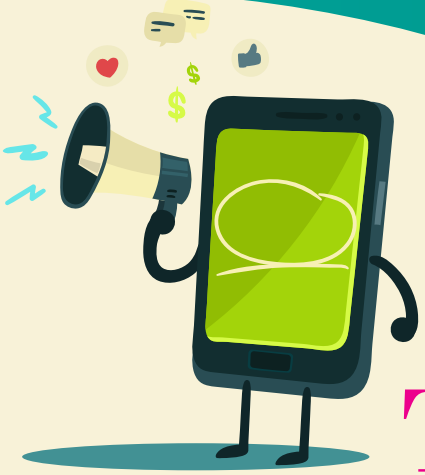
BADAN SIBER DAN SANDI NEGARA



TIP SINGKAT & PRAKTIS di Dunia Siber

dari BSSN untuk Masyarakat

Scan QR code
Info KLIKS:

Ditandatangani secara elektronik oleh:
DIREKTUR PROTEKSI EKONOMI DIGITAL

Anton Setiyawan, S.Si., M.M.
NIP. 19711209 199110 1 001

Tip Singkat & Praktis di Dunia Siber
(Dari BSSN untuk Masyarakat)

Penulis: Team SiberDesk BSSN & Kontributor Majalah KOMITE.ID - ABDI (Asosiasi Big Data & AI)
Tata Letak: Majalah & Portal Berita KOMITE.ID (redaksi@komite.id) - PT. Accessindo Internusa

Penerbit:
Badan Siber dan Sandi Negara (BSSN)
Jl. Harsono RM 70 Ragunan
Pasar Minggu, Jakarta Selatan, 12550
Tel: +62217805814
Fax: +622178844104
Email: kliks.bssn@gmail.com
https://www.bssn.go.id

REDAKSI KITA

Teknologi Informasi (TI) dan Internet (Siber) sudah menjadi bagian yang tidak terpisahkan dari kehidupan manusia modern, dimulai dengan hadirnya PC di perkantoran, warnet, perumahan dan sekolah. Era PC kemudian digantikan Smartphone yang menjadi teman setia kita dimana saja dan kapan saja, termasuk ketika kita berpergian (mobile) tidak pernah ketinggalan, bahkan saat tidur. Jumlah pengguna mobile phone dunia mencapai 5,14 miliar dan pengguna Internet lebih dari 4 miliar (www.statista.com).

Sayangnya perkembangan dunia hitam Internet atau Darkweb malah lebih pesat dan buku ini memberikan peringatan dan tip-tip untuk berselancar di dunia siber dengan aman.

87 juta data akun masyarakat dunia di Facebook (FB), 1,1 juta akun dari Indonesia bocor (data breach) dan dimanfaatkan oleh Cambridge Analytica untuk tujuan manipulasi kampanye pemilu Amerika (AS) 2016. Banyak hatespeech, sindrome post truth beredar di FB yang menyebabkan polarisasi masyarakat oleh isu SARA, politik dan populisme? Bahkan Pemilu negara adidaya AS 2016 pun tidak luput dari serangan peretas, phishing, sosial engineering, ditenggarai oleh aktor negara, dari dinas intelijen Rusia yang menyadap email dan menyuntik malware untuk mencuri data dari database partai demokrat AS, sehingga mencemari hasil pemilu AS 2016.

Anak anak yang gemar posting di sosmed FB juga banyak menjadi korban phishing, bullying, social engineering oleh para predator memanfaatkan sosial media, email dan siber.

Dengan berbagai macam kasus dan modus serangan siber seperti contoh diatas, maka BSSN berinisiatif menyusun buku yang mudah dicerna, berisi tip dan informasi bagaimana berselancar di dunia siber dengan aman dan menghadapi banyaknya serangan siber dan kejahatan siber. Tidak semua modus dan kasus dapat ditulis di dalam buku ini. Maksud & tujuan buku ini untuk memberikan berbagai tip yang dapat bermanfaat bagi masyarakat.

Buku ini juga akan digunakan peserta roadshow sosialisasi Keamanan Siber di 5 daerah Bogor, Bali, Yogya, Jakarta dan Bandung pada bulan Agustus 2018 oleh BSSN. Semoga bermanfaat.

Selamat berselancar dengan aman dan nyaman di dunia Siber.

Salam,

Tim Redaksi
BSSN & KOMITE.ID

DAFTAR ISI

MENGENAL ANCAMAN KEAMANAN & JENIS KEJAHATAN DI DUNIA MAYA

Perkembangan penetrasi Internet sangat cepat, lebih dari 50% atau 4.02 miliar (2018) masyarakat dunia pengguna Internet, 66% atau 5.14 miliar pengguna ponsel dan 3.2 miliar (2018) pengguna sosmed dari 7.6 miliar penduduk dunia (www.wearesocial.com).

