
kaspersky
Halo!
Di buku ini, kamu akan mempelajari istilah penting dalam dunia maya. Kami akan memberitahumu hal bermanfaat apa yang bisa ditemukan di dalamnya dan bahaya apa yang mengintai. Bukalah buku ini dan lanjutkan perjalananmu!
kaspersky
Cybersecurity Alphabet

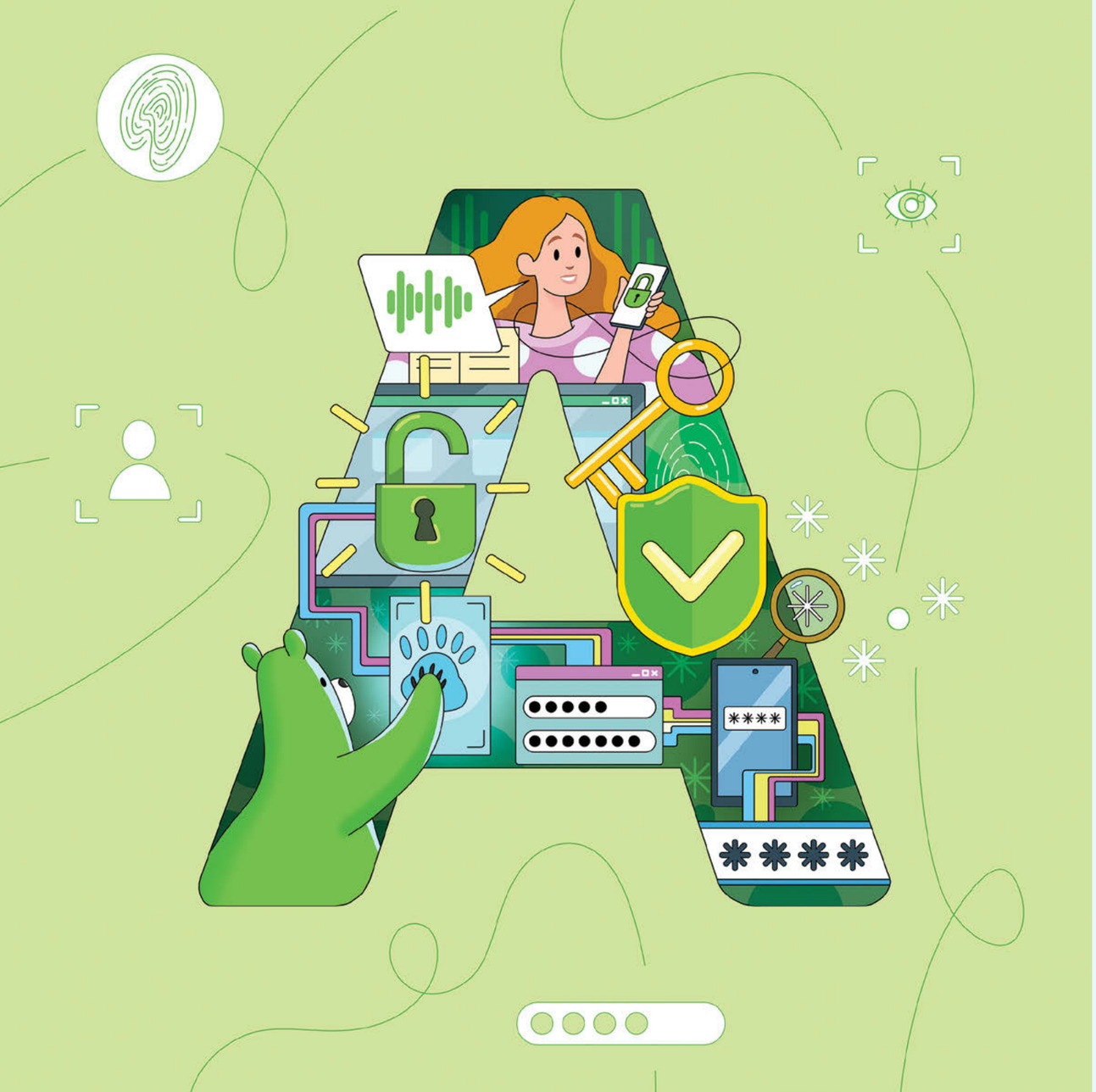
Buku ini milik _____

Halo Sobat,
Kamu lagi membaca buku Kaspersky Cybersecurity Alphabet. Pernah mendengar istilah “cybersecurity”? Cybersecurity atau keamanan siber membantu kita menggunakan teknologi modern — baik ponsel pintar maupun komputer — dengan aman dan kita bisa menjelajahi dunia maya tanpa khawatir dengan potensi ancaman.

Dunia digital ini luas. Kini kamu bisa melakukan banyak hal secara online: bepergian tanpa perlu meninggalkan rumah, atau belajar bahasa asing dengan penutur asli, misalnya. Tentu saja kamu bisa bermain game, bukan hanya dengan teman sekelas, tetapi juga dengan teman lainnya; bahkan dari tempat yang sangat jauh!

Namun, bersamaan dengan kesempatan yang begitu luas ini, ada bahaya di internet, seperti di dunia nyata. Jadi, waspadalah selalu. Tindakan online yang ceroboh dan mengabaikan aturan kesehatan siber bisa menimbulkan dampak buruk: tablet atau ponsel pintar bisa terinfeksi malware, informasi penting dibocorkan kepada penjahat siber, atau orang lain bisa mencuri hadiah dan kemajuanmu di game online favorit.

Di buku ini, kamu bisa mengetahui teknologi baru, mempelajari aturan kesehatan siber utama, mencari tahu cara menghindari ancaman online, dan mengenal trik para penipu. Agar perjalanan online-mu menyenangkan dan bebas dari pengalaman buruk, harap pelajari buku ini dari A hingga Z.



Autentikasi

Autentikasi berarti mempunyai kode rahasia khusus atau kata sandi yang membantumu mengakses komputer, ponsel, atau akun online.

Jika kamu ingin mengakses perangkat penting, seperti ponsel atau komputer sekolah, kamu perlu membuktikan diri sampai perangkat tersebut memercayaimu. Melalui “autentikasi”, kamu dapat memastikan bahwa hanya orang tepat yang diizinkan untuk menggunakan atau melakukan sesuatu di perangkat pribadi. Seperti itulah autentikasi: hanya orang tepat yang dipastikan boleh menggunakan perangkat tertentu!

