



BADAN SIBER DAN
SANDI NEGARA



TIPS SINGKAT & PRAKTIS DI DUNIA SIBER

DARI BSSN UNTUK MASYARAKAT

TIPS SINGKAT DAN PRAKTIS DI DUNIA SIBER

(Dari BSSN untuk Masyarakat)

Penulis: Tim Direktorat Proteksi Ekonomi Digital BSSN

Hak Cipta dilindungi Undang-Undang.

Dilarang mengutip atau memperbanyak sebagian atau seluruh isi buku ini tanpa ijin tertulis dari Badan Siber dan Sandi Negara (BSSN).

Diterbitkan oleh :

Badan Siber dan Sandi Negara (BSSN)

Jl. Harsono RM 70 Ragunan

Pasar Minggu, Jakarta Selatan 12550

Tel : +6221 7805814

Fax : +6221 78844104

Email : kliks@bssn.go.id

<https://www.bssn.go.id>

© Februari 2019 | Badan Siber dan Sandi Negara



**BERPIKIR
SEBELUM
KLIK**



REDAKSI KITA

Budaya internet atau cyberculture adalah budaya yang muncul dari penggunaan jaringan komputer untuk komunikasi, hiburan dan bisnis. Jumlah pengguna internet yang besar dan semakin berkembang menjadi fenomena sosial terkait bentuk lain komunikasi jaringan, seperti komunitas online, game multi-player online, serta jejaring sosial, penggunaan smartphone, transaksi perbankan online dan aplikasi mobile internet. Fenomena tersebut mencakup masalah identitas, privasi, dan pembentukan jaringan, serta hubungan antar manusia, komputer dan kepribadian di dunia maya.

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. Namun, istilah tersebut juga digunakan dalam kegiatan kejahatan tradisional di mana komputer atau jaringan komputer menjadi alat untuk mempermudah atau memungkinkan kejahatan itu terjadi.

Mempertimbangkan berbagai macam kasus dan modus serangan siber yang terjadi, BSSN berinisiatif menyusun buku berisi tips dan informasi yang mudah dicerna terkait berselancar di dunia maya dengan aman dan menghadapi serangan kejahatan internet. Tidak semua modus dan kasus dapat dituliskan dalam buku ini, namun diharapkan dapat bermanfaat bagi masyarakat.

Buku ini juga akan digunakan BSSN dalam acara Roadshow Sosialisasi Keamanan Siber Tahun 2019 di daerah-daerah di seluruh Indonesia.

Selamat berselancar dengan aman dan nyaman di dunia Siber, semoga bermanfaat.

Salam,
Tim Redaksi
BSSN



DAFTAR ISI

- (3) · REDAKSI KITA
- (4) · DAFTAR ISI

TIPS-TIPS :

- (5) · ATURAN BERPONSEL UNTUK ANAK ANDA
- (6) · PLAY IT SMART ONLINE
- (7) · ATURAN AMAN BERMEDIA SOSIAL PADA ANAK
- (8) · KEAMANAN BERINTERNET UNTUK ANAK
- (9) · KESALAHAN UMUM DALAM PASSWORD
- (10-11) · 10 CARA TERBAIK MELINDUNGI KELUARGA ANDA KETIKA ONLINE
- (12) · 10 HAL YANG PERLU DIKETAHUI TENTANG JEJAK DIGITAL
- (13) · SAYA BISA MENJADI WARGA DIGITAL (NETIZEN) JIKA
- (14-15) · TENTANG INTIMIDASI SIBER (CUBERBULLYING)
- (16) · MENGHADAPI INTIMIDASI SIBER (CUBERBULLYING)
- (17) · TIPS CERDAS MENANGANI AGRESI ONLINE
- (18-19) · CARA MENDETEKSI EMAIL PHISHING
- (20) · TIPS UNTUK MENGHINDARI SERANGAN SOCIAL ENGINEERING
- (21) · TIPS BERTRANSAKSI AMAN MELALUI MOBILE & INTERNET BANKING
- (22) · BERTRANSAKSI ONLINE DENGAN AMAN & NYAMAN
- (23) · TIPS AMAN BERBELANJA ONLINE



