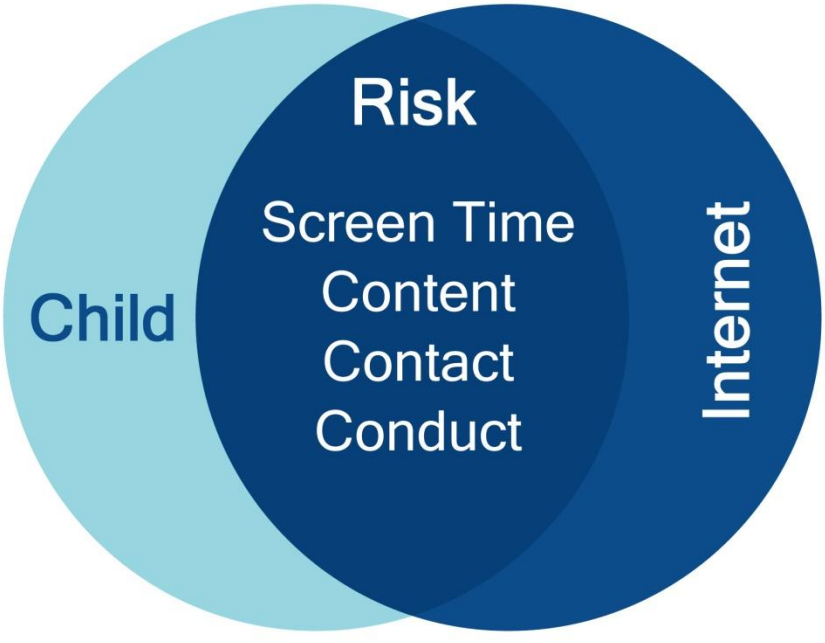
Keamanan Berinternet

Bagi Anak & Remaja

Edisi Perdana
Februari 2017



Tisna Rudi
Anti Bullying Indonesia

DAFTAR ISI

Kata Pengantar 4
Gelombang Tsunami Internet 5
- Apa itu Internet?
- Apa itu World Wide Web (WWW)?
- Kenapa Perlu Browser?

Memahami Risiko Online 12
- Klasifikasi Risiko
- Risiko Layanan Online

Cerdas dan Bijak Menggunakan Internet 18
- Informasi Pribadi
- Reputasi Digital
- Privasi
  - Apa itu Privasi?
  - Apa Hubungannya Dengan Internet?
  - Kenapa Privasi Online Anak Penting?
  - Panduan Privasi Online Untuk Anak dan Remaja
- Pemeriksaan Reputasi Online

Screen Time 30
- Anak-anak dan TV
- Dampak Media Exposure pada anak-anak
- Apa yang Dapat Orang Tua Lakukan?

Media Sosial 40
- Apa Sih Media Sosial itu?
  - Media Sosial Sebagai Web 2.0
  - Media Sosial Sebagai Big Data
  - Media Sosial Sebagai Habit Forming Product
- Risiko Media Sosial Bagi Anak-Anak

Memahami Cyber Bullying 48
Definisi
Karakteristik Cyber Bullying
Jenis-Jenis Cyber Bullying
Kenapa Orang Melakukan Cyberbullying?
Target Korban
Tanda-Tanda Korban Cyber Bullying
Apa yang Dapat Orang Tua Lakukan?
Dampak Terhadap Korban
Dampak Terhadap Pelaku
Pencegahan Cyber Bullying
Phishing 62
Modus Phishing
Identifikasi Phishing Email
Identifikasi Phishing Website
Tips Menghindari Phishing
Keamanan Menggunakan Internet 73
Parental Control
Tips Untuk Orang Tua
Peraturan Umum Keamanan
Tips Untuk Anak dan Remaja
Menjadi Netizen Yang Baik 87
Netiquette
Rujukan 98
Lampiran 103
Daftar Istilah di Internet dan Pengertiannya
Tentang anti Bullying Indonesia 106

Kata Pengantar

Ebook ini saya buat setelah membaca Hasil Survey 2016 Asosiasi Penyelenggara Jasa Internet Indonesia (APJII).

Dari 132,7 juta pengguna internet di Indonesia, 76,4% (101,3 Juta) diantaranya berpendapat bahwa Keamanan Berinternet bagi Anak Tidak Aman.

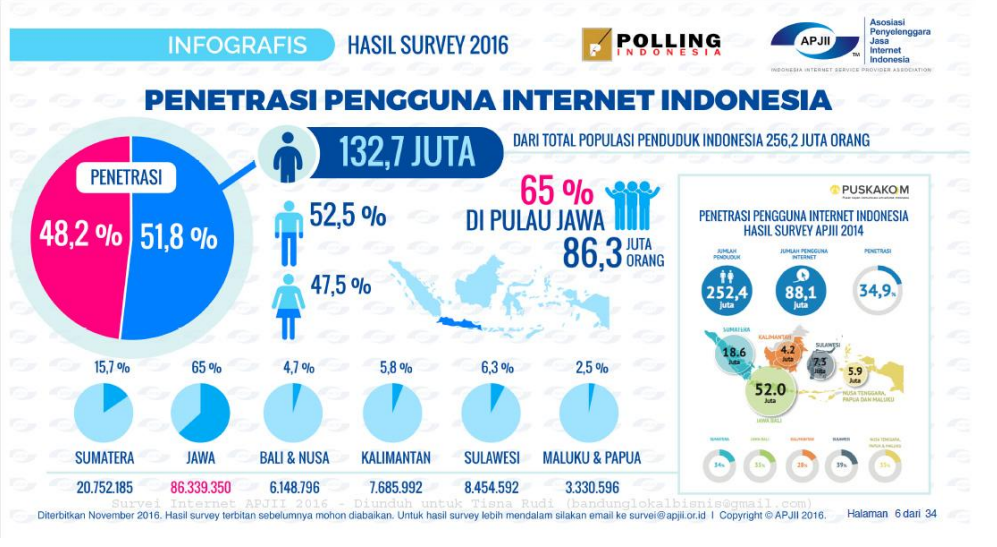
Tanggal 7 February 2017 juga diperingati sebagai Safer Internet Day di berbagai Negara.

Bandung, 3 Februari 2017.

Tisna Rudi

Gelombang Tsunami Internet

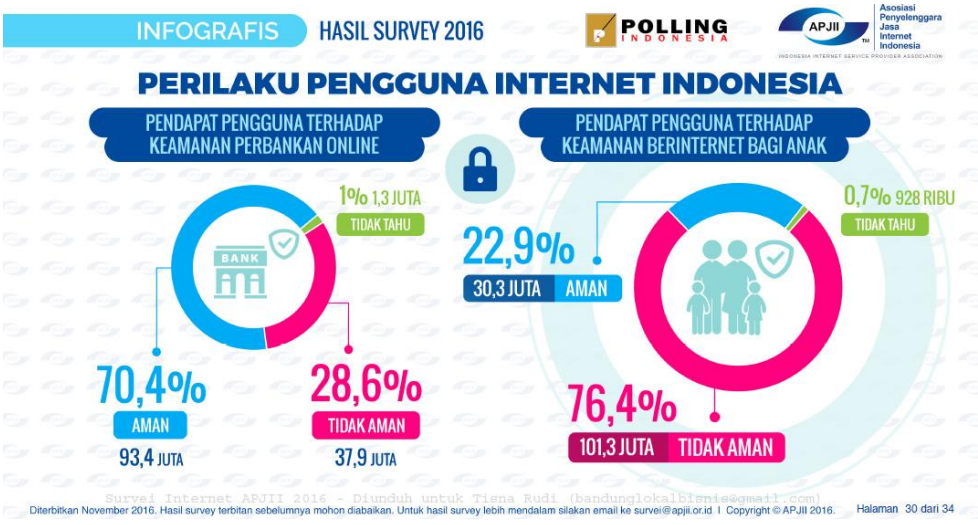
Pengguna internet di Indonesia setiap tahun meningkat. Berdasarkan Survey Tahun 2014 yang dilakukan APJII hanya ada 88,1 juta pengguna internet. Kemudian Tahun 2016 menjadi 132,7 juta pengguna internet dari jumlah total penduduk Indonesia 256,2 juta orang.



Hasil Survey 2016 Asosiasi Penyelenggara Jasa Internet Indonesia

Peningkatan ini tidak dibarengi dengan kesadaran masyarakat dan orang tua mengenai keamanan online.

Berdasarkan Hasil Survey Asosiasi Penyelenggara Jasa Internet Indonesia pada Tahun 2016, sekitar 76,4% (101,3 Juta) pengguna internet di Indonesia berpendapat bahwa Keamanan Berinternet bagi Anak **Tidak Aman**.



Hasil Survey 2016 Asosiasi Penyelenggara Jasa Internet Indonesia

Orang tua membelikan smartphone, tablet, atau laptop untuk anak, tapi keamanan penggunaannya kurang pengawasan dari orang tua.

Orang tua harus mendidik dirinya sendiri dan kemudian mengajarkan kepada anggota keluarganya mengenai keamanan berinternet bagi anak-anaknya.

Tidak sedikit juga orang yang beranggapan karena berada di dunia maya dan merasa tidak ada yang mengawasi, terus merasa bebas ber-ekspresi atau menggunakan bahasa yang kasar dalam memberikan komentar.

Padahal berada di dunia maya sama juga dengan berada di tempat umum di dunia nyata. Kita harus pandai menjaga diri, ada etika, dan peraturan. Bahkan dapat dilacak (Cyber Forensic).

Apa itu Internet?

Internet adalah jaringan sistem telekomunikasi yang menjangkau ke seluruh dunia, menyediakan koneksi untuk jutaan jaringan lainnya, yaitu jaringan-jaringan yang lebih kecil. Karena itu, internet sering juga disebut sebagai jaringan dari sekumpulan jaringan-jaringan (network of networks).

Internet menyediakan komunikasi lintas jarak antar pengguna komputer dengan berbagai sistem operasi dan jenis komputer berbeda sehingga satu sama lain dapat terhubung.

Internet Service Provider (ISP) menyediakan akses internet untuk pengguna melalui servernya. Anda dapat melakukan koneksi ke internet melalui kabel telepon, modem, Wi-Fi, dan Smartphone.

Apa itu World Wide Web (WWW)?

Internet merupakan kumpulan dari berbagai sistem dan protokol berbeda-beda. Salah satunya adalah protokol World Wide Web.

Dua protokol lainnya yang sangat penting adalah Transmission Control Protocol (TCP) dan Internet Protocol (IP). Melalui kedua protokol ini komputer dapat mengirimkan data ke internet, dan secara virtual, dapat berkomunikasi satu sama lain dengan komputer lainnya.

