

TIPS PRAKTIS DI DUNIA SIBER



TIPS PRAKTIS DI DUNIA SIBER



DIREKTORAT JENDERAL INFORMASI DAN KOMUNIKASI PUBLIK
KEMENTERIAN KOMUNIKASI DAN INFORMATIKA

TIPS AMAN DI DUNIA SIBER

Cetakan: Pertama

ISBN: 978-623-90784-7-8 (PDF)

Penyusun

Tim Indonesiabaik.id

Pengarah

Prof. Dr. Widodo Muktiyo

Pemimpin Redaksi

Sumiati

Wakil Pemimpin Redaksi

Dimas Aditya Nugraha

Redaktur Pelaksana

Andrean W Finaka

Editor

Edy Pang

Tim Redaksi & Kontributor

Siap Bangun Negara

Yuli Nurhanisah

Titania Nurrahim

Ali Ridho

Muhammad Rifqi

Rokayah

Lestari

Riana Rizkinandini

Reaza Rahmatika

Karina Listya Widyasari

April Lokita Sulasmi

Desain & Ilustrasi

Ananda Syaifullah

Chyntia Devina

M. Ishaq Dwi Putra

Oktanti Putri Hapsari

Alamat Redaksi

Direktorat Pengelolaan Media

Direktorat Jenderal Informasi dan Komunikasi Publik

Kementerian Komunikasi dan Informatika

Jl. Merdeka Barat No.9 Jakarta Pusat 10110

Telepon (021) 384 4309

Penerbit

Direktorat Jenderal Informasi dan Komunikasi Publik

Kementerian Komunikasi dan Informatika

Jl. Merdeka Barat No.9 Jakarta Pusat 10110

Telepon (021) 384 4309

PENGANTAR REDAKSI

Assalamualaikum Warahmatullahi Wabarakatuh,
Salam sejahtera bagi kita semua

Puji syukur kita panjatkan ke hadirat Tuhan YME, atas berkat dan rahmat-Nya booklet dengan judul **“Tips Praktis di Dunia Siber”** dapat diterbitkan.

Bagian pertama dari booklet E-Safety mengetengahkan latar belakang masifnya jumlah pengguna internet dan smart phone di dunia. Perkembangan budaya internet diikuti berkembangnya kejahatan internet yang umumnya mengacu pada aktivitas kejahatan dengan komputer serta jaringannya.

Fenomena sosial pun terbentuk sesuai jumlah pengguna internet yang semakin masif dan semakin berkembang hingga menjadi fenomena sosial terkait bentuk lain komunikasi jaringan, seperti komunitas online, game multi-player online, serta jejaring sosial. Akibatnya, muncul berbagai macam kasus dan modus serangan siber, pengguna harus mampu menghadapinya.

Booklet infografis ini merangkum berbagai informasi dan kiat berselancar di dunia siber dengan aman dan menghadapi banyaknya kejahatan siber. Semoga informasi yang disampaikan dapat diterima dengan baik oleh publik dan pembaca setia indonesiabaik.id. Saran dan kritik membangun sebagai umpan balik sangat kami harapkan untuk pembuatan konten yang lebih baik kedepannya.

Terima kasih.
Wassalamualaikum Warahmatullahi Wabarakatuh,

Jakarta, Oktober 2019

Redaksi

PENGANTAR DIRJEN IKP

Assalamualaikum Warahmatullahi Wabarakatuh,
Salam sejahtera bagi kita semua

Puji syukur kita panjatkan ke hadirat Tuhan YME, atas berkat dan rahmat-Nya booklet dengan judul **“Tips Praktis di Dunia Siber”** dapat diterbitkan.

Jumlah pengguna internet yang besar dan semakin berkembang menjadi fenomena sosial terkait bentuklain komunikasi jaringan, seperti komunitas online, game *multi-player online*, serta jejaring sosial. Bahkan, menurut Statista jumlah pengguna mobile phone dunia mencapai 5,14 miliar dan pengguna Internet lebih dari 4 miliar.

Perkembangan budaya internet diikuti pula dengan perkembangan kejahatan internet yang tidak kalah pesat. Umumnya kejahatan internet mengacu pada aktivitas kejahatan dengan komputer atau jaringan komputer sebagai unsur utama.

Oleh karena itu, dengan berbagai macam kasus dan modus serangan siber, pengguna harus mampu menghadapinya. Buku ini berisi tip dan informasi bagaimana berselancar di dunia siber dengan aman dan menghadapi banyaknya kejahatan siber. Semua itu dirangkum dalam booklet infografis ini. Terakhir, semoga informasi yang disampaikan dapat diterima dengan baik oleh para pembaca. Terima kasih.