Backup (Cadangan)

Cadangan adalah salinan informasi digital yang tidak ingin kamu hilangkan.

Cukup bayangkan: Salah satu game favorit ketinggalan di rumah saat kamu pergi berlibur, tetapi untunglah ibumu mempunyai salinannya di tempat penyimpanan khusus. Jadi, cadangan merupakan tempat khusus untuk menyimpan semua foto, video, dan berkas penting, supaya tidak hilang. Terkadang, hal tidak terduga dapat terjadi, atau ada kesalahan pada perangkat kita; perangkat dapat hilang atau tidak berfungsi. Namun, jika ada cadangannya, kita tidak perlu khawatir karena semua berkas favorit tersimpan di tempat aman. Jadi, ingatlah: selalu punya cadangan, supaya barang digital kita selalu terlindungi!

Captcha

Captcha merupakan tes khusus untuk memeriksa apakah kamu orang sungguhan yang menggunakan komputer atau robot yang menyamar menjadi manusia.

Pernahkah kamu diminta memecahkan teka-teki atau memilih gambar tertentu sebelum diizinkan untuk mengakses situs web atau bermain game online? Itulah Captcha! Kamu akan diminta melakukan sesuatu yang tidak bisa dilakukan robot dengan benar, seperti mengeklik kotak bergambar mobil atau lampu lalu lintas, atau mengetik huruf dan angka sulit. Cara ini akan melindungi situs web dan aplikasi dari robot jahat, alias spambot, yang mungkin berupaya untuk melakukan hal yang tidak pantas.

Digital footprint (Jejak digital)

Jejak digital merupakan jejak informasi kecil yang kita tinggalkan saat melakukan sesuatu di internet. Ibarat meninggalkan jejak di pasir saat kita berjalan di pantai.

Segala hal yang kita lakukan, seperti memosting gambar, menulis komentar, atau bahkan menyukai posting, bisa dilihat orang lain secara online. Penting untuk diingat bahwa jika sesuatu ditampilkan secara online, jejak digitalnya akan selalu ada selamanya. Oleh sebab itu, kita harus berhati-hati dengan perbuatan dan ucapan kita di internet, karena bisa berdampak terhadap cara pandang orang lain kepada kita.

E

Enkripsi

Enkripsi merupakan kode khusus untuk menjaga kerahasiaan. Saat mengirim pesan, kita menggunakan enkripsi untuk mengacak kata-katanya supaya tidak bisa diakses orang asing.

Enkripsi sangatlah penting karena melindungi pesan kita dari orang lain yang tidak berhak untuk melihatnya. Enkripsi akan senantiasa mengamankan informasi, seperti kata sandi dan informasi pribadi. Aplikasi dan situs web secara otomatis menggunakan alat enkripsi untuk menjaga kerahasiaan informasi.

Saat kita mengobrol dengan teman atau mengirim foto di media sosial, enkripsi juga digunakan untuk menjaga kerahasiaan pesan. Jadi, jika ada orang yang berupaya untuk mencuri pesan kita dari aplikasi yang memiliki fitur enkripsi, orang jahat ini hanya akan melihat huruf-huruf acak.

F

Fraud (Penipuan)

Disebut penipuan ketika ada orang yang melakukan tipu daya untuk mendapatkan detail pembayaran, uang, atau informasi pribadi korban mereka.

Para penipu menyamar menjadi orang lain, seperti teman atau orang kepercayaan. Mereka ingin kamu menceritakan rahasia atau memperdayamu supaya kamu mau membeli barang mereka yang sebenarnya tidak ada untuk menipu uang dan menyalahgunakan informasimu. Hindari para penipu dengan tidak mengunjungi situs web yang tidak diketahui, mengeklik pop-up, atau tautan yang tidak dikenal. Jangan percaya jika mereka mengatakan bahwa kamu memenangkan PlayStation atau uang. Dan tentu saja, jangan mengobrol secara online atau mengirim pesan kepada orang yang tidak dikenal. Dan jika seseorang membuatmu merasa janggal atau memintamu melakukan hal buruk, kabari orang dewasa yang kamu percayai.

Geolokasi

Geolokasi adalah teknologi yang memberi tahu perangkat, seperti ponsel dan komputer, lokasi kita di dunia. Teknologi ini dapat membantu kita saat bepergian, seperti menemukan toko es krim terdekat atau memberi tahu seberapa jauh lokasi teman kita.

Geolokasi merupakan rahasia terbesar. Jadi, kamu harus selalu memastikan bisa memercayai orang yang akan mendapatkan informasi ini. Baguslah jika Ayah dan Ibu mengetahui posisimu, tetapi jangan berikan geolokasimu secara online kepada orang yang tidak dikenal. Jika ada aplikasi yang meminta izin untuk mendapatkan geolokasi, tanyakan kepada diri sendiri: “Apakah aplikasi ini benar-benar membutuhkan lokasiku?”. Jika tidak, jangan berikan geolokasi kepada aplikasi ini.

Honeypot

Honeypot adalah perangkap yang dipersiapkan oleh pakar komputer untuk menangkap orang jahat yang berupaya melakukan hal buruk di internet.

Ini mungkin terlihat seperti situs web sungguhan, game, atau sesuatu yang menyenangkan, tetapi sebenarnya ini adalah perangkap untuk menangkap orang jahat. Pakar komputer akan mengawasi segala tindak tanduk orang jahat dan mempelajari trik mereka supaya kita tetap aman. Jadi, honeypot ini ibarat "alat mata-mata" yang melindungi kita di internet!

IP adress (Alamat IP)

Alamat IP merupakan alamat khusus yang menghubungkanmu ke internet.

Dengan alamat IP, internet bisa mengetahui ke mana informasi akan dikirimkan saat kamu menggunakan internet. Ibarat alamat rumahmu supaya petugas pos tahu ke mana surat diantar. Masing-masing titik koneksi internet memiliki alamat IP tersendiri.
Jika kamu bepergian dan membawa perangkat, alamat IP rumah tidak akan tertera di perangkat. Karena perangkatmu menggunakan jaringan lain (Wi-Fi di hotel, bandara, kafe) untuk menggunakan internet.

Jailbreak

Disebut jailbreak ketika seseorang melanggar aturan tentang cara kerja ponselnya.

