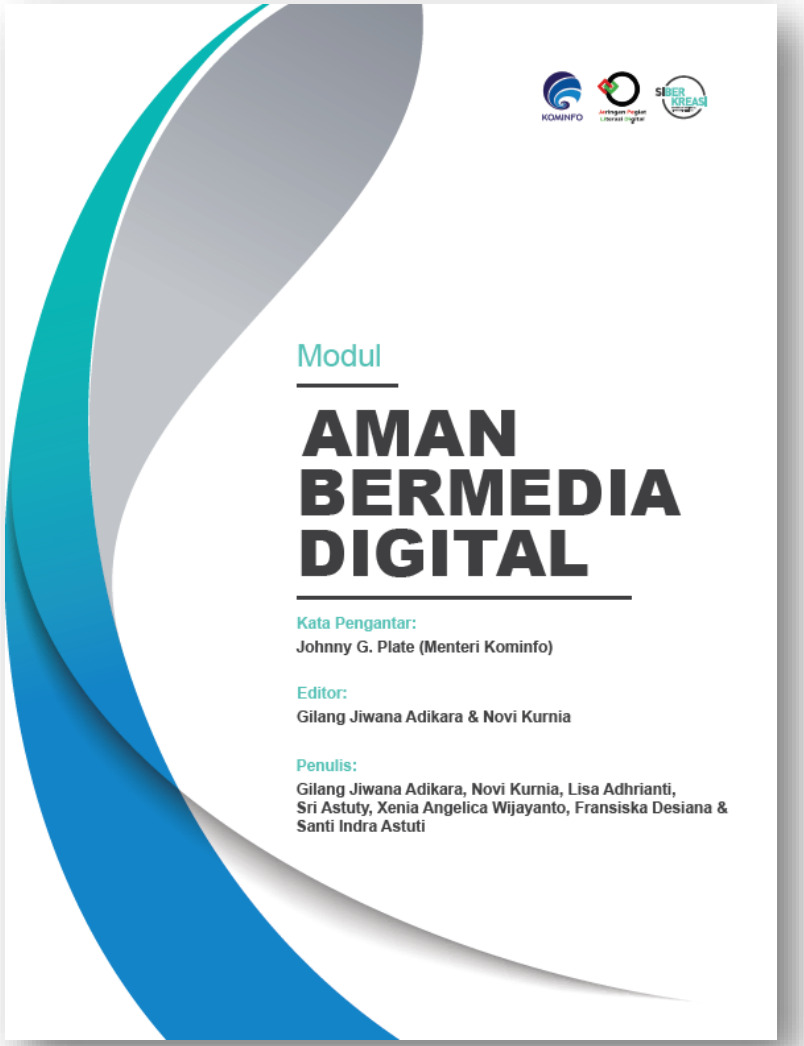
SIBER KREASI
GERAKAN NASIONAL LITERASI DIGITAL

AMAN BERMEDIA DIGITAL

SIBERKREASI | 2021



Modul
AMAN BERMEDIA DIGITAL

AMAN BERMEDIA DIGITAL

01 Pengantar: Aman di Ruang Digital

02 Proteksi Perangkat Digital

03 Perlindungan Identitas Digital dan Data Pribadi

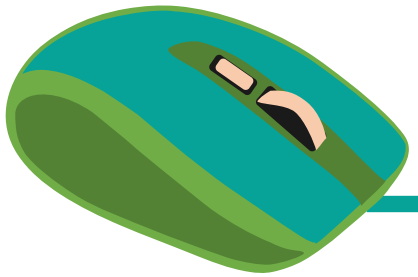
04 Waspada Penipuan Digital

05 Rekam Jejak Digital

06 Keamanan Anak di Dunia Digital

07 Tantangan Keamanan Digital

AGENDA



BAB I
PENGANTAR: AMAN DI RUANG DIGITAL

PENGANTAR

Perkembangan teknologi informasi di dunia terus berkembang secara masif. Pengguna Internet Indonesia mencapai 202juta pengguna*

Perubahan gaya hidup menjadi serba digital menawarkan kemudahan dan kepraktisan dalam melakukan berbagai aktivitas.

Masyarakat semakin nyaman dan percaya dalam melakukan aktivitas keuangan digital yang selama ini dianggap berisiko tinggi

Di sisi lain tingginya aktivitas digital juga membuka potensi buruk, seperti penipuan dan pencurian akun

Diperlukan pemahaman masyarakat terkait keamanan digital

*Hootsuite, 2021

KEAMANAN DIGITAL

Sebuah proses untuk memastikan penggunaan layanan digital, baik secara daring maupun luring dapat dilakukan secara aman.

Tidak hanya untuk mengamankan data yang kita miliki melainkan juga melindungi data pribadi yang bersifat rahasia.

