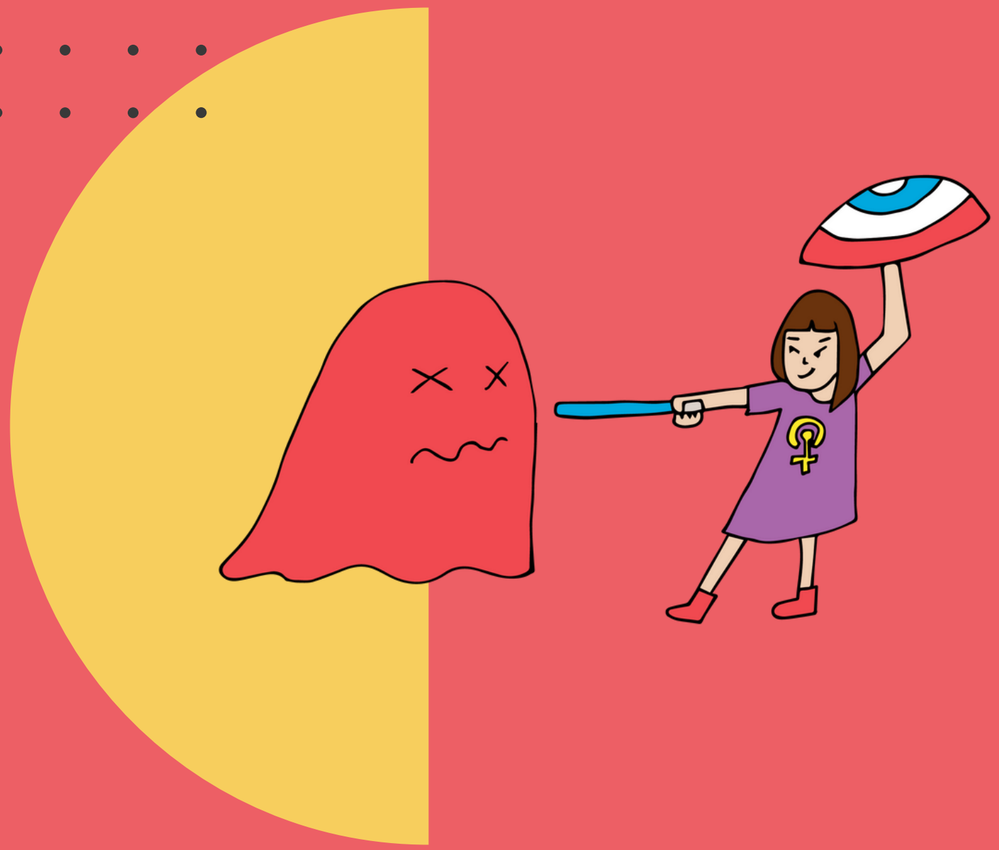
BASIC DIGITAL HYGIENE AND SECURITY

dhyta caturani - PurpleCode Collective

01 Kebersihan Gawai

Jaga kebersihan gawaimu dari infeksi virus, malware dan spyware yang bisa menyebabkan pengaksesan gawaimu dan pencurian data tanpa seijin dan sepengetahuanmu atau dari kerusakan data dan gawai. Lakukan proteksi dengan memasang Anti Virus.



