kaspersky

Ciao!
Con questo libro imparerai i termini più importanti del mondo digitale. Ti spiegheremo quali sono gli aspetti positivi e i pericoli che invece si nascondono al suo interno.
Apri il libro e inizia il viaggio!

kaspersky

L'alfabeto della Cybersecurity

Questo libro appartiene a _____

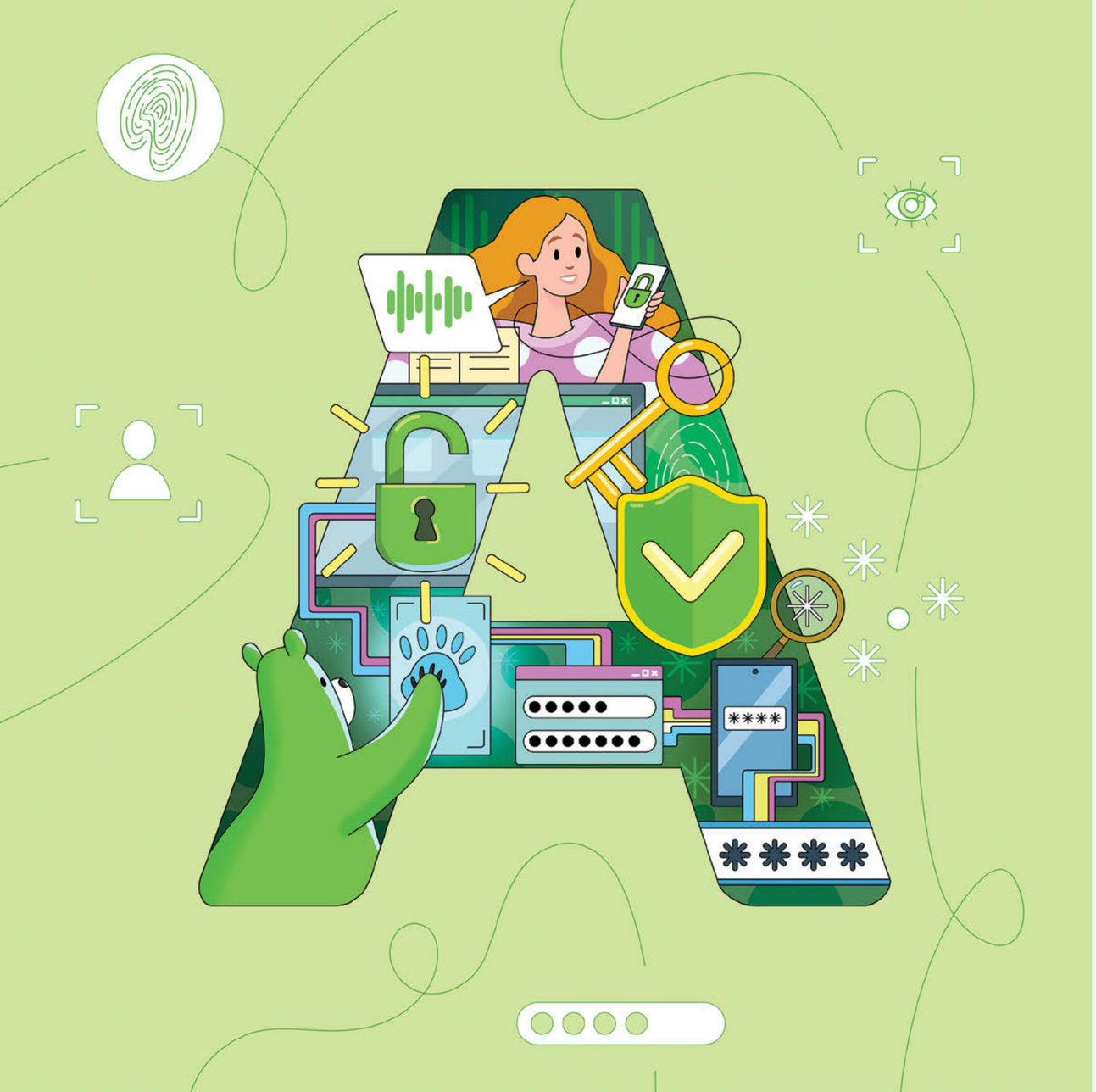
Caro amico,
stai tenendo tra le mani L'alfabeto della Cybersecurity di Kaspersky. Hai mai sentito parlare di cybersecurity? La cybersecurity o sicurezza informatica ci aiuta a utilizzare le moderne tecnologie - smartphone o computer - in modo sicuro e a esplorare il mondo online senza preoccuparci di eventuali minacce.

Il mondo digitale è immenso e oggi si possono fare molte cose online, ad esempio viaggiare senza uscire di casa o studiare lingue straniere parlando con persone madrelingua. E, naturalmente, si può giocare, non solo con i compagni di classe, ma soprattutto con gli amici, anche con quelli lontani!

Oltre alle infinite opportunità, su Internet ci sono anche alcuni pericoli, proprio come nella vita reale. È quindi necessario essere sempre attenti. Le azioni imprudenti online e non rispettare le regole di sicurezza informatica possono avere gravi conseguenze: si può infettare il tablet o lo smartphone con malware, esponendo informazioni importanti ai criminali informatici, oppure possono essere rubati i premi e i progressi ottenuti nel proprio gioco online preferito.

In questo libro potrai conoscere le nuove tecnologie, imparare le principali regole di sicurezza informatica, scoprire come evitare le minacce online e riconoscere i trucchi dei truffatori. Per essere certi che il tuo viaggio online sia entusiasmante e privo di esperienze negative, leggi attentamente questo libro dalla A alla Z.

Per aiutare i bambini a esplorare in sicurezza lo spazio online, abbiamo creato un'applicazione per genitori digitali: Kaspersky Safe Kids.



Autenticazione

L’autenticazione equivale ad avere un codice segreto speciale o una password che ti aiuta a entrare nel tuo computer, telefono o account online.

