Yayasan LKiS

HANDBOOK DIGITAL SAFETY

Disusun Oleh: Ayik Teteki, Bambang Muryanto & Gilang Adikara

HANDBOOK
DIGITAL SAFETY

Ayik Teteki, Bambang Muryanto & Gilang Adikara

Yayasan LKiS

2023

HANDBOOK DIGITAL SAFETY

Yayasan LKiS 2023
Penulis: Ayik Teteki, Bambang Muryanto & Gilang Adikara
Sampul: Akhmad Luthfi Aziz
Ilustrasi & Penata isi:

Cetakan Pertama, Agustus 2023
v + 66 Halaman
14.8 x 21 cm

Diterbitkan Oleh Yayasan LKiS
Alamat: Jalan Pura 203 Sorowajan Banguntapan Bantul
Daerah Istimewa Yogyakarta 55198

Yayasan LKiS
Yayasanlkis@yahoo.com atau lkisjogja@gmail.com

KATA PENGANTAR

Laporan Situasi Hak-Hak Digital 2022 yang dirilis oleh SAFEnet selama tahun 2022, terjadi insiden keamanan digital sebanyak 302 kali. Artinya, rata-rata terjadi lebih dari 25 insiden tiap bulan. Angka tersebut meningkat dibandingkan dua tahun sebelumnya yaitu 147 insiden (2020) dan 193 insiden (2021) atau naik sekitar 54 persen dibandingkan tahun sebelumnya. Hal ini juga menunjukkan bahwa selama tiga tahun insiden keamanan digital di Indonesia terus meningkat.

Kelompok kritis seperti aktivis, jurnalis, pekerja media, dan organisasi masyarakat sipil merupakan kelompok yang paling banyak mengalami serangan digital, hampir 50 persen dari total jumlah korban serangan. Korban serangan digital selama 2022 paling banyak terjadi pada lembaga publik (62), staf organisasi masyarakat sipil dan aktivis (55), jurnalis dan pekerja media (50), mahasiswa dan pelajar (37), serta organisasi masyarakat sipil (23). Banyaknya lembaga publik yang menjadi korban itu terkait dengan banyaknya kebocoran data sekaligus menunjukkan betapa lemahnya pertahanan siber di negeri ini.

Pertengahan tahun 2022 lalu Yayasan LKiS memberikan sentuhan baru dengan mengajak para pelaku aktivis media terutama admin media sosial untuk membangun admin kolaborasi media sosial yang terdiri dari berbagai komunitas, lembaga dan jaringan untuk memproduksi dan menyebarkan kampanye isu masing-masing komunitas, lembaga dan jaringan untuk dapat dikampanyekan bersama dan menjadi isu bersama.

Namun sayangnya belum semua admin media memiliki bekal untuk melakukan mitigasi terkait dengan keamanan digital. Ketika akun direntas dan hilang baru melakukan upaya pengembalian akun hasilnya nyaris tidak kembali. Apalagi ketika membangun narasi kampanye media yang sensitif. Untuk itu Yayasan LKiS mencoba mengajak pengiat media (Dwitasari/Ayik Teteki), akademisi (Gilang Adikara), dan jurnalis (Bambang Muryanto) untuk menuliskan tentang buku saku Digital Safety yang akan diperuntukkan untuk admin media sosial.

Harapannya, buku Saku ini dapat digunakan oleh komunitas maupun lembaga untuk menjaga keamanan digital sertamemitigasi kejahatan digital yang sewaktu-waktu jika diserang oleh oknum yang tidak bertanggung jawab, bisa mengetahui langkah-langkah apa saja yang perlu ditempuh dalam mengamankan media sosial organisasi maupun pribadi.

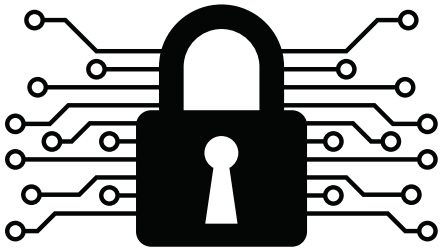
Buku ini membahas tentang keamanan digital dan prinsip-prinsip keamanan digital, pentingnya kesadaran soal keamanan digital, Q&A seputar keamanan digital dan sedikit membahas tentang keamanan digital untuk kelompok rentan dan etika digital (berkaitan dengan mengolah teks dan konten) agar tidak terjerat UU ITE.

Kami berterima kasih kepada Yayasan Keadilan Perdamaian Indonesia dan semua pihak atas dukungan, apresiasi serta sambutannya sehingga buku ini dapat sampai di tangan para pembaca.

SELAMAT MEMBACA!

DAFTAR ISI

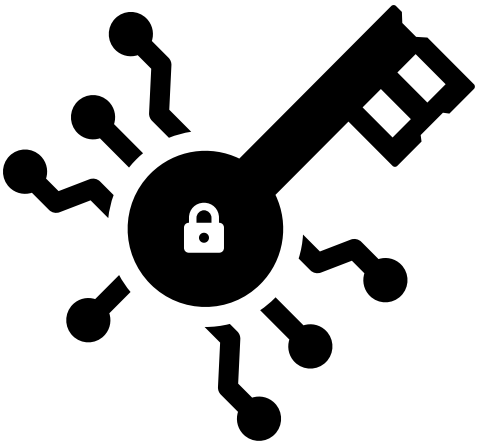
BAB PERTAMA



KEAMANAN DIGITAL DAN PRINSIP-PRINSIP KEAMANAN DIGITAL

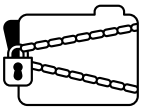
Keamanan digital telah menjadi isu yang semakin penting di era teknologi informasi dan komunikasi yang telah memberikan banyak manfaat bagi masyarakat. Akan tetapi teknologi baru ini juga memperkenalkan risiko baru. Ancaman keamanan digital dapat berupa serangan malware, peretasan, virus komputer, phishing, pencurian data, dan banyak lagi. Ancaman semakin kompleks dan sering kali mengakibatkan dampak yang merugikan, baik bagi individu maupun organisasi, baik secara materiil maupun psikologis.

Berangkat dari situasi ancaman digital tersebut, maka penting untuk membekali pengguna internet dan media sosial untuk melindungi informasi, data, perangkat dan infrastruktur digital dari ancaman, serangan dan kejahatan di melalui teknologi digital. Ini mencakup segala hal yang terkait dengan keamanan komputer, jaringan komputer, sistem operasi, aplikasi dan data yang disimpan dalam lingkungan digital.



Prinsip-prinsip keamanan digital adalah panduan atau pedoman yang digunakan untuk memastikan keamanan sistem, data dan infrastruktur digital. Prinsip-prinsip ini membantu dalam melindungi informasi sensitif dari akses yang tidak sah, menjaga integritas data dan memastikan ketersediaan layanan yang kritis. Berikut ini adalah beberapa prinsip utama keamanan Digital:

PRINSIP-PRINSIP KEAMANAN DIGITAL



Kerahasiaan
(Confidentiality)

Prinsip kerahasiaan berfokus pada perlindungan informasi agar hanya dapat diakses oleh pihak yang berwenang. Prinsip kerahasiaan memastikan bahwa data sensitif tetap terlindungi dari akses yang tidak sah atau pengungkapan yang tidak diinginkan.

Integritas
(*Integrity*)

Prinsip integritas menjamin bahwa data dan informasi tetap utuh, tidak diubah atau dimanipulasi secara tidak sah. Prinsip integritas memastikan bahwa data tidak terpengaruh oleh perubahan yang tidak sah atau kehilangan integritasnya.

Ketersediaan
(*Availability*)

Prinsip ketersediaan menekankan pentingnya memastikan bahwa sistem, data dan sumber daya terkait tersedia ketika dibutuhkan. Prinsip ketersediaan memastikan bahwa layanan tetap dapat diakses dan digunakan oleh pengguna dengan minimal gangguan.