ATURAN BERPONSEL UNTUK ANAK ANDA



1. Selalu tanya orang tua sebelum mendownload aplikasi baru.*
2. Jangan berikan nomor telepon kepada orang yang tidak dikenal atau mempostingnya secara online.
3. Beri tahu orang tua jika menerima sesuatu hal yang dirasa tidak nyaman.
4. Jangan menjawab panggilan atau pesan teks dari nomor yang tidak dikenal.
5. Pikirkan tentang pesan yang akan kamu sampaikan. Apakah lebih tepat disampaikan secara langsung atau tidak.
6. Jangan mengirim teks atau bermain game sambil berjalan.**

* Tidak semua aplikasi aman dan gratis.

** Ini adalah penyebab utama kecelakaan lalu lintas.

PLAY IT SMART

ONLINE



SAFE

Tidak pernah memberikan informasi pribadi (nama lengkap, alamat email, nomor telepon, alamat rumah, gambar, nama sekolah) kepada siapa pun yang ditemui saat/ketika di media online.

MATERIALS

Tidak mengakses situs web atau materi yang tidak pantas. Hanya akses bahan pendidikan pada perangkat sekolah.

ACCEPT

Tidak menerima email, file, atau pesan dari orang yang tidak dikenal



RELIABLE

Tidak semua yang anda baca online itu adalah benar, dan orang-orang mungkin tidak seperti yang mereka katakan.

Periksa informasi sebelum mempercayainya



TELL

Beri tahu orang tua, guru, atau orang dewasa terpercaya lainnya jika seseorang atau sesuatu membuat saya gugup, khawatir, atau tidak nyaman secara online. Saya akan melaporkan pelecehan/intimidasi dunia maya jika melihatnya terjadi.





ATURAN AMAN BERMEDIA SOSIAL PADA ANAK

1 DISKUSIKAN TENTANG “KEINGINAN UNTUK BERBAGI”

Anak-anak memiliki dorongan untuk berbagi foto dan detil lain tentang kehidupan mereka. Lakukan percakapan positif tentang nilai privasi untuk mengurangi keinginan itu.

2 MEMAHAMI KONTEN YANG BERTAHAN LAMA

Ingatkan anak bahwa tidak ada konten di media sosial yang dapat dihapus. Apa pun yang mereka bagikan adalah permanen (bahkan jika mereka telah menghapusnya), itu akan mendorong mereka untuk berpikir kembali apa yang akan mereka posting.

3 AJARI MEREKA TENTANG “ORANG TIDAK DIKENAL” DALAM JARINGAN (ONLINE)

Pastikan anak-anak mengenal kontak yang menghubunggi atau meminta pertemuan di media sosial, karena pelaku kejahatan dapat menggunakan media sosial untuk menghubunginya.

BAGAIMANA CARA

MEMBUAT LINGKUNGAN YANG AMAN

 18 + Jangan ijin kan anak dibawah umur menggunakan media sosial.

 Batasi jumlah waktu online anak anda di media sosial.

 Pastikan pengaturan akun media sosial anak anda dalam mode privat.

 Pantau aktivitas online anak anda. Pastikan konten yang mereka posting tidak berbahaya.



Keamanan Berinternet

“UNTUK ANAK”



1 Jangan pernah memberikan informasi pribadi seperti nomor telepon, alamat, nama sekolah, foto, dan kata sandi.

2 Bicaralah dengan orang tua, guru, atau wali kamu jika merasa tidak nyaman dengan apa yang kamu lihat di internet.

3 Bersikaplah sopan dan hormati orang lain secara online. Jangan pernah mengirim pesan yang menyakiti orang lain.

4 Jangan pernah sendirian jika bertemu dengan teman online. Pastikan kamu bersama orang tua atau orang dewasa yang terpercaya.

5 Jangan terlalu mengumbar informasi pribadi saat chatting online.



KESALAHAN UMUM DALAM PASSWORD

MENCEGAH KATA SANDI ANDA DARI



PERETASAN



KATA KUNCI LEMAH

Apakah ini terdengar akrab?