Quando vuoi accedere a un dispositivo importante, come il tuo telefono o il computer, devi dirgli che sei davvero tu e che può fidarsi. Grazie all’autenticazione, puoi essere sicuro che solo la persona giusta sia autorizzata a usare o a fare qualcosa sul tuo dispositivo. L’autenticazione serve proprio questo: assicurarsi che solo le persone autorizzate possano utilizzare dispositivi speciali!

Backup

Il backup è una copia delle informazioni digitali che non si vogliono perdere.

Prova a immaginare: hai perso uno dei tuoi giochi preferiti durante una vacanza, ma per fortuna tua mamma ne ha conservato uno identico in un luogo speciale. Allo stesso modo, il backup è un luogo speciale dove riporre tutte le foto, i video e i file importanti, in modo che non vadano mai persi. A volte capitano incidenti o problemi con i dispositivi, possono essere persi o smettere di funzionare. Ma con il backup non devi preoccuparti, perché tutte le tue cose preferite sono in un posto sicuro. Ricordati quindi di eseguire sempre un backup e i tuoi oggetti digitali saranno così protetti!

Captcha

Il captcha è un test speciale per verificare se sei una persona reale che utilizza un computer o un robot che finge di essere una persona.

Ti è mai capitato che ti sia stato chiesto di risolvere un puzzle o di selezionare alcune immagini prima di poter continuare a visitare un sito web o a giocare a un gioco online? Di solito si tratta di un captcha! Ti chiede di fare qualcosa che i robot non sono in grado di fare molto bene, come cliccare su caselle con automobili o semafori o digitare lettere e numeri difficili. Serve a proteggere i siti web e le app dai robot cattivi, noti anche come spambot, che provano a fare qualcosa di sconveniente.

Digital footprint

Il digital footprint o impronta digitale è una piccola traccia di informazioni che lasci dietro di te ogni volta che fai qualcosa su Internet. Proprio come lasciare le orme quando si cammina su una spiaggia.

Tutto ciò che fai, come postare foto, scrivere commenti o anche mettere like ai post, può essere visualizzato da altre persone online. È importante ricordare che quando qualcosa è online, ci rimane per sempre. Per questo motivo devi fare attenzione a quello che fai e dici su Internet, perché può influenzare il modo in cui gli altri ti vedono.

Encryption

La crittografia (encryption) è come un codice speciale che mantiene un segreto. Quando vogliamo inviare un messaggio, usiamo la crittografia per codificare le parole e renderle inaccessibili agli estranei.

La crittografia è molto importante perché aiuta a proteggere i messaggi da persone che non dovrebbero vederli. Mantiene al sicuro le tue informazioni, come password e dati personali. Le applicazioni e i siti web utilizzano automaticamente strumenti di crittografia per proteggere le informazioni. Anche nei social media, ad esempio quando chatti con i tuoi amici o invii foto, la crittografia viene utilizzata per mantenere privati i tuoi messaggi. In questo modo, se qualcuno tenta di accedere al tuo messaggio e l'app è dotata di crittografia, il malintenzionato vedrà solo caratteri criptati.

Frode

Si parla di frode quando alcune persone ci ingannano per farsi dare dati di pagamento, denaro o informazioni personali.

I truffatori fingono di essere chi non sono, come un amico o qualcuno di cui ti fidi. Vogliono che gli sveli qualcosa di segreto o ti inducono ad acquistare oggetti che non sono reali, in modo da rubarti il denaro e utilizzare le tue informazioni per fare qualcosa di brutto. Per essere al sicuro dai truffatori, non andare su siti web sconosciuti, non cliccare su pop-up o link che non conosci. Non credere quando ti dicono che hai vinto una PlayStation o del denaro. E naturalmente, non chattare online o non inviare messaggi a persone che non conosci nella vita reale. Inoltre, se qualcuno ti fa sentire strano o ti chiede di fare cose poco piacevoli, dillo a un adulto di cui ti fidi.

Geolocalizzazione

La geolocalizzazione è una tecnologia che indica ai dispositivi, come smartphone e computer, la tua posizione. La geolocalizzazione ti aiuta a spostarti da un luogo all'altro, ad esempio a trovare la gelateria più vicina o a sapere quanto solo lontani i tuoi amici.

La geolocalizzazione è il più grande segreto che hai. Per questo motivo, devi sempre essere sicuro di poterti fidare delle persone con cui condividi queste informazioni. È bello che mamma e papà sappiano dove ti trovi, ma non dovresti condividere la tua geolocalizzazione con estranei online. Se un'app ti chiede il permesso di avere accesso alla tua geolocalizzazione, dovresti domandarti: "Questa app ha davvero bisogno di sapere dove mi trovo?". In caso contrario, non dovresti autorizzare l'accesso alla localizzazione a questa app.

Honeypot

Un honeypot è una trappola creata da esperti informatici per catturare i malintenzionati che cercano di fare cose scorrette su Internet.

Potrebbe sembrare un sito web reale, un gioco o qualcosa di divertente, ma in realtà è un trucco per catturare i malintenzionati. Gli esperti informatici osservano tutto ciò che fanno i cybercriminali e imparano a conoscere i loro trucchi per proteggerci. Gli honeypot sono quindi "strumenti segreti di spionaggio" che ti aiutano a difenderti su Internet!

Indirizzo IP

Un indirizzo IP è un indirizzo speciale che ti collega a Internet.

Aiuta Internet a sapere dove inviare le informazioni quando si utilizza la rete. È come l'indirizzo di casa che indica al postino dove consegnare le lettere. Ogni punto di connessione a Internet ha un proprio indirizzo IP. Se sei fuori casa per un viaggio e porti con te il tuo device, l'indirizzo IP di casa non è collegato al dispositivo perché utilizzerà una rete diversa (Wi-Fi di un hotel, di un aeroporto o di un bar) per collegarsi a Internet.