02

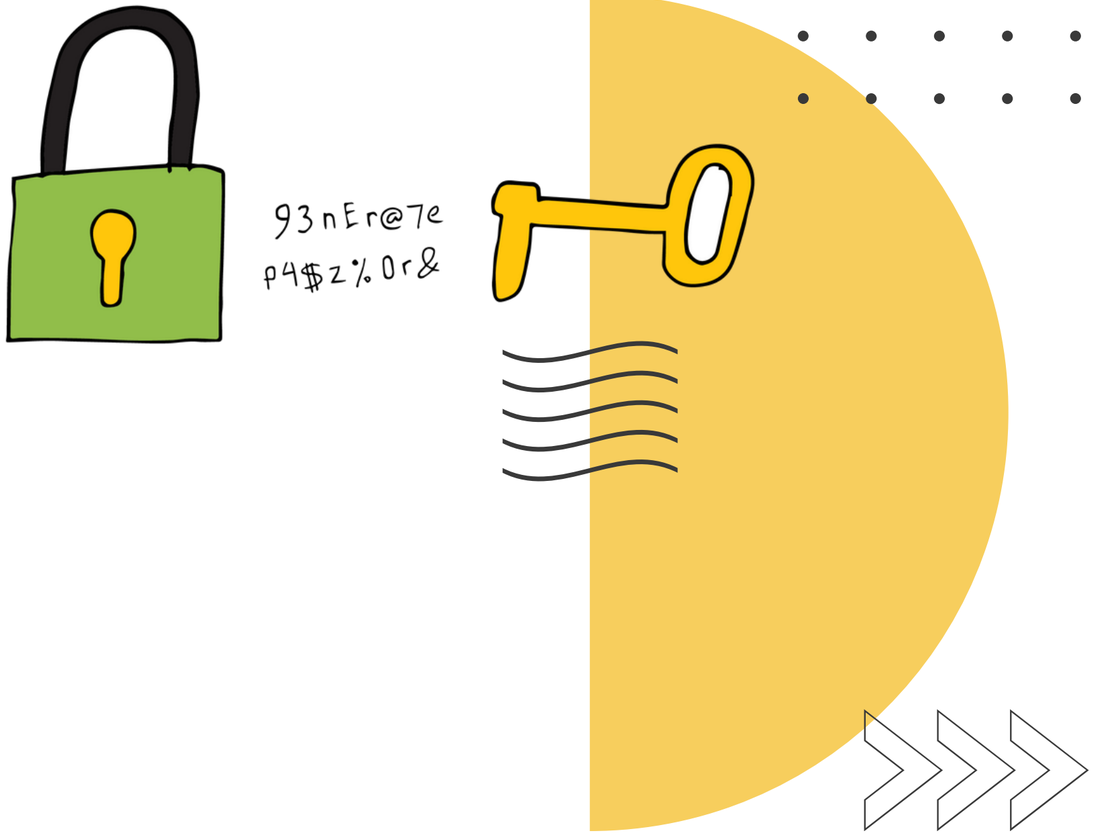
UPDATE OPERATING SYSTEM (OS) DAN APPS/SOFTWARE

Selalu update/perbarui Operating System (OS) dan Aplikasi atau Software di gawaimu. OS, Apps dan Softwares selalu diperbarui atau dikembangkan oleh developernya untuk memperbaiki performa dan memperkuat fitur-fitur keamanan untuk menangkal virus, malware dan spyware terbaru. Maka penting untuk OS, apps dan softwaremu untuk selalu up-to-date. Tunggu beberapa saat setelah versi terbaru diluncurkan untuk memastikan versi terbaru tersebut sudah stabil.