Tantangan Keamanan Digital

01 Kontrol keamanan data pengguna otomatis berada di tangan masing-masing pengguna internet

02 Penipuan dengan memanfaatkan kelengahan pengguna

03 Internet menghubungkan antarpengguna secara luas dan *anonim*

04 Interaksi digital juga melibatkan anak-anak dan orang berusia lanjut yang rentan

Kompetensi Keamanan Digital

- Mengamankan Perangkat Digital
- Mengamankan Identitas Digital
- Mewaspadai Penipuan Digital
- Memahami Rekam Jejak Digital
- Memahami Keamanan Digital bagi Anak

BAB II
MEMPROTEKSI PERANGKAT DIGITAL

Pentingnya Melindungi Perangkat Digital

- Perangkat digital memiliki peran vital dalam melakukan aktivitas digital
- Perangkat digital memiliki beragam informasi penting: galeri foto dan video pribadi, daftar kontak, data keuangan
- Menghindari perangkat digital disalahgunakan oleh orang lain

HATI-HATI MALWARE

Malicious Software: perangkat lunak yang dirancang untuk mengontrol perangkat secara diam-diam, bisa mencuri informasi pribadi milik kita atau uang dari pemilik perangkat.

Bagaimana Malware masuk ke ponsel kita?

Menginstal aplikasi dari luar PlayStore atau AppStore	Adanya situs-situs berbahaya yang melakukan pengunduhan otomatis saat dibuka	Menyaru sebagai aplikasi yang kita kenal

Jenis-jenis Fitur Proteksi Perangkat Digital

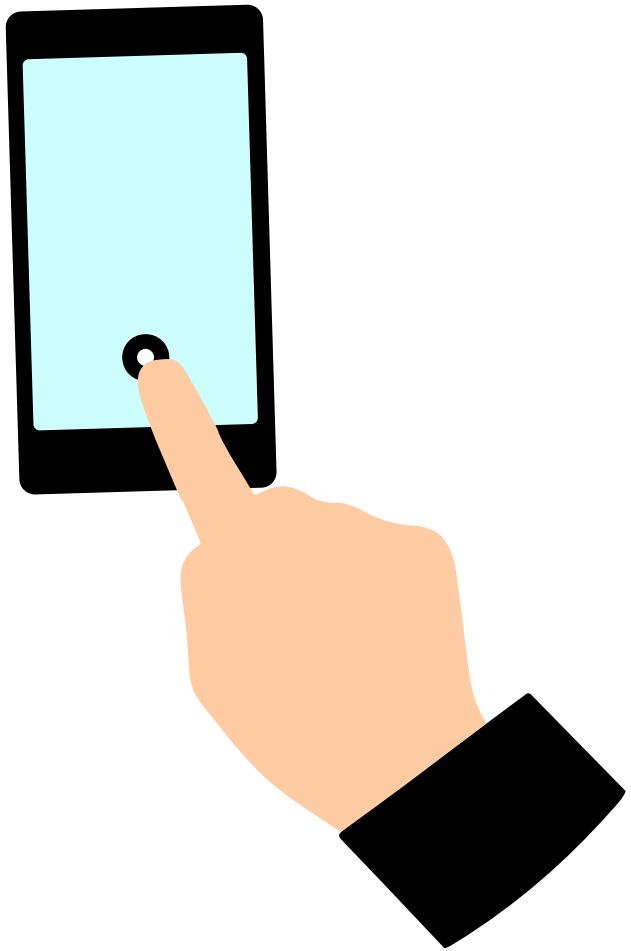
Proteksi Perangkat Keras

- Kata Sandi
- *Fingerprint Authentification*
- *Face Authentification*

Proteksi Perangkat Lunak

- *Find My Device*
- *Back Up* Data
- Anti*virus*
- Enkripsi *Full Disk*
- *Shredder*

Cara Aman Menggunakan Kata Sandi



01 Pastikan di sekeliling kita tidak ada orang lain Ketika akan membuka kata sandi

02 Menutup layer saat memasukkan kata sandi

03 Rutin mengganti kata sandi secara berkala

Fingerprint Authentication dan *Face Authentication*

Fingerprint Authentication	*Face Authentication*
Fitur perlindungan perangkat ponsel dengan sistem deteksi sidik jari	Fitur kunci ponsel dengan menyocokkan wajah pengguna untuk membuka kunci perangkat
Proteksi cukup baik karena sidik jari setiap orang berbeda-beda	Tingkat keamanan yang tinggi namun sedikit merepotkan

Proteksi Perangkat Lunak

Fitur	Fungsi
Find My Device	Fitur yang bisa diaktifkan untuk mencari perangkat digital yang hilang, mengunci file, bahkan melakukan remote wipe
Back Up Data	Langkah yang digunakan untuk mencegah kehilangan data yang ada di telepon pintar, tablet, komputer dan laptop
Anti*virus*	Menggunakan perangkat lunak yang baik untuk melindungi sistem perangkat digital
Enkripsi *Full Disk*	Fitur yang memungkinkan seluruh kapasitas hard drive computer untuk dienkripsi, mencakup sistem, program, dan semua data yang tersimpan di dalamnya
Shredder	Fitur yang mampu memusnahkan data secara total sehingga tidak dapat dimanfaatkan oleh pihak lain