Jailbreak

Il jailbreak avviene quando qualcuno infrange le regole di utilizzo del proprio telefono.

Normalmente, è possibile scaricare solo le applicazioni consentite dall'app store ma quando si esegue il jailbreak, si può effettuare il download e utilizzare tutti i tipi di app che di solito non sono permessi. Può sembrare divertente, ma può metterti nei guai. Può far sì che il dispositivo non funzioni bene o addirittura permettere a persone malintenzionate di usarlo in modo scorretto. È quindi importante seguire sempre le regole e non eseguire il jailbreak dei nostri dispositivi. È molto meglio usare i nostri dispositivi nel modo in cui devono essere usati! E ricorda che ci sono molte applicazioni e giochi divertenti che sono sicuri e non necessitano di jailbreak.

Keylogger

Un keylogger è un tipo speciale di programma per PC in grado di registrare segretamente tutto quello che viene digitato su un computer.

Un keylogger ricorda ogni tasto premuto e lo salva. In questo modo, può conservare informazioni come messaggi e password. Per evitare i keylogger, non scaricare nulla da siti web di cui non sei sicuro... alcuni luoghi online sono pericolosi, proprio come nel mondo reale! Alcuni siti web tentano di ingannare le persone per far loro scaricare file dannosi come i keylogger, quindi salva solo da siti web affidabili e chiedi il permesso ai tuoi genitori.

Login

Il login è il nome utente o l'indirizzo e-mail e la password che consentono di accedere al sito web, al gioco o all'applicazione preferiti. È come una chiave speciale per aprire la porta!

Permette al sito web o all'app di sapere chi sei e ti consente di fare cose divertenti come giocare, guardare video o chattare con gli amici. Il login è come un codice segreto che solo tu devi conoscere, così puoi tenere al sicuro le tue cose e divertirti nel tuo spazio speciale!

Crea un nome utente unico che hai solo tu. Ricorda che non deve includere il tuo vero nome o la tua data di nascita. Cerca di creare qualcosa di unico!

Malware

Il malware è un virus informatico subdolo e cattivo che può far ammalare il computer o il tablet.

Può nascondersi in diversi oggetti su cui clicchi o che scarichi, come giochi o immagini, soprattutto se ti trovi su siti web non affidabili. Se lo si lascia entrare per sbaglio, può incasinare i file o cercare di rubare le informazioni personali come password o immagini. Ma non preoccuparti! Proprio come lavarsi le mani aiuta a tenere lontani i germi, è possibile utilizzare programmi di protezione informatica per tenere il computer al sicuro dai malware.

Per proteggere i tuoi dispositivi dal malware, non dimenticare di installare e usare una soluzione di sicurezza completa e affidabile, come Kaspersky Premium.

NFT

Immagina di avere una carta speciale che tutti desiderano. Ma non è una carta qualsiasi: è una carta unica e può appartenere solo a te. Questa carta si chiama Non-Fungible Token, NFT.

Un NFT è un oggetto digitale speciale che può rappresentare opere d'arte, musica, video o persino animali domestici virtuali. È diverso dal denaro o dalle classiche carte collezionabili perché ogni NFT è unico, proprio come te! Non può essere scambiato con altri oggetti dello stesso valore.

Gli NFT sono come un certificato o una prova di possesso di qualcosa di speciale nel mondo digitale. Le persone possono comprare e vendere NFT utilizzando una tecnologia chiamata blockchain. È come avere una rete di computer speciale che registra chi possiede ogni NFT, in questo modo ci si assicura che nessuno imbrogli o finga di possedere un NFT che in realtà non è suo.

Oversharing

Si parla di oversharing quando si racconta a qualcuno online più di quanto si dovrebbe.

Fai sempre attenzione a dire a persone che non conosci veramente qualcosa di personale su di te: informazioni che permettono di distinguerti dagli altri (nome, compleanno, dati di contatto, scuola, località e così via). Fai attenzione anche a fatti che non sembrano così importanti, come il compleanno del tuo cane o del tuo gatto. Le tue informazioni personali o i fatti che racconti a qualcuno su di te e sulla tua vita online possono essere utilizzati da sconosciuti per ottenere la tua fiducia. Prima di condividere o pubblicare informazioni su di te online, chiediti se le diresti a un estraneo che incontri per strada.

Phishing

Il phishing consiste nel tentativo da parte dei criminali informatici di ingannarti e di rubare le tue informazioni, come nome e cognome, login o numero di conto corrente (se tu o i tuoi genitori lo utilizzate per acquistare qualcosa online).

Potrebbero inviarti e-mail e messaggi o persino creare siti web falsi che sembrano reali, ma in realtà stanno cercando di rubare le tue informazioni. È quindi importante fare attenzione e non condividere mai i tuoi dati personali con nessuno, a meno che non si sia assolutamente certi che siano al sicuro. Sfortunatamente, non tutti quelli che si incontrano online sono brave persone, ed è davvero importante fare attenzione a chi si rivela il proprio indirizzo e-mail. A volte le persone possono tentare di ingannare l'utente per indurlo a fornire le proprie informazioni personali, ma non bisogna mai fornire a nessuno online informazioni come nome e cognome, indirizzo, numero di telefono o password, a meno che non sia un adulto fidato a dirlo.

QR code

QR Code corrisponde a “quick response”, cioè risposta rapida. Si presenta come un’immagine quadrata composta da tanti piccoli moduli neri disposti all’interno di un riquadro bianco.

Anche se sembra una strana immagine, un codice QR è in realtà come una chiave magica che apre una porta segreta. Per aprirla, base puntare la fotocamera del telefono o di un altro dispositivo e cliccare. In un attimo, il codice si trasforma in una mappa del tesoro che ti condurrà in luoghi speciali. Allo zoo, si può scansionare il QR code e compare un sito web con informazioni interessanti sull’animale che si sta osservando. In un libro, può rimandare a un sito web divertente che racconta la storia. Purtroppo, anche i criminali informatici sanno come utilizzare i QR Code ma per compiere azioni dannose. Per fortuna esiste un programma speciale che ti dice se il QR code è sicuro. Ricorda di non scaricare mai un’applicazione da un QR Code, ma solo quelle sicure dall’App Store o da Google Play.