Keaslian
(*Authenticity*)

Prinsip keaslian berfokus pada memverifikasi identitas dan keaslian entitas yang terlibat dalam transaksi atau komunikasi digital. Metode otentikasi seperti penggunaan kata sandi, kunci publik/privat atau sertifikat digital digunakan untuk memastikan bahwa entitas yang berpartisipasi adalah yang mereka klaim menjadi. Prinsip keaslian mencegah serangan pengguna palsu atau penggunaan identitas yang tidak sah.

Kontrol Akses
(*Access Control*)

Prinsip kontrol akses berarti akses data atau sistem jaringan hanya diberikan kepada orang tertentu, hanya diberikan terbatas kepada beberapa orang dengan role atau departemen tertentu dalam suatu organisasi. Orang yang tidak diberi akses tidak dapat melihatnya, apalagi pihak eksternal organisasi.

Kebutuhan Paling Sedikit
(*Least Privilege*)

Prinsip ini menyatakan bahwa setiap entitas harus diberikan hak akses minimal yang diperlukan untuk menjalankan tugas atau fungsi mereka. Hal ini membantu mencegah penyalahgunaan atau akses yang tidak sah, karena setiap entitas hanya memiliki hak akses yang dibutuhkan secara spesifik.

Pertahanan Dalam Kedalaman
(*Defense in Depth*)

Prinsip ini melibatkan penggunaan serangkaian lapisan pertahanan dan kontrol keamanan untuk melindungi sistem dan data. Ini mencakup penggunaan firewall, deteksi serangan, enkripsi, pembaruan perangkat lunak dan kebijakan keamanan yang komprehensif. Prinsip pertahanan dalam kedalaman memastikan bahwa jika satu lapisan pertahanan gagal, masih ada lapisan lain yang melindungi sistem.

Prinsip-prinsip keamanan digital ini saling berkaitan dan saling mendukung untuk menciptakan lingkungan digital yang aman dan terlindungi. Dengan menerapkan prinsip-prinsip ini, organisasi dan individu dapat mengurangi risiko serangan dan melindungi informasi mereka dengan lebih efektif.

BAB KEDUA

PENTINGNYA ADMIN MEDSOS MENYADARI KEAMANAN DIGITAL

SEBERAPA RENTAN MEDSOS KITA?

Berdasarkan riset literasi digital yang dilakukan Kementerian Komunikasi dan Informatika, aspek keamanan digital adalah aspek terendah dari empat kelompok literasi digital lain seperti kecakapan digital, etika, dan budaya digital. Data indeks literasi digital menunjukkan pada 2022 indeks kecakapan bidang keamanan digital hanya 3,12. Naik 0,02 dari tahun sebelumnya. Hal ini mengindikasikan masyarakat Indonesia masih menjadi sasaran yang empuk bagi para penjahat di dunia digital.

Survei itu juga menunjukkan bahwa masyarakat Indonesia sudah cukup memahami pentingnya mengganti password. Namun warganet di Indonesia masih kesulitan membedakan mana konten spam, phishing, atau aplikasi bersifat malware. Padahal tiga hal ini adalah strategi yang paling umum dipakai oleh para peretas untuk membobol akun media sosial dan akun email kita.

Spam adalah menyebarkan pesan secara massif dan terus menerus. Biasanya spamming dilakukan dengan menyebarkan malware atau tautan phishing. Phishing adalah taktik membuat laman palsu yang membuat orang tanpa sadar memasukkan informasi akun dan pengguna. Pernah bermain sebuah permainan di medsos lalu mendadak diminta memasukkan nama pengguna dan sandi? Berhati-hatilah, bisa jadi itu adalah laman phishing yang dibuat untuk menangkap informasi pribadi kita.

Malware adalah perangkat lunak jahat yang disamarkan dengan berbagai cara. Untuk pengguna ponsel Android, Malware biasanya ditemui melalui aplikasi ilegal atau dikirimkan melalui aplikasi pesan dengan nama file yang tidak mencurigakan, seperti undangan nikah atau resi paket. Berhati-hatilah jika ada file semacam ini.

Pada akhirnya berbagai metode peretasan akun akan terus berkembang. Namun jika kita memahami konsep dasarnya, kita akan jauh lebih sulit menjadi korban peretasan. Mari kita simak!

MENGAMANKAN AKUN MEDSOS

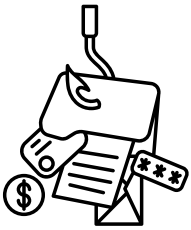
Akun media sosial memiliki nilai. Jumlah follower atau data pribadi di dalamnya bisa dikonversi menjadi keuntungan. Oleh karena itu akan selalu ada orang yang berusaha menguasai akun medsos orang lain dengan berbagai tujuan. Baik untuk melakukan pemerasan, penipuan, maupun memperjualbelikan akun yang berhasil diambil alih.

Untuk mampu melaksanakan aksinya, para peretas memiliki berbagai strategi. Kita perlu memahami berbagai strategi berikut agar kita tahu bagaimana cara kita mengamankan akun digital kita:

Metode B*rute Force*/Paksaan:

Hacker dapat mencoba menebak kata sandi akun media sosial dengan menggunakan metode brute force dengan mencoba semua kombinasi yang memungkinkan dipilih sebagai password atau dengan memanfaatkan beragam informasi pribadi yang dapat ditemukan secara publik, seperti tanggal lahir atau nama anggota keluarga. Untuk melakukan ini, hacker biasanya memanfaatkan mesin untuk menginput data secara otomatis.

Metode *Phishing*/Pengelabuan:



Hacker dapat mencoba memperoleh data login pengguna, termasuk nama pengguna dan kata sandi, melalui serangan *phishing* atau serangan malware yang dirancang untuk mengelabuhi dengan tujuan mencuri informasi login. *Phishing* ialah strategi membuat halaman login palsu yang membuat korban lengah dan tanpa sadar memasukkan informasi username dan password mereka di sana.

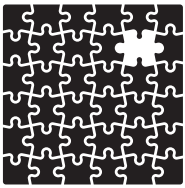
Metode Keylogging:

Keylogging adalah metode di mana hacker menggunakan perangkat lunak yang secara diam-diam mengambil catatan semua kunci yang ditekan oleh pengguna pada keyboard mereka. Perangkat semacam ini kita kenal dengan sebutan Malware. Dengan cara ini, hacker dapat mencatat kata sandi yang dimasukkan oleh pengguna dan mendapatkan akses ke akun media sosial mereka.

Memanfaatkan Kebocoran Data:

Hacker juga dapat mencoba memperoleh data login dari sumber lain yang telah mengalami pelanggaran data dan menggunakannya untuk mencoba masuk ke akun media sosial. Berbagai kasus kebocoran data yang terjadi di Indonesia membuat hacker berpotensi menebak informasi login pengguna. Jadi pastikan selalu memperbarui password secara berkala.

Mencari Celah *Platform*:



Platform media sosial dapat memiliki kerentanan keamanan yang dapat dimanfaatkan oleh hacker. Jika ada kerentanan yang belum diperbaiki, hacker dapat menggunakan metode serangan seperti serangan injeksi SQL, serangan XSS (*Cross-Site Scripting*), atau serangan lainnya untuk mendapatkan akses ke akun media sosial.

Kelemahan Keamanan di Perangkat Pengguna:

Jika perangkat pengguna tidak memiliki keamanan yang memadai, seperti penggunaan kata sandi yang lemah, mengunduh perangkat lunak atau aplikasi dari sumber yang tidak terpercaya, penggunaan jaringan Wi-Fi yang tidak aman atau tidak memperbarui (meng-update) perangkat lunak keamanan, hacker dapat memanfaatkan kelemahan ini untuk mengakses akun media sosial.