03

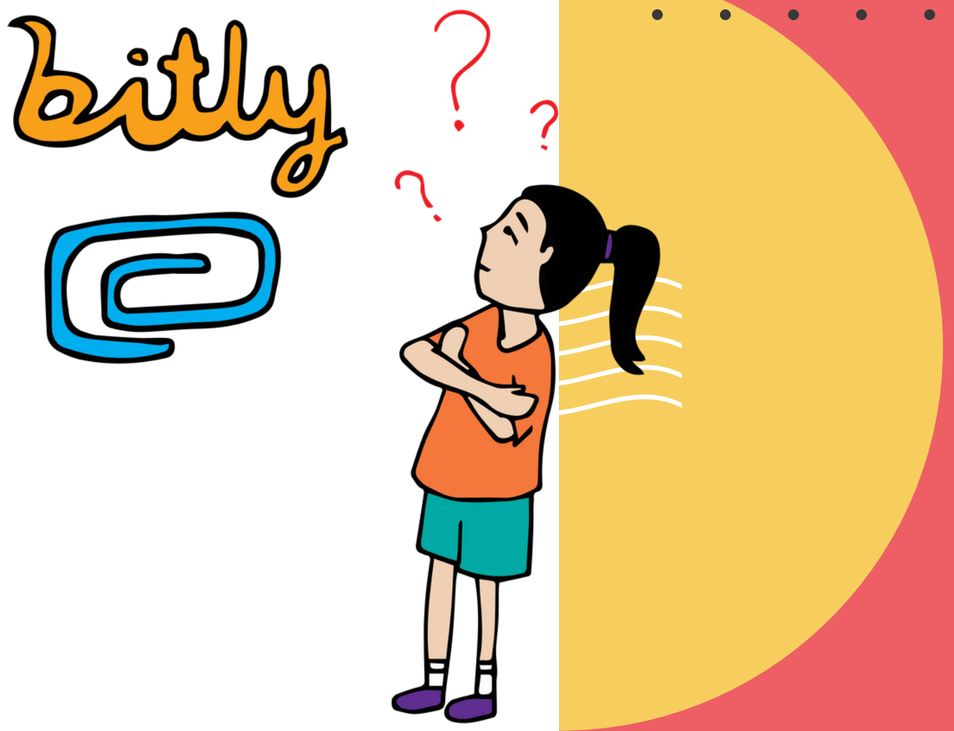
GUNAKAN PASSWORD YANG KUAT

Password atau kata sandi adalah gerbang menuju kehidupan digital kita. Ia menjadi salah satu pengaman pertama di Internet. Kebanyakan peretasan dan pengambil alihan akun adalah karena password kita berhasil diketahui oleh pelaku. Maka password haruslah dibuat sehingga orang tak bisa menebaknya.



04

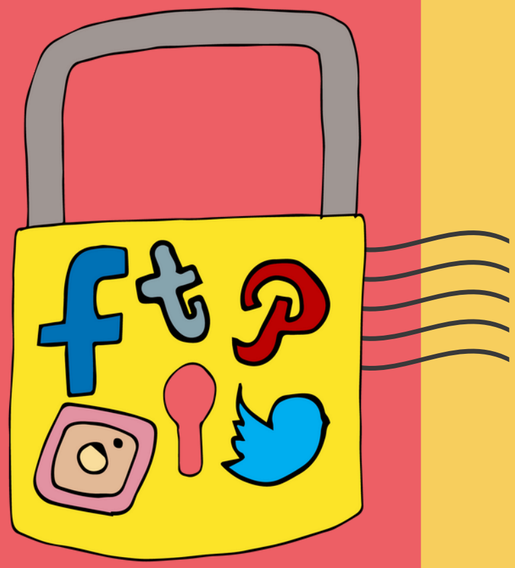
NO PISHING



Pishing adalah metode dimana target dihubungi melalui email, telepon, pesan teks (sms atau chat) yang membuat target menyerahkan data-data sensitif sehingga pelaku bisa mencuri banyak hal darinya.

Jangan sembarangan mengklik link atau mengunduh attachment (lampiran) sebelum memastikan bahwa link atau attachment tersebut bersih dari virus, malware maupun spyware yang membuat tujuan pishing berhasil.

05



ATUR PRIVASI AKUNMU

Lakuan pengaturan privasi di setiap akunmu sesuai kebutuhanmu dalam menggunakan akun tersebut. Ingat bahwa semakin banyak orang bisa melihat unggahanmu, semakin tinggi resikomu. Catatan: pengaturan privasi akun akan melindungimu dari orang lain namun tidak akan melindungimu dari pemilik platform/developer. Perhatikan Privacy Policy (Kebijakan Privasi) setiap akun dan ketahui apa saja yang diatur olehnya.