Ransomware

Il ransomware è un programma informatico in grado di criptare tutti i file presenti sul dispositivo.

Il ransomware si insinua nel computer e sottrae tutti i file importanti: immagini, video e documenti. I malintenzionati che hanno creato il ransomware li portano via, lasciando una nota in cui ti dicono di consegnare loro del denaro per poterli riavere. Non fidarti mai di ciò che dicono! Potrebbero semplicemente sparire lasciandoti con un dispositivo danneggiato anche se hai pagato. Devi dirlo a un adulto, in modo che possa risolvere il problema e tenerti al sicuro. Inoltre, fai un backup: è come salvare un livello in un gioco e se qualcosa va storto, non perderai nulla.

Spam

Lo spam è come la posta indesiderata, ma per la tua e-mail.

Così come a volte ricevi posta che non vuoi o di cui non hai bisogno, anche le persone ti inviano e-mail indesiderate o non necessarie. Queste e-mail possono essere pubblicità di prodotti che non vogliamo acquistare o addirittura truffe che cercano di indurci a fornire i nostri dati personali. È importante fare attenzione alle e-mail di spam ed evitare di aprirle o rispondere, proprio come si butta via la posta indesiderata senza leggerla. Il modo migliore per evitare le e-mail di spam è quello di non fornire il proprio indirizzo e-mail a meno che non sia veramente necessario e di non lasciarlo su siti web sconosciuti.

Trojan

I trojan sono programmi informatici che possono prendere il controllo del computer e utilizzarlo per compiere azioni dannose.

Un trojan finge di essere un gioco per PC o un programma innocuo, ma in realtà è un “furbetto” che vuole entrare nel tuo computer, rubare le tue informazioni e distruggere i tuoi file. I trojan di solito si nascondono in siti web non sicuri e utilizzano molti trucchi: dicono che puoi scaricare gratuitamente giochi costosi o vedere sul tuo computer un film che è in programmazione solo al cinema... Ignora questi finti regali e utilizza solo siti verificati, quelli con una grande segno di spunta verde. Ricorda che, proprio come non lasci entrare estranei in casa tua, fai attenzione a ciò che scarichi perché potrebbe essere un subdolo Trojan.

URL

L'URL è un indirizzo che hanno tutti gli oggetti online: siti web, immagini, libri, ecc.

Proprio come la tua casa ha un indirizzo che permette alle persone di raggiungerla, un URL indica al tuo browser Internet dove trovare un sito web. Si tratta di una combinazione di lettere, numeri e simboli che aiutano a collegarsi al sito web giusto. L'URL di un sito web si trova nella barra degli indirizzi nella parte superiore del browser. Presta sempre attenzione all'indirizzo URL e confrontalo con il nome ufficiale di un'azienda/organizzazione/negozio o altro. Se l'URL ha un aspetto strano o sospetto, potrebbe significare che ti trovi su un sito di phishing o falso.

VPN

La VPN (Virtual Private Network) è uno strumento che rende più sicura la navigazione in Internet.

È come un tunnel segreto su Internet che mantiene le tue attività online private e sicure. Proprio come un nascondiglio a cui solo tu puoi accedere. La VPN sposta i tuoi dati in un luogo speciale protetto e funziona come una maschera: i siti web che visiterai non otterranno le tue informazioni, ma vedranno invece la maschera che il servizio VPN mostrerà loro. Proprio come non vorresti che un estraneo sbirciasse nel tuo diario o nella tua camera, una VPN aiuta a proteggere le tue attività online da estranei che potrebbero cercare di accedere ai tuoi dati personali.

Wi-Fi

Il Wi-Fi è come un walkie talkie che aiuta a comunicare con Internet.

Il Wi-Fi è la scatola nell'angolo della stanza che ti aiuta a navigare su Internet. Gli si dice cosa si vuole fare – andare su un sito web o ascoltare musica – e il Wi-Fi risponde. Senza, non si può accedere a Internet. Per evitare che qualcuno rubi le tue foto o altri file, proteggi il tuo Wi-Fi con una password. Insieme alla tua famiglia, rendi la password difficile da indovinare e comunicala solo alle persone di cui vi fidate. Inoltre, il Wi-Fi più sicuro è quello di casa tua.
Per quanto possa sembrare entusiasmante, non collegarti a quello "gratuito" in negozi o ristoranti, perché potrebbe non essere protetto.