#MakinCakapDigital

DIGITAL SAFETY

Pengelolaan perangkat digital sebelum dijual/dipindahtangankan

- Pastikan tempat penyimpanan file harus ditimpa alias *overwritten* agar tak bisa dipulihkan.
- Menghapus data bawaan Windows sendiri, Cipher, yang biasanya dipakai untuk enkripsi, sekaligus digunakan untuk menghapus file dari hardisk atau membuatnya tidak dapat digunakan.
- Cadangkan data, baik itu yang ada di gawai, komputer, kartu memori, atau penyimpan lain dengan aman sebelum menghapus dari gawai yang mau dijual
- Lepaskan SIM dan kartu penyimpanan dari telepon
- Jika perangkat memakai eSIM, jangan lupa untuk menghapusnya
- Aktifkan autentikasi dua faktor (2FA) untuk akun apa pun
- Jangan lupa untuk *log out* dari semua layanan digital (perbankan, email, media sosial, dan lain-lain) dari gawai yang mau dijual
- Lakukan reset pabrik (*factory reset*) atau format media
- Gunakan program *Virtual Network Computing* (VNC) apabila layar smartphone pecah atau mati

Upaya dan Konsekuensi Proteksi Perangkat Digital

Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah melalui Undang-Undang No. 19 Tahun 2016 (UU ITE) Pasal 45 ayat (1) UU ITE mengatur :

“Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)”

BAB III

PERLINDUNGAN IDENTITAS DIGITAL DAN DATA PRIBADI DI PLATFORM DIGITAL

Jenis Identitas Digital

IDENTITAS YANG TERLIHAT

- Nama Akun
- Foto Profil Pengguna
- Deskripsi Pengguna
- Identitas lain yang Tercantum dalam akun

IDENTITAS YANG TIDAK TERLIHAT

- PIN / *Password* / Sandi
- Two Factor Authentication
- OTP
- Identitas lain

Langkah-Langkah Melindungi Identitas Digital

Pastikan memilih menggunakan identitas asli atau samaran saat mengelola akun *platform* digital serta bertanggungjawab atas pilihan tersebut

Amankan identitas utama yakni alamat elektronik (surel) yang kita gunakan untuk mendaftar suatu *platform* digital

Lindungi dan konsolidasikan identitas digital dalam berbagai *platform* digital yang dimiliki

Jenis Data Pribadi

IDENTITAS YANG TERLIHAT

- Nama
- Jenis Kelamin
- Kewarganegaraan
- Agama
- Tanggal Lahir
- Pekerjaan
- Alamat Rumah
- *E-mail*
- Nomor Telepon dan lainnya

IDENTITAS YANG TIDAK TERLIHAT

- Data Kesehatan
- Data Biometrik
- Data Genetika
- Keuangan
- Ras / Etnis
- Preferensi Seksual
- Pandangan Politik
- Data Keluarga
- Data Kejahatan dan lainnya

#MakinCakapDigital

DIGITAL SAFETY

Tips Perlindungan Data Pribadi

Gunakan *password* (sandi) yang kuat, gunakan secara berbeda di setiap akun platform digital yang dimiliki, dan perbaharui secara berkala

Pahami dan pastikan pengaturan privasi di setiap akun platform digital yang dimiliki sesuai dengan tingkat keamanan yang dibutuhkan

Hati-hati mengunggah data pribadi di platform digital karena keamanan data pribadi kita tidak selalu terjamin

Hindari untuk membagiakn data pribadi kita (tempat tanggal lahir, nama ibu kandung, *password* berbagai akun platform digital)

Hindari berbagi data pribadi orang lain baik keluarga, teman, maupun kenalan di dunia maya sebab data mereka adalah privasi mereka

Hindari memasukkan data pribadi yang penting saat berinteraksi dalam platform digital dengan menggunakan *Wi-Fi* gratis di tempat publik

Pahami dan pilih aplikasi yang dipasang di gawai hanya mengakses data yang dibutuhkan dan bukan data pribadi kita lainnya

Selalu lakukan pembaruan perangkat lunak yang digunakan dalam gawai untuk meminimalisir resiko ada celah kebocoran

Waspada jika ada komunikasi atau aktivitas mencurigakan baik dari akun dengan identitas digital yang kita kenal maupun bukan

Tips menggunakan *Personal Identification Number* (PIN) dengan Baik dan Aman

Hindari memilih kombinasi angka yang mudah ditebak

Gunakan PIN yang berbeda untuk kepentingan yang berbeda

Sebaiknya jangan menuliskan PIN di kartu identitas ataupun secarik kertas yang ditaruh di dompet

Jika kita memasukkan PIN di berbagai mesin, misalnya ATM, di tempat terbuka, selalu tutupkan tangan kita supaya tidak ada orang yang melihatnya

Faktor yang biasa digunakan dalam *Two-factor Authentication* (2FA)

Faktor Pengetahuan	Faktor Kepemilikan	Faktor Biometrik
Informasi yang hanya diketahui pengguna: PIN, *password* (sandi), pertanyaan keamanan tambahan, dan lainnya	Kartu ID, aplikasi telepon pintar, token, dan lainnya	Teknologi sensor seperti sidik jari, wajah, suara, iris mata, dan lainnya