Wassalamualaikum Warahmatullahi Wabarakatuh,

Jakarta, Oktober 2019
Dirjen Informasi dan Komunikasi Publik

Prof. Dr. Widodo Muktiyo, SE. M.Com

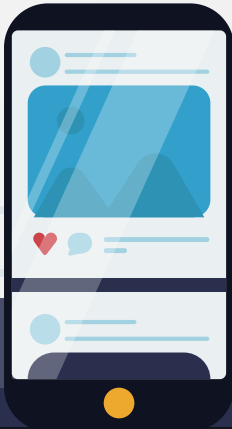
DAFTAR ISI

ISBN dan info buku	ii
Pengantar Plt Dirjen IKP Kominfo	iii
Pengantar Redaksi	iv
Daftar Isi	v
Bijak Memberi Data Pribadi di Media Sosial	2
Mencegah Akun Dari Peretasan	4
Taat Aturan saat Bermedia Sosial	6
Penyelenggara Sertifikasi Elektronik dan Tanda Tangan Elektronik Memudahkan ASN dan Keamanan Siber	8
Cegah Penyalahgunaan Informasi Data Pribadi di Indonesia	10
Denda Konten Ilegal Bagi Platform	12
Penyelenggara Sistem Elektronik di Indonesia Harus Terdaftar atau Kena Pasal	14
Filosofi Sikat Gigi untuk Keamanan Kata Sandi (Password)	16
Gunakan Enkripsi untuk Menjaga Integritas Data	18

Tetap Tenang Hadapi Serangan Siber: Phising dan Social Engineering	20
Cara Tangkal Spam, Malware, Ransomware, Virus, dan Spyware	22
Modus Hoax di Whatsapp	24
Jerat Hukum untuk Penyebar Hoax	26
patrolisiber.id, Memberantas Hoax	28
Cermat Agar Tidak Tertipu saat Belanja Online	30
Wujudkan Keamanan Nasional Bidang Siber	32
Tata Cara Lapor Korban Kejahatan Siber	34
Ancaman Keamanan & Kejahatan di Dunia Siber	36
Identifikasi Nomor IMEI untuk Melindungi Masyarakat	38
Cara Cek IMEI Ponsel Legal atau Ilegal	40
Sumber	42



BIJAK MEMBERI DATA PRIBADI DI MEDIA SOSIAL



Peraturan Perlindungan Data Pribadi (PDP) RI hingga saat ini masih dalam pembahasan. Institusi atau perusahaan yang mengelola database pribadi konsumen atau pengguna yang biasa disebut Data Controller (DCO) dan bertanggung jawab melindungi data pribadi konsumen sebagai pemilik data seperti dalam **PP No.71/2019**.



Setiap perlakuan terhadap data dari seorang klien **harus diberikan secara bebas atau berdasarkan keinginan atau tanpa tekanan** atau dengan kata lain harus dengan persetujuan dan izin dari klien pemilik data.

SEORANG PENGGUNA MEDIA SOSIAL, SITUS, ATAU KONSUMEN E-COMMERCE MEMILIKI HAK PRIVASI:



Agar data pribadi **dihapus atau diremajakan**



Agar data pribadi dilindungi kerahasiaannya, seperti informasi yang dapat mengidentifikasi nama, nomor ID, lokasi data, atau identifikasi dari faktor seperti fisik, genetik, mental, agama, sosial, budaya dan ekonomi seseorang



Agar perekaman, penggambaran dan analisa atas profil suatu objek harus seizin data subjek tersebut termasuk segala bentuk personalisasi, prediksi mengenai kinerja, pekerjaan, ekonomi, keuangan, kesehatan, preferensi personal, ketertarikan, hobi, kelakuan, lokasi dan pergerakannya



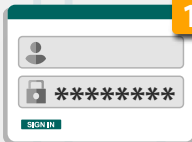
MENCEGAH AKUN DARI PERETASAN



Kemudahan akses yang ditawarkan oleh internet menjadi nilai tambah dunia maya. Bahkan, saat ini pengguna internet di Indonesia sekitar 171 juta. Di Indonesia, **kasus kejahatan digital yaitu peretasan sistem elektronik mencapai angka 126 kasus**

BAGAIMANA CARA MENINGKATKAN KEAMANAN INFORMASI AKUN?

1. Buatlah kata sandi yang rumit



Kata sandi (*password*) yang digunakan untuk mengakses akun aplikasi atau situs web (*website*) **terdiri dari gabungan angka, huruf kecil, huruf kapital, dan huruf khusus**

2. Gunakan *password manager*



Password Manager yaitu perangkat lunak atau jasa yang membantu **menyimpan kata sandi dan nama pengguna** untuk situs web



3. Jangan memberikan kata sandi kepada orang lain

Sebaiknya pengguna berusaha untuk **tidak memberikan kata sandi** kepada orang lain atau pengurus situs web



4. Ubahlah kata sandi secara teratur

Selain merahasiakan kata sandi, pengguna juga harus **mengubah seluruh kata sandi akun dan peranti** paling tidak sekali dalam enam bulan