Domain Name System (DNS)

Alamat di internet disebut IP address, terdiri dari sederetan angka. Karena mengingat sederetan angka itu susah, maka dibuatlah Domain Name System (DNS) untuk menterjemahkan angka-angka IP address menjadi kata-kata. Sebagai contoh, IP address 216.58.198.238 dan 172.217.0.46 susah dihapal, lebih mudah kalau diterjemahkankan menjadi google.com

URL

Alamat untuk website disebut URL (Uniform Resource Locators). Umumnya dimulai dengan http:// (HyperText Transfer Protocol). Atau https:// Huruf "s" singkatan dari secure. Sebagai contoh, URL untuk Google adalah

https://google.com/

Contoh alamat untuk file halaman website yang disimpan dalam folder:

http://namatoko.com/tas/index.html

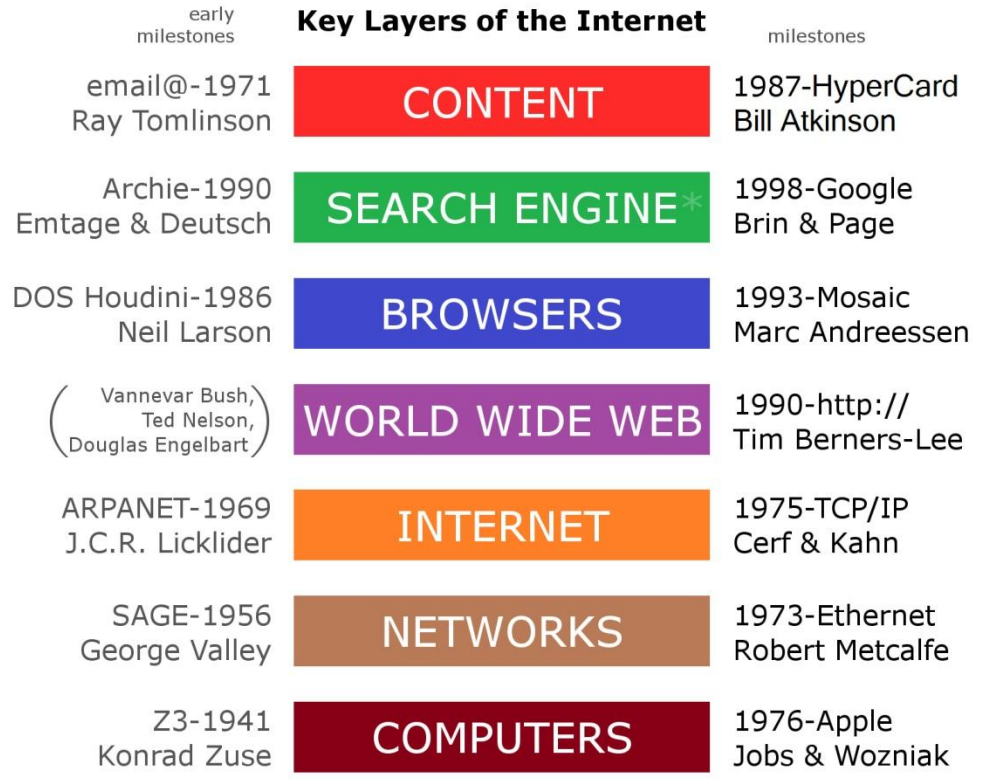
Dalam contoh tersebut diatas, “index.html” adalah nama file yang disimpan dalam folder bernama “tas” di web server namatoko.com.

Kenapa Perlu Browser?

Untuk akses website di internet, kita menggunakan Browser, misalnya Google Chrome, Mozila Firefox, atau Microsoft Internet Explorer. Aplikasi Browser berfungsi untuk membaca dokumen halaman web dan menampilkannya seperti yang Anda lihat di layar komputer.

Pada halaman web, jika anda mengarahkan kursor komputer diatas teks atau gambar tertentu, dan kursor berubah menjadi simbol telunjuk jari tangan, maka itu menandakan sebuah Link yang dapat di klik.

Jika link di klik, maka kita akan diarahkan ke halaman web lainnya, atau bisa juga untuk mengaktifkan program email.



Ilustrasi lapisan utama internet

Source: https://commons.wikimedia.org/wiki/File:Internet_Key_Layers.png

Memahami Risiko Online

Internet bisa menjadi sarana yang bagus untuk belajar, menghubungi teman yang lokasinya berjauhan, mempromosikan produk, belanja, hingga bermain game. Tapi sayang, di internet juga ada berbagai penyalahgunaan yang memanfaatkan ketidaktahuan seseorang untuk melakukan berbagai hal yang dapat merugikan orang lain.

Anak-anak yang masih polos, apalagi di lingkungan yang masih baru baginya, tidak banyak mengetahui bagaimana melindungi dirinya, dan tidak selalu memikirkan akibat dari perbuatannya

Dalam rangka menjaga keamanan anak-anak, orang tua harus mengetahui tentang berbagai risiko online yang dapat membahayakan perkembangan anak.

Dengan mengetahui berbagai kemungkinan bahaya online akan membantu anda sebagai orang tua dan anak anda melakukan antisipasi cerdas dan bijak dalam menggunakan internet.

Klasisifikasi Risiko

Risiko online yang yang dihadapi anak dan remaja dapat diklasifikasikan berdasarkan tabel berikut:

	Content Child as recipent	Contact Child as participant	Conduct Child as actor
Commercial	Advertising, spam, sponsorship	Tracking/ harvesting personal information	Gambling, illegal downloads, hacking
Aggressive	Violent/ gruesome/ hateful content	Being bullied, harassed or stalked	Bullying or harassing another
Sexual	Pornographic/ harmful sexual content	Meeting strangers, being groomed	Creating/ uploading pornographic material
Values	Racist, biased info/ advice (eg, drugs)	Self-harm, unwelcome persuasion	Providing advice eg, suicide/ pro-anorexia

A classification of online risks for children [1]

[1] Livingstone, S, and Haddon, L (2009) *EU Kids Online: Final report*. LSE, London: EU Kids Online. (EC Safer Internet Plus Programme Deliverable D6.5)

Risiko konten:
Anak dan remaja pra dewasa, sebagai penerima dapat menemukan konten berupa pesan teks, foto, atau video tidak senonoh, porno, menakutkan, kekerasan, dan informasi tidak benar.

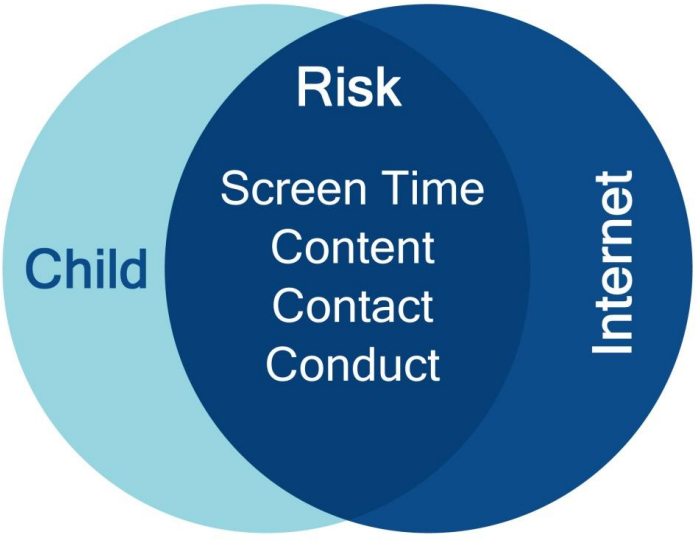
Risiko kontak:
Anak dan remaja pra dewasa, dalam aktifitasnya melalui internet, sebagai peserta dapat bertemu atau berkenalan dengan orang asing, teman sebaya atau laki-laki dewasa berusia 40 tahun yang menyamar sebagai gadis remaja.

Risiko berbuat sesuatu:
Anak dan remaja pra dewasa, sebagai pelaku dapat mem-posting foto atau membuat video yang tidak pantas tentang dirinya dan atau bersama teman-teman sebayanya.

Risiko menggunakan peralatan digital:
Ketika seseorang menggunakan komputer atau smartphone, ada risiko mengalami kelelahan mata dan kelelahan lengan.

Anak dan remaja pra dewasa, berdasarkan usia, screen time nya harus dibatasi. Karena keseringan menghabiskan waktu online dapat menimbulkan masalah kecanduan internet atau kecanduan main game.

Penggunaan internet tidak dilarang dan ada baiknya, tapi jika sudah menjadi kecanduan dapat berdampak terhadap kehidupan seseorang di dunia nyata.



Ilustrasi klasifikasi risiko

Risiko Layanan Online

Selain risiko atas dasar klasifikasi tersebut diatas, risiko online juga dapat terjadi dalam menggunakan layanan.

Layanan pertukaran pesan
Karena ponsel sering dibawa kemana-mana, risiko layanan instan pertukaran pesan seperti WhatsApp, Blackberry Mesenger, ddan Line dapat terjadi kapan saja dan dimana saja.

Kemungkinan menerima pesan teks yang tidak diinginkan atau dihubungi oleh cyberbully.

Layanan media sosial
Facebook, Instagram, Twitter, Youtube (Broadcast Yourself) memberikan fasilitas untuk berbagi informasi. Akibatnya banyak orang yang cenderung terlalu banyak berbagi tentang dirinya sendiri. Hal ini, kalau tidak dipikirkan dulu akibatnya, dapat merusak reputasi online dirinya sendiri atau orang lain.

Layanan situs berbagi file

Kemungkinan file yang diunduh mengandung virus, malware, atau spyware. Juga kemungkinan dapat menimbulkan masalah hukum jika mengunduh atau berbagi file musik, video/film, atau software yang dilindungi oleh undang-undang Hak Kekayaan Intelektual.

Layanan Email

Email secara luas banyak digunakan oleh berbagai kalangan dan usia. Juga digunakan oleh cyberbully, online predator, dan hacker. Kemungkinan menerima spam, dan phising email untuk mencuri informasi pribadi.

Cerdas dan Bijak Menggunakan Internet

Sekali informasi berada di dunia online akan menjadi sulit untuk dihilangkan. Bisa dengan mudah dan cepat disebarkan. Gambar, foto dan kalimat dapat disalahtafsirkan dan diubah dalam perjalanannya disebarluaskan.

Konten yang dimaksudkan untuk group kecil antara teman-teman dapat menjadi persoalan ketika disebarkan keluar group.

Kita harus mempertimbangkan untuk melakukan pengelolaan informasi, pesan dan gambar. Pengaturan privasi di media sosial, kalau perlu diaktifkan untuk melindungi informasi pribadi.

Informasi di dunia maya dapat berada terus disana selamanya, dan informasi pribadi Anda mungkin dilihat oleh orang yang tidak Anda kenal. Termasuk oleh orang yang mungkin akan menjadi karyawan atau Bos di perusahaan tempat kerja.

Informasi Pribadi

Informasi pribadi adalah setiap informasi atau kombinasi informasi yang dapat meng-identifikasi seseorang. Apa saja informasi pribadi ini?

Nama Lengkap
Alamat Rumah
Nomor Telephone
Sekolah
Tanggal dan tempat Lahir
Alamat email
Nama pengguna dan Kata sandi
Detail Akun Bank.

Banyak layanan online mengharuskan penggunanya memberikan berbagai informasi pribadi untuk menggunakannya. Berikut beberapa aktivitas online dimana Anda harus memberikan informasi personal.

Belanja online: untuk verifikasi identitas pembeli, proses pembayaran, dan untuk pengiriman barang.

Mendaftar atau berlanganan berita: paling tidak perlu id username dan alamat email.

Tapi mungkin juga diminta untuk melengkapi informasi tambahan, misalnya usia, jenis kelamin, alamat, dan foto.

Mengikuti perlombaan berhadiah: seringkali memerlukan data demografis dan minat personal untuk promosi produk atau layanan.

Game online: pengguna perlu mendaftar sebelum mulai main.

Reputasi Digital

Semua pengguna internet, apakah anak-anak, remaja, orang dewasa atau orang tua mempunyai jejak digital atau digital footprint. Jejak digital ini berupa pendapat atau pandangan orang lain terhadap seorang pengguna berdasarkan apa yang telah dikatakan dan dilakukannya secara online.

Reputasi digital didefinisikan oleh perilaku anda di dunia maya, konten yang di posting tentang diri sendiri dan orang lain.

Photo yang di tag, posting di blog, interaksi dan komentar di media sosial akan membentuk siapa anda di mata orang lain, online dan oflline, sekarang mau pun di masa akan datang.

Reputasi digital yang buruk dapat mempengaruhi hubungan pertemanan dan pekerjaan. Karena itu sangat penting Anda menyadarinya.

Untuk keamanan dan privasi, sangat penting anak-anak dan remaja menyadari dimana dan bagaimana informasi pribadi mereka terdapat di internet, siapa yang dapat meng-aksesnya, apa yang orang lain lakukan terhadap informasi tersebut, dan kesan apa yang mereka tinggalkan kepada orang lain.

Mereka harus mengerti dan menyadari semua fitur dan syarat-syarat penggunaan layanan media sosial, khususnya bagaimana mengatur profile akunnya menjadi privat.

Bantu mereka untuk mengerti bahwa setiap informasi yang mereka berikan secara online atau melalui layanan pertukaran pesan dapat dibagikan lebih luas dari apa yang mereka pikirkan.

Bahkan meskipun profile mereka diatur privat, mereka tidak bisa mengontrol apa yang akan dilakukan oleh teman-temannya dengan informasi yang mereka terbitkan.

Anjurkan kepada mereka untuk memikirkan terlebih dahulu dan berhati-hati sebelum berbagi foto, memberikan komentar, atau menyebarkan pesan melalui smartphone dan atau komputer.