eXploit

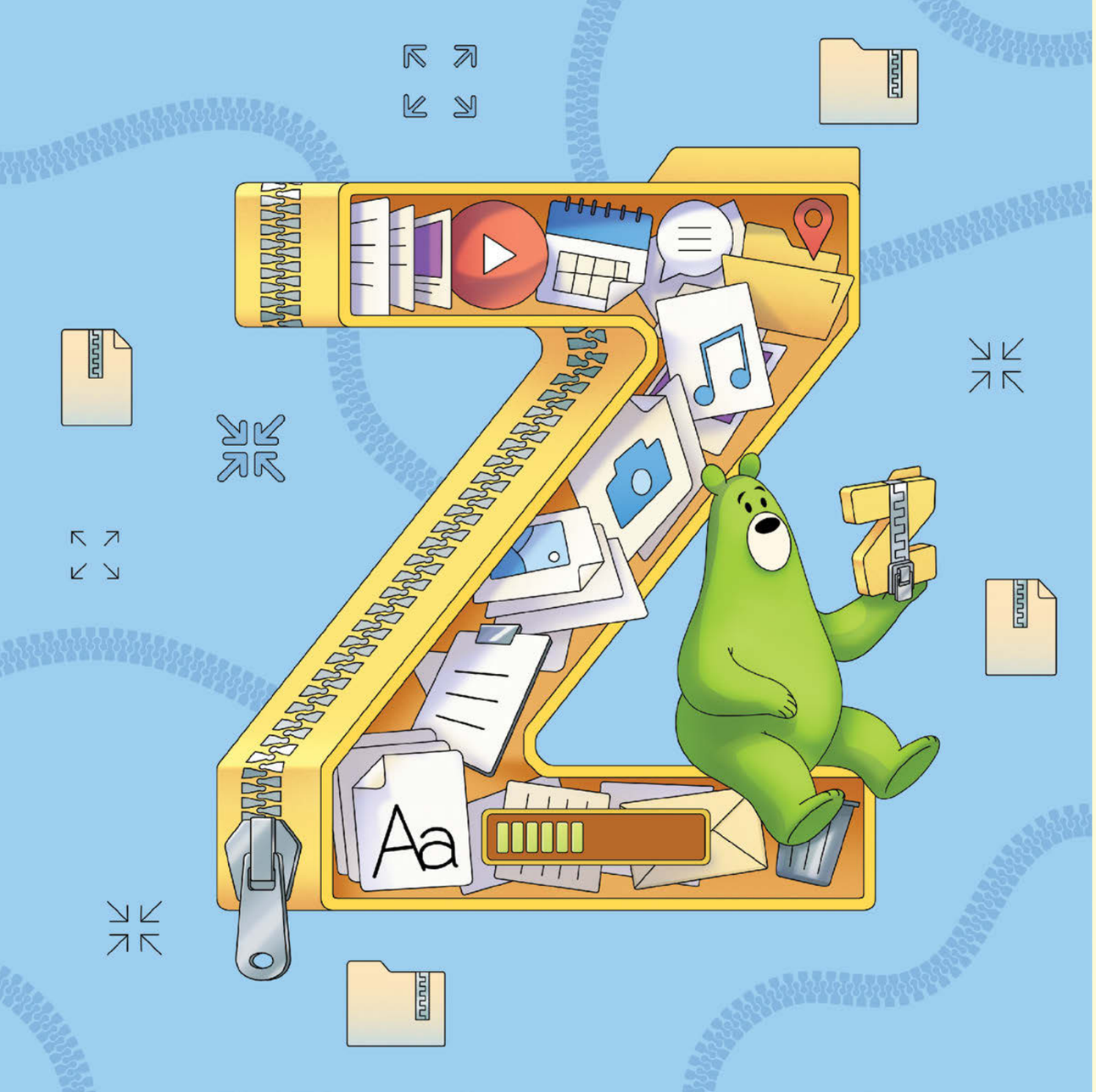
Un exploit è una falla nel computer o nel dispositivo che consente ai criminali informatici di entrare, infettarlo con un programma dannoso e ordinargli cosa fare senza il tuo permesso.

È come un codice cheat in un gioco online: conoscendo questi codici, i criminali informatici possono infrangere le regole e fare quello che vogliono con il tuo dispositivo.

cYberbullismo

Il cyberbullismo si verifica quando qualcuno è cattivo o offensivo nei confronti di altre persone online.

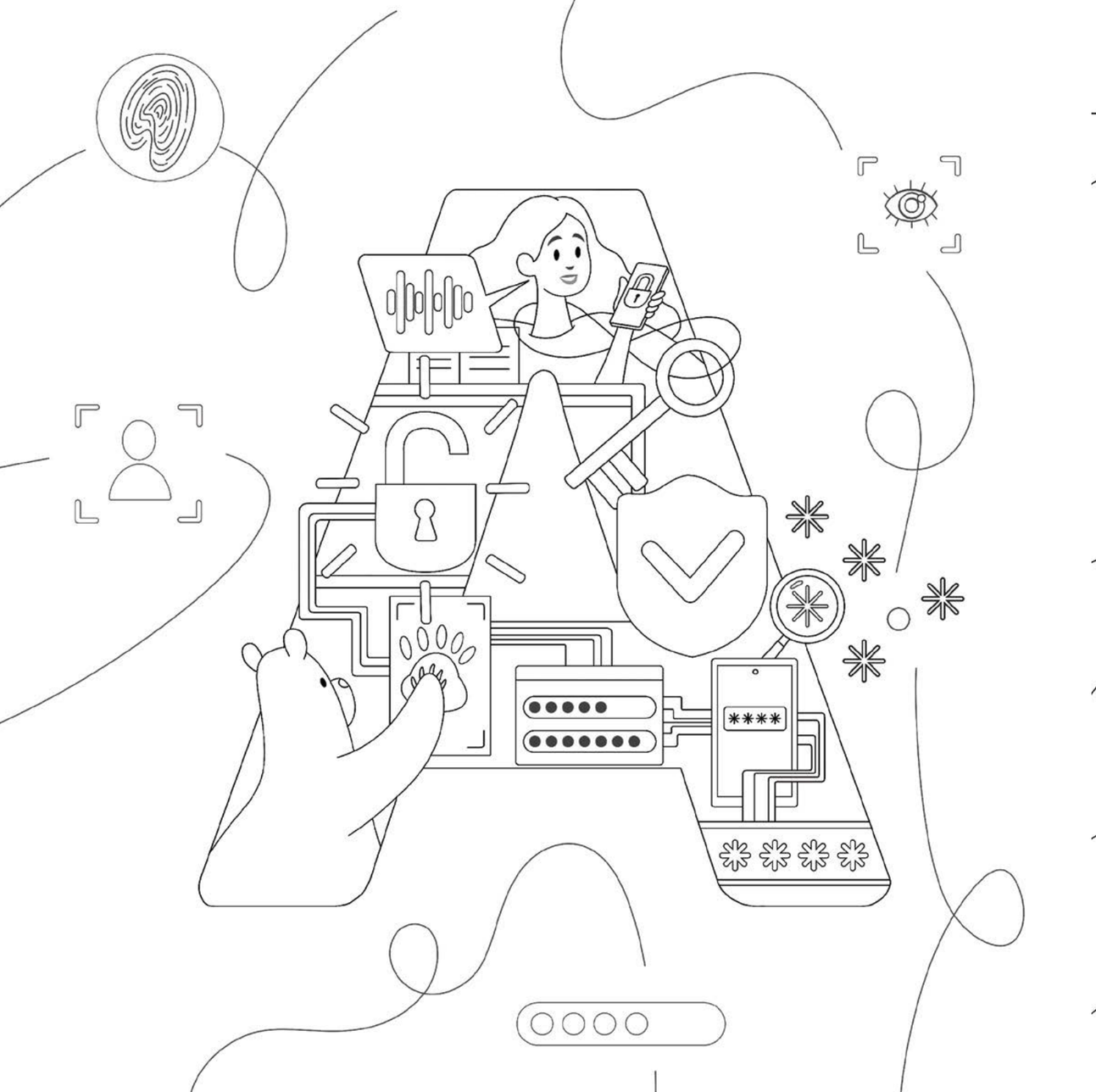
Può avvenire in modi diversi, come l'invio di messaggi cattivi o la diffusione di indiscrezioni su qualcuno online. Il cyberbullismo provoca nelle persone tristezza, imbarazzo o paura. È importante essere gentili con gli altri online, proprio come nella vita reale.
Se credi di essere vittime di bullismo online, condividi i tuoi pensieri con gli adulti di cui ti fidi. Quello che un bullo dice di te non ha nulla a che fare con la tua vera identità quindi non prendere mai sul serio le loro parole. Non cercare di vendicarti del bullo, perché spesso questo può peggiorare le cose. Fai uno screenshot della chat, bloccali e parlane con un adulto.