5. Gunakan *Two-factor Authentication*

Metode ini mempersulit dan mencegah peretas untuk **mengakses informasi** bahkan ketika berhasil menemukan kata sandi pengguna



6. Bacalah Kebijakan Privasi (*Privacy Policy*) dengan hati-hati

Perusahaan apa pun yang memiliki informasi harus **mempunyai Kebijakan Privasi** yang menjelaskan bagaimana perusahaan tersebut menggunakan informasi pribadi

TAAT ATURAN

saat Bermedia Sosial

Dalam rangka menjunjung tinggi Nilai Dasar, Kode Etik, dan Kode Perilaku ASN, serta pembinaan profesi, ditekankan bagi para ASN dalam penyebaran informasi melalui media sosial agar memperhatikan hal-hal berikut,



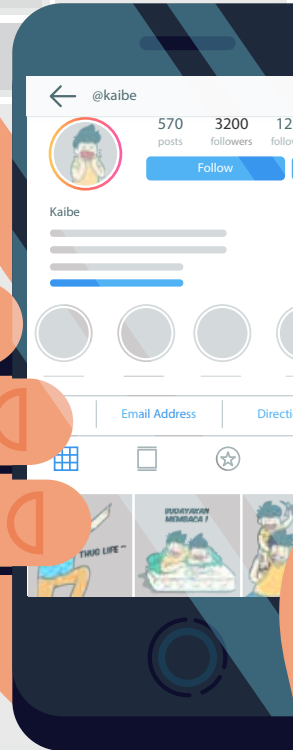
Memegang teguh ideologi Pancasila, dan mempertahankan UUD RI 1945 serta pemerintahan yang sah, mengabdikan kepada negara dan rakyat Indonesia, serta menjalankan tugas secara profesional dan tidak berpihak



Memelihara dan menjunjung tinggi standar etika yang luhur, memegang nilai dasar ASN, dan selalu menjaga reputasi dan integritas ASN



Menjaga kerahasiaan yang menyangkut kebijakan negara, memberikan informasi secara benar dan tidak menyesatkan kepada pihak lain terkait kepentingan kedinasan





Tidak menyalahgunakan informasi intern negara untuk mendapat atau mencari keuntungan atau manfaat bagi diri sendiri atau untuk orang lain



Memastikan bahwa informasi yang disebarluaskan jelas sumbernya, dapat dipastikan kebenarannya, dan tidak mengandung unsur kebohongan



Tidak membuat dan menyebarkan berita palsu (hoax), fitnah, provokasi, radikalisme, terorisme, dan pornografi melalui media sosial atau media lainnya



Tidak memproduksi dan menyebarkan informasi yang memiliki muatan yang menimbulkan rasa kebencian terhadap individu atau kelompok tertentu berdasarkan SARA, melanggar kesusilaan, perjudian, pencemaran nama baik, pemerasan atau pengancaman.

PENYELENGGARA SERTIFIKASI DAN TANDA TANGAN ELEKTRONIK

Memudahkan ASN dan Keamanan Siber

Pada November 2019, Kementerian Komunikasi dan Informatika telah meresmikan Penyelenggara Sertifikasi Elektronik (PSrE) dan Tanda Tangan Elektronik (TTE).

Tujuan PSrE dan TTE



Meminimalkan pemalsuan dokumen milik pemerintah ataupun perusahaan di Indonesia



Memudahkan ASN (Aparatur Sipil Negara) bekerja dimanapun



Bisa meminimalisir dan menangkal kejahatan siber





Penyelenggara Tanda Tangan Elektronik

Badan Pengkajian dan Penerapan Teknologi (BPPT), Badan Siber dan Sandi Negara (BSSN), Perusahaan Umum Percetakan Uang Republik Indonesia (Perum Peruri), Privyld, Vida, Digisign

Layanan Penyelenggara Tanda Tangan Elektronik

Tanda tangan elektronik, Segel elektronik, Preservasi, Otentifikasi, Pengiriman elektronik tercatat, Penanda waktu



Cegah Penyalahgunaan Informasi Data Pribadi di Indonesia

Tahukah SoHIB?

Pada 2019, Facebook selaku **Penyelenggara Sistem Elektronik (PSE) platform media sosial**, membayar denda **USD 5 M** (sekitar Rp70 T dengan kurs 12/11/2019) kepada Komisi Perdagangan Federal AS atas pelanggaran privasi data pengguna.

PP No.71/2019

Pemerintah Indonesia berupaya melindungi kepentingan umum agar **penyalahgunaan informasi dan transaksi elektronik tidak terjadi di Indonesia**.