Konten Surface Web hanya 4% atau sekitar 8 miliar halaman yang diakses melalui browser laiknya Google, Internet Explorer atau Firefox, seperti kita mengakseses marketplace Amazon, Blibli.com, Bukalapak.com atau Tokopedia.com.

Peningkatan konten Dark Web (dunia hitam) dan Deep Web (dunia rahasia) jauh lebih cepat atau lebih dari 96% atau 7.9 zetabytes diakses dengan TOR (the Onion Router) hidden service, seperti pasar gelap, SILK ROAD untuk jual beli barang ilegal seperti senjata, virus, malware, ransomware, hitman, pornografi, narkoba. (http://komite.id/2018/06/26/serangan-masif-cyber-attack-global/).

Berhati hati berselancar di dunia siber, karena hanya 4% yang kasat mata dapat diakses dengan mesin pencari Google, Yahoo, Bing, dll. Sedangkan sisanya merupakan daerah gelap para cracker (peretas), mafia, pengedar narkoba, pornografi, dunia spionase, jual beli senjata dan terorisme. **

RANKING SERANGAN SIBER RI 2015

RANKING SERANGAN SIBER RI 2016

Infografis www.komite.id Edisi 08/2017 – Feb-Mar 2017 halaman 30 – Sumber: Rudi Lumanto-IDSIRTII.

1 BIJAK DALAM MEMBERIKAN DATA PRIBADI DI MEDSOS

Peraturan Perlindungan Data Pribadi (PDP) RI hingga saat ini masih dalam pembahasan, seperti PP 82/2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). Institusi atau Perusahaan yang mengelola data base pribadi konsumen atau pengguna yang biasa disebut Data Controller disingkat menjadi DCO. DCO bertanggung jawab melindungi Data Pribadi Konsumen sebagai pemilik data. Setiap perlakuan terhadap Data dari seorang klien harus diberikan secara bebas atau berdasarkan keinginan atau tanpa tekanan dengan kata lain harus dengan persetujuan dan ijin dari klien pemilik Data.

Seorang pengguna sosmed, website atau konsumen ecommerce (Data Subject) memiliki hak privasinya:

1. Agar Data Pribadi (Personal) dihapus (delete) atau diremajakan (up to date);
2. Agar Data Pribadi (Privasi) dilindungi kerahasiaannya seperti informasi yang dapat mengidentifikasi (identifier): Nama, nomor ID, lokasi data, atau identifikasi dari faktor seperti fisik, genetik, mental, agama, sosial, budaya dan ekonomi seseorang;
3. Agar perekaman, pengambaran dan analisa atas profile suatu objek harus seijin (consent) Data Subjek tersebut termasuk segala bentuk personalisasi, prediksi mengenai kinerja, pekerjaan, ekonomi, keuangan, kesehatan, referensi personal, interest, hobby, kelakuan, lokasi dan pergerakannya.

5 Tip Akutabilitas Perusahaan (DCO) Menjaga Data Pribadi Konsumen atau Masyarakat:

1. DCO wajib menjaga Keamanan terhadap Pembocoran Data Pribadi (Data Breach). Jika terjadi musibah pembocoran data harus segera melaporkan dalam waktu 72 jam setelah mengetahui (discovery).
2. DCO memproses data konsumen dengan cara Sah, tidak melanggar hukum, fair (adil) dan transparan terhadap konsumen untuk tujuan spesifik, jelas/eksplisit, valid & sah, sesuai dengan tujuan yang sudah disepakati oleh konsumen.
3. DCO menjamin ketepatan, akurasi data konsumen, tidak kadaluwarsa, up to date terus diperbarui, sesuai tujuan penyimpanan data yang disetujui oleh konsumen.
4. DCO menjamin Lokasi & format penyimpanan atau database disetujui konsumen dan UU yang berlaku.
5. DCO menjaga integritas (tidak rusak dan hilang) data dan kerahasian (confidentiality) data subjek dengan enkripsi, password dll.

TIP-TIP

2 PENGGUNAAN ENKRIPSI UNTUK MENJAGA INTEGRITAS DATA*

Enkripsi (Encryption) adalahsuatu proses untuk merahasiakan berita agar pihak yang tidak berwenang tidak dapat membaca dan mengerti isi berita. Sebuah konversi dari tulisan yang bisa dibaca manusia (plain text) menjadi tulisan yang diacak (cypher text) menggunakan kunci (key). Namun enkripsi dapat dikembalikan dengan dekripsi (decryption) ke tulisan original (plain text) menggunakan kunci (key).