Bantulah mereka memahami bahwa mereka mungkin melakukan perbuatan kriminal ketika mengambil atau menyebarluaskan foto sensual dirinya atau foto sensual teman-teman sebayanya.

Membuat dan atau menyebarkan foto sensual anak-anak merupakan penyalahgunaan materi pornografi anak-anak.

Membersihkan reputasi digital bukan hal yang tidak mungkin dilakukan. Tapi akan menjadi tugas yang tidak mudah.

Privasi

Apa itu Privasi?

Privasi atau Kerahasiaan Pribadi (Bahasa Inggris: Privacy) adalah kemampuan seorang individu atau sekelompok orang untuk menyendiri atau secara selektif mengontrol informasi dari publik tentang dirinya atau tentang mereka. Privasi dapat dianggap sebagai suatu aspek dari keamanan.

Privasi penting bagi anak-anak karena memberikan mereka kontrol kapan dan berapa banyak informasi yang dapat diungkapkan tentang mereka. Hal ini merupakan faktor penting dalam perkembangan alami anak-anak menjadi dewasa.

Apa Hubungannya Dengan Internet?

Privasi di internet adalah kemampuan untuk mengontrol informasi apa saja yang dapat diungkapkan di internet tentang seseorang, dan untuk mengontrol siapa saja yang yang dapat meng-akses informasi tersebut.

Kenapa Privasi Online Anak Penting?

Pada dasarnya sangat penting untuk mengenal anak dan remaja sebagaimana ketika kita tumbuh menjadi dewasa. Mereka masih naif mengenai mereka sendiri, kehidupan disekitar, dan sedikit mengetahui tentang melindungi mereka sendiri.

Internet dapat menghadirkan berbagai risiko terhadap anak dan remaja. Misalnya cyberbullying, sexting, sexual predator, pelanggaran privasi, dan konten berbahaya.

Eksplotasi komersil mengumpulkan informasi personal anak-anak sebagai data untuk target segmen pasar. Posting foto tidak senonoh yang disebarkan tanpa ijin dan dapat merusak reputasi seseorang.

Ketika anak-anak dan remaja meningkat dewasa, latar belakang profil mereka di internet dan media sosial, dapat menjadi bagian dari pemeriksaan dalam proses masuk ke perguruan tinggi dan melamar pekerjaan.

Panduan Privasi Online Untuk Anak dan Remaja

Ajarkan kepada anak-anak dan remaja bahwa:

- Di internet tidak ada yang 100% privat.
- Informasi yang ada di internet, terutama yang diluar kontrol kita, akan sulit untuk dihapus dan akan ada selamanya.
- Privasi berkaitan dengan jangka panjang dan masa depan mereka.

Anak-Anak Usia Sekolah Dasar

Definisikan untuk mereka apa yang termasuk informasi pribadi:

Nama Lengkap
Alamat Rumah
Telephone rumah dan atau nomor ponsel
Tanggal lahir
Usia
Nama Sekolah
Nama Team olah raga atau klub lainnya.

Beritahu Mereka
Jangan pernah memberikan semua informasi tersebut kepada siapa pun tanpa persetujuan dari orang tua.

Jika mereka ingin bergabung dalam suatu website, ketahui bahwa informasi yang diperlukan hanya: Usia, untuk menentukan jika anak anda dibawah usia 13 tahun, username, dan alamat email orang tua sebagai cara meminta ijin dari orang tua.

“Bahaya orang asing tidak dikenal” juga berlaku di internet. Tidak boleh memberikan informasi personal kepada orang yang bertemu online. Sangat penting bagi mereka untuk dapat melindungi informasinya yang bersifat pribadi.

Anak-Anak Usia Sekolah Menengah
Sejalan dengan bertambahnya usia, dari anak-anak menjadi remaja SMP dan remaja pra dewasa (SMA), hingga awal masuk kuliah, selain informasi tersebut diatas, informasi tambahan dibawah ini juga merupakan informasi personal:

Semua informasi personal sebelumnya ditambah dengan informasi berikut:

Alamat email
Password
Nomor layanan pertukaran pesan
(BBM, WA, Line, Wechat)
Nomor Kartu debet dan Nomor PIN

Nomor e-KTP dan nomor SIM
Nomor PIN Kartu Debit.
Informasi login ke akun Bank di website.

Privasi Online Anak-Anak

- Informasi personal anak-anak dibawah usia 13 tahun tidak boleh dikumpulkan dalam website tanpa ijin dari orang tua atau walinya.
- Orang tua mempunyai hak untuk mengetahui untuk apa informasi personal anak diminta dan bagaimana informasi tersebut digunakan.
- Ijin dari orang tua dan walinya dalam banyak hal harus bisa dibuktikan.
- Anak-anak tidak boleh diminta untuk memberikan informasi lebih dari yang diperlukan sewajarnya untuk berpartisipasi dalam permaianan atau kontes.
- Web sites dan layanan online harus secara jelas mencantumkan kebijakan privasi.

Pemeriksaan Reputasi Online

1	Cari diri sendiri di internet melalui search engine Google dan lihat apa saja yang ditemukan. Periksa juga posting beberapa tahun lalu di media sosial. Jika menemukan hal yang tidak baik mengenai diri sendiri, ambil langkah yang diperlukan untuk menghapusnya.
2	Periksa pengaturan privasi di profil media sosial. Atur posting apa yang dapat dilihat oleh publik, dan yang hanya dapat dilihat oleh teman. Posting teman dan pengaturan privasinya juga dapat mempengaruhi jejak digital anda, misalnya foto anda yang di tag oleh teman.
3	Pikirkan sebelum berbagi. Sebelum memberikan komentar, posting foto sendiri atau foto teman, tanyalah diri sendiri: apakah anda ingin semua orang (teman, keluarga, teman kerja yang sekarang atau yang akan datang) mengetahui?
4	Bangun jejak digital dan reputasi online positif.
5	Non-aktifkan dan hapus akun anda jika berhenti menggunakan media sosial atau forum diskusi online. Dengan demikian tidak dapat dicari dan mencegah akun anda di bajak oleh hacker.

Screen Time

Media digital dan peralatan teknologinya seperti Televisi, DVD, Video game, komputer, tablet, dan smartphone sekarang ini sudah menjadi bagian tidak terpisahkan dari kehidupan sehari-hari.

Tapi jika anak-anak kita, khususnya yang masih Balita menggunakannya secara berlebihan atau terlalu sering dapat menimbulkan dampak serius terhadap perkembangannya.

Dampak ini termasuk masalah keterlambatan bahasa, kegemukan (obesitas), memusatkan perhatian, dan kesulitan tidur.

Karena itu, orang tua perlu membatasi Screen Time bagi anak-anaknya.

Screen Time didefinisikan sebagai aktifitas mengamati atau menggunakan layar monitor, termasuk TV, DVD, Video game, dan Komputer.

Active Screen Time

Active Screen Time merupakan kegiatan yang melibatkan proses kognitif atau aktifitas fisik, misalnya main video game atau menyelesaikan tugas sekolah dengan menggunakan komputer.

Passive Screen Time

Passive Screen Time merupakan kegiatan yang lebih cenderung pasif, hanya mengamati layar monitor, misalnya menonton TV atau DVD.

Anak-anak dan TV

Bayi

Dua tahun pertama perkembangan otak sangat penting. Bayi belajar dan akan berkembang baik dengan berbicara dan bermain bersama orang nyata, bukan bersama orang dalam layar TV.

Menggunakan TV untuk menemaninya, mengalihkan perhatian atau untuk supaya tidur dapat menjadi kebiasaan di kemudian hari.

Usia Prasekolah (4 – 6 tahun)
Gambar-gambar pada layar mulai menarik anak pada usia ini. Tetapi, kebiasaan seumur hidup juga terbentuk pada usia ini.

Anak berusia dibawah 6 tahun mengalami kesulitan memahami perbedaan antara fantasi dan kenyataan. Mereka melihat karakter kartun sebagai kenyataan, dan tidak mengikuti alur cerita.

Anak Usia Sekolah
Anak usia 6 sampai 9 tahun masih kesulitan untuk memahami perbedaan antara fantasi dan kenyataan, terutama kalau kelihatannya seperti hidup nyata. Mereka percaya situasi dalam TV menggambarkan keluarga yang nyata. Cenderung mengagumi dan ingin menjadi seperti tokoh pahlawannya di TV.

Dampak Media Exposure pada anak-anak

Dampak terhadap perkembangan Bahasa.
Beberapa penelitian menunjukan bahwa semakin sering anak-anak menonton TV, semakin besar kemungkinannya mengalami keterlambatan perkembangan bahasa.

Semakin sering nonton TV, bayi berusia 8 – 16 bulan, semakin sedikit perbendaharaan kata-kata yang diketahuinya.

Obesitas dan Menonton TV
Screen Time dapat berkontribusi terhadap masalah kegemukan karena:

1. Duduk di depan TV mengurangi aktifitas.
2. Makanan tidak sehat karena iklan.
3. Aktifitas makan makanan ringan selama screen time meningkat.

Masalah Perilaku

1. Siswa yang menghabiskan waktu nonton TV atau menggunakan komputer lebih dari 2 jam per hari cenderung mengalami masalah emosional, sosial, dan memusatkan perhatian.
2. Perilaku Agresif
3. Bayi usia 3 tahun yang tiap hari nonton TV untuk setiap jam sebanding dengan kemungkinan peningkatan 10% masalah memusatkan perhatian pada usia 7 tahun.

Self Esteem Rendah dan Kegelisahaan

Anak-anak yang lebih banyak menghabiskan waktu untuk menonton TV, Komputer dan bermain game, dapat menimbulkan masalah self esteem rendah, kegelisahan, dan bahkan depresi.

Tidur

Screen time berakibat

- Keterlambatan awal tidur
- Waktu tidur lebih sedikit

Penyebab kurang tidur

- Timing
- Konten
- Emisi cahaya

Apa yang Dapat Orang Tua Lakukan?

- Buat aturan berdasarkan usia anak dengan menggunakan klasifikasi acara TV sebagai panduan.
- Bantu anak memilih program TV yang disukainya atau bermain game bersamanya di ruang keluarga.
- Bimbing dengan memberi contoh. Batasi screen time anda sebagai orang tua.
- Ruang makan bebas dari TV agar ada waktu untuk ngobrol dan belajar tata krama di meja makan.
- Hindari screen time di waktu pagi hari.
- Buat peraturan, tidak boleh nonton TV sebelum pekerjaan rumah atau tugas dari sekolah selesai.
- Atur waktu tidur anak berdasarkan usianya.
- Awasi berapa lama anak menghabiskan waktu di depan komputer dan website yang dikunjunginya.
- Jangan menempatkan TV, komputer, tablet atau smartphone di kamar tidur.

- Dampingi anak ketika melakukan aktifitas screen time.
- Dorong melakukan aktifitas bermain diruangan tanpa TV atau di luar rumah.
- Jika diasuh oleh pengasuh anak, sampaikan aturan-aturan diatas kepada pengasuh.

Mengatur Screen Time

Anak yang tumbuh dengan kebiasaan screen time yang sehat akan cenderung membuat pilihan lebih baik tentang bagaimana mengisi waktu luangnya ketika mereka lebih tua.

Batasan Ideal Screen Time

Batasan screen time akan berbeda antara suatu keluarga dengan keluarga lainnya. Pedoman dibawah ini harus disesuaikan berdasarkan kebutuhan individual dan kemampuan anak.

Usia	Screen Time Limit
0 – 2 Tahun	Nol atau dibatasi harus bersama orang dewasa. Utamakan berbicara dan bermain bersama dengan orang nyata, bukan dengan orang di layar LCD TV.
2 – 5 Tahun	1 jam/hari. Aktifitas fisik dan sosial tetap harus jadi prioritas.
6 – 9 Tahun	1,5 jam/hari
10 – 13 Tahun	1,5 - 2 jam/hari
14+ Tahun	2 jam/hari

Tdak ada pendekatan peraturan yang cocok untuk semuanya (one-size-fits-all). Orang tua harus menyesuaikan strategi dengan usia, interest, dan kebutuhan anaknya, mengingat anak memerlukan dukungan dari mulai bayi sampai remaja-dewasa.