Pasal 14



Pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, adil, dengan **sepengetahuan dan persetujuan dari pemilik data pribadi**



Pemrosesan data pribadi dilakukan sesuai dengan tujuannya **dengan menjamin hak pemilik data pribadi**



Pemrosesan data pribadi dilakukan akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat **dipertanggungjawabkan**



Pemrosesan data pribadi dilakukan dengan **melindungi keamanan data pribadi** dari kehilangan, penyalahgunaan, akses dan pengungkapan yang tidak sah, serta perubahan/perusakan data pribadi

Denda Konten Ilegal Bagi Platform

Pemerintah kini tak lagi aktif melakukan pemblokiran bagi platform (situs, aplikasi, e-commerce, pesan instan, mesin pencari, atau media sosial) yang memuat konten ilegal menurut Undang-Undang. Tapi, pemerintah akan memberlakukan denda yang signifikan.

Rp100-500 juta

Denda per konten bagi platform yang memuat/memfasilitasi konten ilegal

2021

Rencana waktu pemberlakuan denda

Data Januari 2018 Hingga Juni 2019



200 ribu

total aduan konten



Hampir 90 %

situs negatif yang diblokir
bermuatan pornografi

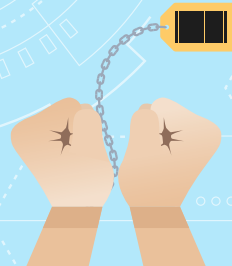


1,09 juta

situs diblokir



Jenis-jenis Konten Ilegal



Penyelenggara **SISTEM ELEKTRONIK** di Indonesia

Harus Terdaftar atau Kena Pajak

Kemenkominfo memberi waktu satu tahun kepada sejumlah *platform* media elektronik dan digital untuk mendaftar sebagai Penyelenggara Sistem Elektronik (PSE). *Platform* yang dimaksud meliputi situs, aplikasi, *e-commerce*, pesan instan, mesin pencari, atau media sosial.



Tenggat Waktu Pendaftaran
10 Oktober 2019 - 10 Oktober 2020

Mengapa harus terdaftar?

Karena setiap penyelenggara sistem elektronik harus menyelenggarakan sistem elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya sistem elektronik sebagaimana mestinya

Mendaftar kemana?

Pendaftaran penyelenggara sistem elektronik diajukan kepada Menteri melalui pelayanan perizinan berusaha terintegrasi secara elektronik sesuai dengan ketentuan peraturan perundang-undangan yang diatur dengan Peraturan Menteri.



Sanksi

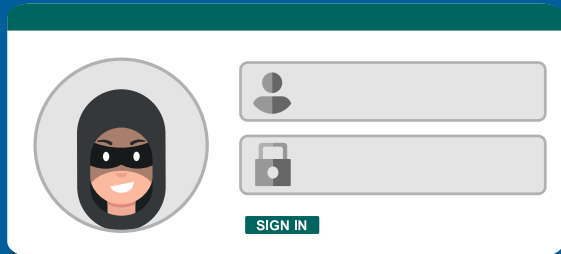
Diberikan kepada Penyelenggara Sistem Elektronik yang tidak mendaftar sesuai tenggat, berupa

- Teguran tertulis
- Denda administratif
- Penghentian sementara
- Pemutusan akses
- Dikeluarkan dari daftar

FILOSOFI SIKAT GIGI UNTUK KEAMANAN KATA SANDI (*PASSWORD*)

Tahukah Sohib?

Peneliti keamanan internet Troy Hunt pada Januari 2019 merilis temuan **lebih dari 770 juta alamat email dan 21 juta kata sandi pengguna di seluruh dunia telah dibobol** untuk diambil datanya!



Kata sandi (*password*) adalah hal utama dalam keamanan saat berselancar di dunia siber. Bagaimana cara membuat *password* yang tidak mudah dibobol peretas (*hacker*) dan mudah diingat?

KATA SANDI (PASSWORD) ITU SEPERTI SIKAT GIGI



1. Pilih yang paling bagus

- **Jangan gunakan password dengan suku kata umum.** Gunakan campuran huruf, angka, tanda baca dan simbol typografi seperti “@!*&%;” dll agar sulit ditebak dan dirangkai oleh peretas
- Jangan gunakan password yang sama di semua platform dan perangkat

2. Ganti secara berkala

- Jangan gunakan *Default Password*. Segera ganti kata sandi yang diberikan pabrik (*Factory set default password*)
- Selalu ganti (*refresh*) password pada perangkat/gawai, komputer, wifi router secara periodik (30, 60, atau 90 hari sekali)

3. Jangan berbagi dengan siapapun

- Jangan menyimpan *password* sembarangan di tempat yang bisa diakses umum atau orang lain

GUNAKAN ENKRIPSI UNTUK MENJAGA INTEGRITAS DATA

Tahukah Sohib?

Mengapa email atau data transaksi perbankan **harus di enkripsi jika ingin aman?**

Enkripsi adalah suatu **proses untuk merahasiakan berita** agar pihak yang tidak berwenang tidak dapat membaca dan mengerti isi yang diberitakan



Agar aman, upayakan agar email atau data transaksi perbankan Anda di enkripsi!