Biasanya kamu hanya bisa mengunduh aplikasi yang diizinkan di app store. Namun, jika kamu melakukan jailbreak, kamu bisa mengunduh dan menggunakan aplikasi apa pun yang tidak diizinkan. Mungkin terkesan menyenangkan, tetapi kamu bisa mendapat masalah. Perangkat bisa berhenti berfungsi, atau disalahgunakan orang jahat. Jadi, lebih baik mengikuti aturan dan tidak melakukan jailbreak pada perangkat kita. Jauh lebih baik jika perangkat digunakan secara wajar! Ingatlah, ada banyak aplikasi dan game menyenangkan yang aman dan tidak memerlukan jailbreak.

Keylogger

Keylogger adalah jenis program komputer yang diam-diam merekam/mencatat semua hal yang kamu ketik di komputer.

Keylogger akan mencatat dan menyimpan semua ketikan tombol-mu, termasuk pesan dan kata sandi. Agar terhindar dari keylogger, jangan mengunduh apa pun dari situs web yang tidak tepercaya... beberapa situs online berbahaya, seperti kehidupan nyata! Beberapa situs web akan memperdaya orang supaya mereka mengunduh peranti jahat seperti keylogger. Jadi, cukup lakukan pengunduhan dari situs web tepercaya dan mintalah izin orang tuamu.

Login

Login merupakan nama pengguna atau alamat email dan kata sandi untuk dapat masuk ke situs web, game, atau aplikasi favorit. Ini ibarat kunci pintu!

Lewat login, situs web atau aplikasi akan mengidentifikasimu, sehingga kamu bisa melakukan hal-hal menyenangkan, seperti bermain game, menonton video, atau mengobrol dengan teman. Login ibarat kode rahasia yang hanya kamu ketahui, sehingga kamu bisa menyimpan segala hal dengan aman dan bersenang-senang di tempat pribadi!

Buatlah nama pengguna unik sendiri. Ingat, jangan menggunakan nama asli atau tanggal kelahiran. Buatlah sesuatu yang spesial!

Malware

Malware ibarat serangga penyusup jahat yang bisa membuat komputer atau tabletmu sakit.

Malware bisa bersembunyi dalam berbagai objek yang kamu klik atau unduh, seperti game atau gambar keren, terutama jika diunduh dari situs web yang tidak tepercaya. Jika kamu membiarkannya masuk tanpa sengaja, malware bisa mengacak-acak berkas atau mencuri informasi pribadi, seperti kata sandi atau foto. Namun, jangan khawatir! Ibarat mencuci tangan untuk membunuh kuman, kamu dapat menggunakan program perlindungan keamanan siber supaya komputer tetap aman dari malware.

Untuk melindungi perangkatmu dari malware, jangan lupa menginstal dan menggunakan solusi keamanan yang komprehensif dan tepercaya, seperti Kaspersky Premium.

NFT

Bayangkan jika kamu mempunyai kartu koleksi spesial yang disukai semua orang. Namun, ini bukan sekadar kartu koleksi, ini kartu unik dan hanya kamu pemiliknya. Kartu koleksi ini disebut Non-Fungible Token, atau disingkat NFT.

NFT merupakan objek digital khusus berupa karya seni, musik, video, atau bahkan hewan peliharaan virtual. Objek ini berbeda dengan uang atau kartu koleksi biasa karena masing-masing NFT unik, seperti dirimu! NFT tidak bisa ditukar dengan objek lain dengan nilai yang sama.

NFT ibarat sertifikat atau bukti kepemilikan sesuatu yang spesial di dunia digital. Orang-orang bisa membeli dan menjual NFT menggunakan sesuatu yang berkaitan dengan teknologi blockchain. Ini ibarat kamu memiliki jaringan komputer khusus yang menyimpan catatan pemilik setiap NFT. Teknologi ini bisa mencegah penipuan atau kebohongan memiliki NFT orang lain.

Oversharing
(Pengungkapan berlebihan)

Pengungkapan berlebihan berarti kita menyampaikan informasi tentang diri sendiri kepada seseorang secara berlebihan.

Berhati-hatilah saat menyampaikan hal pribadi kepada orang yang tidak begitu dikenal, misalnya informasi unik tentang diri sendiri yang bisa membedakanmu dari orang lain (nama, tanggal kelahiran, informasi kontak, sekolah, lokasi, dsb.). Berhati-hatilah juga dengan beberapa fakta yang terkesan tidak begitu penting, seperti tanggal kelahiran hewan peliharaan. Informasi pribadi atau fakta apa pun tentang diri sendiri yang kamu ceritakan kepada seseorang, termasuk kehidupan online pribadi, bisa dimanfaatkan oleh orang asing untuk meraih kepercayaanmu. Sebelum menceritakannya secara online, tanyakan kepada diri sendiri apakah kamu ingin menceritakannya kepada orang asing di jalan.

Phishing

Phishing berarti saat penjahat siber berupaya untuk memperdayamu dan mencuri informasi pribadi, seperti nama depan dan belakang, nama login, atau nomor rekening bank (jika kamu atau orang tuamu menggunakannya untuk membeli barang secara online).

Mereka bisa mengirim email dan pesan, atau bahkan membuat situs web palsu yang terlihat sungguhan, tetapi sebenarnya untuk mencuri informasimu. Jadi, berhati-hatilah dan jangan pernah memberikan informasi pribadi kepada siapa pun, kecuali kamu benar-benar yakin itu aman. Sayangnya, tidak semua orang yang kita temui secara online adalah orang baik. Jadi, berhati-hatilah saat memberikan alamat email kepada orang lain. Terkadang mereka berpura-pura baik agar kamu teperdaya dan mau memberikan informasi pribadi, tetapi jangan pernah memberi tahu nama lengkap, alamat, nomor ponsel, atau kata sandi kepada siapa pun secara online, kecuali orang dewasa yang kamu percayai memperbolehkannya.

QR code (Kode QR)

Istilah QR berasal dari kata Quick Response (Respons Cepat). Tampilannya seperti gambar persegi yang terdiri dari banyak kotak kecil hitam dan putih dalam kotak yang lebih besar.

Walaupun terlihat seperti gambar lucu yang terdiri dari kotak-kotak hitam dan putih, kode QR sebenarnya serupa dengan kunci ajaib yang bisa membuka pintu rahasia. Untuk membukanya, kamu bisa mengarahkan kamera ponsel atau gawai khusus, lalu klik. Secara spontan, ini akan menjadi seperti peta harta karun yang membawamu ke tempat tertentu. Di kebun binatang, kamu bisa memindai kode QR, lalu situs web berisi fakta menarik tentang hewan yang kamu lihat akan muncul. Di buku, kamu akan dibawa ke situs web menyenangkan dengan kisah yang lebih lengkap.