Orang tua tidak harus serta merta beranggapan penggunaan media digital anaknya menimbulkan masalah.

Daripada membatasi screen time berdasarkan perkiraan semena-mena, orang tua dapat mempertimbangkan screen konteks, konten, dan koneksi dengan menanyakan kepada diri sendiri:

a. Apakah anak anda secara fisik sehat dan cukup tidur?
b. Apakah anak anda secara sosial berhubungan dengan keluarga dan teman-temannya?
c. Apakah anak anda terlibat dengan kegiatan di sekolah dan mencapai keberhasilan di sekolah?
d. Apakah anak anda mempunyai ketertarikan terhadap sesuatu dan hobby?
e. Apakah anak anda memperoleh kegembiraan dan belajar dalam menggunakan media digital?

Jika jawabannya lebih kurang “Ya”, maka orang tua dapat mempertimbangkan apakah kekhawatiran nya terhadap penggunaan media digital secara berlebihan sudah cukup baik.

Jika jawabannya lebih atau kurang “Tidak”, maka orang tua perlu membuat peraturan dan pembatasan untuk mengatasi masalah screen time.

Media Sosial

Apa Sih Media Sosial itu?

Media Sosial Sebagai Web 2.0
Ditinjau dari teknologi web, media sosial adalah salah satu jenis Web 2.0, dimana kontennya di update oleh kontribusi penggunanya (User Generated Content) yang meng-upload berbagai jenis konten berupa teks, gambar, foto, dan atau video. Selain update status, pengguna juga dapat melakukan interaksi dengan pengguna lainnya dengan memberikan komentar, like, dan follow.

Kalau Web 1.0, misalnya halaman web tentang Perusahaan, umumnya statis, kontennya disediakan ole pemilik dan diperbaharui oleh pengelolanya saja. Pengunjung web hanya membaca.

Dalam Web 2.0, pengunjung diundang untuk membuat akun sebagai pengguna dan memberikan kontribusi terhadap konten website.

Hal ini selain membuka peluang untuk berdiskusi dengan pengguna lainnya, juga dapat menimbulkan masalah spamming, cyberbullying, penistaan, fitnah, dan ujaran kebencian yang berhubungan dengan SARA (Suku, Agama dan Ras).

Media Sosial Sebagai Big Data

Kalau ditinjau dari Jumlah Penggunanya yang dapat mencapai lebih dari 1 Milyar pengguna, Media Sosial merupakan Big Data.

Lalu untuk apa Big Data tersebut? Sistem media sosial juga dirancang untuk menganalisis informasi demografis penggunanya, misalnya usia, jenis kelamin, pendidikan, pekerjaan, minat dan apa yang disukainya.

Informasi demografis pengguna ini bisa dijual kepada pemasang iklan. Kemudian pemasang iklan membelinya: memasang iklan tertarget sesuai dengan segmen profil demografis pengguna. Jadi Big Data = Uang.

Media Sosial Sebagai Habit Forming Product

Media sosial merupakan salah satu contoh produk yang membentuk kebiasaan, bahkan dapat membuat penggunanya kecanduan (Habit Forming Product).

Habit Forming Product menggunakan empat unsur:

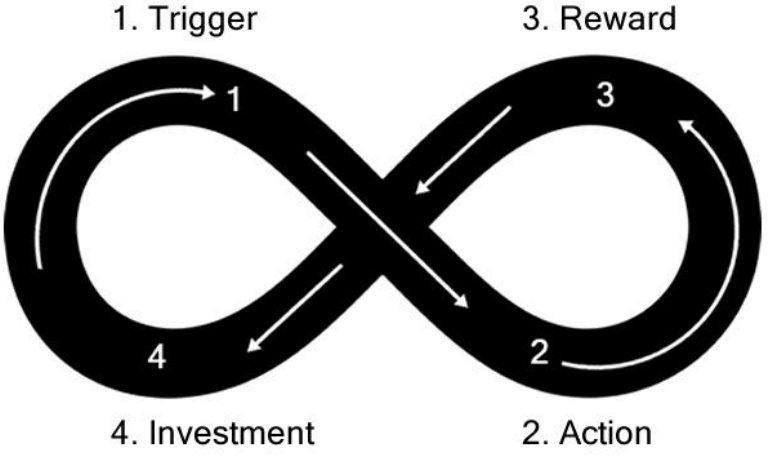
1. Trigger (pemicu). Misalnya kesepian, kebosanan, stress, dan kegelisahan (internal trigger), atau ada rangsangan dari luar berupa pesan dari media sosial, Facebook alert, Twitter notification (external trigger).

2. Action. Misalnya log in ke Facebook.

3. Reward (imbalan). Misalnya Like, komentar, atau imbalan yang tak terduga, posting anda ternyata di share, di Like dan di komentari oleh banyak orang.

4. Investment. Misalnya posting foto atau menyukai update status teman.

Investment merupakan tahap terakhir dari proses pengulangan (loop) dengan memuat trigger selanjutnya. Contoh di Instagram: Pengguna melakukan investasi dengan posting foto. Kemudian follower menyukai atau memberikan komentar atas kontribusinya. Lalu layanan instagram mengirim pemberitahuan yang akan memicu pengguna untuk melakukan proses pengulangan selanjutnya.



Behavior = motivation + ability + trigger

Salah satu unsur Habit Forming Product adalah Reward (imbalan) . Reward ini bergantung pada apa dan bagaimana konten yang kita upload, bisa berupa like, follower bertambah, hingga komentar kritikan dari hater dengan menggunakan bahasa yang kasar.

Unsur reward ini juga mendorong pengguna media sosial melakukan investasi dengan tujuan untuk membuat teman atau follower-nya terkesan.

Demi imbalan, pengguna mungkin posting foto selfie di cafe terkenal, selfie yang dapat membahayakan dirinya di bangunan tinggi, atau membuat sensasi kontroversial.

Demi mempromosikan produk dan meningkatkan follower, melakukan spam komentar di akun selebritis yang followernya ratusan ribu, atau membeli like dan follower.

Risiko Media Sosial Bagi Anak dan Remaja

Cyber Bullying

Salah satu risiko menggunakan layanan media sosial yang sering disebut-sebut adalah cyber bullying. Hal ini terjadi ketika ada pengguna yang menghina atau mengancam seseorang dalam memberikan komentar, atau melalui pesan.

Pencurian Identitas

Anak-anak yang menggunakan layanan media sosial seringkali tidak memahami bagaimana mengatur profil akunnya menjadi privat, tidak dipublikasikan kepada umum, hanya kepada teman-temannya saja. Mereka tidak menyadari risiko mengungkapkan informasi pribadi yang tidak perlu. Hal ini akan membuat mereka dengan mudah jadi korban pencurian identitas.

Foto Tidak Senonoh

Menghabiskan banyak waktu di media sosial seperti facebook, dapat membahayakan anak-anak, mereka mungkin saja kebetulan melihat foto menakutkan atau foto tidak senonoh. Hal ini akan berdampak negatif pada pikiran anak-anak atau terus teringat.

Berbagi Terlalu Banyak

Dalam kehidupan sehari-hari di dunia nyata, kita berinteraksi secara terbatas dengan beberapa teman. Tapi di media sosial kita akan cenderung berbicara terlalu banyak tentang diri sendiri. Apakah tentang apa yang sedang kita pikirkan, aktifitas yang sedang

kita lakukan, atau bahkan sedang galau. Padahal dalam kehidupan nyata, kita mungkin tidak akan melakukannya. Hal ini dapat menjadi bukti nyata dan fatal untuk hubungan kita dengan orang lain.

Online Predator

Di media sosial, orang dewasa bisa saja membuat akun dengan profil palsu untuk berteman dengan anak kecil atau remaja. Menyamar sebagai orang yang sebaya untuk merayu atau memperlihatkan foto-foto tidak senonoh. Atau untuk memperoleh informasi penting, misalnya dimana sekolah dan tempat bermain. Lalu menggunakan informasi tersebut untuk melakukan tindakan kriminal.

Implikasi Emosional

Anak-anak yang self-esteem nya rendah atau kurang percaya diri. Mungkin akan menilai keberhasilan mereka didasarkan pada berapa jumlah teman mereka di media sosial, berapa teman yang me-like postingnya, atau jika mereka dimasukan kedalam group orang-orang tertentu. Hal ini dapat membuatnya semakin kehilangan rasa percaya diri.

Kurang Ketrampilan Antar Perseorangan

Anak-anak yang menghabiskan terlalu banyak waktu di media sosial mungkin akan beranggapan hubungan sosial di dunia maya dapat menggantikan hubungan sosial di dunia nyata.

Dengan seringkali menghabiskan waktu untuk online, mereka menjadi mengabaikan pentingnya perilaku yang pantas dalam melakukan hubungan sosial kontak tatap muka di dunia nyata. Sehingga ketrampilan antar perseorangan yang diperlukan untuk keberhasilan dalam kehidupan di dunia nyata mungkin tidak berkembang sebagaimana mestinya.

Memahami Cyber Bullying

Definisi

Cyber Bullying atau **Perundungan Siber** adalah perbuatan disengaja dan berulangkali untuk menyakiti orang lain dengan menggunakan komputer, ponsel, atau alat komunikasi elektronik lainnya.

Ada unsur:

1. Disengaja. Tidak kebetulan atau tidak sengaja.
2. Berulangkali. Bullying berkaitan dengan pola perilaku.
3. Tidak diinginkan oleh korban. Menyakiti dengan mengejek, menghina, atau mempermalukan.
4. Komputer, ponsel, atau alat komunikasi elektronik lainnya. Menggunakan alat komunikasi elekronik inilah yang membedakan Cyber bullying dengan Traditional Bullying.

Catatan:

Dikutip dari
https://id.wikipedia.org/wiki/Cyberbullying

Cyber bullying dianggap valid bila pelaku dan korban berusia dibawah 18 tahun dan secara hukum belum dianggap dewasa. Bila salah satu pihak yang terlibat (atau keduanya) sudah berusia di atas 18 tahun, maka kasus yang terjadi akan dikategorikan sebagai cyber crime atau cyber stalking (sering juga disebut cyber harassment).

Catatan:

Sejak Januari 2016, Pemerintah menyarankan agar istilah bullying diganti dengan Bahasa Indonesia, yaitu **Perundungan** (berasal dari kata rundung)

http://kbbi.web.id/rundung

https://www.youtube.com/watch?v=hFEeQdvLnWw

Tapi mungkin karena lebih enak didengar, masyarakat dan bahkan media cenderung menggunakan istilah bully, misalnya: "Saya di bully hater" daripada "hater melakukan bullying kepada saya" misalnya.

Istilah **Bullying** berkaitan dengan Perilaku (Bullying behavior).

Istilah **Bully** berkaitan dengan Pelaku bullying (orang yang melakukan bullying).

Menyeragamkan pengertian istilah (apalagi istilah yang berkaitan dengan ilmu pengetahuan) perlu agar tidak terjadi kesalahpahaman atau salah kaprah.

Karateristik Cyber Bullying

Cyber bullying dapat dilakukan melalui media sosial, layanan pertukaran pesan, email, blog, website, SMS, Telephone, atau game online dengan menggunakan Komputer Desktop, Laptop, Tablet PC, dan Smartphone.

Cyber bullying dilakukan dari jarak jauh. Tidak berhadapan muka secara langsung sehingga cenderung lebih berani menyerang.

Kapan saja: sehari 24 jam, seminggu 7 hari, setahun 365 hari, dan darimana saja asal ada koneksi internet.

Pelaku dapat menggunakan identitas palsu, atau menggunakan identitas orang lain (membajak akun orang lain dan berpura-pura sebagai orang yang akunnya dibajak). Karena itulah korban sering tidak tahu siapa pelakunya dan mengapa mereka dijadikan sasaran.

Cyber bullying dapat beredar secara luas sehingga sejumlah besar orang lain dapat mengetahuinya dengan sangat cepat (menjadi Viral).

Jenis-Jenis Cyber Bullying

1. Flaming
Perselisihan online dengan menggunakan bahasa kasar, marah, dan mungkin juga menghina atau mengancam.

2. Harassment
Berungkali mengirimkan pesan dengan bahasa yang kasar, menghina, dan menyakitkan.

3. Denigration
Menyebarkan berita/cerita bohong untuk merusak reputasi dan persahabatan korban.

4. Impersonation (Peniruan)
Membajak atau membobol akun seseorang lalu mengirimkan pesan atau mem-posting sedemikian rupa agar korban yang akunnya dibajak jadi kelihatan buruk dimata teman-temanya.