Kriptanalisis (Cryptanalysis) adalah suatu cara untuk mendapatkan kembali informasi yang telah dienkripsi.Kadang melalui proses berulang kali, (salah satu cara dengan Brute Force Attack yaitu serangan yang mencoba semua kemungkinan rangkaian kunci password) oleh peretas enkripsi. Kunci simetris artinya hanya satu kunci untuk mengunci (enkripsi) dan membuka (dekripsi). Asimetris jika ada dua kunci, kunci privat yang harus selalu disimpan/rahasia dan kunci publik/umum yang diumumkan di website misalnya dan digunakan oleh mitra transaksi anda untuk membuka (dekripsi) transaksi atau berita.Tip penting adalah menjaga kerahasian kunci privat.

Tip mengapa email atau data transaksi perbankan harus dienkripsi jika ingin aman? Upayakan agar email text atau transaksi itu dijaga:

1. Kerahasiannya (Confidential) terhadap upaya penyadapan;
2. Integritasnya (integrity) agar data tidak diubah, dihapus, diganti;
3. Otentikasi (Authentication) dari data agar pengirim ter verifikasi, tidak anonim dan jelas.

Certificate Authority (CA) adalah pihak ketiga yang membuat, memverifikasi publik & private key (kunci privat) untuk menjaga otentikasi pemiliknya.

3 PENGGUNAAN TANDA TANGAN DIGITAL

UU ITE mendefinisikan Tanda Tangan Elektronik (TTE) atau Digital Signature sebagai tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi (UU ITE Pasal 13 ayat 1) Penandatangan adalah subjek hukum yang terasosiasi atau terkait dengan TTE.

Sebuah berita (message) atau transaksi di tandatangan digital (digitally signed) jika dapat dienkripsi oleh pengirim berita dengan menggunakan kunci digital privat agar aman terhadap peretasan, penyadapan, perubahan berita. Penerima membuka dengan kunci publik, jika menggunakan asimetris key/enkripsi.**

* Sumber: Lembaga Sandi Negara, Sumarkidjo (2007), Jelajah Kriptologi

TIP-TIP

4 TANGKIS KONTEN NEGATIF & KECANDUAN

Konten-konten negatif seperti pornografi banyak berseliweran di Internet dan membahayakan pertumbuhan dan pikiran. Meskipun pemerintah sudah melakukan penyensoran satu situs, namun tumbuh 1000 situs baru, karena sifat Internet yang tanpa batas dan industri pornografi yang booming. Berikut tipnya bagi Orang Tua dan Guru:

1 Mengedukasi agar anak-anak dan remaja menjauhi konten pornografi (namun juga pornoaksi, SARA, narkoba, dunia hitam dark web/deep web). Memberikan rasa tanggung jawab dan kepercayaan agar melakukan hal-hal yang positif seperti kursus dan kegiatan ekstra kurikuler sekolah, sehingga mereka tidak kecanduan menggunakan konten Internet dan Sosmed.

2 Mendidik anak-anak agar mengetahui bahwa Indonesia adalah negara hukum, yang memiliki hukum dan sangsi terkait pornografi, yang diatur dalam UU Pornografi No 44/2008 dan UU ITE No 11/ 2008. Penyebarluasan muatan yang melanggar kesusilaan, pornografi melalui Internet diatur dalam pasal 27 ayat 1 UU ITE mengenai Perbuatan yang dilarang dan dikenakan pidana penjara hingga enam tahun dan/atau denda hingga Rp 1 milyar.

3 Menemani anak-anak ketika sedang mengakses Internet atau letakan laptop atau perangkat lainnya di tempat yang terjangkau dari pengawasan orang tua.

4 Menggunakan alat pengontrol internet yang aman di gawai dan memonitor apa saja yang si-kecil lakukan di gawainya seperti apa yang ditonton atau games yang dimainkan memanfaatkan fitur Parental Control.

5 Memberi batas waktu bermain Internet kepada anak-anak, untuk mencegah anak-anak kecanduan bermain Internet.

TIP-TIP

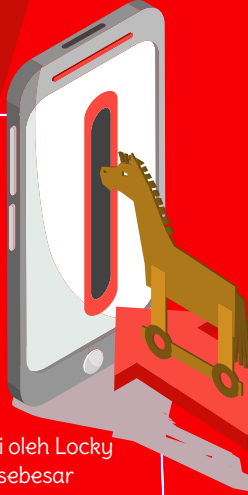
5 PENGGUNAAN PASSWORD*

1. Jangan gunakan password dengan suku kata umum. Gunakan campuran huruf, angka, tanda baca dan symbol typografi seperti "@!AB2-4#%" agar sulit ditebak dan dirangkai oleh botnet.
2. Selalu ganti (refresh) password pada perangkat/gawai komputer, smartphone, wifi router secara berkala/ periodic (30, 60 atau 90 hari).
3. Jangan gunakan password yang sama di semua platform dan perangkat
4. Jangan gunakan Default Password. Segera ganti password yang diberikan pabrik (Factory set default password). Pahami kelemahan user generated password otomatis oleh algoritma mesin.
5. Prioritas password administrator atau akun remote user, karena menjadi target cracker.
6. Jangan menyimpan password sembarangan ditempat yang diakses umum atau orang lain.
7. Gunakan Pengunci Akun (Account Lockout) artinya akan exit ketika cracker mencoba berulang ulang dengan berbagai kombinasi password dikenal dengan upaya Brute Force Attacks.
8. Jangan simpan Password di Harddisk/Memory tanpa dienkripsi alias Plain Text.