Sayangnya, penjahat siber juga mengetahui cara memanfaatkan kode QR untuk berbuat jahat. Namun, untunglah ada program khusus yang memberitahumu apakah kode QR aman. Ingatlah juga untuk tidak mengunduh aplikasi dari kode QR, cukup unduh dari App Store atau Google Play.

Ransomware

Ransomware adalah program komputer yang bisa mengenkripsi semua berkas di perangkatmu.

Ransomware menyusup ke komputer dan diam-diam menguasai semua berkas penting: gambar, video, dan dokumen. Lalu sang pencipta ransomware menahannya dan meninggalkan pesan permintaan uang tebusan sebelum kamu boleh mendapatkan kembali semua berkasnya. Namun, ingatlah, jangan percayai mereka! Mereka bisa saja menghilang dan meninggalkan perangkat rusak meski kamu sudah membayar. Cukup beri tahu orang dewasa yang dipercayai supaya perangkat diperbaiki dan kamu tetap aman. Buatlah juga cadangannya — ibarat menyimpan level dalam game. Jadi, jika ada masalah, semua berkas tidak akan hilang.

Spam

Spam ibarat surat sampah, tetapi untuk email.

Terkadang orang mengirimi kita surat yang tidak dikehendaki atau dibutuhkan, ini juga berlaku dalam email. Email semacam ini bisa berupa penawaran barang yang tidak ingin kita beli atau bahkan berupa penipuan agar kita memberitahukan informasi pribadi. Berhati-hatilah dengan email spam. Jangan klik atau menanggapinya, sama seperti kita mencampakkan surat sampah tanpa membacanya. Cara terbaik untuk menghindari email spam adalah tidak memberitahukan alamat email-mu, kecuali diperlukan, dan jangan berikan kepada situs web yang tidak diketahui.

T

Trojan

Trojan adalah program yang bisa menguasai dan memanfaatkan komputer untuk berbuat jahat.

Trojan bisa menyamar sebagai game komputer atau program yang tidak berbahaya, padahal sebenarnya merupakan program penyusup yang ingin masuk ke komputermu, mencuri informasi, dan merusak berkas. Trojan biasanya bersembunyi di situs web yang tidak aman, dan punya banyak trik: misalnya kamu dijanjikan bisa mengunduh game mahal secara gratis atau menonton di komputer film yang hanya tayang di bioskop... Abaikan semua janji palsu itu dan cukup gunakan situs web terverifikasi dengan tanda centang hijau yang besar. Ingat, ibarat kamu melarang orang asing masuk ke rumah, berhati-hatilah jika ingin mengunduh sesuatu karena bisa saja itu Trojan penyusup. Untuk memastikannya, mintalah izin kepada orang tua sebelum kamu mengunduh apa pun ke komputer.

URL

URL merupakan alamat yang dimiliki semua objek online, misalnya situs web, gambar, buku online, dsb.

Ibarat alamat rumah supaya orang mengetahui lokasinya, URL memberi tahu browser internet ke mana harus mencari sebuah situs web. URL berupa kombinasi huruf, angka, dan simbol yang menghubungkanmu ke situs web yang tepat. URL situs web bisa dilihat di bilah alamat di bagian atas browser. Selalu perhatikan alamat URL, lalu bandingkan dengan nama resmi perusahaan/organisasi/toko atau hal apa pun. Jika URL terlihat janggal atau mencurigakan, mungkin kamu telah masuk ke situs web palsu atau phishing.

Vishing

Disebut vishing (atau phishing suara) ketika orang jahat menelepon atau memperdaya korbannya agar mereka mau menelepon berdasarkan pembenaran yang dibuat-buat, lalu memberitahukan informasi pribadi, seperti kata sandi, nomor kartu kredit, dan sebagainya, lewat telepon.

Misalnya, mereka bisa saja langsung meneleponmu atau mengirimkan email palsu yang terlihat sungguhan, sambil meminta panggilan darurat. Masalahnya jika orang berbicara lewat telepon, perhatian mereka mungkin teralihkan dan sulit berpikir jernih. Orang jahat mendesak dan membuat mereka gelisah, lalu meminta informasi penting, seperti nomor kartu kredit atau nama dan alamat. Kamu akan pura-pura diperingatkan: jika tidak memberikan informasinya sekarang, akan ada banyak uang yang dicuri dari kartumu. Jangan percayai mereka atau mereka akan mencuri uangmu! Selalu waspada dan jangan memberikan informasi pribadi lewat telepon, kecuali kamu yakin itu aman.

Wi-Fi

Wi-Fi ibarat protofon yang membantumu berkomunikasi dengan internet.

Wi-Fi berupa kotak di sudut ruangan yang membantumu menjelajahi internet. Kamu bisa menyampaikan keinginan – mengunjungi situs web atau mendengarkan musik – lalu Wi-Fi akan menanggapinya. Tanpa Wi-Fi, kamu tidak bisa menjelajahi internet. Untuk mencegah orang lain mencuri gambar atau berkas lain, lindungi Wi-Fi dengan kata sandi. Bersama anggota keluarga, buatlah kata sandi yang sulit ditebak dan beri tahukan hanya kepada orang yang dipercayai. Lagi pula, Wi-Fi paling aman ada di rumahmu. Tidak peduli betapa menyenangkan rasanya, jangan mau terhubung ke Wi-Fi gratis di toko atau restoran, karena mungkin itu tidak aman.