Dapat berakibat merusak persahabatan, reputasi, hingga membuatnya dalam masalah atau bahaya.

5. Outing and Trickery
Memperdayai korban untuk menceritakan rahasia atau informasi memalukan, kemudian disebarkan secara online.

6. Exclusion (Pengucilan)
Mengucilkan korban dari group online.

7. Trolling
Dengan sengaja membuat pesan provokatif tentang subyek sensitif untuk menciptakan konflik, membuat orang lain tersinggung dan gusar, sehingga terjadi perkelahian online, atau bahkan berlanjut jadi perkelahian di darat.

8. Cyberstalking
Berulangkali mengirimkan pesan yang membuat korban khawatirkeselamatan dirinya.

Kenapa Orang Melakukan Cyberbullying?

Kemungkinan motivasi atau alasannya:

- Masalah personal, sosial, atau masalah keluarga.
- Pengalaman waktu kecil, termasuk cara pendidikan dalam keluarga.
- Tidak suka terhadap seseorang.
- Terpancing orang lain atau merasa gusar.
- Balas dendam atau mungkin pernah jadi korban cyberbullying.
- Butuh perrhatian atau ingin jadi perhatian.
- Self-esteem rendah (kurang percaya diri), depresi atau tidak dapat mengendalikan diri, dan kemarahan.

- Keinginan menonjolkan diri, meningkatkan popularitas dan status sosial.

- Ketidakmampuan atau ketidakmauan menghargai dan merasakan perasaan orang lain.

- Keinginan untuk merasa berkuasa dan menguasai orang lain.

- Kebosanan, sebagai bentuk hiburan, atau hanya ingin bercanda.

Target Korban

Dalam cyber bullying, sasaran korban belum tentu secara fisik kelihatan lemah dan kurang percaya diri, atau ada perbedaan kekuatan. Orang yang mempunyai predikat Ter... (tercantik, terkenal, tergemuk) juga berpotensi jadi sasaran cyber bullying.

Tanda-Tanda Korban CyberBullying

- Anak tersinggung atau marah setelah menggunakan komputer.
- Tidak tertarik lagi dengan komputer atau menghindarinya.
- Menyembunyikan sesuatu dengan menutup-nutupi layar komputer.
- Menarik diri dari teman-temannya dan dari keluarganya.

Apa yang Dapat Orang Tua Lakukan?

Katakan kepada Anak anda untuk:

- Tidak menanggapi atau membalas.
- Mem-blokir nomor Telepon, Email, dan berhenti mengikuti pelaku cyber bullying (cyber bully).
- Memberitahu orang tua atau Guru jika mengetahui hal yang tidak pantas.

Sebagai Orang tua:

- Mencari tahu sejak kapan kejadiannya dimulai.
- Ambil Screenshot layar komputer/ smartphone sebagai bukti.
- Laporkan penyalahgunaan melalui fitur laporan di website.
- Beritahu Sekolah.

Dampak terhadap korban

1. Merasa sedih, marah, frustasi , dan depresi (murung, tertekan).
2. Merasa tidak berharga, kehilangan kepercayaan terhadap diri sendiri.
3. Takut atau Malu pergi ke sekolah
4. Kesulitan belajar
5. Masalah Kesehatan akibat Psikologis
6. Pikiran untuk bunuh diri.

Dampak terhadap Pelaku

Perilaku bullying pada anak-anak (dibawah 18 Tahun) pada dasarnya dipelajari dan dapat pula tidak dipelajari.

Anak-anak yang masih labil mencari identitas diri, belajar dan dipengaruhi oleh keadaan dirumah, lingkungan disekitar tempat tinggalnya, teman-temannya, tayangan TV, Film, dan game.

Mungkin juga mereka pernah jadi korban dari tindakan kekerasan atau cara pendidikan yang salah dalam keluarga, dan mereka melakukan bullying lagi terhadap teman-temannya.

Jadi sebenarnya Anak pelaku bullying atau cyber bullying juga butuh bantuan untuk merubah perilaku negatifnya.

Kalau dibiarkan, tidak menutup kemungkinan setelah dewasa mereka akan menjadi perilaku kriminal.

Pencegahan Cyber Bullying

Cyber Bullying dan Traditional Bullying tidak akan efektif dicegah dan ditangani hanya dengan sekali-kali mengadakan kampanye anti bullying sesaat, sewaktu-waktu mengadakan seminar dan workshop, atau secara sektoral oleh sekolah saja.

Pendekatan Menyeluruh

Harus dibuat sistem pencegahan yang menyeluruh dan berkelanjutan dengan melibatkan semua pihak yang berkepentingan (Orang tua, guru, Sekolah, pelajar/anak-anak, Pemerintah, LSM, dan unsur masyarakat) yang peduli dan berkomitmen untuk menciptakan kondisi yang aman bagi anak-anak agar potensi mereka sebagai generasi penerus bangsa dapat berkembang membentuk karakter positif.

Sistem berkelanjutan ini terdiri dari:

1. Rumusan kebijakan nasional dan kebijakan di tiap-tiap sekolah dalam menghadapi masalah perilaku bullying dan cyber bullying.

2. Memahami bullying dan cyber bullying secara mendalam dan menyeluruh agar dapat melakukan intervensi secara tepat dan efektif.

3. Membuat mekanisme atau standard operating procedure dalam menangani kejadian bullying dan cyber bullying.

4. Membuat mekanisme atau standard operating procedure dalam menanggapi kejadian bullying dan cyber bullying, termasuk pemulihan korban secepatnya agar tidak menjadi trauma.

5. Membuat mekanisme upaya mengurangi atau mencegah potensi terjadinya bullying dan cyber bullying. Baik terhadap anak yang berpotensi jadi pelaku mau pun terhadap anak yang berpotensi menjadi sasaran korban.

6. Membuat mekanisme bagaimana cara atau apa saja yang harus dilakukan untuk merubah perilaku bullying dan cyber bullying, dan menggantinya dengan kegiatan-kegiatan bermanfaat untuk membentuk karakter positif.

7. Evaluasi point (1) sampai dengan (6) untuk membuat lebih baik, lebih efektif, dan disesuaikan dengan perkembangan.

Phishing

Phishing adalah upaya mengelabui target untuk mencuri informasi pribadi seperti username, password, nomor kartu kredit, dan nomor PIN. Sarana yang digunakan biasanya melalui email atau SMS tiruan yang kelihatannya resmi dari Perusahaan yang sah, misalnya seolah-olah dari Perusahaan Bank yang anda kenal.

Modus Phishing

Target phishing biasanya pengguna situs jual-beli online (marketplace), online shopping, atau internet banking yang melibatkan transaksi melalui website atau layanan telepon selular.

Phiser (Pelaku Phishing) “memancing” target melalui email. Agar tampak meyakinkan, pelaku memanfaatkan logo atau merk dagang milik lembaga resmi, seperti bank atau penerbit kartu kredit.

Kalau korban kurang teliti dan berhasil terpancing, link dalam email phishing di klik, dan korban akan diarahkan ke situs tiruan yang tampilannya dibuat menyerupai situs aslinya.

Pada situs palsu ini, korban mengetikan username dan password pada kolom form login. Informasi yang dikirimkan melalui online form akan direkam atau disimpan dalam database web server pelaku phishing.

Kemudian hacker (pelaku phishing) menggunakan username dan password tersebut untuk masuk ke akun korban.

Berikut contoh alur proses serangan phishing:

1. Anda menerima email yang kelihatannya resmi dari Perusahaan yang sah.
2. Anda mungkin diminta meng-update informasi personal untuk tujuan keamanan.
3. Karena peduli terhadap keamanan, anda klik link dalam email yang menuju ke website tiruan.

4. Anda sampai di halaman website yang tampilannya persis sama dengan yang asli.
5. Anda masukan informasi personal untuk login.
6. Hacker sekarang mendapatkan informasi yang dibutuhkannya. Pelaku dapat membajak akun anda, atau menjual informasi akun anda ke online black market.

Seperti anda lihat, proses peretasan tersebut hanya membutuhkan waktu sebentar saja.

Identifikasi Phishing Email

Dalam banyak kasus, email tiruan dari hacker ini memberitahu bahwa anda harus meng-update informasi personal untuk tujuan keamanan akun anda. Jika tidak di update, akun anda akan dihapus secara permanen. Taktik ini mungkin akan membuat anda khawatir dan tanpa pikir panjang memberikan informasi yang diminta.

Jadi hati-hati dan waspada terhadap pesan email yang mendesak respon segera dan meminta informasi password, akun Bank, atau mengancam

akan menutup akun anda jika tidak segera meng-update informasi.

Perhatikan alamat email pengirim.
Apakah masuk akal? Apakah dari orang yang anda kenal? Jika anda tidak mengenal orangnya, atau akun emailnya tidak berkaitan dengan institusi yang sah, cari dan hubungi nomor telepon resmi untuk mem-verifikasi kebenarannya. Jangan menghubungi nomor telephone yang diberikan dalam email palsu.

Teliti header email, lihat bagian reply-to, disana bisa dilihat jika kita membalas email tersebut maka akan dikirim ke alamat email yang bukan merupakan email domain situs resmi.

Cari Nama anda dalam email.
Kebanyakan serangan phishing dilakukan ke sejumlah banyak orang yang dijadikan sebagai target. Akibatnya, si hacker tidak terlalu peduli dengan personalisasi nama. Hacker hanya ingin meretas akun sebanyak mungkin yang dijadikan sasarannya.

Jadi berhati-hatilah ketika anda menerima email yang tidak menyebutkan nama lengkap anda. Misalnya: “Dear Valued Customer.” Atau “Pelanggan Yang Terhormat”

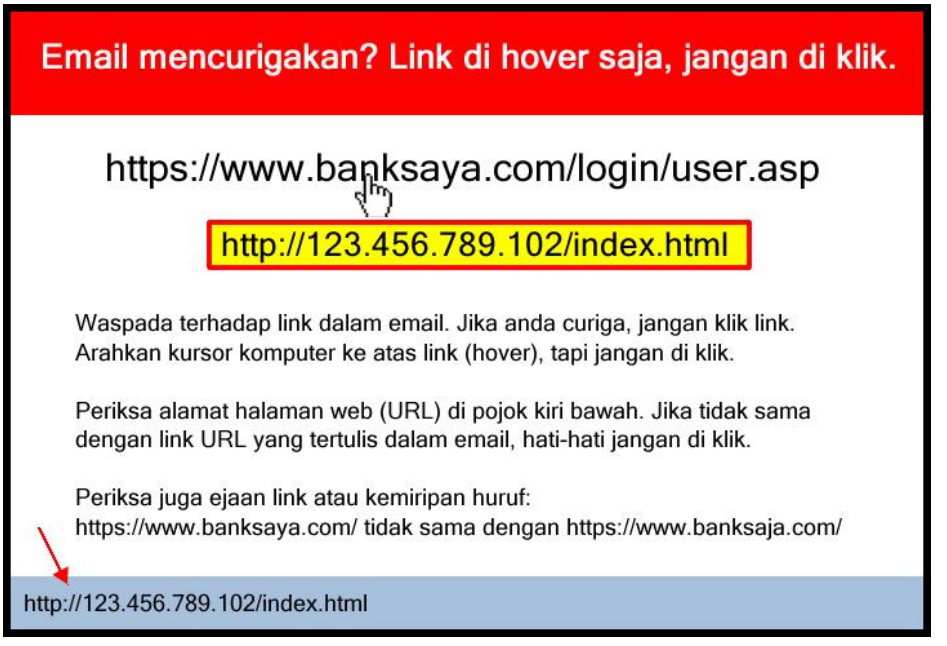
Cari kesalahan tata bahasa dalam email.
Kalau tata bahasanya tidak profesional, dan ejaannya tidak lazim, jangan klik link yang diberikan dalam email.

Arahkan kursor komputer diatas link dalam email, tapi jangan di klik. Anda akan melihat alamat link websitenya. Apakah URL nya diawali https://? Huruf ‘s’ adalah singkatan dari secure.