* https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

6 TIP-TIP

MENGHINDARI & MENANGKAL SPAM, MALWARE, RANSOMWARE, VIRUS & SPYWARE



ID SIRTII (Security Incident Response Team on Internet Infrastructure) mengungkapkan ada lebih dari 150 juta serangan malware (piranti peretas) yang terdeteksi di dunia (2017), antaranya jenis ransomware (piranti peretas yang meminta ransom atau uang tebusan) didominasi oleh Locky dan WannaCry. Ransomware tumbuh sebesar 350% (2018). Spyware piranti spionase peretas yang digunakan untuk mencuri, menyadap file, keyboard, camera, microphone dan disk di gawai anda.

RAJIN UPDATE SISTEM

Malware/virus selalu mencari kelemahan (vulnerability) di setiap sistem agar bisa dibobol. Sistem operasi, 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 ANTI VIRUS (AV)

Gunakan & Update Anti Virus (AV)/ Anti Spam atau Anti Spyware/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 anda.

BACK-UP DATA

Backup dokumen, foto atau berkas penting lainnya ke flashdisk, harddisk cadangan (offline) atau ke layanan google dropbox (online). Agar memiliki data cadangan. Jika data anda hilang karena virus atau di sandera oleh ransomware yang meminta uang tebusan, maka dapat dipulihkan (recovery) dengan data backup.

JANGAN KLIK LINK WEB & DOWNLOAD FILE YG TIDAK DIKENAL

Karena dapat membangunkan malaware, virus, ransomware yang ada di file yang didownload atau attachment yang diklik, konsekwensinya data dalam gawai anda sudah terkontaminasi, termasuk daftar alamat (address book) digunakan oleh peretas untuk fase duplikasi malware dan penyebaran berikutnya.

Berhati-hati Gunakan Wifi Publik

Terutama jika anda ingin melalukan transaksi keuangan, perbankan, ecommerce, credit cards serta aplikasi yang kritis dan strategis.

Tidak Gunakan Perangkat Pribadi

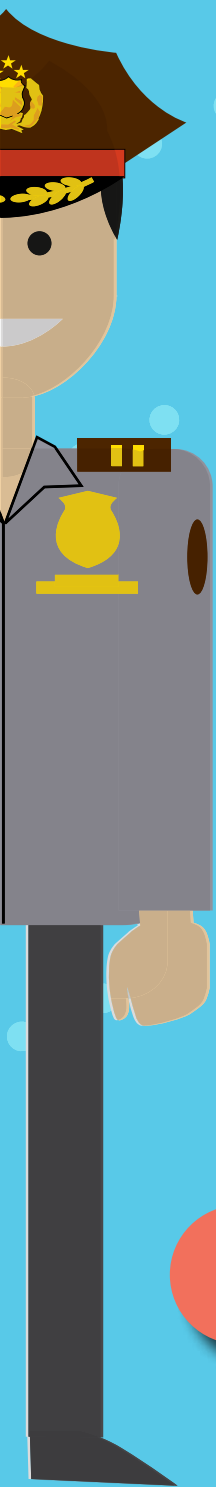
Tidak gunakan perangkat pribadi di tempat bekerja, untuk memproses pekerjaan perusahaan.

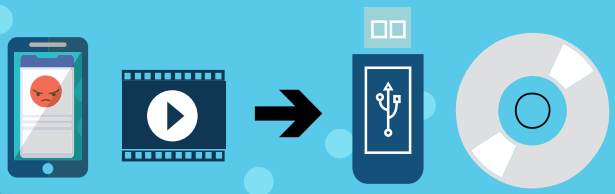
CARA LAPOR KORBAN KEJAHATAN SIBER

Saat ini makin banyak dan beragam kasus kejahatan siber, mulai dari penipuan, pornografi, terorisme, penyadapan, pencemaran nama baik, ujaran kebencian yang diatur dalam UU (SiberLaw/ Kejahatan Siber) No 11/2008 tentang Informasi & Transaksi Elektronik (ITE) dan Amandemen UU ITE No 19/2016.

Sebagai contoh kasus cara melaporkan kejahatan siber kepada aparat penegak hukum digunakan kasus ujaran kebencian (hate speech) menyerang ke lembaga negara, atau SARA (suku, agama, ras, dan antar golongan). Jika pencemaran nama baik menyerang individu, Polisi bisa menindak pelaku hate speech dengan delik murni.*

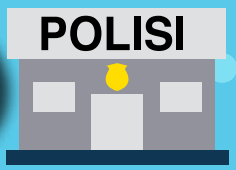
*(Ref: https://news.detik.com/berita/d-3884578/jadi-korban-ujaran-kebencian-begini-cara-lapornya-ke-polisi).