PHISHING

Dari berbagai metode itu, metode phishing adalah yang paling banyak dilakukan untuk meretas akun. Mengidentifikasi situs phishing dapat membantu kita melindungi diri dari upaya pencurian informasi pribadi dan kata sandi. Berikut adalah beberapa tanda yang dapat membantu kita mengenali situs phishing:

1. Periksa URL: Perhatikan dengan cermat URL situs web yang kita kunjungi. Situs *phishing* sering menggunakan URL yang mirip dengan situs asli, tetapi dengan perubahan kecil. Periksa domain, ejaan atau ekstensi yang mencurigakan. Misalnya, situs phishing dapat menggunakan domain seperti "faceb00k.com" atau "faccebook.com" sebagai ganti "facebook.com".

2. Perhatikan keamanan HTTPS: Situs web yang aman menggunakan protokol HTTPS dengan sertifikat SSL. Periksa apakah situs yang kita kunjungi memiliki ikon gembok atau awalan "https://" pada URL. Jika situs tersebut menggunakan protokol HTTP biasa atau menunjukkan peringatan keamanan, waspadalah karena itu bisa menjadi indikasi situs phishing.
3. Tinjau tampilan situs: Situs phishing sering kali memiliki tampilan yang mirip dengan situs asli untuk menipu pengguna. Perhatikan apakah ada perbedaan dalam tata letak, desain, atau logo yang mencurigakan. Jika sesuatu terlihat aneh atau tidak konsisten dengan situs yang biasa kita gunakan, sebaiknya jangan memasukkan informasi login kita.
4. Perhatikan permintaan informasi pribadi yang tidak wajar: Situs phishing sering kali meminta pengguna untuk memasukkan informasi pribadi yang tidak biasa atau tidak relevan, seperti nomor kartu kredit, nomor asuransi sosial, atau informasi rahasia lainnya. Pastikan bahwa situs yang kita kunjungi hanya meminta informasi yang sesuai dan relevan untuk layanan yang mereka berikan.
5. Waspadai pesan atau email yang mencurigakan: Phishing sering kali dimulai dengan pesan atau email palsu yang meminta pengguna untuk mengklik tautan dan memasukkan informasi login mereka. Waspadai pesan yang tiba-tiba atau tidak biasa, terutama jika mereka mengancam konsekuensi negatif jika kita tidak segera bertindak. Jangan pernah memasukkan informasi login atau informasi pribadi ke dalam formulir yang diakses melalui tautan dalam pesan tersebut.

6. Gunakan solusi keamanan: Memasang perangkat lunak keamanan atau ekstensi browser yang dapat memperingatkan kita tentang situs phishing dapat membantu melindungi kita secara proaktif. Beberapa solusi keamanan juga menyediakan daftar situs phishing yang diketahui untuk membantu mengidentifikasi situs berbahaya.
7. Jika kita merasa situs yang kita kunjungi adalah situs phishing, jangan memasukkan informasi pribadi atau kata sandi kita. Jika kita memiliki kecurigaan, lebih baik mencari situs secara manual melalui mesin pencari atau menggunakan bookmark yang sudah kita simpan sebelumnya untuk mengakses situs media sosial atau layanan online yang kita gunakan.

MALWARE

Selan Phishing, cara lain yang juga umum dipakai dan seringkali membuat pengguna lengah adalah dengan menggunakan malware. Malware adalah singkatan dari "malicious software" yang berarti perangkat lunak jahat atau berbahaya yang dibuat oleh penjahat siber. Ini adalah jenis perangkat lunak yang dirancang untuk merusak, mengganggu, atau mengambil alih sistem komputer atau perangkat lainnya tanpa izin atau pengetahuan pengguna. Ada beberapa jenis malware yang dapat menyebabkan kerugian yang berbeda:

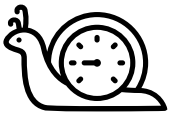
1. **Virus:** Virus adalah program yang dapat menggandakan dirinya sendiri dan menyebar ke komputer atau perangkat lain. Virus cenderung melekat pada file atau program dan akan aktif saat file atau program tersebut dijalankan. Virus dapat merusak data, menghapus file, atau bahkan mengambil alih kendali sistem.

2. **Worm:** Worm adalah program yang dapat menyebar dari satu perangkat ke perangkat lain melalui jaringan, sering kali tanpa interaksi pengguna. Worm dapat menyebabkan kerusakan sistem, menghabiskan sumber daya komputer, atau bahkan membuka pintu bagi serangan lain.
3. **Trojan:** Trojan atau Trojan horse adalah jenis malware yang menyembunyikan dirinya sebagai program yang sah atau berguna, tetapi sebenarnya memiliki niat jahat. Trojan dapat digunakan untuk mencuri informasi pribadi, memata-matai aktivitas pengguna, atau memberikan akses tidak sah ke sistem.
4. **Ransomware:** Ransomware adalah jenis malware yang mengenkripsi data pengguna dan menuntut pembayaran tebusan untuk mendapatkan kunci dekripsi. Ransomware dapat mencegah pengguna mengakses data mereka sendiri sampai tebusan dibayar.
5. **Spyware:** Spyware adalah jenis malware yang dirancang untuk memata-matai aktivitas pengguna dan mengumpulkan informasi pribadi tanpa izin. Spyware dapat merekam keystroke, melacak aktivitas browsing, mencuri informasi login, atau mengakses data sensitif lainnya.
6. **Adware:** Adware adalah jenis malware yang ditujukan untuk menampilkan iklan yang tidak diinginkan kepada pengguna. Adware seringkali datang bersamaan dengan perangkat lunak bebas atau shareware dan dapat mengganggu pengalaman pengguna serta mengumpulkan data pribadi.

Dalam kasus peretasan akun. Jenis malware yang biasa digunakan adalah Trojan dan Spyware. Modus peretasan dengan mengirimkan undangan pernikahan atau surat tilang dengan file apk adalah salah satu cara hacker memperdaya korban untuk memasang perangkat lunak jahat ini di gawainya.

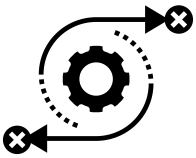
Gawai yang sehat dan belum terjangkit malware idealnya akan bisa bekerja dengan aman dan lancar. Jika gejala ini muncul pada gawai kita, kita patut waspada siapa tahu perangkat kita sudah terkena malware. Berikut beberapa gejalanya:

Kinerja sistem yang lambat:



Jika sistem komputer atau perangkat kita tiba-tiba menjadi sangat lambat atau tidak responsif, ini bisa menjadi indikasi adanya malware. Malware yang berjalan di latar belakang dapat menggunakan sumber daya sistem yang signifikan, sehingga mempengaruhi kinerja umum.

Perubahan yang tidak diinginkan:

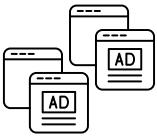


Jika pengaturan sistem, pengaturan browser, halaman beranda, atau mesin pencari default berubah tanpa izin atau tindakan kita, mungkin ada malware yang beroperasi di sistem kita. Malware sering kali melakukan perubahan ini untuk mengarahkan pengguna ke situs phishing atau untuk menampilkan iklan yang tidak diinginkan.

Program yang tidak dikenal:

Periksa daftar program yang diinstal pada sistem kita. Jika kita melihat program yang tidak dikenal, mencurigakan, atau yang tidak kita ingat menginstal, ada kemungkinan itu adalah malware. Selain itu, perhatikan juga ekstensi atau add-on yang terpasang pada browser kita.

Pop-up iklan berlebihan:



Jika kita mulai melihat pop-up iklan yang tidak biasa atau berlebihan, terutama ketika kita sedang menjelajahi internet, ini bisa menjadi indikasi adanya adware atau jenis malware lainnya pada sistem kita.