eXploit

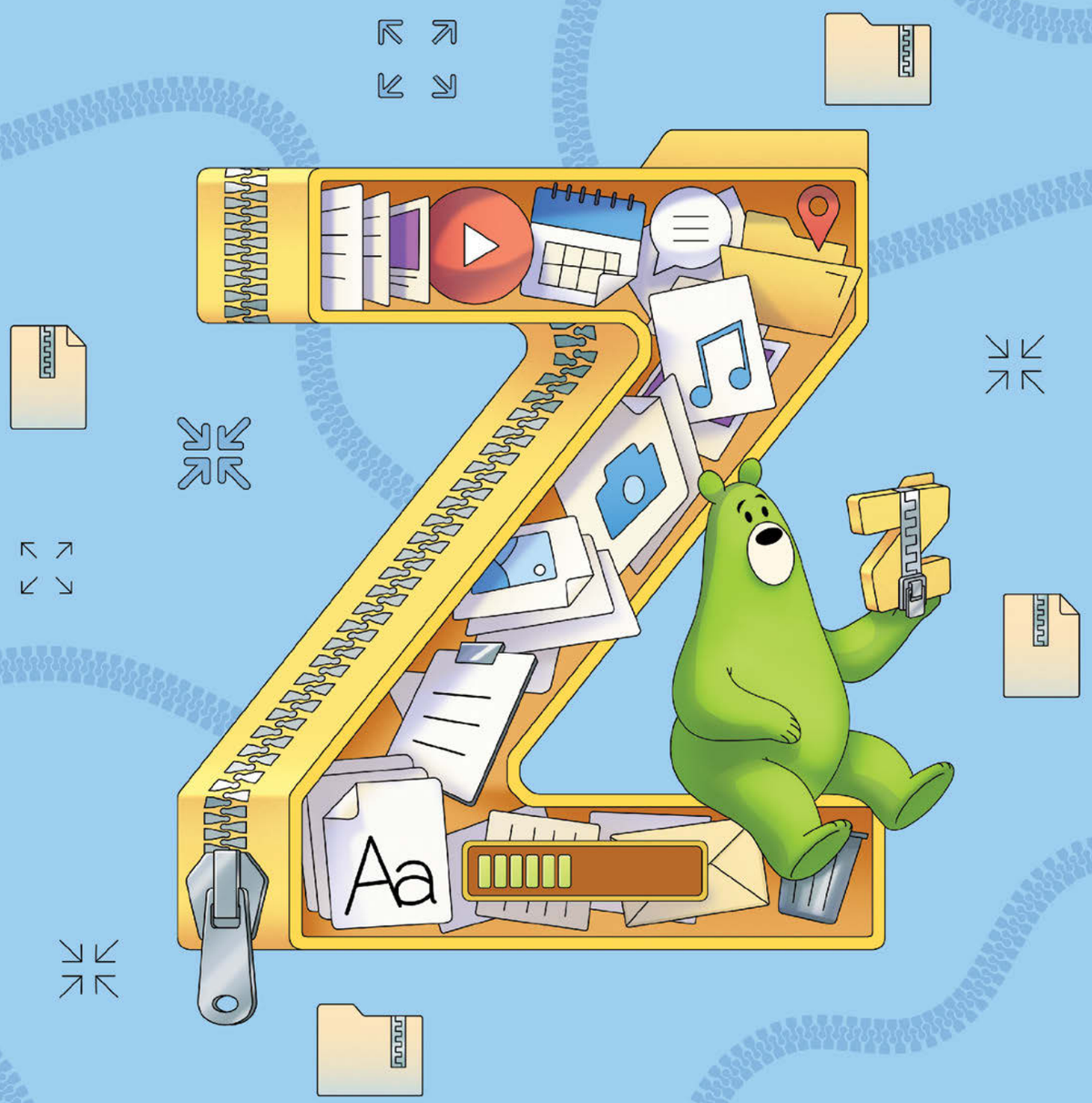
Exploit merupakan celah di komputer atau perangkat di mana penjahat siber bisa memasukinya, menginfeksinya dengan program jahat, dan mengendalikannya tanpa seizin kita.

Ini seperti cheat code di game online - setelah mengetahui cheat code ini, penjahat siber bisa melanggar aturan dan bebas melakukan apa saja di perangkatmu.

cyberbullYing (Perundungan siber)

Disebut perundungan siber jika seseorang bersikap kejam atau menyakiti orang lain secara online.

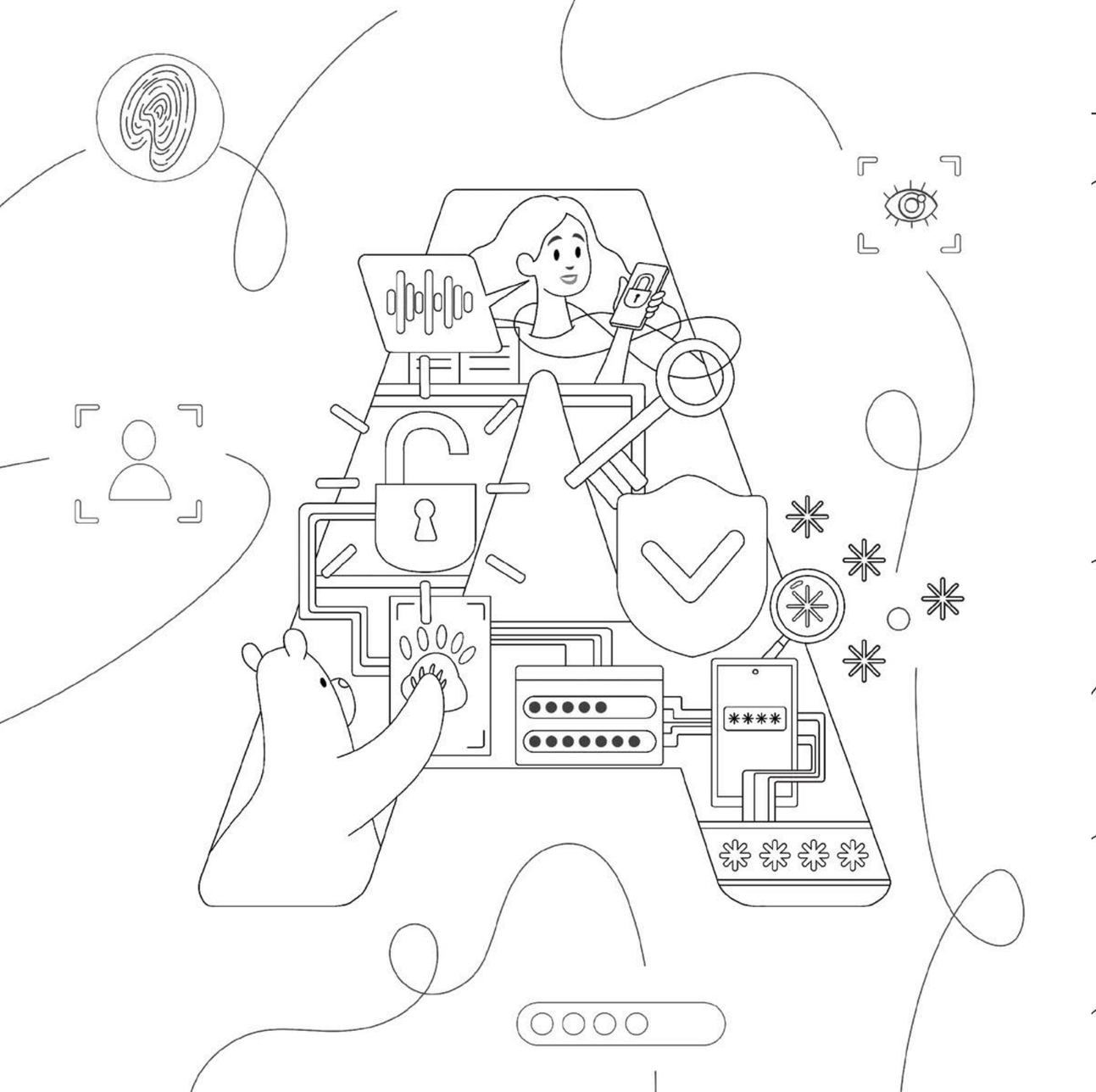
Ini bisa dilakukan dengan berbagai cara, seperti mengirim pesan jahat atau menyebarkan rumor tentang seseorang secara online. Perundungan siber bisa membuat orang lain sedih, malu, atau takut. Sebaiknya kita memperlakukan orang lain dengan baik secara online, seperti di dunia nyata. Jika kamu merasa dirundung secara online, ceritakan perasaanmu kepada orang dewasa yang kamu percayai. Perkataan perundung tentang dirimu tidak ada hubungannya dengan jati dirimu. Jadi, jangan menganggap serius perkataannya. Jangan merundungnya kembali, karena bisa memperburuk keadaan. Ambil tangkapan layar obrolanmu dengan si perundung, lalu blokir dia di platform itu.