KATA SANDI: KRISNA08

"Saya menggunakan nama dan umur cucu saya."
- Tommy

KATA SANDI: MANCINGMANIA

"Saya menggunakan hobi favorit saya sebagai kata sandi saya." - Jarot

KATA SANDI: BRIAN123

"Saya menggunakan kata sandi yang sama untuk semua akun saya. Dengan begitu, saya hanya perlu mengingat satu kata sandi." - Brian

KATA SANDI: 123ABC123

"Kata sandi twitter saya sangat mudah untuk saya ingat. Itu hanya sebuah pola." - Emilia

KATA SANDI KUAT: M&T7T\$DAY

"Saya dulu menulis kata sandi saya, tetapi sekarang saya menggunakan manajer kata sandi yang mengenkripsi semuanya." - Yasmin

PERETAS



Bekerja keras untuk mendapatkan kata sandi Anda

"Hanya butuh 10 menit untuk menebak kata sandi Tommy. Dia memposting nama cucunya di situs berbagi foto."

"Gambar profil Facebook Jarot menunjukkan dia senang memancing. Begitu banyak petunjuk didalam situs media sosialnya."

"Setelah saya memecahkan kata sandinya, saya bisa masuk ke Facebook, Twitter dan akun email."

"Banyak orang menggunakan kata sandi yang berbentuk pola. Mereka tidak menyadari kalau itu yang saya coba dulu."

"Saya masih berusaha mencari tahu kata sandi ini. Dia sepertinya tidak memiliki petunjuk untuk saya sama sekali."



10

CARA TERBAIK UNTUK MELINDUNGI KELUARGA ANDA KETIKA ONLINE

1. PASTIKAN ANAK-ANAK DAPAT BERINTERNET ATAU TIDAK, DAN KOMUNIKASIKAN TENTANG BAHAYA ONLINE.

Ancaman keamanan terbesar online adalah virus yang jumlahnya mencapai 1 juta jenis yang berbeda di seluruh dunia.

2. GUNAKAN ANTIVIRUS TERBARU UNTUK MELINDUNGI DIRI DI DUNIA MAYA.

Lebih dari tiga perempat pengguna internet (79%) menggunakan solusi antivirus untuk melindungi privasi mereka secara online

3. MONITOR KEBIASAAN BERMEDIA SOSIAL ANAK-ANAK DAN ATUR PRIVASI NYA.

Sekitar 70% orang tua telah mendiskusikan privasi jejaring sosial dengan anak-anak mereka.

4. CADANGKAN (BACKUP) DATA SECARA TERUTUR UNTUK MENGHINDARI KEHILANGAN INFORMASI PRIBADI YANG PENTING.

Satu dari empat orang daring (online) tidak pernah membackup data di komputernya.

5. LINDUNGI DIRI DENGAN MEMBUAT KATA SANDI YANG TEPAT.

Kurang dari dua pertiga pengguna internet (61%) dilaporkan menggunakan kata sandi yang tersimpan (save/remember password).



SEKITAR 85% ORANG TUA SEKARANG LEBIH PEDULI DENGAN PRIVASI DAN KEAMANAN ONLINE DARIPADA LIMA TAHUN YANG LALU. RISIKONYA NYATA DAN SOLUSINYA JELAS.



6. AJARI ANAK-ANAK UNTUK MEMINTA IJIN DAHULU SEBELUM MEMBERIKAN INFORMASI SECARA ONLINE.

Hanya 50% pengguna internet mempercayai kontak jejaring sosial mereka untuk menjaga kerahasiaan informasi.

7. SELALU BACA KEBUAKAN PRIVASI ONLINE.



8. AMANKAN JARINGAN WI-FI PRIBADI DAN HINDARI JARINGAN WI-FI TERBUKA (OPEN WI-FI).

Sekitar 32% pengguna internet mengaku menggunakan jaringan wifi tetangga mereka.