Perangkat lunak keamanan noaktif:

Jika antivirus atau perangkat lunak keamanan lainnya tiba-tiba dinonaktifkan atau tidak berfungsi dengan benar tanpa interaksi kita, bisa jadi malware telah menonaktifkannya untuk melindungi dirinya sendiri.

Aktivitas jaringan yang mencurigakan:

Jika ada aktivitas jaringan yang mencurigakan pada perangkat kita, seperti penggunaan bandwidth yang tinggi atau koneksi internet yang lambat, malware mungkin sedang mengirim atau menerima data dari luar sistem kita. Dan bisa jadi, hal superit ini bisa menjadi salah satu tanda data pribadi kita tengah dicuri.

Peringatan dari perangkat lunak keamanan:

Jika perangkat lunak keamanan kita mengeluarkan peringatan tentang deteksi malware atau ancaman yang mencurigakan, jangan abaikan peringatan tersebut. Perangkat lunak keamanan yang baik akan memindai dan memonitor sistem kita untuk mendeteksi malware.

Jika kita mencurigai adanya malware pada sistem kita, sebaiknya kita menjalankan pemindaian lengkap dengan perangkat lunak keamanan yang terpercaya atau menghubungi profesional keamanan IT untuk membantu mengidentifikasi dan menghapus malware tersebut.

Untungnya, ada cara untuk menghindari Malware. Berikut tips atau cara yang bisa kita lakukan untuk menghindarinya:

1. **Gunakan perangkat lunak keamanan yang terpercaya:** Instal dan perbarui perangkat lunak keamanan yang handal, termasuk antivirus, firewall, dan perlindungan malware lainnya. Pastikan untuk mengaktifkan pembaruan otomatis sehingga perangkat lunak keamanan kita selalu diperbarui dengan definisi terbaru untuk mendeteksi dan melawan ancaman yang baru.

2. **Perbarui sistem operasi dan perangkat lunak secara teratur:** Perangkat lunak dan sistem operasi yang tidak diperbarui dapat memiliki kerentanan yang dapat dimanfaatkan oleh malware. Pastikan untuk menginstal pembaruan keamanan dan patch yang dirilis oleh vendor secara teratur untuk menjaga sistem kita tetap aman.

3. **Hati-hati saat mengklik tautan:** Jangan asal mengklik tautan yang mencurigakan dalam email, pesan instan, atau situs web yang tidak terpercaya. Tautan tersebut dapat mengarahkan kita ke situs phishing atau mengunduh malware secara langsung ke sistem kita. Selalu verifikasi keaslian tautan sebelum mengkliknya dengan memeriksa URL yang ditampilkan dan menghindari tautan yang mencurigakan atau tidak dikenal.

4. **Hindari mengunduh dari sumber yang tidak terpercaya:** Hindari mengunduh file atau program dari situs web yang tidak terpercaya atau sumber yang tidak dikenal. Pastikan kita hanya mengunduh perangkat lunak dari situs resmi atau sumber yang dapat dipercaya.

5. **Waspadai lampiran email yang mencurigakan:** Jangan membuka lampiran email yang tidak kita harapkan atau dari pengirim yang tidak kita kenal. Lampiran dapat berisi malware yang dapat diaktifkan begitu kita membukanya.

6. **Jaga kehati-hatian saat berselancar di internet:** Jangan mengklik iklan yang mencurigakan atau pop-up yang muncul secara tiba-tiba. Hindari mengunjungi situs web yang ilegal atau mencurigakan yang mungkin menyebabkan pemasangan malware tanpa sepengetahuan kita.

7. **Aktifkan firewall:** Aktifkan firewall pada sistem kita untuk membantu melindungi dari serangan jaringan dan mengontrol lalu lintas masuk dan keluar.

8. **Periksa izin aplikasi:** Ketika menginstal aplikasi pada perangkat seluler, periksa izin yang diminta oleh aplikasi tersebut. Jika izin yang diminta tidak sesuai dengan fungsi aplikasi atau tampak mencurigakan, pertimbangkan untuk tidak menginstal aplikasi tersebut.

9. **Gunakan kata sandi yang kuat:** Gunakan kata sandi yang kuat dan unik untuk akun-akun online kita. Hindari menggunakan kata sandi yang mudah ditebak atau terlalu sederhana. Lebih baik menggunakan kombinasi huruf besar dan kecil, angka, dan karakter khusus.

10. **Pendidikan diri:** Tingkatkan pengetahuan kita tentang ancaman keamanan dan praktik keamanan yang baik secara umum. Tetap up-to-date dengan tren malware terbaru dan cara-cara penyebarannya agar kita dapat mengidentifikasi modus baru penyebaran malware.

AKUN SUDAH DIHACK BAGAIMANA?

Jika kita mencurigai bahwa akun media sosial kita telah diretas, berikut adalah langkah-langkah yang dapat kita ambil untuk mengatasi situasi tersebut:

Ganti kata sandi:

Segera ganti kata sandi: Langkah pertama yang harus kita lakukan adalah mengganti kata sandi akun media sosial yang dihack. Gunakan kata sandi yang kuat dan unik yang belum pernah kita gunakan sebelumnya. Pastikan kata sandi baru tersebut tidak mudah ditebak dan sulit dipecahkan.

Periksa & perbaharui akun:

Periksa dan perbarui informasi akun: Setelah mengganti kata sandi, periksa informasi akun kita, termasuk alamat email yang terhubung, nomor telepon, dan pertanyaan keamanan. Pastikan tidak ada perubahan yang tidak sah dilakukan oleh penyerang. Jika ada perubahan yang mencurigakan, segera pulihkan informasi akun tersebut.

Aktifkan autentikasi dua faktor:

Aktifkan autentikasi dua faktor (2FA): Aktifkan fitur autentikasi dua faktor pada akun media sosial kita jika belum melakukannya. Dengan 2FA, kita akan memerlukan kode verifikasi tambahan, selain kata sandi, untuk masuk ke akun kita. Ini akan memberikan lapisan keamanan tambahan dan membuat sulit bagi penyerang untuk mengakses akun kita.

Lapor pada platform:

Laporkan kejadian kepada platform media sosial: Segera laporkan peretasan akun kepada platform media sosial yang bersangkutan. Banyak platform memiliki proses pelaporan yang ditujukan untuk membantu pengguna yang mengalami masalah keamanan. Ikuti panduan yang diberikan oleh platform tersebut untuk melaporkan insiden dan mendapatkan bantuan dalam memulihkan akun kita.

Periksa sesuatu atau hapus hal mencurigakan:

Periksa dan hapus konten yang mencurigakan: Cek aktivitas akun kita dan periksa apakah ada postingan, pesan, atau aktivitas lain yang mencurigakan atau tidak diakui oleh kita. Jika ada, hapus konten tersebut dan beri tahu pengikut kita bahwa akun kita telah dihack sehingga mereka tidak menjadi korban penipuan.

Periksa akun lain yang terhubung:

Periksa akun lain yang terhubung: Jika kita menggunakan akun media sosial untuk masuk ke layanan atau aplikasi lain, periksa juga keamanan dan aktivitas akun-akun tersebut. Jika ada tautan atau akses yang mencurigakan, ubah kata sandi dan ambil langkah-langkah perlindungan yang diperlukan pada akun terkait.

Pindai dengan antivirus:

Periksa perangkat dan lakukan pemindaian antivirus: Lakukan pemindaian antivirus pada perangkat yang kita gunakan untuk mengakses akun media sosial. Ini akan membantu mengidentifikasi adanya malware atau keylogger yang mungkin telah memfasilitasi peretasan akun kita.

Perbaharui perangkat:

Perbarui keamanan perangkat dan lindungi diri kita ke depannya: Pastikan perangkat kita memiliki sistem operasi dan perangkat lunak yang diperbarui dengan patch keamanan terbaru. Gunakan perangkat lunak keamanan yang terpercaya, aktifkan firewall, dan jaga kehati-hatian saat menjelajahi internet dan menerima pesan atau tautan yang mencurigakan.