Fungsi Enkripsi



Kerahasiaannya terlindungi dari upaya penyadapan



Integritasnya terjamin, agar data tidak diubah, dihapus, atau diganti



Otentisitas data pengirim terverifikasi, jelas dan tidak anonim





TETAP TENANG HADAPI SERANGAN SIBER: *PHISHING DAN SOCIAL ENGINEERING*

Saat ini, banyak modus serangan siber di dunia maya seperti phishing dan social engineering (SosEng) yang sulit sulit ditangkal karena memanfaatkan kelalaian pengguna

Jumlah Pengguna Media Sosial



Phishing dan Social Engineering



Social Engineering (SosEng) menggunakan metode penyamaran, misalnya menyuar sebagai bos perusahaan dan menelpon satpam atau admin web untuk mendapatkan informasi rahasia seperti password

Phishing adalah upaya menyuar sebuah situs untuk melakukan penipuan

Tips Menghadapi Phishing

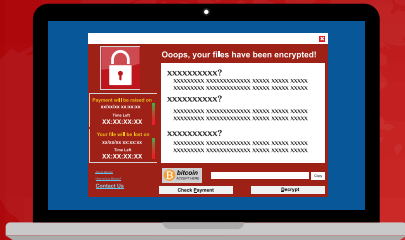


- **Jangan panik** dan tetap tenang menghadapi serangan phishing
- **Segera hubungi call center** atau datangi kantor dari perusahaan yang asli atau sebenarnya
- **Laporkan ke polisi** agar situs penyamar pelaku phishing segera di blokir, ditutup dan pelaku phishing dikejar
- **Rubah semua password** dan login informasi agar tidak disusupi oleh cracker

Tips Menghadapi Social Engineering



- **Segera laporkan ke instansi yang bersangkutan** informasi yang tanpa sengaja anda bocorkan kepada pelaku SosEng
- **Laporkan cara, kelemahan dan kerugian** yang anda alami akibat SosEng
- **Sosialisasi modus SosEng yang digunakan** untuk melakukan SosEng kepada semua pihak
- **Laporkan kepada aparat penegak hukum** dinas *Sibercrime* untuk menangkap pelakunya



CARA TANGKAL *SPAM*, *MALWARE*, *RANSOMWARE*, *VIRUS*, DAN *SPYWARE*

Tahukah SoHIB?

Security Incident Response Team on Internet Infrastructure mengungkapkan ada lebih dari **150 juta serangan malware** (piranti peretas) yang terdeteksi di dunia (2017)!

Contohnya:

- **Jenis ransomware** (piranti peretas yang meminta ransom/uang tebusan)
- Didominasi oleh **Locky dan WannaCry**
- Ransomware tumbuh sebesar **350%** pada 2018
- **Spyware** adalah **piranti spionase peretas** yang digunakan untuk mencuri, menyadap file, keyboard, kamera, mikrofon, dan disk di gawai



Bagaimana Menangkalnya untuk Keamanan Siber?



Rajin Update Sistem: Malware/virus selalu mencari kelemahan di setiap sistem agar bisa dibobol. Karena itu, sistem operasi dan software anti virus komputer dan smartphone harus diperbarui (update) sesuai rekomendasi pabrik, sehingga sistem keamanan sudah menggunakan sistem yang terbaru dan sudah diuji coba terhadap malware versi sebelumnya



Gunakan Antivirus: Gunakan dan update antivirus/antispam/antispysware/worm untuk PC, gawai dan smartphone agar selalu mempunyai penangkal virus/spam terbaru. Scan secara menyeluruh dan berkala untuk mencegah program malware, virus, spam, worm yang ingin masuk ke dalam komputer/smartphone



Back-up Data: Back-up dokumen, foto atau berkas penting lainnya ke flashdisk, harddisk cadangan (offline) atau ke layanan google dropbox (online). Agar memiliki data cadangan, jika data hilang karena virus atau di sandera oleh ransomware yang meminta uang tebusan, maka dapat dipulihkan dengan data back-up



Jangan Klik Link Web dan Download File yang tidak dikenal: Karena dapat membangunkan malware, virus, ransomware yang ada di file yang di download atau attachment yang di klik, konsekuensinya data dalam gawai sudah terkontaminasi, termasuk daftar alamat digunakan oleh peretas untuk fase duplikasi malware dan penyebaran berikutnya



Hati-hati Gunakan Wi-fi Publik: Terutama jika SoHlB ingin melakukan transaksi keuangan, perbankan, e-commerce, kartu kredit serta aplikasi yang kritis dan strategis



Tidak Menggunakan Perangkat Pribadi untuk memproses pekerjaan perusahaan

MODUS HOAX DI WHATSAPP

Kementerian Komunikasi dan Informatika (Kemenkominfo) mencatat pertumbuhan hoax kian meningkat. Hingga tahun 2019, penyebaran hoax paling masif terjadi melalui platform sosial media WhatsApp