Website yang berhubungan dengan informasi sensitif akan diproteksi dengan menggunakan https://, sementara website yang tidak diproteksi menggunakan http://. Jika link-nya tidak sama dengan alamat website yang asli, jangan di klik.

Seringkali anchor teks atau teks link dalam email phishing ditulis benar sesuai aslinya, tapi kalau di klik akan membawa anda ke website tiruan yang

digunakan untuk mendapatkan informasi melalui formulir online.



Nama domain yang mirip juga sering digunakan hacker untuk menjebak user yang kurang berhati hati, dan kurang cermat.

Untuk lebih memahami hal tersebut, perhatikan kode HTML untuk membuat link:

Kode HTML

```
<a href="http://123.456.789.102/index.html" target="_blank">
https://www.banksaya.com/login/user.asp
</a>
```

Kode diatas oleh browser dan dalam email akan ditampilkan anchor teks nya saja yang berada diantara <a> dan sebagai link yang bisa di klik, yaitu:

https://www.banksaya.com/login/user.asp

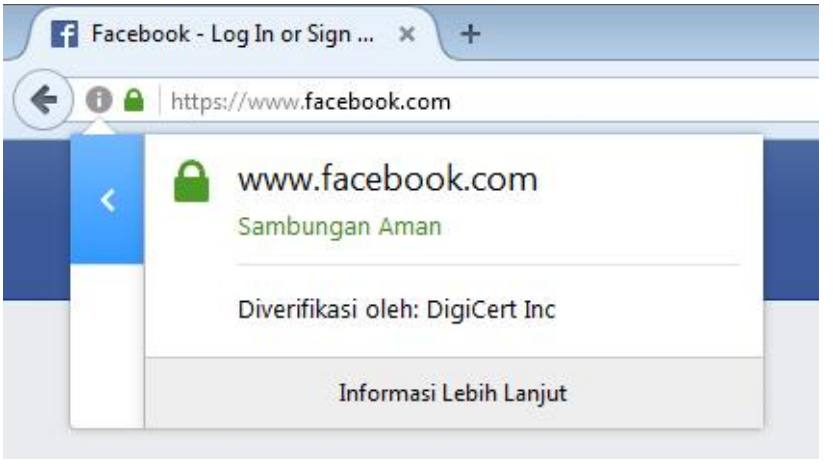
Tapi kalau link tersebut di klik, akan diarahkan ke alamat halaman web: http://123.456.789.102/index.html yang terbuka di tab baru (target="_blank")

Identifikasi Phishing Website

Jika link-nya terlanjur di klik, anda masih bisa melihat bahwa alamat atau URL website tersebut palsu. Perhatikan alamat website di pojok kiri atas browser.

Halaman website untuk login, untuk keamanan, biasanya diawali dengan https:// dan simbol kunci gembok berwarna hijau yang terkunci. Jika anda tidak melihatnya, jangan login.


Facebook - Log In or Sign ...
https://www.facebook.com
www.facebook.com
Sambungan Aman
Hak Akses
Anda belum memberikan izin khusus apa pun untuk situs ini.


Facebook - Log In or Sign ...
https://www.facebook.com
www.facebook.com
Sambungan Aman
Diverifikasi oleh: DigiCert Inc
Informasi Lebih Lanjut

Tips Menghindari Phishing

Pada dasarnya kita harus cermat dan berhati hati. Jika menerima email yang meminta username, email address, dan password, abaikan saja meskipun email tersebut terlihat sama dengan email asli dari perusahaan yang telah Anda kenal.

Jangan mudah terbuai iming-iming hadiah lewat online, apalagi mengaku-ngaku sebagai pihak terpercaya.

Jangan andalkan tautan dalam email atau dari search engine, karena tautan tersebut mungkin palsu.

Jangan menggunakan nomor telephone atau alamat email yang ditemukan dalam email phishing atau dalam website phishing. Cari dan gunakan informasi kontak yang ada pada kartu nama Bank atau kartu nama Perusahaan.

Selalu log in dengan membuka browser baru dan ketik alamat web tersebut. Awali alamat web (atau URL) dengan “https”, dan periksa simbol gembok warna hijau di pojok kiri atas browser .

Selain dalam email, phishing juga dapat ditemui pada akun media sosial dengan menggunakan foto porno menyerupai sebuah video yang memancing korban untuk mengkliknya. Karena itu cermati URL alamat website tujuannya.

Gunakan software anti virus yang asli dan selalu di-update. Software anti virus yang asli biasanya dilengkapi dengan fitur Internet Security yang dapat mendeteksi gejala kemungkinan phishing.

Jika install aplikasi baru, baca izin akses yang diminta oleh aplikasi, dan tentukan apakah anda merasa aman memberikan izin.

Jangan lupa selalu log out dari situs dimana anda memasukkan informasi pribadi.

Jika curiga komputer anda terkena virus atau malware, jangan pernah menggunakan komputer tersebut untuk melakukan transaksi online.

Untuk diketahui...
Institusi yang sah misalnya Bank tidak akan pernah meminta informasi personal dan informasi finansial melalui email atau website yang tidak diamankan dengan https://

Informasi personal dan sensitif berikut JANGAN PERNAH dibagikan melalui email:

- Nomor KTP dan atau SIM
- Password
- Nomor Kartu Kredit atau Kartu Debet
- Nomor PIN
- Nomor rekening Bank
- Nama lengkap, alamat rumah, email, dan nomor telephone yang berhubungan dengan data personal.
- Informasi catatan finansial, kesehatan, dan catatan nilai hasil pendidikan.
- Nama gadis ibu Anda
- Ulang tahun Anda

Keamanan Menggunakan Internet

Parental Control

Saat ini kita sudah memasuki era Generasi Alpha yang lahir antara Tahun 2011 – 2015. Teknologi Digital dan Teknologi Informasi sudah merambah ke segala usia.

Anak-anak, remaja, sampai orang tua lanjut usia sudah menggunakan Smartphone, Tablet, Laptop, atau Komputer Desktop yang dapat terkoneksi ke internet.

Melalui internet yang merupakan gudang informasi, segala macam informasi mulai dari informasi berguna sampai informasi sampah dan dapat membahayakan bisa dicari dan ditemukan, baik dalam bentuk teks artikel, gambar, foto, audio, atau video.

Bagi Anak-Anak yang masih rentan dan Remaja yang sedang mencari jati diri, konten atau informasi yang tidak sesuai dengan usia mereka dan dapat berdampak tidak baik bagi perkembangan mereka harus disaring dengan software yang dikenal sebagai Parental Control.

Fungsi Parental Control ini untuk menyeleksi atau menyaring situs web yang tidak aman untuk anak-anak atau remaja. Memantau dengan cara merekam aktifitas online anak; laman apa saja yang sengaja atau tidak sengaja dikunjunginya.

Juga dapat membatasi berapa lama atau disaat kapan saja mereka boleh online berdasarkan kesepakatan bersama orang tua.

Perangkat komputer, tablet, smartphone, dan beberapa game console sudah dilengkapi dengan fitur built-in parental contol.

Orang tua harus belajar cara mengaktifkan dan mengatur pembatasannya.

Berikut ini gambaran dari berbagai parental control yang tersedia.

Control Panel System Operasi Windows 7

Sistem Operasi Komputer

Microsoft Windows dan Apple Mac OS X untuk komputer sudah dilengkapi dengan built-in parental control. Setiap pengguna dapat dibuatkan User Accounts masing-masing dan harus login berdasarkan profil-nya.

Web Browser

Browser Mozilla Firefox, Google Chrome, Apple Safari, dan Internet Explorer adalah perangkat lunak yang digunakan untuk menjelajah di Internet. Masing-masing browser menawarkan cara yang berbeda dalam menyaring situs web yang Anda tidak ingin anak-anak Anda mengunjunginya.

Smartphone dan Tablet

Sistem Operasi untuk Perangkat mobile (Android dan IOS) juga dilengkapi built-in parental control. Anda dapat juga mengunduh aplikasi parental control untuk melacak dan mengendalikan aktivitas online, termasuk pesan teks dan media sosial.

Game Console
Beberapa System Video Game yang menggunakan parental control.

PlayStation 4
Xbox (console)
Xbox 360
Xbox One
Nintendo DSi

Tips Untuk Orang Tua

Parental control dan peraturan saja tidak cukup. Orang tua tetap harus melakukan komunikasi dengan anak dalam membuat pilihan terbaik.

Orang tua harus terlibat dalam kehidupan online anaknya. Bergabung dan berteman dengan anak di media sosial untuk memahami bagaimana cara kerja media sosial.

Orang tua harus mengetahui informasi batasan usia anak yang diperbolehkan untuk menggunakan layanan media sosial dan layanan pertukaran pesan.

Kalau belum cukup usia, anak-anak jangan dibiarkan membuat akun di media sosial.

Taati Batasan Usia Penggunaan Media Sosial				
13 Tahun	14 Tahun	16 Tahun	17 Tahun	18 Tahun
Twitter Facebook Instagram Snapchat Google+	Linkedin	WhatsApp	Vine	Path Youtube Flickr Wechat

Jika sudah cukup usia memiliki akun di media sosial, sedini mungkin ajarkan soal keamanan, tanggungjawab, dan cara mengaktifkan fitur privasi pada akunnya di media sosial.

Ketahui Aplikasi yang akan di-install. Periksa sebelum mengunduh aplikasi dan pelajari cara pengaturannya.

Peraturan Umum

1. Didik diri sendiri tentang internet. Kemudian ajarkan kepada anak. Meskipun tidak mempunyai komputer di rumah, Anak dapat meng-akses di sekolah, di rumah temannya, di warnet, atau melalui smartphone.

2. Jika di rumah mempunyai komputer dan akses internet, komputer sebaiknya di ruang keluarga agar dapat diawasi orang tua dan anggota keluarga lainnya.

3. Buat kesepakatan keluarga mengenai batasan waktu penggunaan internet dan smartphone.

4. Buat peraturan kesepakatan bersama dalam menjaga privasi keluarga. Ajarkan kepada Anak untuk jangan pernah memberikan informasi pribadi kepada orang yang tidak dikenal di internet. Termasuk informasi tentang anggota keluarga. Nama, alamat, umur, nomor telepon, ulang tahun, alamat email, di mana Anak sekolah, nomor kartu kredit, dan informasi pribadi lainnya, jangan pernah

diberikan kepada orang lain tanpa orang tua memeriksa terlebih dahulu.

5. Instal software original keamanan dan secara teratur di update untuk melindungi komputer dari virus, spyware dan malware.

6. Gunakan parental control untuk anak.

7. Buat dan cantumkan peraturan untuk anak dalam menggunakan internet:

- Ajarkan kepada Anak bahwa berbicara dengan orang yang tidak dikenal di internet sama dengan berbicara dengan orang tidak dikenal di jalan. Anak harus berteman di internet dengan orang yang dikenalnya dan dipercaya di dunia nyata.
- Jangan mengirim photo untuk orang lain yang tidak dikenal.
- Jangan pernah setuju untuk bertemu langsung di darat dengan orang yang hanya kenal di media sosial.

- Pikirkan dulu setiap konten (teks kalimat, foto, gambar, atau video) sebelum diposting atau disebarkan.
- Beritahu Anak Anda untuk terlebih dahulu memperlihatkan foto yang akan diposting di media sosial atau website, dan kepada siapa mereka mengirimkannya.

8. Buatlah password yang tidak mudah diterka, terdiri dari delapan karakter atau lebih dengan menggunakan kombinasi huruf besar, huruf kecil, angka, dan simbol. Jangan berbagi password dengan siapa pun (kecuali dengan orang tua).

9. Ajarkan sikap kritis terhadap kebenaran informasi di internet. Dorong perilaku tanggung jawab dan sikap kritis terhadap suatu berita. Cari tahu, tanyakan, dan pikirkan dulu sebelum menyebarkan informasi di media sosial atau melalui pertukaran pesan. Jika anak anda mempunyai email, beritahu agar berhati-hati sebelum meng-klik link dalam email.