Jika akun media sosial Anda sudah diretas dan Anda tidak bisa mengaksesnya, berikut adalah langkah-langkah yang dapat Anda ambil:

1. **Gunakan opsi pemulihan akun:** Setiap platform media sosial umumnya memiliki opsi pemulihan akun yang dapat membantu Anda mendapatkan kembali akses ke akun Anda. Coba gunakan opsi pemulihan seperti "Lupa Kata Sandi" atau "Pulihkan Akun" yang disediakan oleh platform. Ikuti petunjuk yang diberikan untuk mengidentifikasi diri Anda dan memulihkan akses ke akun Anda.

2. **Hubungi layanan pelanggan platform:** Jika Anda tidak dapat menggunakan opsi pemulihan akun atau mengalami kesulitan lainnya, hubungi layanan pelanggan platform media sosial. Sampaikan masalah Anda dan mintalah bantuan untuk memulihkan akun Anda. Mereka mungkin meminta informasi tambahan atau dokumen identitas untuk memverifikasi kepemilikan akun sebelum membantu Anda memulihkannya.

3. **Laporkan kejadian ke platform media sosial:** Selain menghubungi layanan pelanggan, laporkan peretasan akun kepada platform media sosial tersebut. Mereka dapat memberikan panduan tambahan dan mengambil langkah-langkah untuk melindungi akun Anda dan mencegah aktivitas yang tidak sah.

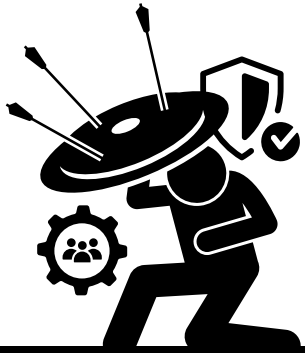
4. **Laporkan kejadian kepada penegak hukum:** Jika akun Anda diretas dan digunakan untuk melakukan tindakan ilegal atau merugikan, laporkan kejadian ini kepada pihak penegak hukum. Ajukan laporan polisi atau hubungi unit kejahatan komputer terdekat untuk memberi tahu mereka tentang insiden yang terjadi.

5. **Informasikan kepada kontak Anda:** Beri tahu kontak Anda, teman, dan pengikut bahwa akun Anda telah diretas. Ini akan membantu mencegah penyebaran informasi palsu atau penipuan yang mungkin dilakukan oleh penyerang melalui akun Anda yang diretas.

6. **Perbarui keamanan perangkat:** Selain memulihkan akun media sosial Anda, pastikan untuk memeriksa keamanan perangkat yang Anda gunakan untuk mengakses akun tersebut. Perbarui sistem operasi, lakukan pemindaian antivirus, dan pastikan tidak ada perangkat lunak berbahaya atau malware yang mempengaruhi perangkat Anda.

7. **Selalu ingat untuk menggunakan kata sandi yang kuat,** mengaktifkan autentikasi dua faktor (2FA), dan menjaga keamanan perangkat Anda agar mengurangi risiko peretasan akun media sosial di masa depan.

Two Factor Autentication/Otentikasi Dua Arah (2FA) adalah metode keamanan yang melibatkan penggunaan dua faktor verifikasi saat mengakses akun online. Metode ini memberikan lapisan tambahan perlindungan di luar kata sandi tradisional. Biasanya, 2FA melibatkan beberapa kombinasi kata kunci seperti sandi yang biasa kita pakai, One Time Password, maupun sandi biometrik yang menggunakan wajah atau sidik jari kita.



JANGAN LUPA, AMANKAN JUGA SITUS ORGANISASI KITA

Berbeda dengan mengelola akun media sosial, mengelola situs organisasi jauh lebih rumit dan memerlukan literasi akses yang lebih tinggi. Hal ini disebabkan oleh peran kita sebagai pengelola langsung platform yang kita bangun. Sementara jika kita menggunakan media sosial, kita hanyalah penguna. Di pusat platform media sosial yang kita pakai sudah ada tim pengelola situs yang memang pakar di bidangnya.

Meskipun demikian, bukan berarti kita tidak boleh membuat situs. Jika sudah memiliki situs, selalu pastikan keamanan sistem Anda dengan penyedia layanan domain dan hosting. Selalu pastikan untuk menggunakan fitur keamanan yang mereka sediakan untuk menghindari hal yang tidak diinginkan.

Selain itu, prinsip pengamanan situs pada dasarnya memiliki kesamaan dengan mengelola media sosial. Selama password kita terjaga dan kita tidak mengunduh atau memasang perangkat lunak yang didapat dari sumber yang tidak terpercaya maka situs yang kita kelola akan relatif aman.

Q: Bagaimana saya bisa tahu jika akun media sosial saya telah diretas?

A: Tanda-tanda bahwa akun media sosial Anda telah diretas termasuk aktivitas yang mencurigakan, seperti postingan atau pesan yang tidak Anda buat, perubahan informasi akun tanpa izin Anda, atau pengaturan privasi yang berubah secara tiba-tiba.

Q: Apa yang harus saya lakukan jika akun media sosial saya telah diretas?

A: Jika akun media sosial Anda telah diretas, segera lakukan tindakan berikut: ganti kata sandi Anda, laporkan kejadian tersebut ke platform media sosial, periksa dan hapus postingan yang tidak sah, dan pastikan komputer atau perangkat yang Anda gunakan tidak terinfeksi malware.

Q: Apa yang harus saya lakukan jika saya tidak bisa mengakses akun media sosial saya setelah diretas?

A: Jika Anda tidak bisa mengakses akun media sosial setelah diretas, hubungi dukungan platform media sosial dan laporkan masalah ini kepada mereka. Mereka akan memberikan petunjuk lebih lanjut tentang proses pemulihan akun.

Q: Apa yang harus saya lakukan jika hacker mengubah informasi kontak atau alamat email di akun media sosial saya?

A: Jika hacker mengubah informasi kontak atau alamat email di akun media sosial Anda, segera hubungi dukungan platform media sosial dan berikan bukti kepemilikan akun. Mereka akan membantu Anda memulihkan akses ke akun dengan memverifikasi identitas Anda.

Q: Bagaimana saya dapat melindungi akun media sosial saya dari serangan peretasan?

A: Beberapa langkah yang dapat Anda ambil untuk melindungi akun media sosial Anda dari serangan peretasan termasuk menggunakan kata sandi yang kuat dan unik, mengaktifkan autentikasi dua faktor (2FA), tidak membagikan informasi pribadi yang sensitif di platform, dan memperbarui perangkat lunak keamanan secara teratur.

Q: Apa yang harus saya lakukan jika hacker mencoba meminta uang atau informasi pribadi dari kontak saya setelah meretas akun media sosial saya?

A: Jika hacker mencoba meminta uang atau informasi pribadi dari kontak Anda setelah meretas akun media sosial Anda, beri tahu kontak Anda bahwa akun Anda telah diretas dan mereka harus mengabaikan permintaan tersebut. Laporkan juga kejadian ini kepada platform media sosial dan polisi setempat.

Q: Apa yang harus saya lakukan jika saya menemukan akun palsu yang menggunakan nama dan foto saya?

A: Jika Anda menemukan akun palsu yang menggunakan identitas Anda di media sosial, laporkan hal tersebut

Q: Bagaimana saya dapat mencegah serangan peretasan lebih lanjut setelah akun media sosial saya diretas?

A: Setelah akun media sosial Anda diretas, perkuat keamanan dengan mengganti kata sandi, mengaktifkan autentikasi dua faktor (2FA), memeriksa dan menghapus izin aplikasi pihak ketiga yang tidak dikenal, dan mengamankan perangkat Anda dengan perangkat lunak keamanan yang terkini.