1 **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, harddisk, CD/DVD, dan lainnya. Satu bukti yang kuat sudah cukup.

2 **Datang ke kantor polisi**, dianjurkan setidaknya tingkat Polres untuk tindak pidana siber.



3 **Menuju ke ruang SPKT** kantor polisi untuk menyampaikan laporan & bukti- buktinya ke petugas.

4 **Petugas akan mengajukan beberapa pertanyaan** yang berhubungan dengan laporan ujaran kebencian, mengetik dan mencetak bukti pelaporan.

5 **Menunggu pemberitahuan** selanjutnya dari polisi.

Tidak ribet bukan? Jadi, jangan ragu untuk laporkan ujaran kebencian, pencemaran nama baik dan kejahatan siber lainnya ke kantor polisi.

8 SUPAYA ANAK AMAN BERMAIN INTERNET

Orang tua dan Guru sering kesulitan memantau aktivitas anak-anak ketika berselancar di dunia maya, mengingat anak-anak (generasi muda) lebih akrab dan mobilitas tinggi dengan gawai. Pada era masyarakat informasi, Internet bagaikan pedang bermata dua, dapat memberikan manfaat, informasi publik dan global yang positif terhadap perkembangan anak dan memberikan banyak informasi publik. Namun Internet juga memiliki dark web, dunia hitam berisi konten yang merugikan dan membahayakan, yang membutuhkan bimbingan pengawasan orang tua.

1. Komunikasi dan Edukasi

Orang tua harus terbuka dan memberikan edukasi sebelum anak-anak mulai akses Intenet. Merekomendasikan situs-situs yang baik dengan muatan edukatif kepada anak-anak. Ingatkan anak-anak untuk tidak memberikan informasi data pribadi, identifikasi personal seperti nama lengkap, alamat rumah, usia, gender, nama ibu, ayah, akun sandi atau akun bank. Jaga informasi profil di akun Sosmed dan Siber, karena sifatnya abadi sulit dihapus dan menjadi referensi untuk karir si anak. Pastikan bahwa profil sosmed terlindungi password dan gunakan privacy mode yang sesuai.

2. Parental Control

Orang tua menganjurkan anak menggunakan alat pengontrol konten kekerasan, pornografi di internet dan sensor umur di gawai, game dan browser. Monitor teman dan yang di tonton dan lakukan anaknya di gawainya. Biasakan akses TV, games atau gawai di ruang publik, kamar tamu bersama orang tua.

3. Batas Waktu dan Tempat

Berikan batas waktu bermain Internet baik di gawai nya, untuk mencegah kecanduan ketika bermain game online, Chat group (ie: Whatsapp group), Internet. Tidak bermain Internet saat makan, tidur, dikamar mandi, dikelas, rapat dan berjalan di tempat umum..

4. Hukuman Bagi Anak

Saat anak melanggar peraturan, orang tua dapat memberikan hukuman seperti tidak boleh memegang gawai selama 24 jam.

5. Berteman di Media Sosial

Agar anak-anak berinteraksi dengan teman sebaya/seumur, keluarga, orang tua dan hindari akun serta orang yang tidak dikenal untuk menghindari pemangsa/predator anak dan mencegah intaian orang jahat dan teror. Hormati privasinya.

6. Beri Contoh Teladan yang Baik

Orang tua jangan bermain gawai ketika mengemudi mobil atau motor, atau sambil makan atau tidur. Biasakan melihat hal positif dari dunia siber.

7. Gunakan Filter, Proxy (VPN)

Biasakan anak melihat hal yang positif dan bukan konten dewasa/ pornografi serta cegah pelacakan oleh situs berbahaya. Jaga alamat IP privat dan aman dibelakang proxy.

9 MELINDUNGI ANAK DARI SIBER BULLYING

Kasus Siberbullying (perundungan) dapat berbentuk sebuah komentar pedas, miring, cemooh, ejekan, intimidasi, atau segala hal yang bertujuan untuk mempermalukan atau melecehkan. Namun dampaknya sungguh negatif bagi perkembangan sang buah hati, seperti cemas, takut, merasa dipermalukan, dan lain sebagainya akan sangat menghantui anak.

Menurut KPAI (Komisi Perlindungan Anak indonesia) menilai komitmen perlindungan terhadap anak masih rendah di Tanah Air pada Hari Anak Nasional.

1 Orangtua turut berperan aktif dan proaktif, komunikatif untuk memperhatikan perilaku anak, terutama, jika anak terlihat seperti depresi, aneh dan mengalami perubahan perilaku seperti langsung terbuka, menutupinya, atau hanya diam saja ketika ditanya orangtua.