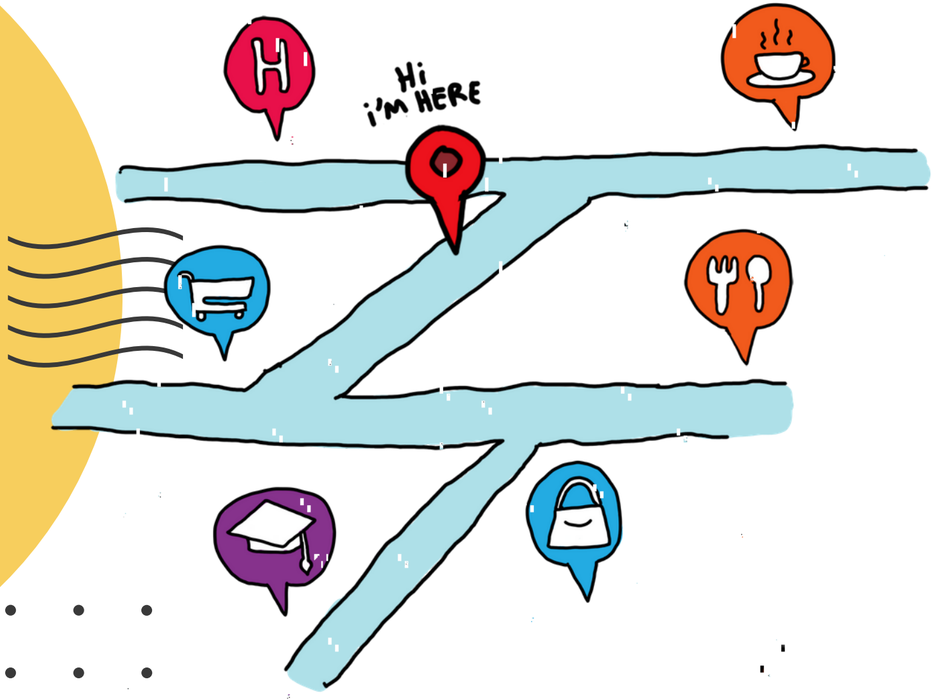
06

Jangan Melakukan Doxing

Jangan mempublikasikan informasi-informasi personalmu maupun orang lain yang dapat membuat orang mengidentifikasi siapa dirimu atau orang lain tersebut. Identifikasi diri ini bisa mempermudah orang untuk melakukan kejahatan baik online maupun di ruang fisik.

07

BIJAK GUNAKAN GEOTAG DAN GPS



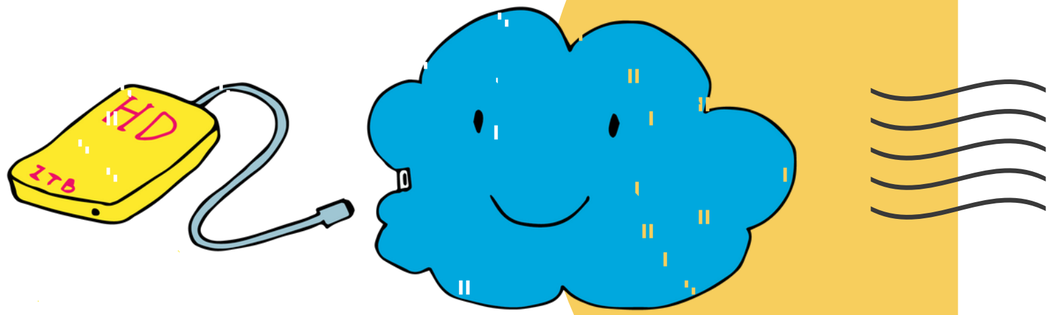
Jangan sembarangan menggunakan geo tagging (penanda lokasi) yang bisa memberitahu orang dimana kita tengah berada.

Selain itu upayakan untuk mematikan GPS bila tidak sedang digunakan. GPS bisa digunakan untuk melacak keberadaan kita.

08

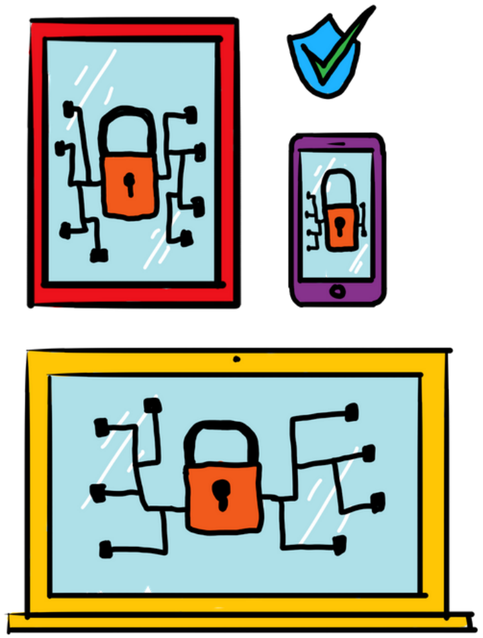
BACK UP DAN PENYIMPANAN AMAN

Lakukan back up data dan menyimpannya dengan aman secara berkala dan lebih dari satu copy. Back up dan penyimpanan bisa dilakukan di external drives atau cloud yang aman. Praktik ini untuk menghindarkanmu dari kehilangan data karena gawai atau file yang rusak dan juga membuatmu tidak bepergian dengan terlalu banyak data/informasi yang bisa membahayakan. Terlebih bila data/informasi tersebut dikategorikan sebagai sensitif.



09

ENKRIPSI GAWAI



Enkripsi sistem dalam gawaimu (komputer dan HP). Mengenkripsi gawai dapat mengamankan seluruh data yang ada di dalamnya. Jika kamu kehilangan gawaimu, orang bisa memindahkan CPU (Central Processing Unit) ke dalam gawai lain dan membaca data yang ada. Dengan mengenkripsinya, hal ini tidak bisa dilakukan bila pelaku tak memiliki password untuk membuka enkripsi tersebut

Bila kamu menggunakan komputer Apple (MacOS) maka kamu bisa memasang enkripsi ini dengan mengaktifkan FileVault yang ada di System Preference. Di komputer Windows bisa menggunakan BitLocker. Di HP Android biasanya ada di pengaturan Security/Keamanan. Di iPhone, sistem otomatis akan terenkripsi bila kamu memasang password untuk HPmu.