Q: Bagaimana seorang hacker dapat mengambil alih akun media sosial?

A: Hacker dapat mengambil alih akun media sosial dengan menggunakan metode seperti phishing, serangan brute force, pencurian informasi login, atau eksploitasi kerentanan keamanan.

Q: Apa itu serangan phishing pada akun media sosial?

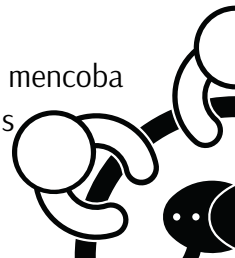
A: Serangan phishing adalah metode di mana hacker mencoba memperoleh informasi login pengguna dengan menyamar sebagai entitas tepercaya melalui pesan atau situs web palsu.

Q: Bagaimana hacker menggunakan email phising untuk
A: **mengambil alih akun media sosial?**

Hacker dapat mengirim email phishing palsu yang tampak seperti email resmi dari platform media sosial untuk meminta pengguna memberikan informasi login mereka. Jika pengguna memasukkan informasi tersebut, hacker dapat menggunakannya untuk mengambil alih akun.

Q: Apa yang dimaksud dengan serangan brute force pada akun media sosial?

A: Serangan brute force adalah metode di mana hacker mencoba semua kombinasi password yang mungkin secara otomatis untuk mendapatkan akses ke akun media sosial.



Q: Bagaimana hacker mencuri informasi login dari akun media sosial?

A: Hacker dapat mencuri informasi login dari akun media sosial dengan menggunakan teknik seperti keylogging, memanfaatkan kerentanan di perangkat pengguna, atau mengarahkan pengguna ke situs web palsu yang tampak seperti platform media sosial.

Q: Apa yang dimaksud dengan eksploitasi kerentanan keamanan pada akun media sosial?

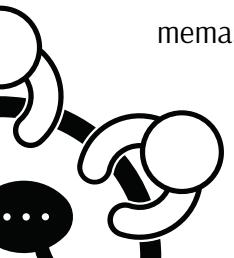
A: Eksploitasi kerentanan keamanan adalah praktik hacker memanfaatkan celah atau kelemahan dalam sistem atau platform media sosial untuk mendapatkan akses tidak sah ke akun pengguna.

Q: Apa yang harus saya lakukan untuk melindungi akun media sosial saya dari serangan pengambilalihan?

A: Beberapa langkah yang dapat Anda ambil untuk melindungi akun media sosial Anda termasuk menggunakan kata sandi yang kuat dan unik, mengaktifkan autentikasi dua faktor (2FA), tidak membagikan informasi login kepada orang lain, dan memperbarui perangkat lunak keamanan secara teratur.

Q: Apa yang harus dilakukan jika saya mencurigai adanya upaya pengambilalihan akun media sosial saya?

A: Jika Anda mencurigai adanya upaya pengambilalihan akun media sosial Anda, segera ganti kata sandi akun Anda, periksa aktivitas terakhir di akun Anda, laporkan kejadian tersebut ke platform media sosial, dan periksa keamanan perangkat Anda untuk memastikan tidak ada malware atau perangkat yang diretas.



Q: Bagaimana saya dapat mencegah serangan phishing terhadap akun media sosial saya?

A: Beberapa langkah yang dapat Anda ambil untuk mencegah serangan phishing terhadap akun media sosial Anda adalah berhati-hati dengan tautan yang mencurigakan, jangan membagikan informasi pribadi melalui tautan yang tidak terverifikasi, periksa alamat URL yang sebenarnya sebelum memasukkan informasi login, dan selalu periksa keamanan dan reputasi situs web sebelum memasukkan informasi sensitif.

Q: Apa yang harus saya lakukan jika saya menerima pesan mencurigakan atau link berbahaya melalui pesan pribadi di akun media sosial saya?

A: Jika Anda menerima pesan mencurigakan atau link berbahaya melalui pesan pribadi di akun media sosial Anda, jangan mengklik link tersebut. Jangan berikan informasi pribadi atau login. Laporkan pesan tersebut ke platform media sosial dan blokir pengirimnya.

Q: Bagaimana cara saya membedakan antara akun media sosial asli dan akun palsu?

A: Beberapa tanda bahwa sebuah akun media sosial mungkin palsu termasuk kurangnya aktivitas, sedikit atau tanpa teman, kurangnya postingan atau foto yang relevan, permintaan pertemanan dari orang-orang yang tidak Anda kenal, dan tautan yang mencurigakan. Periksa juga verifikasi akun dan periksa tautan profil yang terverifikasi.

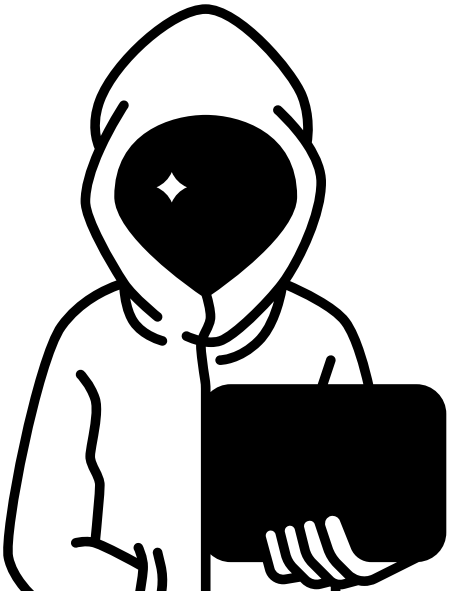
BAB KETIGA

KEAMANAN DIGITAL
UNTUK KELOMPOK RENTAN

Kelompok rentan yang dimaksud di sini adalah kelompok yang memilik kemungkinan lebih tinggi jadi target serangan digital. Dibandingkan dengan pengguna biasa teknologi digital, kelompok ini sering jadi sasaran utama dari serangan digital, seperti spam, phising, trolling dan lain sebagainya.

Siapakah kelompok rentan dalam dunia digital ini? SAFEnet dalam penelitian berjudul "Sudah Rentan, Kurang Waspada Pula" (2022) menyatakan ada tiga kriteria untuk menilai kelompok rentan dalam dunia digital. Tiga kriteria itu adalah aktif menggunakan teknologi digital, berasal dari kelompok minoritas, dan bekerja untuk kepentingan publik.

Jika kita menggunakan kriteria ini maka kelompok rentan itu bisa merujuk kepada kelompok pegiat hak-hak perempuan, penghayat atau agama lokal, difabel, transgender, usia lanjut, jurnalis warga, warga yang mempertahankan hak ekologinya, dan lainnya. Celakanya, seperti dalam temuan SAFEnet, kelompok rentan ini umumnya tidak memiliki kapasitas yang memadai untuk urusan keamanan digital.



Bila tiga kriteria ini secara bersamaan menempel dalam suatu kelompok, maka kelompok ini tentu sangat rentan mendapat serangan digital. Misalnya, seorang penganut agama lokal yang sangat minoritas, dan aktif menggunakan teknologi digital untuk membela hak asasi manusia (bekerja untuk kepentingan publik).

Kelompok minoritas yang aktif menggunakan teknologi digital untuk bekerja memperjuangkan hak asasi manusia sering menjadi serangan digital karena kondisi demokrasi di Indonesia masih jauh dari ideal. Pemerintahan dikuasai oleh kelompok oligarki yang mengutamakan kekuasaan dan kekayaan. Sementara wacana publik masih didominasi oleh perspektif yang konservatif, patriarkis, tidak menghormati keberagaman, dan kemudian dihantam gelombang post truth yang antifakta dan membabibuta membela ideologinya saja.