9. PELAJARI CARA MENGENALI PENIPUAN DAN KELOLA AKTIVITAS EMAIL SECARA EFektif.

10. AJARI KELUARGA TERDEKAT UNTUK BERHATI-HATI SECARA ONLINE DAN GUNAKAN AKAL SEHAT.

Sekitar 92% orang tua percaya anak-anak mereka berbagi terlalu banyak informasi tentang diri mereka sendiri secara online.



10 Hal

YANG PERLU DI KETAHUI TENTANG JEJAK DIGITAL (DIGITAL FOOTPRINT)



1

Saat anda mencari dan berinteraksi secara online, anda meninggalkan jejak digital.

2

Jejak-jejak digital anda dapat dicari atau dibagikan.

3

Jejak digital bisa bermanfaat atau merugikan reputasi anda sekarang dan di masa depan.

4

Sekali online, segala sesuatu akan tersimpan selamanya (walaupun sudah dihapus).

5

Berpikir dahulu sebelum anda memposting secara online.

6

Informasi pribadi atau opini yang dikirim ke satu orang dapat **DISEBARKAN** kepada khalayak ramai.

7

Googling diri sendiri bisa menjadi latihan yang bermanfaat untuk melihat jejak digital anda.

8

Akun lama atau yang sudah tidak aktif harus dinonaktifkan dan dihapus.

9

Rahasiakan informasi pribadi dan kendalikan pengaturan privasi di akun anda.

10

Pertimbangkan jejak digital orang lain (misal. ijin sebelum memberi tag pada foto).



SAYA BISA MENJADI Warga Digital (NETIZEN)

JIKA...



"Menggunakan teknologi secara tepat dan dengan izin orang tua."

"Melindungi informasi pribadi dan tidak membagikannya di internet."

"Menjelajah ke situs web dengan izin dari guru atau orangtua."

"Tidak akan membagikan kata sandi saya dengan orang lain."

"Menghargai diri saya dan orang lain secara online.
Saya akan menggunakan kata-kata yang baik."



BICARALAH DENGAN ANAK ANDA Tentang Pelecehan / Intimidasi Siber (CYBERBULLYING)

“ Ajukan pertanyaan kepada anak dengan lemah lembut untuk mengetahui kondisi sebenarnya dan penyebabnya ”



“ Anjurkan anak-anak untuk berani menceritakan jika dirinya atau temannya mengalami pelecehan/intimidasi. ”



“ Jelaskan bahwa “like” atau “share” konten yang menyakiti tidak dapat diterima. ”



“ Ajari anak tentang dampak dari pelecehan/intimidasi siber. ”

“ Anjurkan anak untuk berani memberikan dukungan kepada teman yang diganggu. ”



APA YANG HARUS ANDA LAKUKAN JIKA ANAK ANDA DILECEHKAN?

DOKUMENTASIKAN BUKTI PELECEHAN/INTIMIDASI

Simpan cuplikan layar (screenshot) dari pesan atau perilaku kasar sebagai bukti untuk pelaporan pada aparat terkait.



BICARALAH DENGAN PARA GURU DI SEKOLAH

Pastikan mereka mengetahui situasi cyberbullying yang terjadi kepada anak anda.

EXIT



LAPORKAN TINDAKAN CYBERBULLYING.

Anda dapat melaporkan tindakan cyberbullying ke otoritas terkait. Jika anak anda menerima ancaman, lapor ke pihak berwajib.



BICARALAH DENGAN ORANG TUA LAIN DAN ANJURKAN UNTUK BERBICARA KEPADA ANAK-ANAK MEREKA



Tips menghadapi INTIMIDASI SIBER

“ CYBERBULLYING ”

1. Tetap tenang
2. Hentikan kegiatan atau abaikan si pelaku
3. Katakan pada si pelaku untuk berhenti
4. Beri tahu orang dewasa yang anda percaya
5. Blokir pelaku bullying
6. Jika anda mengetahui si pelaku, kirimkan salinan bukti pelecehan kepada orang tuanya. Minta mereka untuk menghentikannya secara sopan
7. Hubungi penyedia layanan Internet anda
8. Jika pelecehan ini menjadi ancaman serius, hubungi Polisi atau pihak terkait



TIPS CERDAS

CARA MENANGANI AGRESI ONLINE



1 MELEPASKAN DIRI

Lepaskan diri anda dari pengaruh negatif, jangan ikut-ikutan mengintimidasi orang lain.