Faktor Lokasi	Faktor Waktu
Lokasi temat pengguna login dalam sistem yang diidentifikasi	Adanya waktu yang ditentukan oleh sistem untuk membatasi waktu penggunanya

Sumber : Socs.binus.ac.id. (2019, Juni 11)

#MakinCakapDigital

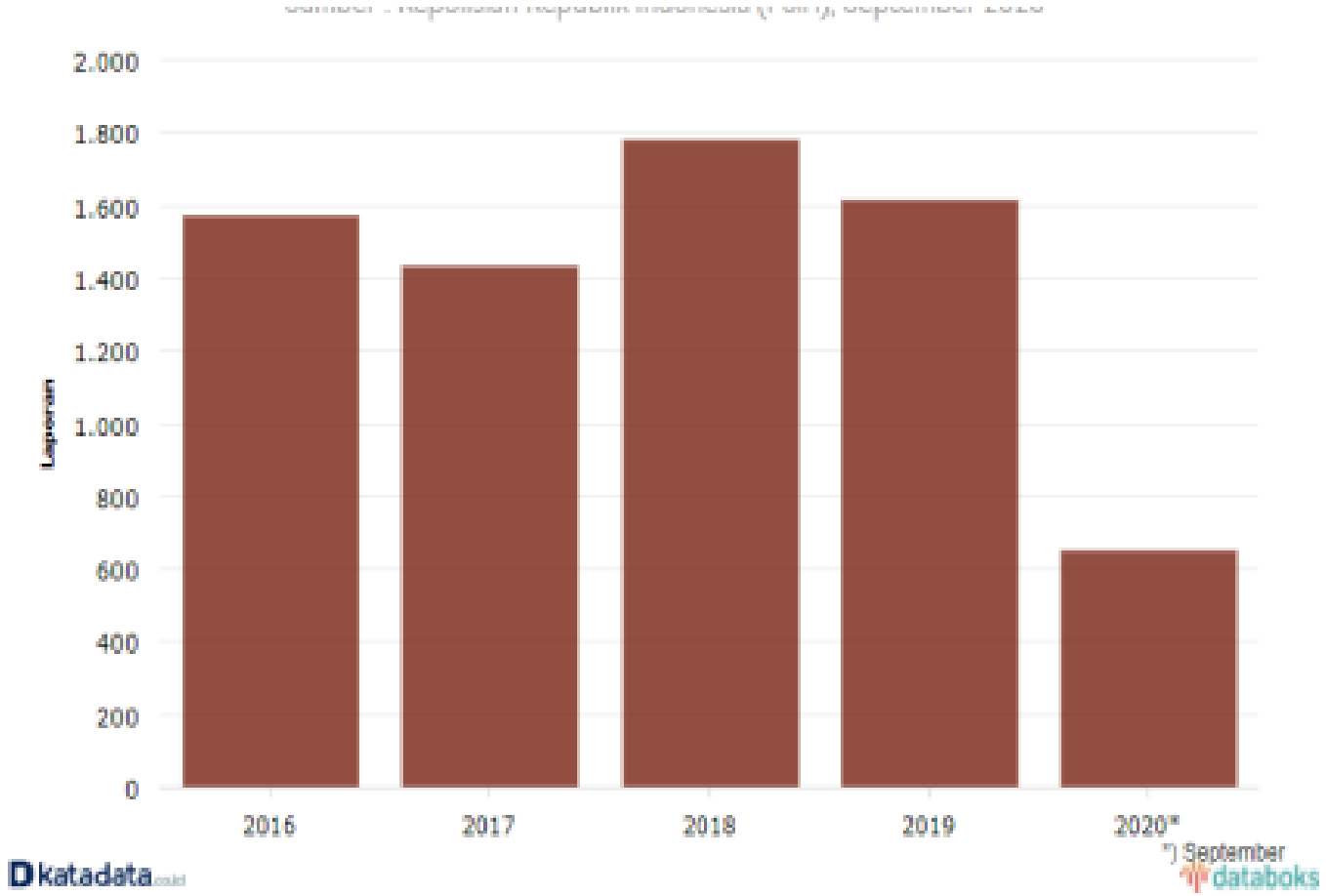
DIGITAL CULTURE

Perlindungan terhadap Penggunaan *One-time Passwords* (OTP)

- Pahami modus calon pembobol OTP yang menggunakan nomor ponsel calon korban dengan memilih opsi "lupa *password*"
- Waspada jika ada calon pembobol OTP yang menelepon untuk menawarkan hadiah atau meminta bantuan
- Jangan berikan kode OTP pada calon pembobol yang bertanya dengan berbagai macam alasan
- Ragulah terhadap semua telepon dan SMS yang menawarkan hadiah
- Kenali berbagai modus penipuan supaya tidak mudah terseret menjadi korban penipuan
- Segera lapor ke pihak terkait jika terlanjur memberikan kode OTP kepada orang lain