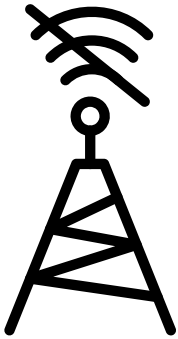
Serangan terhadap kelompok rentan ini juga terus terjadi karena penyelesaian secara hukum nyaris tidak ada sehingga tidak menimbulkan efek jera. Selain itu, secara teknis pelakunya masih sulit dicari dan aparat penegak hukum juga tidak serius mendalami persoalan ini.

Pada dasarnya kelompok-kelompok rentan ini mendapat berbagai macam serangan digital seperti yang menimpa pada orang lain pada umumnya. Tetapi ada beberapa serangan yang belum dijelaskan di depan.

Trolling:

Memberikan komentar secara bertubi-tubi dan bersamaan di media sosial yang biasanya dilakukan oleh para buzzer (pendengung) atas pesanan orang yang merasa dirugikan. Ini adalah bentuk serangan secara halus yang tujuannya adalah untuk menyerang kondisi psikologis dari orang yang menjadi target.

Pemutusan atau pelambatan jaringan internet:



Kasus seperti ini menimpa para aktivis hak asasi manusia di Papua dan warga Desa Wadas, Purworejo, Jawa Tengah yang tanahnya dipaksa diambil oleh pemerintah. Akibatnya mereka tidak bisa mengabarkan situasi dan kondisi di wilayah itu kepada dunia luar.

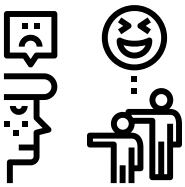
Penyelesaian persoalan ini berada di wilayah pemerintah sebagai pemangku kepentingan pengadaan jaringan internet. Yang dapat dilakukan warga terdampak adalah menjalin kerja sama dan kampanye agar pemerintah memulihkan jaringan internet. Selain itu warga juga bisa menggugat kasus ini ke pengadilan karena melanggar hak digital yang sudah jadi bagian dari hak asasi manusia.

Doxing:

Menyebarkan informasi data pribadi dari target dengan tujuan meruntuhkan moral atau mengintimidasi. Cara ini biasanya cukup meresahkan orang yang menjadi sasaran.

Bila ini terjadi, nonaktifkan media sosial dan nomor handphone untuk sementara. Jika merasa terancam laporkan ke polisi, berlindung di rumah aman dan berjejaring untuk menguatkan keamanan.

Bullying:



Mengejek atau menghina target melalui media digital. Cara ini juga merupakan bentuk teror psikologis untuk menjatuhkan mental orang yang jadi sasaran.

Matikan media sosial untuk menurunkan tekanan psikologis. Bila merasa terganggu, konsultasi kepada psikolog.

Impersonansi:

Pelaku membuat akun palsu di media sosial dari target korban pelaku kemudian menggunakan akun itu untuk tujuan-tujuan yang bisa membuat korban menjadi malu atau untuk keuntungan finansial dari pelaku.

Untuk menanggulanginya, bisa dibuat pengumuman yang disebarkan di media sosial bahwa ada orang yang melakukan impersonansi. Tentu dilengkapi dengan seruan agar jangan mau menuruti apa yang diminta atau dikatakan oleh akun palsu itu.

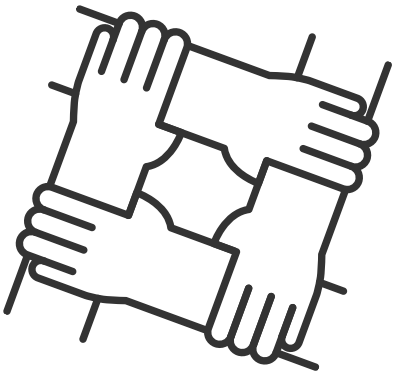
Cara lainnya adalah melaporkan kepada aplikasi yang bersangkutan bahwa ada yang membuat akun palsu atas dirinya. Harapannya, pengelola aplikasi akan menghapus akun palsu tersebut.

Pemblokiran:

Pemblokiran, website, aplikasi, dan penutupan akun media sosial. Bila ini terjadi yang bersangkutan bisa melaporkan kepada platform dan menjelaskan duduk perkaranya. Tetapi jika yang menutup adalah pemerintah, mungkin jalur hukum bisa ditempuh.

Untuk mengurangi ancaman seperti dijelaskan di atas, kelompok rentan perlu meningkatkan kapabilitas soal keamanan digital. Risiko keamanan digital selalu ada dan tidak bisa dihilangkan sama sekali. Yang bisa dilakukan adalah menguranginya.

BAB KEEMPAT



ETIKA DIGITAL

Etika digital adalah kumpulan prinsip, nilai, dan norma-norma moral yang mengatur perilaku individu dan kelompok dalam menggunakan teknologi digital. Etika digital berkaitan dengan tanggung jawab, kesadaran, dan perilaku yang etis dalam berinteraksi dengan teknologi, seperti internet, media sosial, perangkat elektronik, dan aplikasi digital.

Etika digital sangat penting karena penggunaan teknologi digital telah menjadi bagian integral dari kehidupan sehari-hari kita. Berikut adalah beberapa alasan pentingnya mengetahui etika digital:

Perlindungan Privasi: Etika digital sangat memperhatikan serta mempertimbangkan hak privasi individu serta perlindungan data pribadi. Dengan mematuhi etika digital, kita dapat menghindari berbagai pelanggaran-pelanggaran privasi, esperti pencurian identitas atau penyalahgunaan informasi pribadi.

Keamanan dan Perlindungan: Etika digital bertujuan menjaga keamanan di dunia digital. Ini mencakup perlindungan terhadap malware, phishing, peretasan, dan serangan siber lainnya yang dapat merugikan individu dan organisasi.

Pencegahan Penyebaran Informasi Palsu: Kita diharapkan untuk memeriksa kebenaran informasi sebelum membagikannya, mempromosikan keakuratan, dan memerangi penyebaran berita palsu.

Cyberbullying dan Pelecehan Online: Etika digital mendorong penanganan yang bertanggung jawab terhadap isu-isu seperti cyberbullying, pelecehan online, dan perilaku merugikan lainnya di ruang digital.

Dampak Sosial dan Moral: Hal ini mencakup pertimbangan tentang bagaimana tindakan online kita dapat mempengaruhi orang lain, masyarakat, dan lingkungan di sekitar kita.

Pembentukan Identitas Digital: Etika digital membantu dalam pembentukan identitas digital yang positif dan profesional. Dengan mematuhi etika digital, kita dapat menciptakan reputasi yang baik secara online dan membangun hubungan yang sehat dengan orang lain.

Penggunaan Teknologi yang Bertanggung Jawab: Etika digital mendorong penggunaan teknologi yang bertanggung jawab dan bijaksana. Ini mencakup penggunaan yang seimbang, menghindari ketergantungan berlebihan, serta menyadari dampaknya terhadap kesehatan fisik dan mental.

Etika digital membantu menciptakan lingkungan online yang lebih aman, beretika, dan bermanfaat bagi semua pengguna. Dengan memahami dan menerapkan prinsip-prinsip etika digital, kita dapat memanfaatkan teknologi digital dengan lebih baik dan meminimalkan risiko serta dampak negatif yang mungkin terjadi.

PRINSIP ETIKA DIGITAL

Berikut adalah beberapa prinsip untuk mengolah konten agar sesuai dengan etika digital dan tidak menjadi konten yang provokatif:

Berpikir Sebelum Memposting:

Pertimbangkan dampak dari konten yang Anda buat atau bagikan sebelum mempostingnya. Tanyakan pada diri sendiri apakah konten tersebut mempromosikan pemahaman, toleransi, dan dialog yang sehat, atau justru memprovokasi perselisihan dan konflik. Serta, perhatikan Kode Etik Jurnalistik dalam membuat postingan.