10

BERKOMUNIKASI DENGAN AMAN

Selalu berkomunikasilah dengan aman. Pilih platform chat/video call atau email yang memiliki fitur End-to-end Encryption yang membuat pesanmu tidak bisa dibaca pihak lain saat dalam perjalanan. Saat pesan sudah tiba di gawaimu, rajin-rajinlah menghapus pesan yang sudah terbaca terutama seandainya pesan tersebut mengandung informasi yang sensitif.

BEBERAPA PLATFORM ALTERNATIF

Adanya banyak platform yang menawarkan End-to-end Encryption seperti WhatsApp, Telegram, Line, dll, tapi platform-platform tersebut terbukti memiliki beberapa kelemahan keamanan dan berhasil mengalami peretasan. Ini adalah beberapa platform yang direkomendasikan karena memiliki sistem keamanan yang kuat.

Chat

Signal

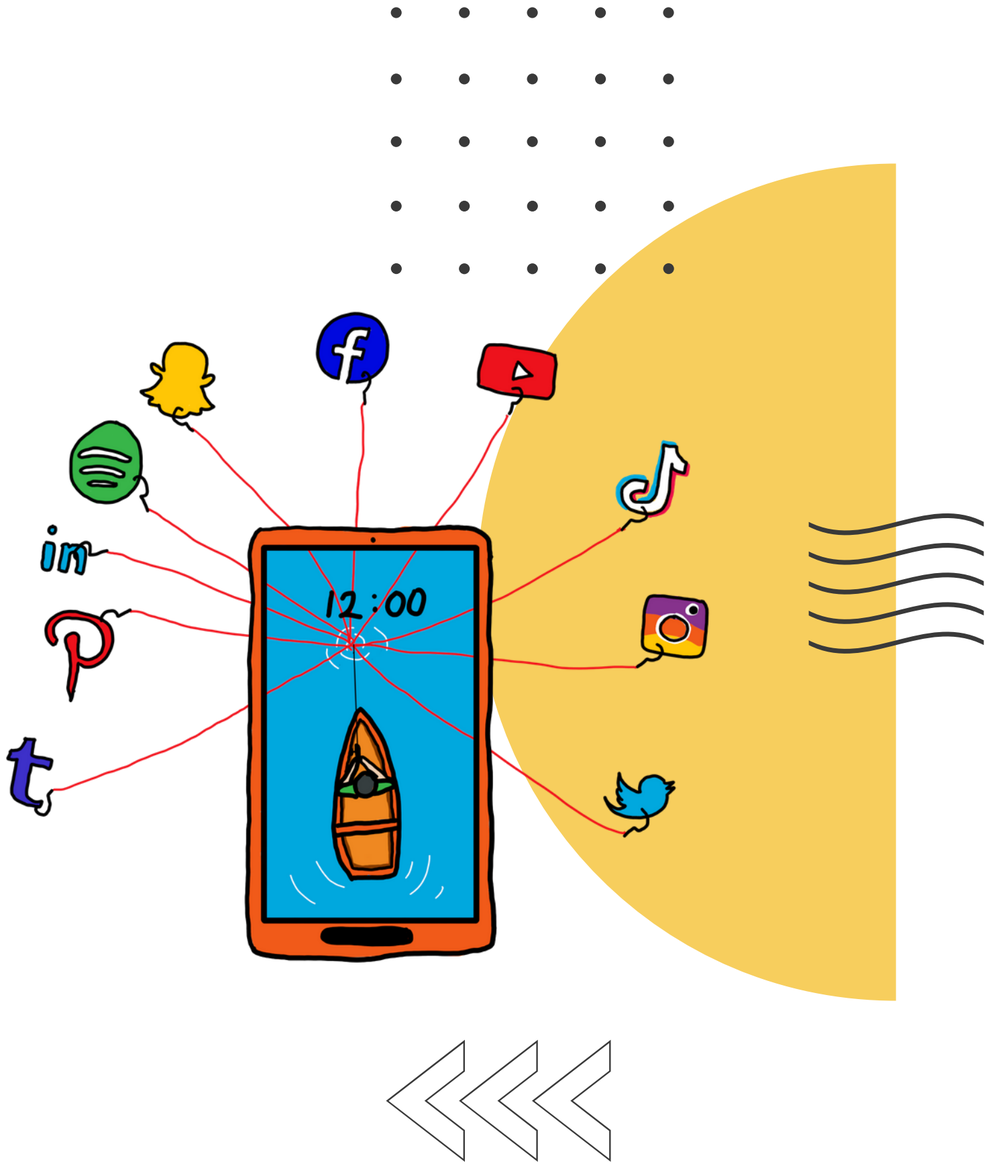
Wire

Email

11

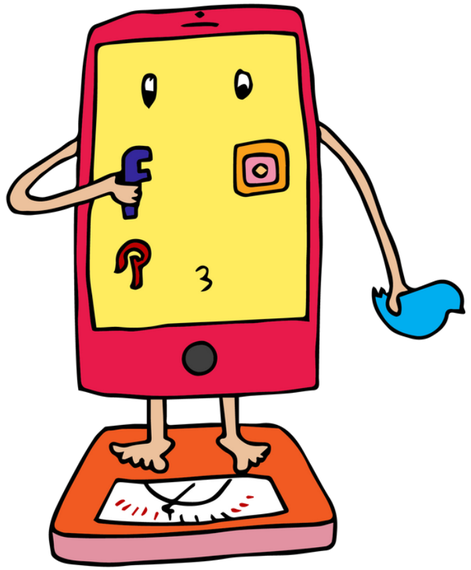
JANGAN TAUTKAN MEDIA SOSIALMU

Semakin kamu menghubungkan media sosialmu satu sama lain, semakin banyak data/informasi yang kamu berikan pada banyak pihak. Data/informasi di semua media sosial yang saling terhubung akan membuat orang mampu mengetahui identitasmu secara lengkap dan membuat profil tentangmu yang bisa digunakan untuk kepentingan komersial maupun (bisa jadi) politik.



12

LAKUKAN DATA DETOX



Ada baiknya bila kamu memeriksa kembali unggahan-unggahanmu di Internet selama ini. Apabila ada data/informasi personal atau sensitif yang pernah kamu unggah, lakukan penghapusan. Tentu jejak digital akan tetap ada, namun melakukan data detox akan membantu mengurangi jejak digital tersebut.

13

BERHATI-HATI MENGGUNAKAN WIFI PUBLIK