BAB IV
MEMAHAMI DAN MENGHINDARI PENIPUAN DIGITAL

Jumlah Laporan Penipuan Daring per Tahun



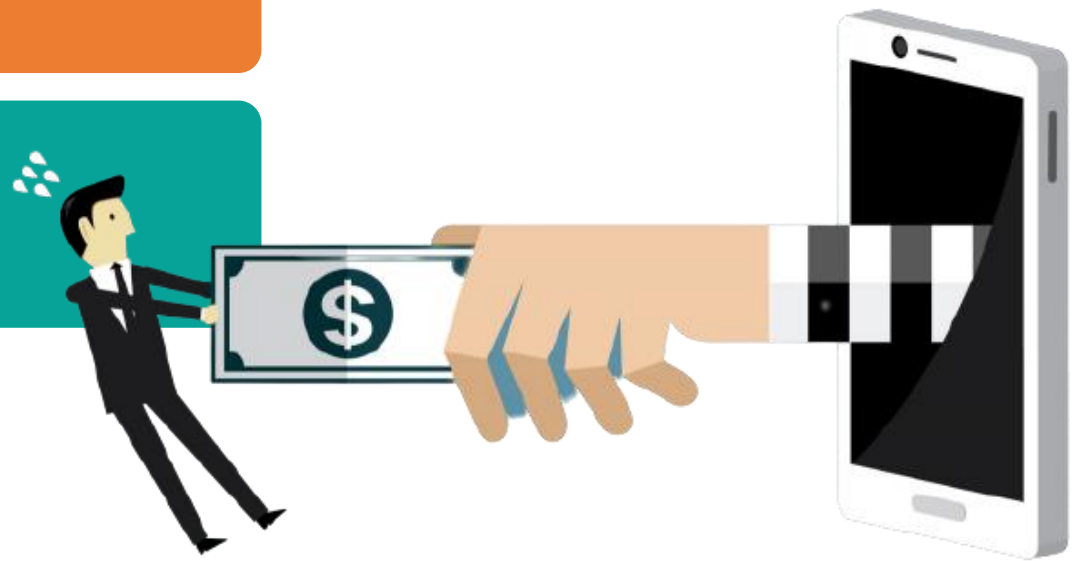
Sumber : Kepolisian Republik Indonesia, September 2020

Modus Penipuan Digital di Media Sosial

Penipuan harga diskon barang atau produk yang ditawarkan

Identitas pelaku usaha atau konsumen fiktif

Ketidaksesuaian barang atau produk yang diterima dengan yang di pesan



Ragam Penipuan Digital

Scam	Memanfaatkan empati dan kelengahan pengguna
Spam	Informasi mengganggu yang berbentuk iklan secara halus. Baik berupa pemalsuan data, penipuan atau pencurian data yang dilakukan bertubi-tubi atau berulang-ulang
Phising	Menjebak korban dengan target menyasar kepada orang-orang yang percaya bahwa informasi yang diberikannya jatuh ke orang yang tepat
Hacking	Tindakan dari seorang yang disebut sebagai *hacker* yang sedang mencari kelemahan dari sebuah sistem komputer

Contoh-Contoh Modus Scam

Para pelaku meminta uang dengan alasan ada kerabat yang sakit dan ingin dilarikan ke rumah sakit

Mengirimkan barang untuk korban, namun tertahan di imigrasi. Para pelaku meminta uang untuk barang yang tertahan agar segera dikirim ke korban

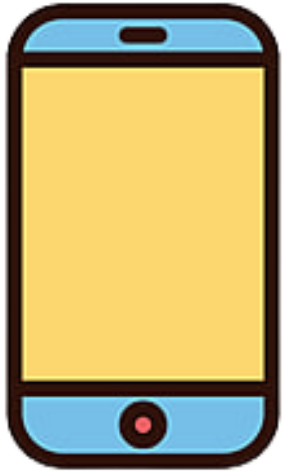
Keluarga dari pelaku tiba-tiba hilang dan pelaku meminta uang kepada korban untuk mencari keluarganya

Para korban biasanya dimintakan sejumlah uang untuk biaya kesehatan pelaku

Dengan alasan perbaikan untuk kendaraannya, para pelaku meminta uang kepada korban untuk hal tersebut

Contoh-Contoh Modus Spam

E-mail



Telepon

SMS

Contoh-Contoh Modus *Phising*

- Menjual Informasi Curian
- Mencuri Data Korban
- Mencuri Uang dari Rekening milik Korban
- Menyerang Kontak dalam Jaringan Rekanan Korban

Contoh- Contoh Modus *Hacking*

Umumnya cara kerja para hacker adalah dengan melakukan **pembobolan/peretasan** sampai dengan **percobaan keamanan situs-situs** web dan komputer dapat mereka lakukan

Contoh Kasus :

Akun Tokopedia yang dibobol hacker	Pemberitahuan virus yang dapat membobol akun	Hack situs web KPU Yogyakarta

Hukum untuk Pelaku Kejahatan Scam, Spam, *Phising* dan *Hacking* (1)

UU ITE Pasal 45A Ayat (1)

"Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik" dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)

UU No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang

"Setiap Orang yang menerima atau menguasai penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau menggunakan Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)"

Memahami Pelaporan Penipuan dan Pengecekan Secara Digital (1)