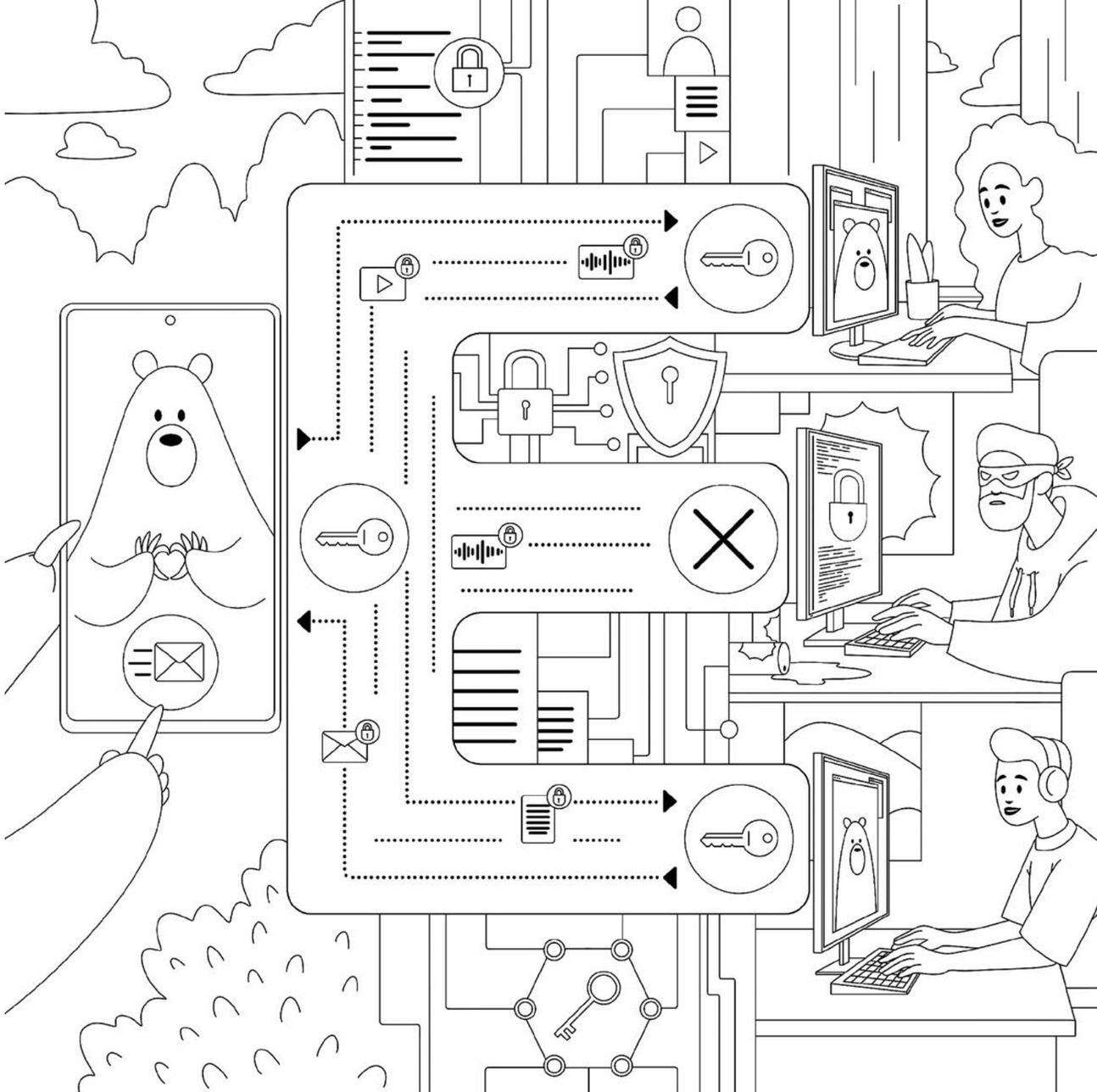


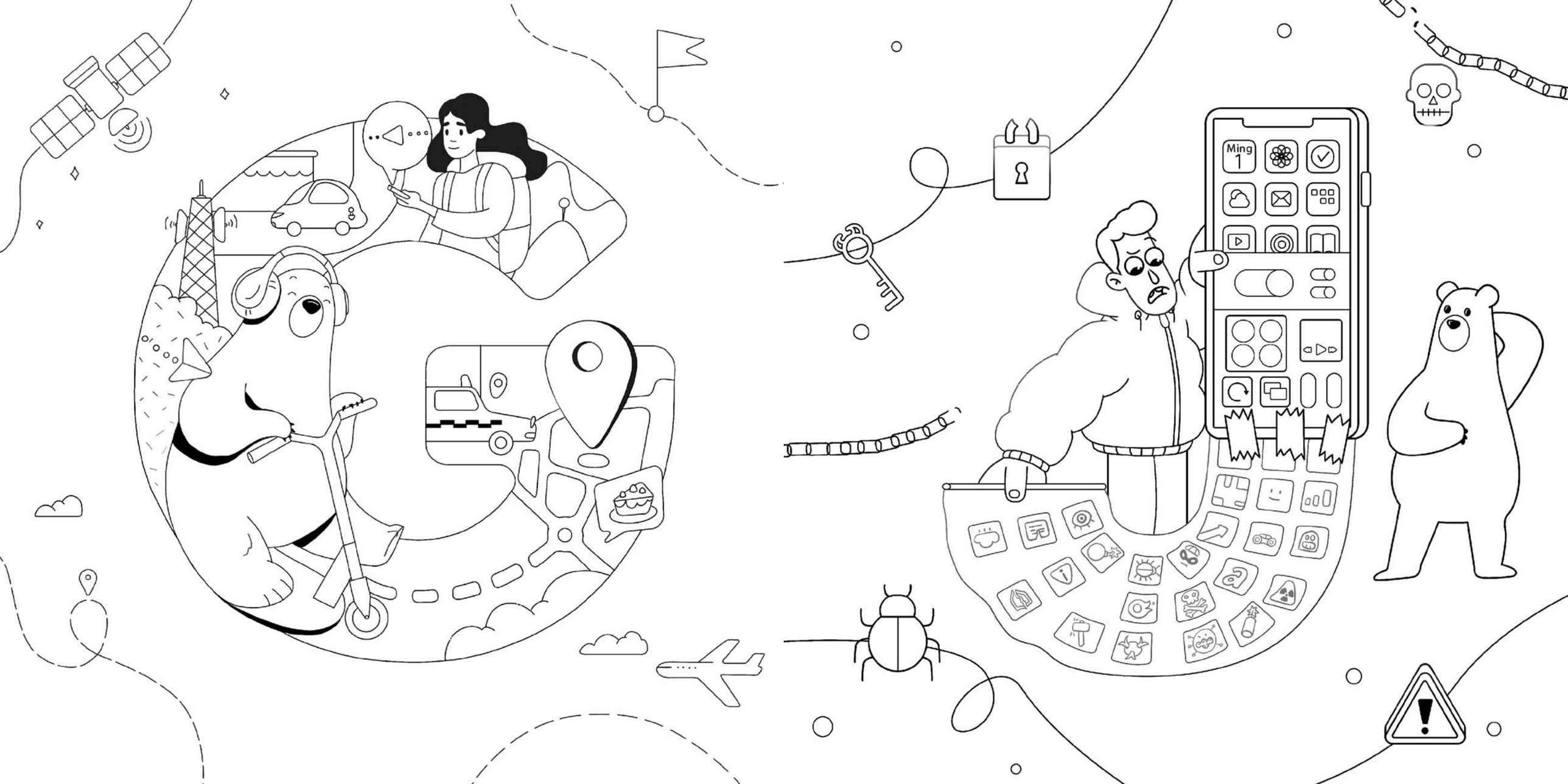
ZIP file (Berkas ZIP)