PENYEBARAN HOAX VIA WHATSAPP



Pembuatan akun palsu di sosial media selain Whatsapp



Membuat postingan berupa informasi hoax



Pelaku menangkap layar atau screen capture foto



Menyebarkan melalui platform WhatsApp



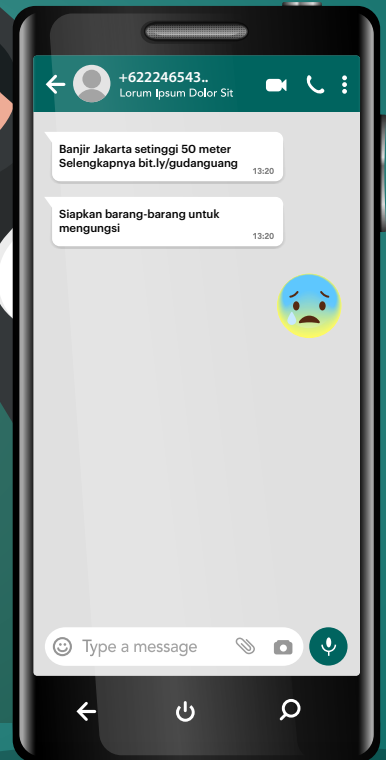
Pelaku menutup akun palsu yang dibuat untuk menghilangkan jejak digital



YUK CEGAH PENYEBARAN HOAX



- *Upstream* atau literasi digital melalui 90 siber kreasi
- *Downstream* dengan penegakan hukum oleh aparat kepolisian
- *Midstream* atau menengah dengan melakukan edukasi, pemutusan akses atau pemblokiran



JERAT HUKUM

UNTUK PENYEBAR

HOAX



Pertumbuhan pengguna smartphone dan media sosial yang tidak diimbangi literasi digital menyebabkan berita palsu alias hoax merajalela. Tidak hanya melalui situs online, hoax juga beredar di pesan chatting



HUKUMAN PENYEBAR HOAX



Terancam Pasal 28 ayat 1 Undang-Undang Informasi dan Transaksi Elektronik atau Undang-Undang ITE (UU ITE)

“Setiap orang **dengan sengaja**, dan **tanpa hak** menyebarkan **berita bohong** dan **menyesatkan** yang mengakibatkan **kerugian konsumen** dalam Transaksi Elektronik”

Dapat diancam pidana berdasarkan Pasal 45A ayat (1) UU 19/2016

yaitu dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1 miliar



CARA MELAPORKAN BERITA HOAX



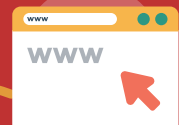
Screenshot disertai URL
Link berita/informasi hoax



Kirimkan data ke
aduan konten@mail.kominfo.go.id
dan lakukan verifikasi data



Kerahasiaan
pelapor dijamin



Aduan konten dapat diakses
di trustpositif.kominfo.go.id



PATROLISIBER.ID MEMBERANTAS HOAKS



Jumlah penyebaran hoaks periode Januari – Desember 2018 yang ditangani Polri mencapai 52 perkara. Namun sejak Januari – Juni 2019, **jumlah penyebaran hoaks yang ditangani Polri mencapai 51 kasus!**

Polri berupaya meningkatkan keamanan siber nasional, salah satunya melalui platform digital pemberantas hoaks di Whatsapp grup (WAG) yaitu ***patrolisiber.id***.



BAGAIMANA MEKANISME MELAPORKAN HOAKS DI WAG KE PATROLISIBER.ID?



Pihak Kepolisian melakukan patroli siber sekaligus menunggu pengaduan masyarakat terkait narasi hoaks yang beredar di WAG



Polisi bersama Kemenkominfo akan memeriksa pengadu secara mendalam, menyita barang bukti (smartphone) pengadu, serta menelisik alur komunikasi hoaks yang beredar di smartphone pengadu



Barang bukti tersebut selanjutnya akan diteliti di laboratorium forensik Polri



Jika pihak Kepolisian mendeteksi adanya penyebaran hoaks secara masif melalui bukti-bukti yang kuat, barulah **perwakilannya masuk ke dalam WAG untuk memantau**



Penegakan hukum akan dilakukan berdasarkan hasil pemantauan polisi, jika memang terbukti ada pelaku penyebar hoaks/tindak kriminal di WAG tersebut

KEMENKOMINFO JUGA MENYEDIAKAN BEBERAPA SARANA PELAPORAN KONTEN HOAKS LHO!

***Aplikasi Aduan Konten**

***08119224545**

***aduankonten@mail.kominfo.go.id**

CERMAT AGAR TIDAK TERTIPU SAAT BELANJA ONLINE



Selama 2019 (hingga April) Satgas Waspada Investasi Otoritas Jasa Keuangan (OJK) mencatat jumlah aduan masyarakat (konsumen) terkait **penipuan belanja online mencapai 19 ribu kasus** (sudah bayar tapi barang tidak diterima)!



