi peraturan mengenai kesehatan dan keselamatan.
d. Mematuhi petugas yang bertanggung jawab mengenai aktivitas digital (misalnya penanggung jawab aktivitas digital di kantor maupun dalam aktivitas belajar di sekolah).
e. Penuhi tanggung jawab etik dan hukum yang berhubu ngan dengan aksesibilitas, kesehatan, kesetaraan, dan inklusi (misalnya peraturan ketenagakerjaan mengenai lembur, UU ITE, dsb)
f. Menyediakan pelatihan, kesempatan belajar, pen dampingan, dan bantuan partisipasi dalam kegiatan digital (misalnya peningkatan kapasitas kemampuan digital bagi pekerja maupun siswa)
g. Memahami potensi dampak positif maupun negatif dari aktivitas digital pada kesejahteraan individu
h. Menyediakan sistem, perlengkapan, dan konten digital yang inklusif dan mudah diakses.

Oleh sebab itu, kita sebagai subjek dalam dunia digital memiliki hak dan kewajiban berupa (Council of Europe, n.d):

a. Akses dan tidak diskriminatif, artinya kita memiliki hal untuk terhubung dengan internet (kecuali jika diputuskan oleh pengadilan). Selain itu, akses internet juga harus terjangkau dan tidak diskriminatif.
b. Kebebasan berekspresi dan mendapatkan informasi
    i. Kita berhak untuk berekspresi, mengakses informasi, dan opini di dunia maya namun tetap berkewajiban menghormati privasi orang lain.
    ii. Pihak berwajib juga berkewajiban menghormati dan melindungi hak kebebasan berekspresi dan mendapatkan informasi ini.
    iii. Kita bisa memilih untuk tidak menunjukkan identitas diri secara daring, namun kita berkewa jiban mengikuti peraturan mengenai sejauh mana kita harus menunjukkan identitas diri pada hukum.
c. Kebebasan berkumpul, berkelompok, dan partisipasi. Kita bebas menggunakan situs web, aplikasi, atau layanan lain untuk berhubungan dengan rekan dalam sebuah kelompok. Kita juga berhak untuk mengajukan protes daring secara damai. Namun, kita harus tetap memahami bahwa kita bisa berhadapan dengan hukum jika merugikan pihak lain.
d Perlindungan privasi dan data. Data pribadi kita hanya bisa digunakan atas persetujuan kita atau jika dike hendaki pengadilan. Kita harus diinformasikan jika data pribadi kita diproses atau dipindah-tangankan

oleh pihak tertentu, kapan, oleh siapa, dan untuk tujuan apa.

e. Pendidikan dan literasi. Kita berhak memiliki akses ke pendidikan dan pengetahuan untuk melatih hak dan kebebasan kita di dunia maya.

f. Perlindungan terhadap anak. Jika kita tergolong anak-anak, maka kita memiliki perlindungan dan panduan khusus untuk melakukan aktivitas di dunia maya.

g. Hak mendapatkan pertolongan terhadap pelanggaran hak asasi. Hal ini tidak selalu jalur hukum, bisa dari kebijakan penyedia layanan internet, pihak berwajib, institusi HAM, dan sebagainya tergantung dari pelang garan yang dilakukan, hasilnya dapat berupa penjelasan, permintaan maaf, kompensasi, dan sebagainya.

DAFTAR PUSTAKA

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
Baase, S. (2008). *A gift of fire: Social, legal, and ethical issues for computing and the Internet.*

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

Berners-Lee, T., & Fischetti, M. (2001). *Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor. DIANE Publishing Company.*
https://www.bbc.com/news/blogs-magazine-monitor-35428300

Cerf, V., Dalal, Y., & Sunshine, C. (1974). *RFC 675—Specification of Internet Transmission Control Program (RFC675).*
http://www.faqs.org/rfcs/rfc675.html

Cohen-Almagor, R. (2013). *Internet history. In Moral, ethical, and social dilemmas in the age of technology: Theories and practice (pp. 19-39). IGI Global.*

Copeland, B. J. (2017). *The Modern History of Computing. In E. N. Zalta (Ed.), The Stanford Encyclopedia of Philosophy (Winter 2017). Metaphysics Research Lab, Stanford University.*
https://plato.stanford.edu/archives/win2017/entries/computing-history/

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

Goffman, Erving. (1959). *The Presentation of Self in Everyday Life. University of Edinburgh. 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/

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/

Grigg, D. W. (2010). *Cyber-aggression: Definition and concept of cyberbullying. Journal of Psychologists and Counsellors in Schools, 20(2), 143-156.*

Internet Matters.org. (2021).*Online grooming: facts & advice,*

Get expert tips to support children.
https://www.internetmatters.org/issues/online-grooming/

internetlivestats. (2016). Internet Users By Country (2016).
https://www.internetlivestats.com/internet-users-by-country/

Kaplan, A. M., & Haenlein, M. (2010). *Users of The World, Unite! The Challenges and Opportunities of Social Media. Business horizons, 53(1), 59-68.*

Kleinrock, L. (2010). *An early history of the internet [History of Communications]. IEEE Communications Magazine, 48(8), 26–36.*

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

Luppicini, R., & Adell, R. (Eds.). (2008). *Handbook of research on technoethics. IGI Global.*

O'Regan, G. (2016). *Introduction to the history of computing: A computing history primer. Springer.*
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

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). *A review of online grooming: Characteristics and concerns. Aggression and violent behavior, 18(1), 62-70.*
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/

Zhao, S. (2005). *The digital self: Through the looking glass of telecopresent others. Symbolic interaction, 28(3), 387-405.*