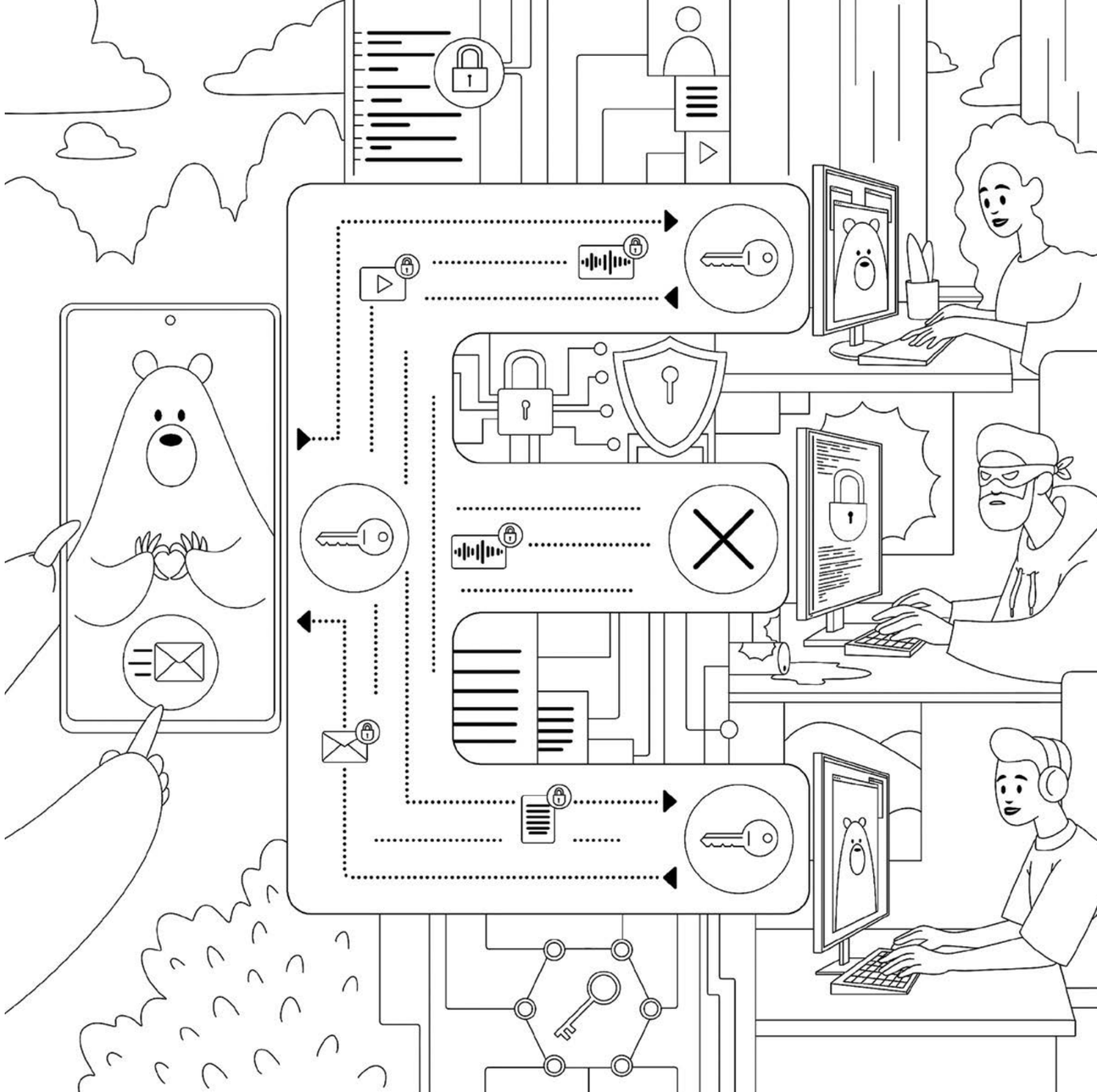


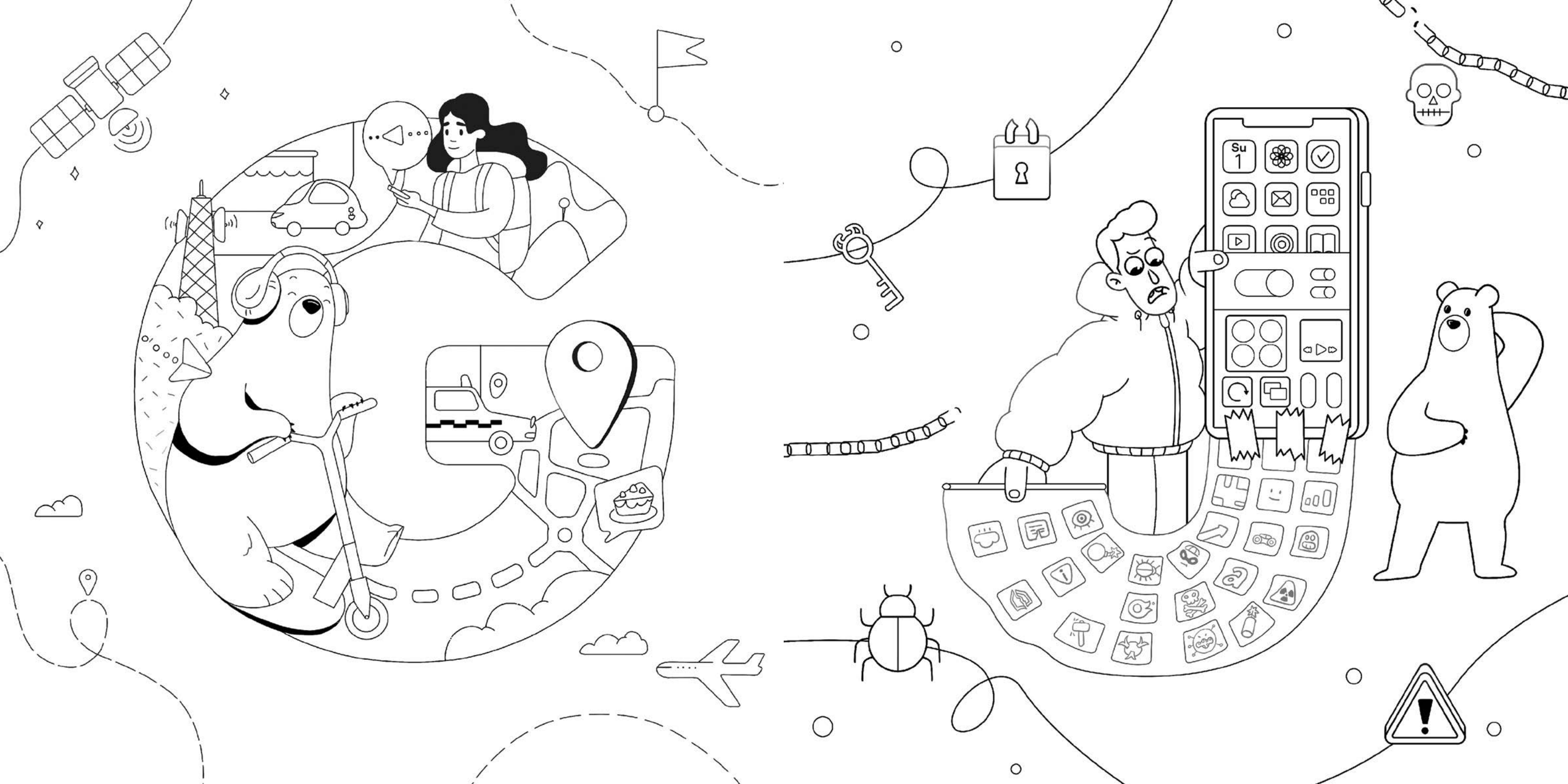
ZIP file