10. Bangun reputasi digital positif. Ajarkan perilaku baik di internet. Tidak membuat status atau memberi komentar kalau sedang galau, emosi, atau marah. Dorong anak untuk bisa mengatasi masalah, misalnya menghadapi perilaku cyberbullying, kontak dengan orang yang diinginkan, atau komentar kasar. Situs apa saja yang biasa dikunjunginya, dan cara melaporkan jika ada masalah.

Tips Untuk Anak dan Remaja

Jagalah informasi personal kamu saat menggunakan internet. Nama, alamat, umur, nomor telepon, ulang tahun, alamat email, di mana kamu sekolah, dan hal-hal lain tentang informasi pribadi, jangan dibagikan dengan orang lain tanpa orang tua memeriksa terlebih dahulu.

Buatlah password yang tidak mudah diterka, terdiri dari minimal delapan karakter atau lebih dengan menggunakan kombinasi huruf besar, huruf kecil, angka, dan simbol. Jangan berbagi password dengan siapa pun (kecuali dengan orang tua).

Atur profile menjadi privat, dan periksa setiap saat untuk memastikan pengaturan tidak berubah.

Jagalah nama baik diri sendiri, nama baik keluarga, dan nama baik Sekolah atau Kampus. Jangan posting video, foto, atau teks pesan yang dapat mempermalukan diri sendiri atau mempermalukan orang lain. Kita tidak tahu siapa siapa saja yang melihat-lihat profil kita di media sosial. Tidak ada jaminan meskipun fitur privasi diaktifkan. Orang lain mungkin mengambil screenshot posting kamu dan kemudian disebarkan untuk mempermalukan kamu.

Kenali teman online kamu sebagaimana kamu mengenal teman-teman yang lainnya.

Cermati foto yang di tag oleh teman, dan hilangkan tag yang tidak relevan atau bersifat menyerang

Jangan pernah meninggalkan Smartphone tanpa pengawasan. Gunakan password untuk mencegah orang lain mengakses ponsel kamu.

Koneksi ke Internet hanya jika diperlukan saja. Matikan koneksi internet dan Wi-Fi jika tidak menggunakannya.

Hati-hati jika mengungkapkan lokasi dimana kamu sekarang sedang berada. Matikan akses lokasi.

Jangan berkomunikasi secara online dengan orang yang tidak dikenal. Jangan mengirim photo untuk orang lain yang tidak dikenal. Jangan pernah setuju untuk bertemu langsung di darat dengan orang yang hanya ngobrol dengan kamu di media sosial. Ingat bahwa orang kamu temui di internet kemungkinan tidak seperti yang kamu lihat.

Jangan pernah menanggapi komentar dan pesan email yang mengancam, tidak senonoh, cabul, atau memanas-manasi. Laporkan setiap email yang membuat kamu merasa tidak nyaman.

Hati-hati jika ada seseorang menawarkan sesuatu secara gratis.

Segera katakan kepada guru atau orang tua jika kamu menemukan informasi yang membuat kamu merasa tidak nyaman.

Pikirkan dulu setiap konten (teks kalimat, foto, gambar, atau video) sebelum diposting atau disebarkan.

Biasakanlah untuk keluar (log out) dari akun media sosial atau dari akun email setelah selesai menggunakannya.

THINK Sebelum Berbagi di Media Sosial

Truth = Apakah Benar?

Helpful/Hurt = Apakah akan Bermanfaat?

atau Apakah akan Menyakiti orang lain?

Inspiring = Apakah dapat memberikan inspirasi?

Necessary = Apakah Perlu atau Penting?

Kind = Jika diungkapkan apakah akan membawa kebaikan?

Jaga keseimbangan aktifitas. Atur waktu untuk online, tidak perlu begadang sepanjang malam atau menghabiskan sepanjang waktu di depan komputer. Internet cara yang hebat untuk berkomunikasi, tapi bukan satu-satunya cara!

Menjadi Netizen Yang Baik

Istilah Netizen berasal dari kata Internet dan Citizen (Warga). Netizen berarti “Warga Internet”, yaitu orang yang aktif terlibat dalam komunitas online atau dengan internet secara umum. Netizen kadang disebut juga sebagai Cybercitizens (Warga siber).

Internet menciptakan dunia baru, dan budaya baru. Menawarkan berbagai kemungkinan perubahan sosial. Netizen yang berpengalaman mempunyai tanggung jawab agar internet digunakan secara konstruktif. Mengembangkan kebebasan bicara dan akses terbuka bagi siapa saja.

Internet dapat diakses oleh siapa saja, kapan saja, dan dimana saja: sehari 24 jam, setahun 365 hari, asal ada koneksi internet.

Sebagai warganya, netizen harus mempunyai harapan tentang sekumpulan peraturan perilaku yang pantas ketika berinteraksi dengan warga online lainnya, yang disebut sebagai Netiquette.

Netiquette

Istilah Netiquette berasal dari kata Network (jaringan, dalam hal ini jaringan internet) dan Etiquette (Etiket). Etiket berarti tata cara atau tata krama yang diperlukan dalam kehidupan sosial. Jadi Netiquette adalah sekumpulan peraturan bagaimana berperilaku baik ketika sedang berinternet di wilayah baru yang disebut cyberspace.

Ketika seseorang masuk kedalam wilayah baru dan memiliki budaya tersendiri, kemungkinan besar orang tersebut melakukan kesalahan. Mungkin membuat orang lain terganggu atau tersinggung, tapi tidak bermaksud atau disengaja. Mungkin juga orang baru tersebut salah paham terhadap apa yang dikatakan oleh orang lain.

Ketika sedang berada di ranah siber, dikarenakan sebagian dari kita lupa bahwa orang lain yang sedang online adalah manusia juga, dan sebagaian karena ada yang tidak tahu kaidah berinternet, terutama yang masih baru (newbie), maka terjadilah berbagai bentuk kesalahan.

Karena itulah, terutama bagi yang masih baru, perlu belajar Netiquette untuk mengurangi berbuat kesalahan, dan bagi yang sudah berpengalaman agar membantu mengajarkan kepada yang masih baru.

Di wilayah baru ini, lebih baik kita menambah pertemanan daripada kita mempunyai musuh atau bermusuhan.

Peraturan 1: Ingat Manusia
Bayangkan kalau kamu berada dalam situasi dan posisi sebagai orang lain. Dapat memahami apa yang dipikirkannya, dan merasakan apa yang sedang dirasakannya. Dalam psikologi, hal ini dikenal sebagai empaty. Di internet, netizen harus **Ingat Manusia**: ada orang lain disana.

Ketika seseorang berkomunikasi menyampaikan pesan teks melalui komputer, yang dilihatnya adalah tulisan di layar komputer. Hanya kata kata saja, tidak bisa menggunakan ekspresi wajah, gesture, dan nada suara dalam menyampaikan pesan. Mungkin dapat menambahkan emoticons senyuman dan tanda seru, tapi ekspresi wajahnya sebenarnya datar-datar saja.

Karena itu, kualitas komunikasi melalui medium alat elektronik jadi kurang personal. Tapi karena menggunakan alat elektronik hal tersebut biasanya bisa diterima atau dimaklum.

Dalam Netiquette, hal tersebut tidak bisa diterima. Kita harus ingat manusia: Disana ada orang nyata yang akan menerima pesan dan membacanya.

Peraturan 2: Pikirkan Sebelum Berbagi

Jangan tergesa-gesa membalas email, memberikan komentar, atau update status di media sosial. Ambil waktu untuk membacanya lagi, dan pikirkan tentang cara terbaik untuk merespon atau menyampaikan pendapat. Kata-kata berpengaruh kuat dan dapat ditafsirkan dengan cara yang berbeda dari yang apa yang dimaksud. Sampaikan ide sesederhana dan sejelas mungkin, dengan cara yang pantas dan sopan.

Jika membuat pesan teks, memberikan komentar, atau update status di media sosial, sebelum dikirimkan, tanya kepada diri sendiri:

“Apakah kamu mau mengatakan pesan tersebut secara langsung di depan umum atau langsung berhahadapan muka dengan orang yang akan menerima pesan?

Jika jawabannya tidak, tulis ulang dan baca ulang. Ulangi proses tersebut hingga merasa nyaman jika mengatakannya secara langsung dihadapan orang lain sebagaimana kamu mengirimkannya secara online.

Pikirkan juga bagaimana jika ada orang lain yang menangkap layar pesan kamu sebagai alat bukti yang akan mempermalukan kamu sendiri atau menimbulkan masalah hukum? Sekarang atau mungkin bertahun-tahun kemudian?

Alasan lain untuk tidak menyerang dengan kata-kata yang menyakitkan atau menghina secara online adalah perkataan kamu tertulis.

Pesan tertulis yang kamu kirim mungkin disebarkan oleh yang menerimanya atau oleh orang lain yang melihatnya, atau diambil screen capture-nya sebagai alat bukti.

Dalam situasi demikian, kamu tidak punya kontrol, dan kelak, mungkin bisa saja akan jadi masalah buat kamu.

Peraturan 3: Taati Standar Perilaku yang sama dengan Perilaku kehidupan di dunia nyata.

Di internet orang bisa menjadi anonymous (tidak diketahui siapa sebenarnya). Menyembunyikan identitas yang sebenarnya. Membajak akun orang lain dan menyamar sebagai orang yang akunnya dibajak. Menggunakan proxy lain atau membajak web server A, lalu dari web server A, menyerang ke web server B, sehingga B mengira A yang melakukan penyerangan.

Mungkin karena itu, sebagian orang jadi berpikir, peluang untuk diketahui, kemungkinannya kecil. Atau mungkin karena orang kadang lupa dengan peraturan yang pertama, sehingga mengabaikan etika dan berpikir bahwa di internet perilaku buruk bisa diterima.

Taati standar perilaku yang sama dengan perilaku kehidupan di dunia nyata. Hormati diri sendiri. Hormati orang lain. Ingat Manusia, ingat ada orang lain di internet.

Meskipun kamu tidak secara langsung bertatap muka, tapi kamu berkomunikasi dengan orang lain yang memiliki perasaan dan patut menerima dihormati sebagaimana kamu juga.

Jika kamu sudah dewasa, jujurlah katakan yang sebenarnya dalam profil di media sosial, tidak ada gunanya berbohong tentang diri sendiri dan kepada orang lain dengan membuat rumor.

Jika kamu ingin menggunakan informasi, dokumen, download gambar atau foto.... periksa hak kekayaan intelektual, etika dalam mengutip, dan menyebutkan sumbernya.

Jangan lupa juga bahwa kamu tidak sendirian di internet. Kamu mungkin tidak terlibat langsung, tapi mungkin berada dalam situasi dimana kamu mengetahui seseorang atau sesuatu yang salah, maka kamu harus mengingatkan.

Peraturan 4: Ketahui sedang dimana berada.
Netiquette berbeda-beda antara satu website dengan website lain. Apa yang dapat diterima di forum online A, mungkin di forum lain dianggap sebagai sesuatu yang sangat kasar. Karena itu, sangat penting mengetahui dimana kita sedang berada.

Kenali dan hormati perbedaan. Pikirkan bahwa ketika mengunakan diskusi online, kita berinteraksi dengan orang dari daerah dengan budaya yang berbeda, mempunyai latar pendidikan yang berbeda, dan kemampuan meng-ekspresikan dirinya dalam bahasa mungkin berbeda di lingkungan online.

Peraturan 5: Bangun Reputasi Baik.
Kualitas tulisan, komentar, dan foto yang di tag oleh teman, sangat penting dan mencerminkan siapa diri kita sendiri.

Karena itu, baca ulang apa yang ditulis, periksa ejaan, tata bahasa, dan tanda baca untuk mencegah salah komunikasi atau salah tafsir. Jangan menulis dengan huruf besar semua karena dapat menimbulkan kesan BERTERIAK.

Kalau menulis tentang sesuatu, pastikan tahu apa yang dibicarakan, periksa kebenaran faktanya sebelum diterbitkan atau dikirim. Berita atau informasi buruk dapat menjalar ke sejumlah besar orang dengan cepat dan menjadi viral di internet.

Peraturan 6: Berbagi Keahlian dan Pengetahuan
Kalau punya minat besar terhadap sesuatu dan banyak mengetahui tentang sesuatu, jangan ragu-ragu untuk berbagi pengetahuan dan keahlian dengan orang lain yang bertanya atau punya minat yang sama.