NAH, BAGAIMANA CARA AGAR KITA TIDAK MENJADI KORBAN PENIPUAN BELANJA ONLINE?



Lakukan riset terhadap situs tempat berbelanja
Periksa nomor telepon si penjual dan hubungi



Amankan PC (komputer personal)
Minimal PC harus punya antivirus. Lebih baik lagi kalau punya anti spyware dan firewall



Periksa kebijakan situs terhadap data privasi
Jangan sampai pada kebijakan itu ada poin yang menyebutkan kalau pengelola situs web boleh memberikan data ke pihak lain





Baca kebijakan pengembalian barang

Periksa Karena barang yang dibeli tidak bisa dilihat secara fisik, harus ada garansi kalau barang yang dikirim cacat



Jangan mudah tergoda barang murah

Jangan terburu-buru jatuh cinta pada tawaran barang dengan harga miring (murah sekali) yang datang dari e-mail, apalagi meminta ID dan kata kunci (password) tanpa izin dari pemilik e-mail



Periksa paket barang dengan membaca deskripsi produk baik-baik

Curigai pada barang bermerek yang dijual dengan potongan harga yang jauh dari normal



WUJUDKAN KEAMANAN NASIONAL BIDANG SIBER

Tahukah SoHIB?

Pada tahun 2017 saat dibentuknya Badan Siber dan Sandi Negara (BSSN), Indonesia berada di peringkat 70 dalam peringkat keamanan siber dunia.

Pertimbangan Pembentukan BSSN



Keamanan siber telah menjadi isu prioritas dunia semenjak teknologi informasi dan komunikasi dimanfaatkan dalam berbagai aspek kehidupan



Tingkat pemanfaatan teknologi informasi dan komunikasi berbanding lurus dengan tingkat risiko dan ancaman penyalahgunaan teknologi informasi



Tugas Badan Siber dan Sandi Negara

Melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber



Fungsi Badan Siber dan Sandi Negara



Pemulihan; Dukungan mitigasi; Diplomasi siber; Penapisan; Evaluasi; Persandian; Pemantauan;



Pengendalian proteksi e-commerce; Sentra informasi; Identifikasi; Pusat kontak siber;



Penanggulangan; Pusat manajemen krisis siber; Proteksi; Deteksi



BSSN menjamin terselenggaranya kebijakan dan program pemerintah di bidang keamanan siber!

Tata Cara Lapor Korban Kejahatan Siber (Cyber Crime)

Tahukah SoHiB?

Sepanjang 2018, tercatat sebanyak **232,4 juta serangan siber ke Indonesia!**

Anda pernah jadi korban serangan siber?

Salah satu kasusnya bisa penipuan, pornografi, terorisme, penyadapan, pencemaran nama baik, ujaran kebencian, pencurian data?

Kalau iya, berikut cara lapor korban kejahatan siber (*cyber crime*)!



Jangan ragu untuk melaporkan tindak kejahatan siber!



1



Ke Polisi

Siapkan bukti yang cukup: seperti tangkapan layar (screenshot), url, foto, atau video dari ujaran kebencian yang akan dilaporkan. Bisa dikumpulkan dalam media penyimpanan seperti flashdisk, hardisk, cd/dvd, dll. Satu bukti yang kuat sudah cukup



Datang ke kantor polisi: dianjurkan setidaknya tingkat Polres untuk tindak pidana siber



Menuju ke ruang SPKT (Sentra Pelayanan Kepolisian Terpadu) untuk menyampaikan laporan & bukti-buktinya ke petugas



Petugas akan mengajukan sejumlah pertanyaan yang berhubungan dengan laporan ujaran kebencian, mengetik, dan mencetak bukti pelaporan



Menunggu **pemberitahuan selanjutnya** dari polisi

2



Ke patrolisiber.id

Diluncurkan pada **Agustus 2019**

Acuan: UU No.11/2008 tentang Informasi dan Transaksi Elektronik (ITE) dan Amandemen UU ITE No.19/2016

Ancaman Keamanan & Kejahatan DI DUNIA SIBER



Tahukah SoHIB?

Konten kasat mata yang dapat diakses dengan mesin pencari (google, yahoo, bing, internet explorer, firefox, dll) di dunia siber hanya sebesar 4% atau sekitar 8 miliar halaman



Sisa dari total persentase halaman di dunia siber merupakan daerah gelap (*dark web dan deep web*)!





Pengguna Daerah Gelap di Dunia Siber
Peretas (hacker), mafia, pengedar
narkoba, pornografi, spionase, jual beli
barang ilegal/pasar gelap (senjata,
virus, malware, ransomware, hitman
dll), terorisme

IDENTIFIKASI NOMOR IMEI

untuk Melindungi Masyarakat

Tahukah Sohib?