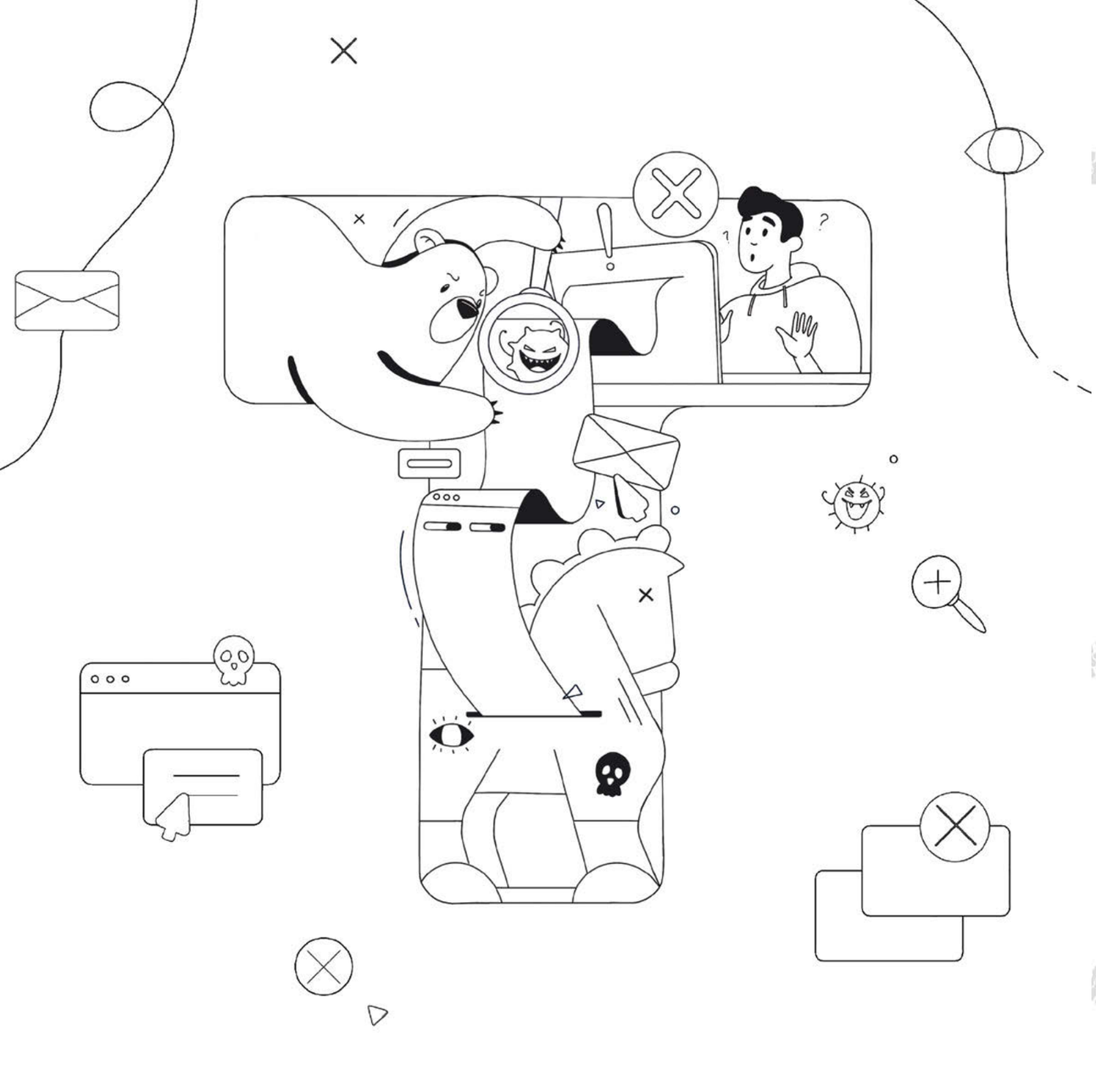
Un file ZIP è come una borsa in cui si possono mettere molte cose.