1. Laporkan kejahatan siber di sekitar kita melalui www.patrolisiber.id

2. Laporkan SMS spam ke Badan Regulasi Telekomunikasi Indonesia (BRTI) dengan cara melakukan tangkapan layar pada SMS spam dan nomor pengirim dengan menyertakan identitas ponsel kita yang telah teregistrasi NIK dan KK atau kirim aduan ke Twitter BRTI @aduanBRTI melalui direct message (DM)

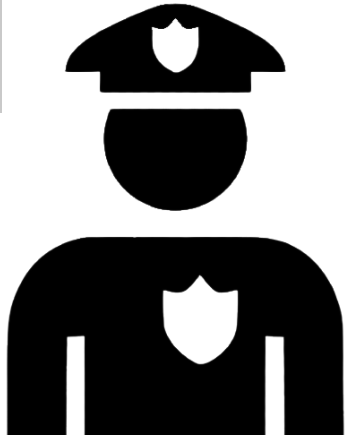
3. Melakukan pengecekan dan pelaporan rekening penipu mulai dari nama pemilik, nama bank, hingga rekaman transaksi sehingga nomor rekening penipu dapat dibekukan melalui:
    - CekRekening.id
    - Kredibel.co.id
    - Otoritas Jasa Keuangan (OJK) melalui layanan pengaduan ke 1-500-655 atau email ke konsumen@ojk.go.id

Memahami Pelaporan Penipuan dan Pengecekan Secara Digital (2)

4. Situs resmi Kepolisian Republik Indonesia Lapor.go.id atau dapat juga mengadu melalui SMS ke 1708, aplikasi LAPOR! atau melalui akun Twitter@LAPOR1708 dengan menyematkan #lapor

5. Melapor ke CS KK maupun CS penyedia layanan produk/CS ecommerce seperti CS Shopee, CS Bukalapak, CS Tokopedia dan seterusnya

6. Instagram @indonesiablacklist



BAB V
MELINDUNGI REKAM JEJAK DIGITAL

Bentuk Rekam Jejak Digital (*Digital Footprints*)

Jejak Digital Pasif

Jejak data yang kita tinggalkan secara daring dengan tidak sengaja dan tanpa sepengetahuan kita. Biasanya digunakan untuk mencari tahu profil pelanggan, target iklan, dan lain sebagainya

Jejak Digital Aktif

Mencakup data yang dengan sengaja kita kirimkan di internet atau di platform digital*
Contohnya seperti mengirim email, mempublikasikan di media sosial, mengisi formulir daring, dan lain sebagainya.

*Vonbank, 2019

Jejak Digital Yang Kita Tinggalkan

Untuk memastikan bahwa situs dan aplikasi yang kita gunakan **tidak membahayakan jejak digital** kita, maka ada baiknya bila kita *memeriksa dan membandingkan* sistem keamanan situs web, aplikasi, dan metode transaksi elektronik yang ditawarkan oleh perorangan, toko, perusahaan, dan penyedia jasa perantara sebelum melakukan transaksi daring.

(Kurnia, dkk., 2021)

10 Kompetensi untuk Mengelola Jejak Digital

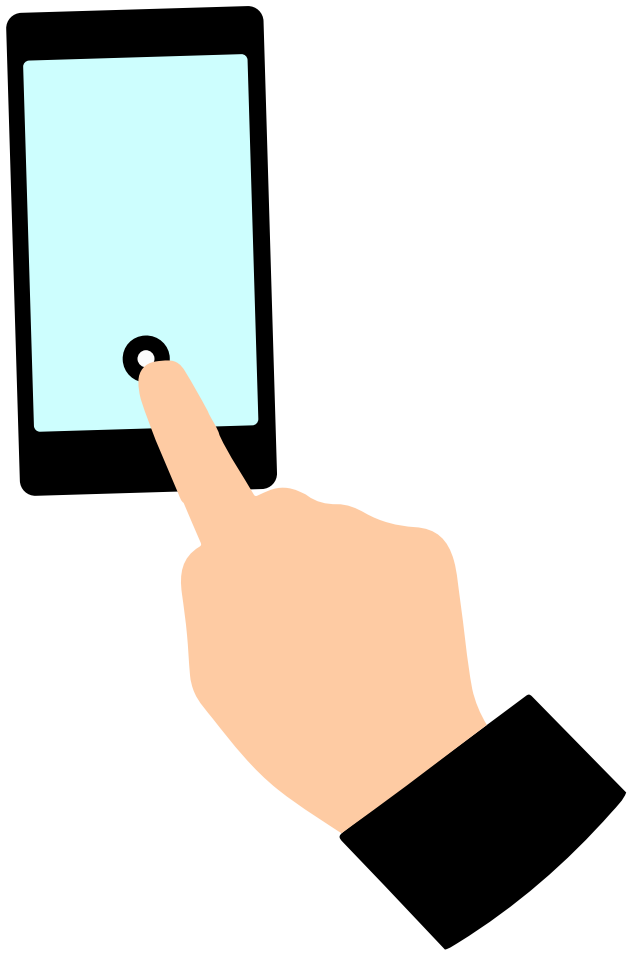
- Memiliki kemampuan untuk mengakses atau secara aktif menggunakan sarana internet dalam kehidupan sehari-hari
- Mengasah kompetensi atau kemampuan tentang jejak digital
- Mengetahui bentuk-bentuk rekam jejak digital
- Menyeleksi apa saja yang kita unggah
- Verifikasi untuk memastikan apakah langkah yang akan kita lakukan dapat berpotensi meninggalkan jejak digital yang berdampak buruk atau tidak
- Evaluasi atas berbagai kegiatan daring
- Ketika kita mendistribusikan informasi dengan menggunakan perangkat digital, maka kita telah meninggalkan jejak digital
- Meningkatkan kemampuan kita dalam memproduksi rekam jejak digital yang baik
- Membagikan pengetahuan yang telah kita dapatkan tentang rekam jejak digital
- Berkolaborasi dengan berbagai pihak dalam rangka partisipasi menjaga rekam jejak digital