2 LOG OFF & BLOKIR PELAKU PELEHAN

Agar perilaku intimidasi tidak terulang pada media sosial kita, Lakukan Log off & blokir pelaku Intimidasi.

3 JANGKAU ORANG DEWASA YANG TERPERCAYA

Ketika melihat perkataan atau perlakunya intimidasi terhadap seseorang, sebaiknya berdiskusi dengan orang dewasa terpercaya untuk mendapat masukan positif.

4 GUNAKAN PENGATURAN PRIVASI

Pengaturan privasi menjadikan akun kita terkendali dari orang atau pun diskusi yang negatif, kita dapat menyeleksi teman di media sosial.

5 AMBIL TANGKAPAN LAYAR (SCREENSHOT)

Ketika ada intimidasi di media sosial kita, maka ambil bukti dan tegur pelaku menggunakan bukti tersebut melalui orang dewasa terpercaya agar perbuatan tersebut tidak terulang.

6 LAPORKAN

Ketika terdapat akun yang bersifat intimidatif terhadap orang lain atau negatif, laporan ke pengelola media sosial atau pihak yang berwajib

7 JADILAH PENGARUH POSITIF

Jangan "like" atau "share" konten negatif.



8 PERTIMBANGKAN

Sebelum memposting sesuatu, pertimbangkan dahulu apakah hal tersebut dapat menyakiti orang lain

9 ITU BUKAN SALAHMU

Ketika ada yang melakukan intimidasi terhadap orang lain atau tindakan negatif di media sosial anda, jangan khawatir untuk melaporkannya. Yakinlah hal itu bukan kesalahan anda, tetapi kesalahan si pelaku Intimidasi.



10 JADILAH TEMAN

Jika anda melihat orang lain diintimidasi dan dikucilkan, jangan ikut mengucilkan orang atau korban tersebut. Jadilah teman yang selalu mendukung



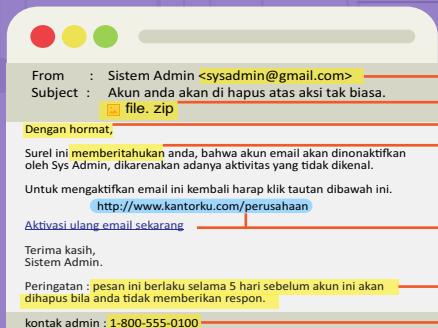


CARA MENDETEKSI EMAIL PHISHING

Sekitar 300 email phishing dikirim per hari dan efektif. Setiap 60 detik, 250 komputer diretas. Pelanggaran ini merugikan perusahaan \$ 388 miliar setahun dalam rahasia bisnis dan kekayaan intelektual yang dicuri. Inilah yang harus dilihat untuk menghindari phishing.



ANATOMI EMAIL PHISHING



- 1 Email dikirim bukan dari alamat email korporasi
- 2 Jangan percaya link atau attachment dalam email yang tidak dikenal.
- 3 Kata pembuka yang terlalu biasa untuk pesan resmi.
- 4 Ada kesalahan pengetikan pada pesan.

- 5 Alamat website dengan tujuan website yang tidak jelas, dan terkadang terdapat kesalahan pengetikan.
- 6 Pesan tambahan yang menekankan situasi seolah-olah darurat.
- 7 Kontak telepon yang tidak dapat dihubungi.

APA YANG HARUS DI LAKUKAN ?

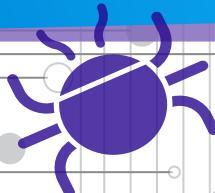
1. Jangan pernah memberikan informasi pribadi atau sensitif melalui email apa pun.
2. Jangan percaya link atau attachment dalam email yang tidak dikenal.
3. Verifikasi tujuan link yang sebenarnya, meskipun berasal dari sumber terpercaya.
4. Ketikkan alamat situs web, daripada menggunakan link dari email yang tidak dikenal.
5. Waspadai nomor telepon dalam email. Gunakan nomor telepon yang ditemukan di daftar kontak Anda atau di direktori terpercaya seperti buku telpon.