Wifi publik seringkali menjadi poin masuk (access point) peretasan atau serangan digital. Virus, malware dan spyware juga bisa ditanamkan melalui Wifi ini. Berhati-hatilah dalam menggunakan Wifi publik ini. Terutama jangan pernah menggunakan Wifi publik yang tidak menggunakan password. Bila kamu terpaksa harus menggunakan, upayakan menggunakan VPN/Proxy untuk terkoneksi ke Internet.

14

JANGAN TINGGALKAN GAWAI TANPA DIKUNCI ATAU PENGAWASAN

Jangan tinggalkan gawaimu di tempat di mana kamu tidak sendirian tanpa pengawasan sama sekali. Dan bila diawasi oleh orang yang kamu percayai sekalipun, pastikan dalam keadaan terkunci. Ini bukan soal kemampuan mempercayai atau dipercayai orang terdekat, tapi soal membiasakan praktik aman dalam setiap situasi dan di setiap saat.

15

BERHATI-HATILAH BILA BEKERJA DI TEMPAT PUBLIK

Bila bekerja dengan gawaimu di tempat publik, perhatikan sekelilingmu. Pilihlah tempat duduk yang bisa menjamin terjaganya privasimu saat bekerja. Pastikan layar gawaimu hanya menghadap padamu dan tak ada orang lain yang bisa melihat atau mengintip apa yang tengah kamu kerjakan di gawaimu.

16
DISCONNECT BILA DIPERLUKAN

Internet terutama media sosial bisa menjadi faktor penyebab stress terutama apabila kita mengalami kekerasan/serangan. Ia juga bisa membuat kita kewalahan dengan banyaknya informasi yang ada. Sesekali memutus koneksi kita tidak apa-apa dan bahkan diperlukan untuk menjaga kesehatan mental dan juga fisik kita. Ingat keamanan yang holistik!

Disusun oleh: Dhyta Caturani
Ilustrasi oleh: Efi SH