2 Ajari si anak untuk tidak memberikan informasi pribadi yang dapat menyebabkan pelecehan atau dipermalukan, seperti foto bayi, deskripsi fisik dll.

TIP-TIP

10 MELINDUNGI ANAK DARI PREDATOR ONLINE

Predator kerap mengincar anak-anak dengan menyamar di chatroom jejaring sosmed, email, messenger sebagai seseorang yang ramah, baik, sebaya dan berusaha menjadi teman dengan meraih kepercayaan dari calon korbannya. Predator menyamar sosok yang tampan dan idola dan korban yang termakan bujuk rayu, menjadi budak seks, terlibat aksi teroris, pemalakan atau memuaskan hasrat seksual predator. Mulai dari minta foto pose tak senonoh via webcam hingga diajak kopi darat untuk melakukan hubungan intim.

Tip lindungi anak dari predator online:

1. Hati-hati dengan informasi profil, personal (usia/gender) dan keluarga di akun Sosmed, messenger.
2. Jangan mengunduh gambar dari sumber yang tidak dikenal dan berpotensi mengandung materi berbau seksual atau kekerasan/teroris dan konten berbahaya.
3. Orang tua bisa menggunakan layanan penyaring/sensor e-mail. Hentikan kontak e-mail dan pesan instan jika sudah menjurus pada pertanyaan personal atau berkonotasi seksual, bullying atau teror.
4. Tempel aturan online yang disepakati keluarga di dekat komputer sehingga anak bisa melihat dan membacanya setiap saat mereka online.

11 TIP-TIP

BAHAYA DAN CARA HINDARI PENIPUAN PHISHING & SOCIAL ENGINEERING DI INTERNET

Banyak oknum-oknum yang tidak bertanggung jawab termasuk cracker (peretas) memanfaatkan beragam cara untuk melakukan tindak kriminal, mulai dari pencurian identitas, perusakan data, hingga pencurian uang. Banyak sekali modus serangan siber di dunia maya dan antaranya adalah phishing & Sosial Engineering (SosEng). Serangan siber lainnya seperti virus, spam, malware dapat dicegah dengan implementasi hardware misalnya firewall yang baik. Sementara Phishing dan Sosial Engineering sulit ditangkal karena memanfaatkan kelalaian si korban sendiri misalnya operator dan cracker menyaru sebagai orang yang berpengaruh, kecuali dengan implementasi pelatihan dan sosialisasi terhadap karyawan atau masyarakat akan bahaya Phishing dan SosEng.

Sosial Engineering (SosEng) menggunakan metode penyamaran, misalnya menyaru sebagai bos perusahaan dan menelpon satpam atau admin web untuk mendapatkan informasi rahasia seperti password. Modus SosEng yang lain adalah mengaku customer service sebuah bank atau kartu kredit dan minta informasi pribadi seperti pin atau data pribadi lainnya.

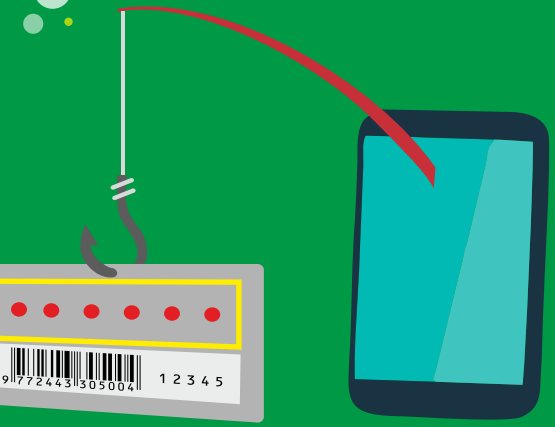
Phishing adalah upaya menyaru sebuah situs untuk melakukan penipuan. Kasus phishing terkenal pernah menimpa Klikbca.com Si cracker ini menyaru Klikbca.com dengan membuat beberapa situs yang mirip misalnya clickbca.com, clikbca.com atau Klik-bca.com. Nah korban yang tidak teliti membaca domain akan tertipu masuk situs phishing milik cracker. Selanjutnya cracker ini akan melakukan data mining pasword, login yang diketik oleh si korban, karena si korban sekarang bukan masuk ke situs BCA resmi tapi masuk ke situs si Cracker. Akhirnya si Cracker memiliki login dan password si korban dan dengan cepat menguras saldo si korban dengan cara phishing.

Bahaya sekali bukan?

Phishing adalah masalah keamanan yang serius. Tip jika menjadi korban Phishing:

1. Jangan panik dan tetap tenang menghadapi serangan phishing.

Tip jika menjadi korban Social Engineering (SosEng):



1. Segera laporkan ke instansi yang bersangkutan informasi yang tanpa sengaja anda bocorkan kepada pelaku SosEng agar informasi yang bersifat rahasia segera direset dan diganti.
2. Laporkan cara, kelemahan dan kerugian yang anda alami akibat SosEng.
3. Sosialisasi modus SosEng yang digunakan untuk melakukan SosEng kepada semua pihak agar tidak ada yang menjadi korbank kemudian hari.
4. Laporkan kepada aparat penegak hukum dinas Sibercrime untuk menangkap pelakunya.