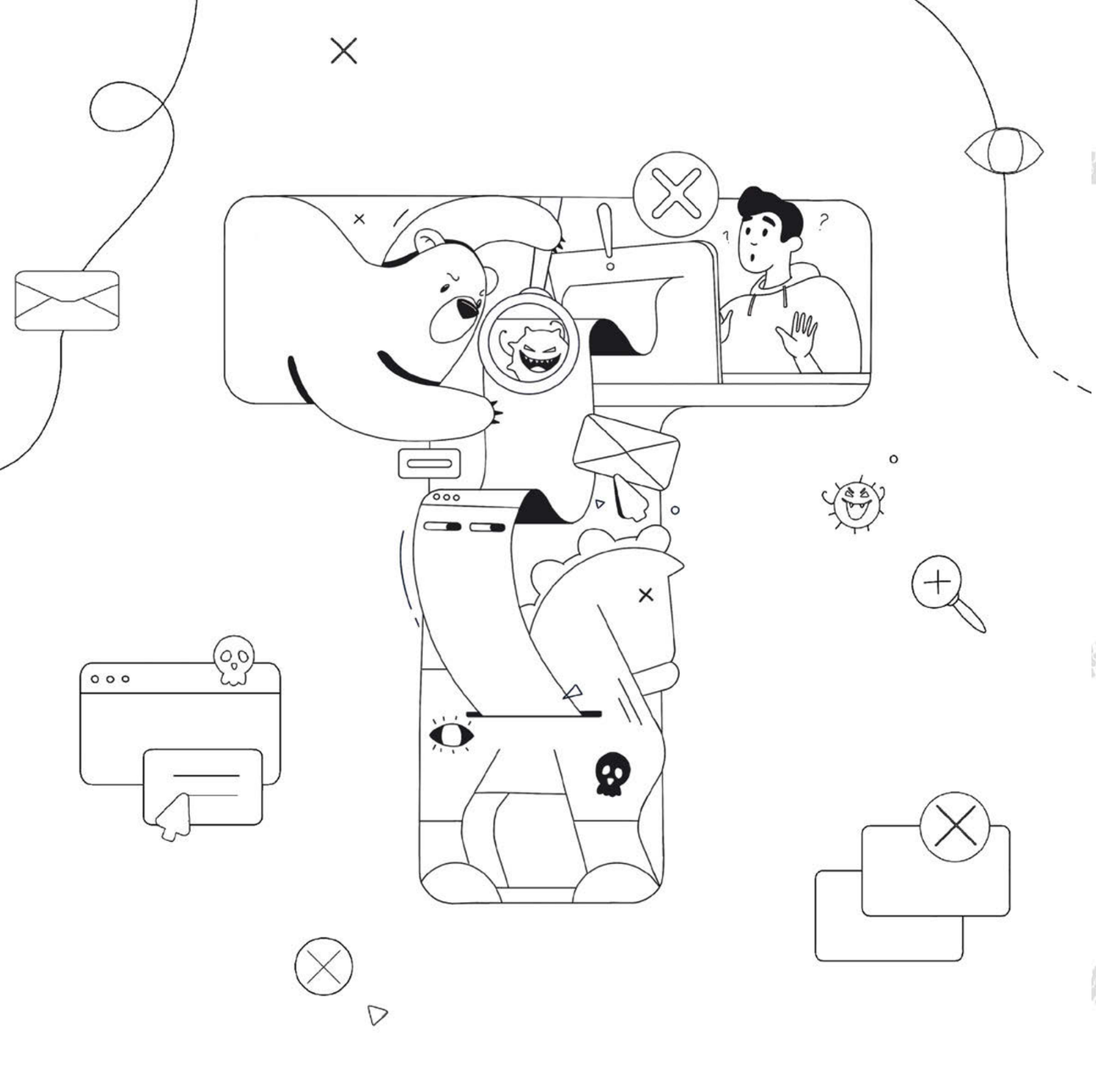
Berkas zip ibarat kantong yang bisa memuat banyak barang.