BAB VI
KEAMANAN ANAK DI PLATFORM DIGITAL

#MakinCakapDigital

DIGITAL SAFETY

URGENSI KEAMANAN ANAK



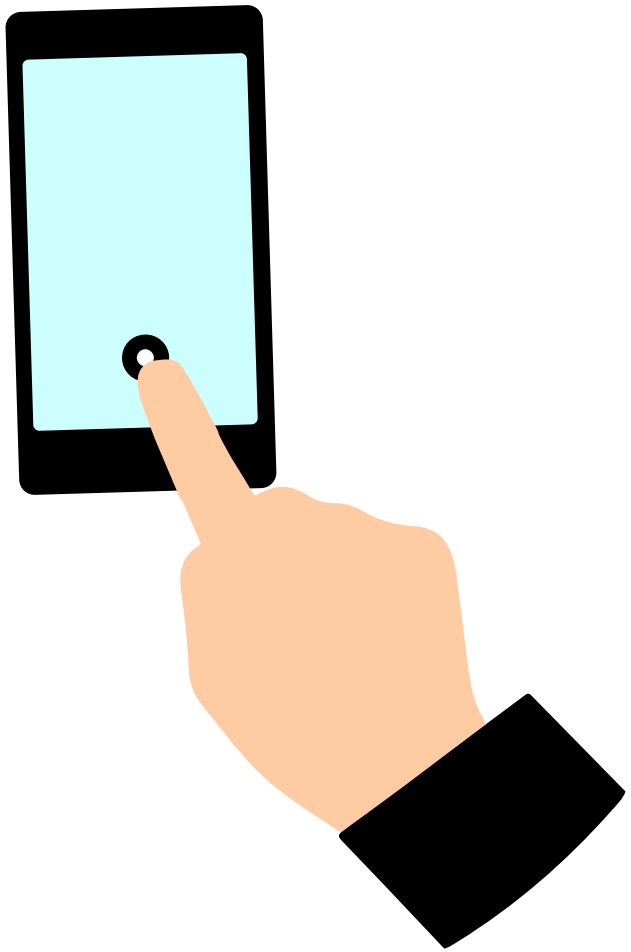
1. Semua orang dapat membuat pesan sehingga anak-anak pun tertarik memiliki akun sendiri, menampilkan diri dan berinteraksi dengan orang lain yang tidak dikenaL
2. Sifat pesan media digital sangat beragam sehingga memungkinkan anak-anak menerima aneka pesan yang sangat mungkin tidak sesuai dengan nilai-nilai agama dan budaya keluarga
3. Penyedia layanan media digital ingin mendapatkan keuntungan ekonomi maka mereka merancang medianya agar menarik
4. Jika digunakan secara baik media digital adalah sumber pengetahuan tak terbatas

Aspek-aspek Keselamatan Anak Di Media Digital

1. Perundungan (*Bullying*)
2. Perdagangan Orang
3. Pencurian Data Pribadi
4. Pelecehan Seksual dan Pornografi
5. Penipuan
6. Kekerasan
7. Kecanduan

Nilai-Nilai Penting dalam Bermedia Digital

1. Mengembangkan kreativitas di era digital melalui berbagai pengalaman menggunakan media digital
2. Mengajarkan anak untuk berinteraksi dan bekerjasama dengan orang dari beragam latar belakang budaya dan keterampilan
3. Mengajarkan anak untuk kritis dalam berpikir
4. Memiliki kompetensi yang memadai dalam mengarahkan anak-anak sehingga dapat mencegah mereka menjadi pelaku atau korban dari penggunaan media digital



Tips Meningkatkan Kemampuan dalam Mengakses Media Digital

1. Kemampuan membagi informasi
2. Kemampuan mengemas informasi
3. Kemampuan mengenal teman dan lingkungan

Tips Meningkatkan Kemampuan dalam Mendistribusikan Informasi melalui Media Digital

1. Kemampuan memilih media sosial

2. Kemampuan menyaring informasi

3. Kemampuan mengatur waktu

Tips Meningkatkan Kemampuan dalam Partisipasi terkait Media Digital

1. Kemampuan menyampaikan informasi yang baik dan etis
2. Kemampuan menggunakan media digital secara produktif
3. Kemampuan melaporkan pelanggaran dalam penggunaan media digital
4. Kemampuan berkata ‘tidak’ terhadap ajakan negatif