APA ITU PHISHING ?

Istilah phishing dalam bahasa Inggris berasal dari kata fishing (memancing), dalam hal ini berarti memancing informasi dan kata sandi pengguna Internet.

Phisher biasanya membuat email atau sms palsu dengan menyamar sebagai orang atau bisnis yang terpercaya. Email ini biasanya mencoba untuk mendapatkan informasi pribadi, seperti nama, alamat dan nomor kartu kredit atau informasi rahasia lainnya. Biasanya mereka menggunakan tautan atau embed link yang mengarahkan pengguna ke situs web yang terlihat tampak sah, tetapi sebenarnya web buatan phisher.



TIPS UNTUK MENGHINDARI SERANGAN REKAYASA SOSIAL (SOCIAL ENGINEERING ATTACK)



BATASI INFORMASI PUBLIK

Batasi informasi pribadi yang anda bagikan secara online.



SKEPTIS

Selalu mempertanyakan permintaan informasi yang sensitif.



VERIFIKASI

Jangan berbagi informasi sebelum anda dapat memverifikasi segala bentuk permintaan melalui media apapun.



No PASSWORD

Jangan pernah membagikan kata sandi anda dengan siapa pun melalui telepon.



TIPS BERTRANSAKSI AMAN MELALUI MOBILE & INTERNET BANKING



APLIKASI & LAYANAN

Gunakan aplikasi dan layanan perbankan digital yang resmi dari Bank terkait.



PASSWORD

Ubah password secara berkala. Jangan aktifkan fitur **save password** pada komputer.

RAHASIA

Jaga kerahasiaan user-ID dan password. Pihak Bank tidak pernah menanyakan informasi ini.



SMS & EMAIL

Aktifkan fitur notifikasi sms dan email untuk memonitor aktivitas rekening.



LAPORKAN

Segera lapor ke Bank terkait jika terdapat transaksi mencurigakan

ANTI VIRUS

Khusus internet banking install **antivirus** pada computer

HAPUS

Hapus history dan lakukan **clear cache** setelah bertransaksi





"PASTIKAN NOMOR HANDPHONE ANDA SUDAH TERDAFTAR"
Bank hanya mengirimkan OTP (One Time Password) ke nomor yang sudah di daftarkan.



"RAHASIAKAN C V V (CARD VERIFICATION VALUE) ANDA"
Jangan pernah memberikan 3 (tiga) digit nomor dibelakang kartu kredit anda.



"SELEKTIF DALAM MEMILIH SITUS ONLINE"
Transaksilah di merchant yang telah kerjasama dengan Bank..



"BERTRANSAKSILAH DI KOMPUTER ATAU GADGET ANDA SENDIRI"
Untuk menghindari pencurian data/identitas.



"SIMPAN BUKTI TRANSAKSI"
Berguna untuk menelusuri jika terjadi kesalahan transaksi.



"CEK TESTIMONIAL DARI PENGGUNA LAIN"
Bermanfaat untuk mencari informasi dari pengguna lain yang pernah bertransaksi sebelumnya.



TIPS

BERTRANSAKSI ONLINE

DENGAN AMAN & NYAMAN

PENAWARAN YANG TERLALU MENGGIURKAN
BISA JADI PALSU

BERHATI-HATI DENGAN
TYPoSQUATTING ATAU URL PALSU

PASTIKAN PASSWORD CUKUP
AMAN, PANJANG & KOMPLEKS

TIPS AMAN

BERBELANJA ONLINE

PASTIKAN JARINGAN NIRKABEL YANG
TERHUBUNG AMAN

JIKA RAGU MENGKLIK TAUTAN DI EMAIL, LIHAT DAHULU
KE MANA TUJUAN URL SEBENARNYA



0 Februari 2019 | Badan Siber dan Sandi Negara