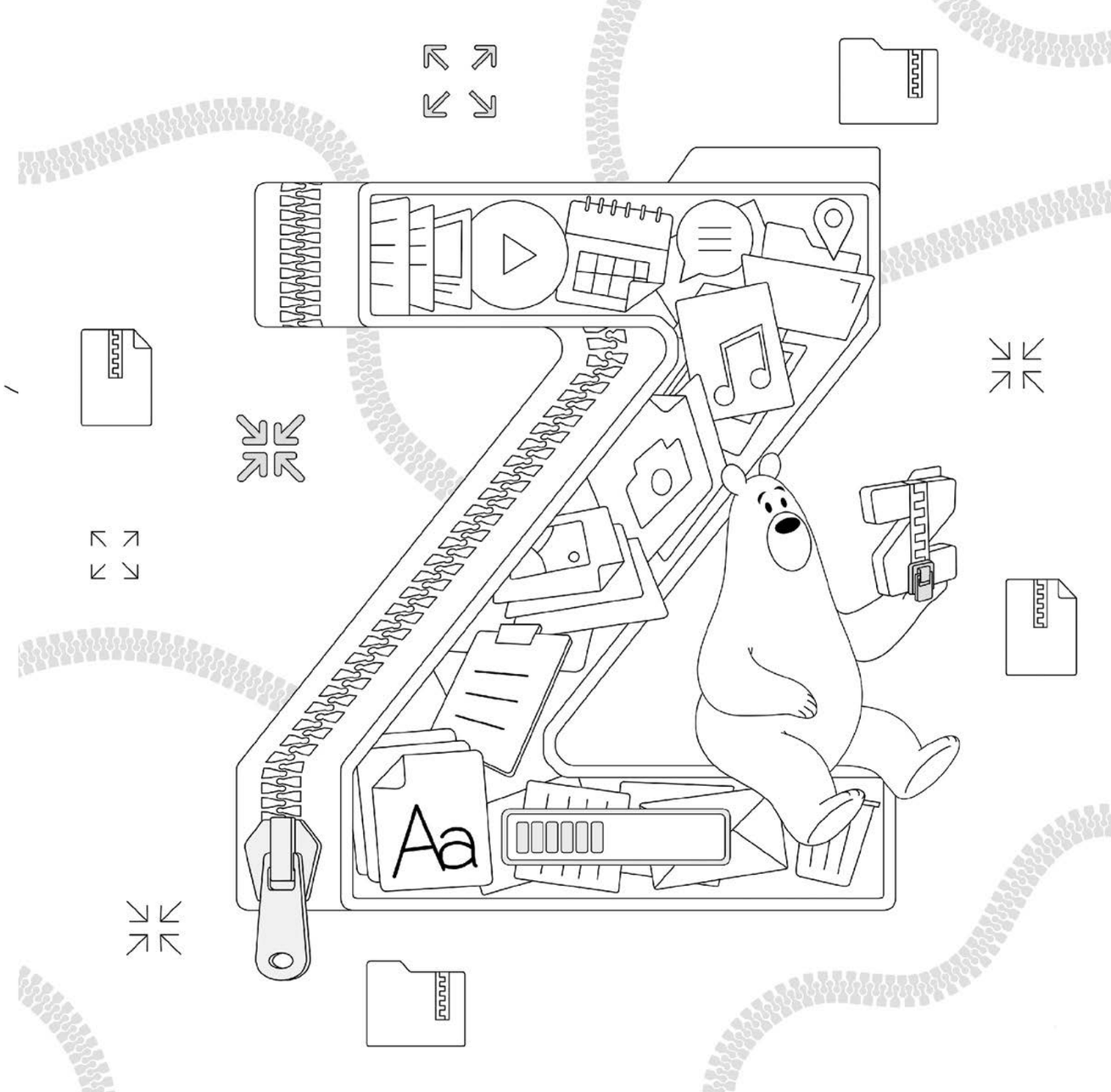
Berkas zip bisa menyimpan semua gambar, berkas, dan folder di satu tempat. Jika menggunakan sebuah berkas zip, kamu bisa memperkecil atau “mengompres” semua item, mengurangi ukurannya supaya bisa ditempatkan di ruang kecil dalam komputer. Ini seperti memampatkan semua barang sekaligus. Dan jika kamu ingin menggunakan objek-objek itu lagi, cukup buka kantong zip dan keluarkan semuanya.






Ming
1




Aa

Catatan

Halo Penjelajah Siber,

Sungguh pertualangan yang luar biasa! Dari A hingga Z, kamu telah melewati berbagai hal tidak terduga dalam keamanan siber. Namun, ingatlah bahwa keamanan di dunia maya sama seperti keamanan di dunia nyata. Ibarat pahlawan super, kamu punya kemampuan untuk menentukan pilihan cerdas secara online, seperti memilih kata sandi kuat, menjaga kerahasiaan informasi pribadi, dan berpikir dua kali sebelum mengeklik tautan yang tidak dikenal.

Pertualanganmu tidak berakhir sampai di sini. Dunia digital senantiasa berubah, dan ada begitu banyak hal yang bisa dipelajari. Pertahankan rasa ingin tahu, ajukan pertanyaan, dan tetap perbarui kecerdasan sibermu. Ajari teman-teman dan keluargamu abjad ABC keamanan online ini. Bersama-sama kita membangun dunia maya yang lebih aman.

Desain grafis, layout, dan ilustrasi oleh Agen Thoughtform:
www.behance.net/Thoughtform