Selain berbagi pengetahuan, ingat bahwa kamu juga dapat membantu dan mengajarkan kepada orang lain untuk menjadi netizen yang baik.

Peraturan 7: Bantu mengendalikan perselisihan.
Perdebatan seru di forum diskusi atau di media sosial dapat menyenangkan untuk dibaca dan diberi komentar.

Tapi Netiquette melarang perang atau perselisihan online di media sosial atau di forum diskusi secara terus-menerus, umumnya didominasi oleh dua atau

tiga orang saja yang berapi-api saling serang dengan tulisan kemarahan. Hal ini tidak adil bagi anggota lainnya didalam group.

Bantulah untuk mengendalikan kemarahan dan meredakan suasana. Jagalah kedamaian. Jangan membuat perselisihan dengan saling menghina. Jadilah teman baik di internet, jangan jadi cyberbully.

Peraturan 8: Hormati Privasi Orang Lain
Jangan terlalu banyak berbagi informasi yang terlalu personal, atau menanggapi pertanyaan personal. Hargai privasi diri sendiri dan privasi orang lain.

Peraturan 9: Jangan Menyalahgunakan Kekuasaan.
Sebagain orang mempunyai kelebihan daripada yang lain, entah itu berupa kepandaian dalam bidang tertentu, popularitas, harta, jabatan, atau status sosial sebagai anak pejabat.

Mempunyai kelebihan dan mengetahui lebih banyak daripada orang lain, atau mempunyai kekuasaan daripada apa yang dapat orang lain kerjakan, tidak berarti memberi kita hak untuk kepentingan diri sendiri, mengambil keuntungan sebanyak mungkin dari orang lain.

Peraturan 10: Pemaaf

Setiap orang pernah jadi newbie atau pemula. Jadi kalau ada seseorang melakukan kesalahan sepele, bersikaplah baik. Hindari asumsi dan penilaian terburu-buru. Maafkan kesalahan sepele, dan minta maaf kalau membuat kesalahan.

Jika memutuskan untuk memberitahu kesalahan seseorang, beritahulah dengan sopan dan sampaikan melalui pesan privat. Jangan pernah sombong atau merasa benar sendiri.

Rujukan

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)
Penetrasi & Perilaku Pengguna Internet Indonesia 2016
Diunduh Desember 2016 dari
https://www.apjii.or.id/

Sonia Livingstone and Leslie Haddon
Coordinator, EU Kids Online
The London School of Economics
and Political Science
EU Kids Online: Final Report
Retrieved January 31, 2017, from
http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf

Dr. Ann E. Barron.
Co-author: Dr. Frank Breit, David Tai, David Hoffman, Karen Ivers, Lorraine Sherry. Florida Center for Instructional Technology
College of Education,University of South Florida,
The Internet:Ideas, Activities, and Resources
Retrieved January 30, 2017, from
http://fcit.usf.edu/internet/
http://fcit.usf.edu//internet/internet.pdf

UK Council For Child Internet Safety. Advice on child internet safety 1.0
Retrieved January 29, 2017, from
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251455/advice_on_child_internet_safety.pdf

Greg Writer. Children's Educational Network.
A Family Guide to Internet Safety
Retrieved January 29, 2017, from
http://web.richmond.k12.va.us/Portals/0/assets/Parents/pdfs/kidsafe_safetyguide.pdf

McAfee. McAfee's 10 Step Internet Safety Plan For Your Family
Retrieved January 29, 2017, from
https://promos.mcafee.com/en-us/pdf/mcafeeinternetsafetyplan.pdf

Ruth Johnson.ProtectMiChild.com
Internet Safety. A Guide for Teachers and Parents
Retrieved January 29, 2017, from
https://www.protectmichild.com/cybertips/cybertips.pdf

Internet Sehat. Digital Literasi
Retrieved January 29, 2017, from
http://internetsehat.id/literasi/

Childnet International.
Online Reputation Checklist
Retrieved January 29, 2017, from
http://www.childnet.com/ufiles/Online%20Reputation%20Checklist.pdf

Dr Serena Tung
Child Developmental Unit Natonal University Hospital
Media Use and its Developmental Effects
Retrieved January 29, 2017, from
https://www.nuh.com.sg/wbn/slot/news/ah01/3eb6db36f_u1661.pdf

Penelope Sweetser,Daniel Johnson,Anne Ozdowska,Peta Wyeth
Queensland University of Technology
Active versus Passive Screen Time for Young Children
Retrieved January 29, 2017, from
http://www.ledevoir.com/documents/pdf/screen_time.pdf

Queensland Government. Departement of Education and Training.
Tip Sheet for Parents. Screen time and children
Retrieved January 29, 2017, from
http://deta.qld.gov.au/earlychildhood/pdfs/tip-sheets/pts-screen-time-and-children.pdf

Learning Works for Kids.
A Parent’s Guide to Screen Time
Retrieved January 29, 2017, from
http://learningworksforkids.com/wpcontent/uploads/ParentGuideScreenTime.pdf

Bernard Marr.
How Big Data Can Help You Make Sense of Social Media.
Retrieved January 29, 2017, from
http://data-informed.com/how-big-data-can-help-you-make-sense-of-social-media/

Harini Santhosh.
6 Positive And 4 Negative Effects Of Social Media On Children.
Retrieved January 29, 2017, from
http://www.momjunction.com/articles/negative-effects-of-social-media-on-children_00353633/

Children’s Online Privacy. Questions and Answers
Retrieved January 29, 2017, from
http://www.gov.pe.ca/photos/original/oipc_copqa.pdf

Online Privacy | A Tutorial for Parents and Teachers
Retrieved January 29, 2017, from
https://www.symantec.com/content/en/us/home_homeoffice/media/theme/familyresource/OnlinePrivacyBrochure_FF_6-20.pdf

Children's Online Privacy. How to Help Preserve Your Child's Confidential Information
Retrieved January 29, 2017, from
https://www.dioceseofbmt.org/wp-content/uploads/2015/05/ParentTraining86.pdf

The Protection of Children Online. Recommendation of the OECD Council Report on risks faced by children online and policies to protect them
Retrieved January 29, 2017, from
https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf

Protecting Children's Privacy Online – A Guide for Parents, Carers and Educators
https://www.comparitech.com/blog/vpn-privacy/protecting-childrens-privacy/

Ten privacy tips for parents and carers
Retrieved January 29, 2017, from
https://www.oaic.gov.au/resources/individuals/privacy-fact-sheets/general/ten-privacy-tips-for-parents-and-carers.pdf

Nancy Willard, M.S.,J.D.
Educator's Guide to Cyberbullying and Cyberthreats
Retrieved January 29, 2017, from
https://education.ohio.gov/getattachment/Topics/Other-Resources/School-Safety/Safe-and-Supportive-Learning/Anti-Harassment-Intimidation-and-Bullying-Resource/Educator-s-Guide-Cyber-Safety.pdf.aspx

Dr. Michele Borba, Ed.D,
The Essential 6 R's of Bullying Prevention
Retrieved January 30, 2017, from
http://info.character.org/blog/bid/163381/Michele-Borba-s-Essential-6-R-s-of-Bullying-Prevention
http://www.micheleborba.com/Borba-6_Rs_To_Bullyproof.pdf

Juderson Jean-Baptiste
MTE Explains: How Email Phishing Works and Why Clicking That Unknown Link Can Be A Dangerous Act.
Retrieved January 29, 2017, from
https://www.maketecheasier.com/how-email-phising-works/

David Bisson
6 Common Phishing Attacks and How to Protect Against Them
Retrieved January 29, 2017, from
https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

The Truth About Clicking Links in Email and What To Do Instead
Retrieved January 29, 2017, from
https://tiptopsecurity.com/the-truth-about-clicking-links-in-email-and-what-to-do-instead/

Michigan State University. Secureit.
Phising
Retrieved January 29, 2017, from
https://secureit.msu.edu/phishing/

Pengertian Phising , Cara Mengenali dan Terhindar dari Phising
Retrieved January 29, 2017, from
http://www.meretas.com/pengertian-phising/

4 Simple Steps to Protect Yourself from Phishing
Retrieved January 29, 2017, from
http://techtalk.pcpitstop.com/2013/05/06/dont-click-that-unknown-email-link/

Virginia Shea . The Core Rules of Netiquette
Retrieved January 29, 2017, from
http://www.albion.com/netiquette/corerules.html

https://en.wikipedia.org/wiki/Privacy
https://en.wikipedia.org/wiki/Internet_privacy
https://id.wikipedia.org/wiki/Kerahasiaan_pribadi
https://en.wikipedia.org/wiki/Web_2.0
https://en.wikipedia.org/wiki/User-generated_content
https://en.wikipedia.org/wiki/World_Wide_Web
https://en.wikipedia.org/wiki/Internet
https://en.wikipedia.org/wiki/Big_data
https://id.wikipedia.org/wiki/Cyberbullying
https://en.wikipedia.org/wiki/Online_predator
https://en.wikipedia.org/wiki/Parental_controls
https://en.wikipedia.org/wiki/Internet_safety
https://id.wikipedia.org/wiki/Pengelabuan
https://id.wikipedia.org/wiki/Media_sosial

LAMPIRAN

Daftar Istilah di Internet dan Pengertiannya

HTTP (Hypertext Transfer Protocol)

HTTPS (Hypertext Transfer Protocol Secure)
HTTPS menjamin keamanan data yang dikirimkan, berbeda jika hanya menggunakan protocol HTTP biasa. HTTPS menggunakan SSL (Secure Socket Layer), dan TLS (Transport Layer Security).

Hypertext
Teks Hyper yang maksudnya adalah sebuah teks yang berkaitan dengan dokumen lainnya

IP Address
Internet Protocol Address, berfungsi sebagai identitas perangkat yang mengakses jaringan.

ISP (Internet Service Provider)
Perusahaan yang menyediakan layanan koneksi akses internet untuk penggunanya. Penyelenggara jasa internet

Link
Tautan, pranala.

Offline
Luring (luar jaringan), tidak terhubung, terputus
Keadaan seorang pengguna atau komputer itu sendiri ketika tidak terhubung ke internet.

Online
Daring (dalam jaringan), terhubung, tersambung.
Keadaan seorang pengguna atau komputer itu sendiri ketika sedang terhubung ke internet (kebalikan offline).

Password
Kata kunci yang umumnya berupa kombinasi huruf, angka atau simbol dan bersifat rahasia untuk mengamankan suatu informasi pribadi seperti akun di internet.

Spam
Pesan komersial atau iklan yang ditujukan kepada penerima (umumnya di e-mail) namun sebenarnya pengguna tidak menginginkan pesan tersebut masuk.

SSL (Secure Socket Layer)
Teknologi keamanan yang memungkinkan untuk dilakukan enkripsi pada data yang akan ditransmisikan antara server dan client.

Upload
unggah, muat naik. Kegiatan yang dilakukan untuk mengunggah/mengirim data berupa file, dokumen, foto, video atau audio dari komputer pribadi ke internet.

URL (Uniform Resource Locator)
Sistem yang digunakan untuk mengidentifikasi alamat website, contoh: http://www.google.com

Website (Situs)
Kumpulan halaman web yang digunakan untuk menampilkan informasi teks, gambar, animasi, suara, atau video, baik bersifat statis maupun dinamis, membentuk suatu rangkaian halaman web yang saling terkait dihubungkan dengan berbagai link.

Wi-Fi (Wirelles Fidelity)
Bentuk transfer data untuk mengakses internet yang dilakukan secara nirkabel (tanpa kabel).

Tentang Anti Bullying Indonesia

Indonesian anti bullying didirikan Desember 2009 oleh Tisna Rudi dengan membuat blog tentang bullying di WordPres. https://bigloveadagio.wordpress.com/

Tahun 2015 membuat website antibullyingindonesia.org Awal Tahun 2017 nama domain tersebut tidak diperpanjang, dan konten websitenya dipindahkan ke

Anti Perundungan

Media Sosial

Facebook Group Indonesian Anti Bullying

Facebook Page Indonesian anti Bullying

Google Plus

Twitter | Anti Perundungan

Kontak:
Tisna Rudi
bandunglokalbisnis@gmail.com