2

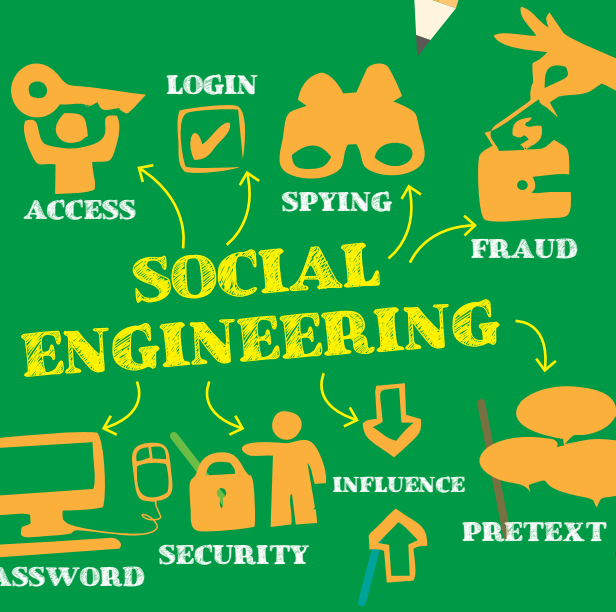
Segera hubungi call center atau datangi kantor dari perusahaan yang asli atau sebenarnya. Jelaskan anda ditenggarai menjadi korban phishing, agar informasi rahasia korban yang sudah dimiliki pelaku phishing segera di reset dan diubah agar pelaku phishing tidak dapat menguras rekening bank si korban.

3

Laporkan ke polisi agar situs penyamar pelaku phishing segera di blokir, ditutup dan pelaku phishing dikejar.

4

Rubah semua password dan login informasi agar tidak disusupi oleh cracker tersebut.



TIP-TIP

12 ETIKA SELANCAR DI DUNIA SIBER & SOSMED

Dunia Siber menjadi media/ruang virtual sosmed, yang mendekatkan teman yang jauh di ruang siber (keintiman virtual), namun menjauhkan teman yang dekat dan realitas atau fakta/kebenaran yang ada. Pada kehidupan sehari hari di dunia nyata, Negara yang berdaulat hadir melindungi warga negara dengan perundang undangan dan hukum agar menghormati satu dengan yang lain. Negara mempunyai hak menghukum, apabila ada yang mengganggu hak tetangganya sebagai manusia, sehingga tercipta Keteraturan, Kepastian Hukum dan Keamanan (Law and Order) di dunia nyata. Media mainstream mempunyai ijin resmi untuk menulis dan menyebarkan berita melalui media cetak, media elektronik sesuai fakta dan kebenaran yang ada.

Banyak pendatang baru di dunia siber tidak paham mengenai UU ITE atau peraturan yang ada didunia siber serta batasan ruang, waktu dan batas negara, sehingga sering kebablasan ketika berselancar di dunia siber. Setiap insan di sosial media dan chatgroupnya dapat mengirim berita tanpa batas, disebut citizen journalist mengalahkan dan mendisrupsi media tradisional mainstream yang mempunyai prosedur check dan recheck dengan fakta dan kenyataan oleh editornya.

Media online beredar bebas, instant tanpa kendali, check dan recheck di chat room dan sosial media, sehingga jauh dari realitas, kenyataan dan kebenaran yang ada. Berita di sosmed semakin cepat dan viral, banyak yang menjadi berita bohong atau Hoax. Fenomena Post Truth (Pasca Kebenaran) dimana Kebenaran digantikan oleh Pembenaran dan Kebenaran baru, the New Norm termasuk Hoax. Di sisi lain berita di sosmed juga sering campur aduk antara berita fakta dengan informasi asumsi, dugaan dan opini, akhirnya berpotensi menjadi berita hoax.

Ketika masyarakat tidak lagi berpikir kritis & menelan mentah-mentah informasi dari sosmed termasuk hoax, karena dianggap sesuai perasaan atau keyakinan pribadi atau populis, terkadang menggunakan isu SARA (keSukuan, Agama, Ras dan Antar golongan) untuk Divide et Impera Digital, yang memecahkan persatuan bangsa.