Potensi kerugian penerimaan pajak dari penjualan *smartphone* yang timbul akibat beredarnya ponsel ilegal (*black market/bm*) di Indonesia sekitar **Rp2,8 T.**



45 juta

Jumlah total unit *smartphone* yang beredar di Indonesia (2018)



9 juta

Kirasan jumlah unit *smartphone* ilegal (*black market*) yang beredar di Indonesia (2018)



Pemerintah dengan Permenkominfo Nomor 11/2019 hadir untuk memberantas peredaran ponsel ilegal melalui identifikasi nomor IMEI



Tujuan Identifikasi IMEI Ponsel

- Melindungi masyarakat dari penggunaan alat dan/atau perangkat telekomunikasi yang tidak memenuhi persyaratan teknis dan/atau hasil kejahatan
- Mendukung pencegahan dan mengurangi peredaran alat dan/atau perangkat telekomunikasi yang dinyatakan ilegal sesuai dengan ketentuan peraturan perundang-undangan

Catatan

Semua ponsel yang sudah terhubung ke jaringan seluler sampai dengan peraturan ini berlaku (18 April 2020), tidak akan mendapatkan pemblokiran!



Cara Cek IMEI Ponsel Legal atau Ilegal

Mulai 18 April 2020, nomor IMEI (International Mobile Equipment Identity) telepon seluler yang beredar di Indonesia harus terdaftar di Kemenperin, jika tidak terdaftar akan dianggap ilegal dan tidak dapat menggunakan jaringan operator dalam negeri (hanya wi-fi saja).

IMEI

- Nomor identitas internasional yang terdiri dari 15 digit desimal unik yang dialokasikan Global System for Mobile Association untuk mengidentifikasi secara unik alat dan/atau perangkat telekomunikasi yang tersambung ke jaringan bergerak seluler
- Nomor IMEI akan sama dengan jumlah slot SIM card ponsel



Mekanisme Cek Nomor IMEI Ponsel Legal atau Ilegal

- 1 Cek nomor IMEI di smartphone Android > masuk ke Settings > About Phone
- 2 Atau ketik *#06# di dialer ponsel
- 3 Salin nomor IMEI dan cek di laman <https://imei.kemenperin.go.id/>



Kementerian
Perindustrian
REPUBLIK INDONESIA

Cek IMEI



DAFTAR SUMBER

2-3 Bijak Memberi Data Pribadi di Media Sosial

BSSN, PP No.71/2019

4-5 Mencegah Akun Dari Peretasan

Berbagai Sumber

6-7 Taat Aturan saat Bermedia Sosial

Kementerian PANRB

8-9 Penyelenggara Sertifikasi Elektronik dan Tanda Tangan Elektronik Memudahkan ASN dan Keamanan Siber

Kemenkominfo

10-11 Cegah Penyalahgunaan Informasi Data Pribadi di Indonesia

PP No.71/2019

12-13 Denda Konten Ilegal Bagi Platform

PP No.71/2019, Kemenkominfo

14-15 Penyelenggara Sistem Elektronik di Indonesia Harus Terdaftar atau Kena Pasal

PP No.71/2019

16-17 Filosofi Sikat Gigi untuk Keamanan Kata Sandi (Password)

18-19 Gunakan Enkripsi untuk Menjaga Integritas Data

Badan Siber dan Sandi Negara

20-21 Tetap Tenang Hadapi Serangan Siber: Phising dan Social Engineering

BSSN, antaranews.com

22-23 Cara Tangkal Spam, Malware, Ransomware, Virus, dan Spyware

BSSN

24-25 Modus Hoax di Whatsapp

Kementerian Kominfo

26-27 Jerat Hukum untuk Penyebar Hoax

UU ITE dan Kementerian Kominfo

28-29 Patrolisiber.id, Memberantas Hoax

Polri, patrolisiber.id, Kemenkominfo

30-31 Cermat Agar Tidak Tertipu saat Belanja Online

OJK

32-33 Wujudkan Keamanan Nasional Bidang Siber

Badan Siber dan Sandi Negara, Perpres No.53/2017, Perpres No.133/2017

34-35 Tata Cara Lapor Korban Kejahatan Siber

36-37 Ancaman Keamanan & Kejahatan di Dunia Siber

Badan Siber dan Sandi Negara

38-39 Identifikasi Nomor IMEI untuk Melindungi Masyarakat

Permenkominfo No.11/2019, Asosiasi Ponsel Seluruh Indonesia

40-41 Cara Cek IMEI Ponsel Legal atau Ilegal

Kemenperin, Permenkominfo No.11/2019

010 10110 0010010 10110 010
1101001 010 01000101001
010011110101 010
10110 0100010101001 10110 0100110



DIREKTORAT JENDERAL INFORMASI DAN KOMUNIKASI PUBLIK
KEMENTERIAN KOMUNIKASI DAN INFORMATIKA

ISBN 978-623-90784-7-8 (PDF)



9 786239 078478