Fakta dan Kebenaran:

Pastikan konten yang Anda bagikan didasarkan pada fakta yang terverifikasi dan kebenaran. Jangan menyebarkan informasi palsu, hoaks, atau klaim yang tidak memiliki dasar yang kuat. Verifikasi informasi sebelum membagikannya dan gunakan sumber yang terpercaya.

Keberimbangan dan Keadilan:

Pastikan konten yang Anda buat atau bagikan seimbang, objektif, dan adil. Hindari menyampaikan informasi yang memihak atau merugikan satu pihak secara berlebihan. Berikan perspektif yang beragam dan berikan ruang bagi sudut pandang yang berbeda.

Menghormati Privasi:

Jagalah privasi orang lain dalam konten yang Anda buat atau bagikan. Hindari mengungkapkan informasi pribadi tanpa izin yang jelas dan hindari mencemari privasi orang lain dengan membagikan informasi yang dapat merugikan atau memalukan mereka. Privasi orang lain yang dimaksud, salah satunya adalah data pribadi.

Jerat hukumnya, UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

- Pasal 26 (1) Kecuali ditentukan lain oleh peraturan perundang-gundangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan Orang yang bersangkutan. (2) Setiap Orang yang dilanggar haknya sebagaimana dimaksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.
- Pelaku penyebaran data pribadi dapat dijerat dengan Pasal 32 dan Pasal 48 UU ITE. Tak main-main, ancaman pidana bagi pelaku penyebaran data pribadi adalah paling lama delapan sampai sepuluh tahun penjara dan/atau denda paling banyak Rp 2 miliar hingga Rp 5 miliar.
- Ketentuan lebih lanjut mengenai perlindungan data pribadi terdapat dalam UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Undang-undang ini merupakan produk hukum terbaru terkait perlindungan data pribadi yang disahkan pada 17 Oktober 2022 lalu.

- Mengacu pada Pasal 67, setiap orang yang dengan sengaja dan melawan hukum mengungkapkan data pribadi yang bukan miliknya akan dipidana paling lama empat tahun penjara dan/atau denda paling banyak Rp 4 miliar. Sementara setiap orang yang dengan sengaja dan melawan hukum menggunakan data pribadi yang bukan miliknya akan dipidana paling lama lima tahun penjara dan/atau denda paling banyak Rp 5 miliar.

Menghindari Diskriminasi & Kebencian:

Hindari konten yang mengandung diskriminasi, kebencian, atau pelecehan terhadap individu atau kelompok berdasarkan ras, agama, gender, orientasi seksual, atau faktor-faktor lainnya. Jaga bahasa dan sikap yang inklusif serta hindari membuat pernyataan yang merugikan atau memprovokasi. Penting untuk diperhatikan bahwa ujaran kebencian, penghinaan, pelecehan atau stigmatisasi pada kelompok tertentu menciptakan kerentanan baik dari sisi yang memposting maupun yang dimaksud dalam postingan

Ujaran kebencian adalah (hate speech) sendiri adalah tindakan komunikasi yang dilakukan oleh suatu individu atau kelompok dalam bentuk provokasi, hasutan, ataupun penghinaan kepada individu atau kelompok yang lain dalam hal berbagai aspek, seperti: ras, warna kulit, gender, cacat, orientasi seksual, kewarganegaraan, agama, dan lain-lain.

Stigmatisasi adalah tindakan mengeksklusifkan seseorang atau kelompok yang dibangun secara sosial. Stigma biasanya berupa labelling, stereotip, separation, serta diskriminasi yang dapat mempengaruhi diri seorang individu secara keseluruhan. Stigma muncul karena masyarakat melihat ada sesuatu yang berbeda terjadi pada diri orang lain atau hal yang mereka lihat tidak sesuai dengan nilai-nilai yang dianut atau yang seharusnya di dalam masyarakat.

Pelanggaran atas konten/ unggahan mengandung kebencian dan penghinaan

- Pasal 243 ayat (1) jo ayat (2) UU KUHP baru yang berbunyi: "Setiap orang yang menyiarkan, mempertunjukkan, atau menempelkan tulisan atau gambar sehingga terlihat oleh umum atau memperdengarkan rekaman sehingga terdengar oleh umum atau menyebarluaskan dengan sarana teknologi informasi, yang berisi pernyataan perasaan permusuhan dengan maksud agar isinya diketahui atau lebih diketahui oleh umum, terhadap satu atau beberapa golongan atau kelompok penduduk Indonesia berdasarkan ras, kebangsaan, etnis, warna kulit, agama, kepercayaan, jenis kelamin, disabilitas mental, atau disabilitas fisik yang berakibat timbulnya kekerasan terhadap orang atau barang, dipidana dengan pidana penjara paling lama 4 (empat) tahun atau pidana denda paling banyak kategori IV".

- Pasal 243 ayat (1) jo ayat (2) UU KUHP baru yang berbunyi: "Jika setiap orang sebagaimana dimaksud pada ayat (1) melakukan tindak pidana tersebut dalam menjalankan profesinya dan pada waktu itu belum lewat 2 (dua) tahun sejak adanya putusan pemidanaan yang telah memperoleh kekuatan hukum tetap karena melakukan tindak pidana yang sama, pelaku dapat dijatuhi pidana tambahan berupa pencabutan hak sebagaimana dimaksud dalam Pasal 86 huruf f". Pasal 86 huruf f mengatur pidana tambahan berupa pencabutan hak tertentu berupa pencabutan hak untuk menjalankan profesi tertentu.

Menghormati Hak Cipta:

Pastikan konten yang Anda bagikan tidak melanggar hak cipta orang lain. Gunakan sumber yang sah dan beri atribusi jika Anda menggunakan konten orang lain. Hindari penggunaan ilegal atau tidak pantas terhadap materi milik orang lain.

Pasal yang melindungi hak cipta, UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

- Pasal 25 Informasi Elektronik dan/atau Dokumen Elektronik yang disusun menjadi karya intelektual, situs internet, dan karya intelektual yang ada di dalamnya dilindungi sebagai Hak Kekayaan Intelektual berdasarkan ketentuan Peraturan Perundang-undangan.
- Jerat hukumnya Sesuai dengan Undang-Undang (UU) Nomor 8 Tahun 2014 tentang Hak Cipta, pelaku pelanggaran hak cipta dakn ditindak tegas dengan hukuman penjara dan denda.

Menghormati Hukum dan Peraturan:

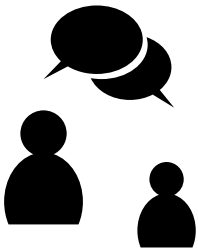
Pastikan konten yang Anda buat atau bagikan sesuai dengan hukum dan peraturan yang berlaku dalam ruang digital. Hindari pelanggaran hak kekayaan intelektual, penghinaan, ancaman, atau perilaku ilegal lainnya.

Konten yang mengandung pelanggaran perilaku lainnya, misalnya konten penyiksaan hewan, perjudian, melanggar kesusilaan, dll.

Jerat pidana untuk konten melanggar kesusilaan: UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

- Pasal 45 (1) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Berinteraksi dengan Hormat: Saat berinteraksi dengan orang lain secara online, berusahalah untuk berkomunikasi dengan hormat, mempertimbangkan perasaan dan perspektif mereka. Hindari menghina, menyebarkan kebencian, atau memicu konflik dengan komentar atau tanggapan yang merugikan.



Jerat Hukum: UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG-UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK

- Pasal 45A (2) Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan informasi yang ditujukan untuk menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Mengikuti prinsip-prinsip ini dapat membantu Anda mengolah konten dengan etika digital yang baik dan mencegahnya menjadi konten yang provokatif. Penting untuk berpikir secara kritis dan bertanggung jawab saat menciptakan dan menyebarkan konten di dunia digital.

BAB KELIMA

DAFTAR LINK PENTING

HANDBOOK
DIGITAL SAFETY