TIP MENGETAHUI INFORMASI HOAX (BOHONG):

1. Sumber berita media atau domain situs tidak jelas atau bodong, meragukan dan tidak familiar.
2. Tanyakan pada penyebar informasi untuk konfirmasi asal informasi yang dikirim.
3. Informasi waktu, tempat, lokasi yang tidak jelas, bahkan mencatut nama tokoh palsu.
4. Berisikan opini seseorang bukan fakta atau sejarah.
5. Sering terdengar mustahil ditunjang oleh penelitian palsu.
6. Cek dan Recheck dengan Media Masa Mainstream (Populer). Google aja!
7. Desain halaman yang aneh. Menggunakan huruf besar dan tanda seru. Menggunakan kata Heboh & Profokatif karena Hoax disebarkan untuk timbulkan kehebohan & kekacauan publik!
8. Baca ulang informasi secara utuh dan lihat lebih detail dan teliti isi dan maksudnya.

4 TIP MELAWAN Imformasi HOAX

1. Crosscheck & Klarifikasi: Jangan cepat percaya pada yang tidak jelas kebenarannya & bersikap kritis karena tidak semua yang ditulis di Internet itu benar.
2. Jangan mudah curiga dan berburuk sangka terhadap kawan dan lawan.
3. Berbicara yang Positif: Jangan mencari kesalahan pihak lain. Sampaikan kritik yang konstruktif dengan santun.
4. Sabar: Jangan mengikuti hawa nafsu; memecah belah (divide et impera) digital dengan isu SARA dan ikut mengumbar hate speech (ujaran kebencian).

TIP-TIP

13 HACKING & CRACKING & SERANGAN DARI INTERNAL, PENYADAPAN

Hacking adalah tindakan peretas dan penetrasi sistem yang lemah (vulnerable) oleh Hacker. Ada golongan White (hat) Hacker, yang memiliki etika tidak merusak sistem korban ketika melakukan serangan penetrasi (Penetration Test/Pentest), namun memberi tip agar korban memperbaiki kelemahan sistem. Mereka sering berkumpul misalnya di komunitas Black Hacker conference di Las Vegas (2011), saling tukar pengalaman yang positif. Blackhat Hacker atau Cracker sangat berbahaya menyerang (attack), merusak (Replay attack), menghancurkan, mencuri uang (sistem ebanking), mencuri data (data breach/theft), merubah (deface) web portal korban, menyadap (MiiT – Man In the middle) attack, penyadapan (intercept) dijalur Internet atau komunikasi. Membuat backdoor, menguasai webcam, kamera PC, microphone, layar PC anda. Cracker menggunakan malware, ransomware mengacak dan enkripsi data, harddisk korban sehingga tidak dapat di baca kecuali membayar ransom dengan bitcoin di Deep Web.

Tip untuk penjagaan berlapis serangan cracker dari Internet dan dalam Sistem:

1. Memasang proteksi perimeter di peripheri (pagar) seperti Firewall, Router untuk sistem LAN internal perusahaan anda. Proxy di peripheri untuk memisahkan IP Internet Siber yang beresiko (compromised) dengan IP Private untuk semua PC dan gadget dilingkungan LAN Perusahaan. Proxy untuk memisahkan IP dunia cyber yang berbahaya (compromised) dengan IP Private untuk semua PC dan gadget dilingkungan LAN Perusahaan.
2. Anti virus, Anti Spam, Anti Malware, Sensor konten di Server dan disetiap PC serta peralatan Anti Insider Threat yang merupakan pertahanan berlapis (defence in depth) bagi sebuah korporasi dan enterprise.

Menjaga serangan dari dalam disebut Insider Threat (ancaman) atau Attack (serangan) lebih sulit, karena musuh sudah masuk dan tidur (hibernasi) di dalam LAN atau di PC, menunggu saat momentum tepat menyerang, saat sistem dalam kondisi lemah. Pemerintah AS membuat proyek CINDER (Siber Insider Threat) melalui DARPA riset militer AS, setelah sistem dan data rahasia (classified) pemerintah AS diretas oleh Julian Assange dan disebar di Wikileaks. Edward Snowden sebagai karyawan kontraktor NSA (Badan Security Siber milik Pemerintah AS) menjadi whistleblower dengan metode insider threat. Statistik menggambarkan serangan dari dalam lebih rentan, baik disengaja atau tidak, kecerobohan pegawai, manajer bahkan kontraktor perusahaan.*

*(Ref: http://komite.id/2018/06/26/serangan-masif-cyber-attack-global/)

PETA KONTEN DARI
DUNIA SIBER

Google

Bing

YAHOO!

Estimasi hanya 4% dari total Content Web (Laman Internet)

Surface Web
(Konten di Permukaan)

Deep Web
(Konten Jauh & Dalam)

- Academic Databases
- Medical Records
- Financial Records
- Legal Documents
- Some Scientific Reports
- Some Government Information
- Some Organization Specific Repositories

Estimasi 96% dari total Laman Internet

Dark Web
(Konten Gelap)

- TOR Hidden Services
- Political Protest
- Drug Trafficking & Other Ilegal Activities
- Silk Road Anonymous marketplace

https://www.facebook.com/kliks.bssn.1 @BssnKliks https://www.instagram.com/kliks.bssn