Tips Meningkatkan Kemampuan dalam Melakukan Kolaborasi melalui Media Digital

Kemampuan untuk bergabung dalam forum atau komunitas

Kemampuan menciptakan pertemanan

Tips Keamanan Digital bagi Anak-Anak

Batasi Informasi Pribadi	Batasi Penggunaan Gawai	Kenali Ancaman Keselamatan	Saring sebelum *Sharing*
Ingatkan anak-anak agar tidak gegabah saat memberikan informasi yang sifatnya pribadi ketika berinteraksi di media digital. Berhati-hati ketika berbagi nomor kontak, alamat rumah, sekolah atau informasi lain yang memungkinkan orang-orang yang tidak bertanggung jawab melacaknya.	Beri batasan waktu yang tegas kepada anak-anak saat menggunakan media digital. Dengan adanya pembatasan waktu, dapat meminimalisir berbagai ancaman keselamatan bagi anak-anak.	Ajak dan tunjukkan kepada anak-anak berbagai potensi ancaman termasuk modus yang biasa digunakan. Biasakan anak-anak terbuka. Latih anak-anak untuk mengendalikan emosinya dan bila memungkinkan mengalihkan emosi tadi pada kegiatan yang positif.	Pikirkan dengan baik sebelum berbagi pesan, karena sekali tersebar, sulit di hapus. Biasakan anak-anak untuk tidak begitu saja membuka pesan termasuk tautan yang diterima. Pastikan dahulu kejelasan pengirimnya.

BAB VII
TANTANGAN KEAMANAN DIGITAL

Tips Aman Bermedia Digital

Memahami berbagai konsep dan mekanisme proteksi baik terhadap perangkat digital (lunak maupun keras) maupun terhadap identitas digital dan data diri

Mempunyai kesadaran bahwa keamanan digital bukan sekadar tentang perlindungan perangkat digital sendiri dan data diri sendiri

Melakukan perlindungan identitas digital dan data diri

Tantangan Keamanan Digital

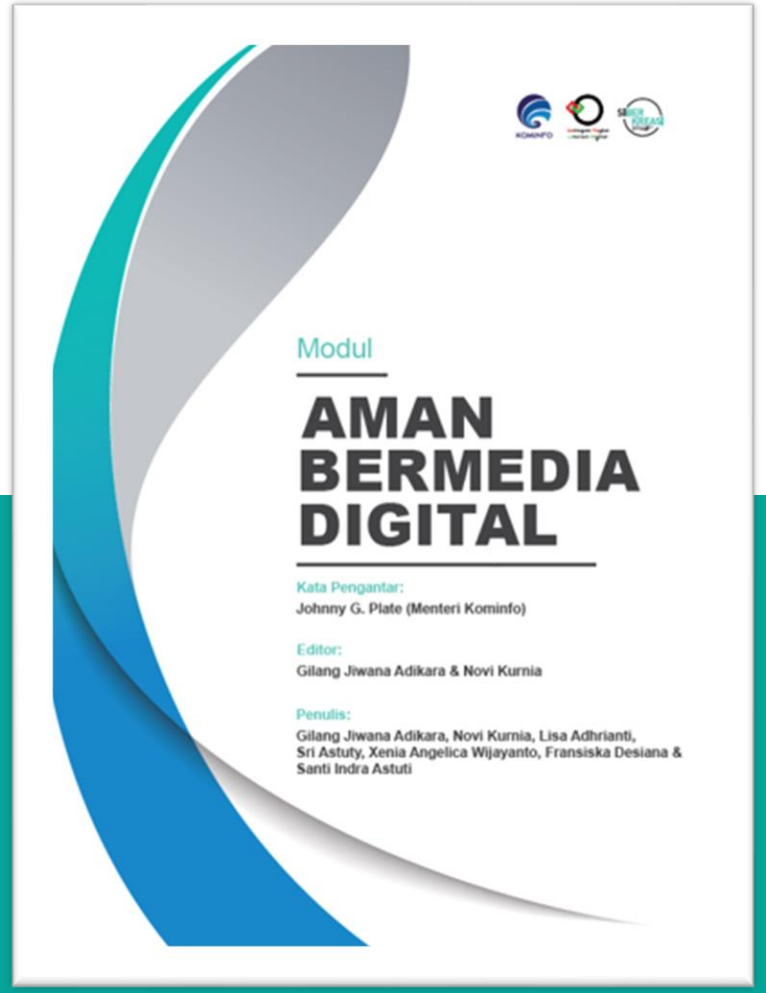
01 Fitur proteksi yang semakin beragam dan platform yang semakin berkembang

02 Kompleksitas identitas digital dan data pribadi yang tak mudah untuk dilindungi

03 Ragam penipuan digital yang semakin banyak

04 Rekam jejak yang dimanfaatkan lebih banyak negatifnya dari positifnya

05 *Minor safety* untuk anak yang semakin menantang terutama saat pandemi



Modul
AMAN BERMEDIA DIGITAL
(KOMINFO – JAPELIDI – SIBERKREASI)

Follow IG
@siberkreasi