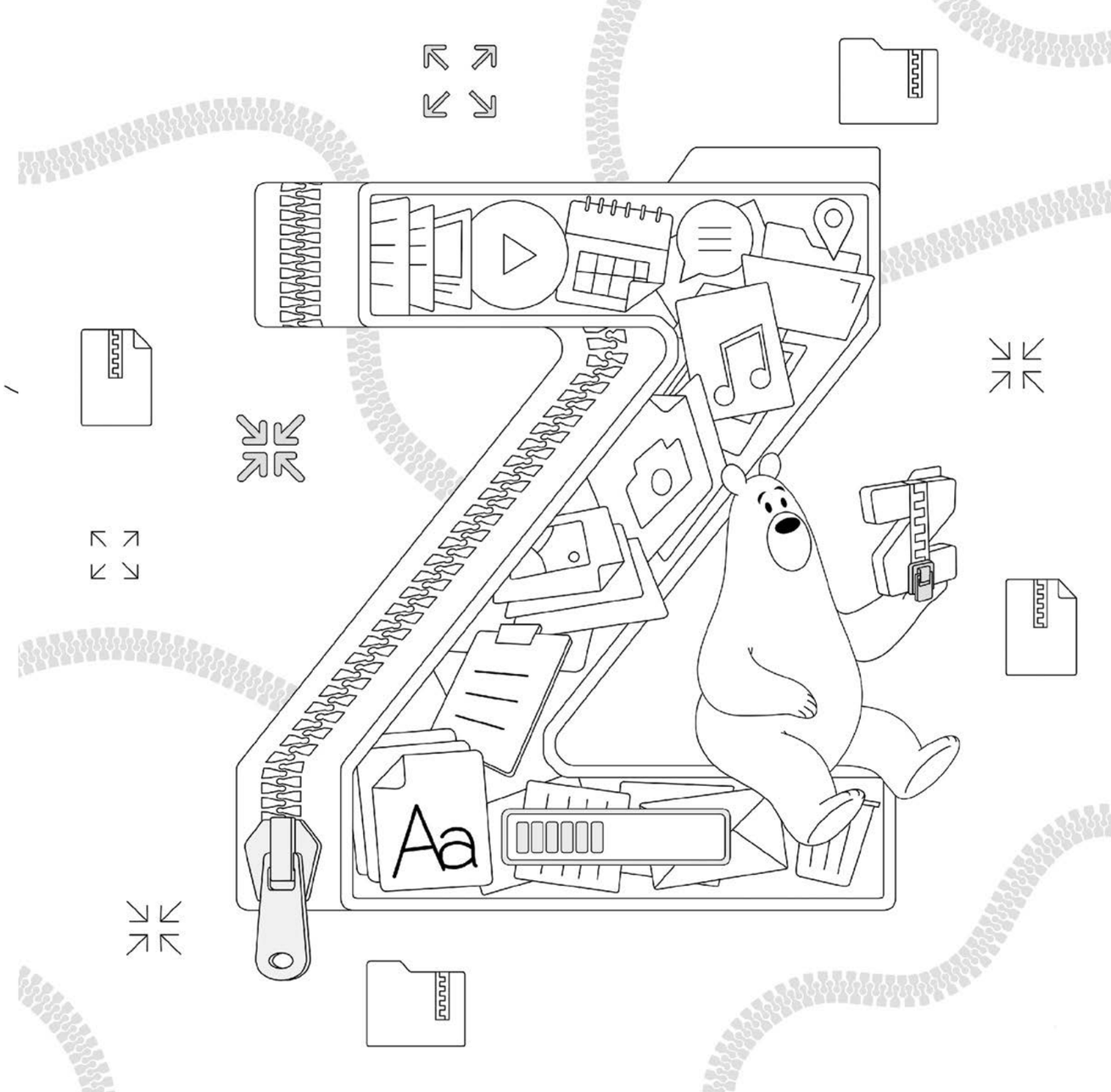
Aiuta a tenere insieme tutte le immagini, i file e le cartelle in un unico posto. Quando si utilizza un file ZIP, è possibile ridurre o "comprimere" tutte queste cose rendendole piccole in modo da occupare meno spazio sul computer. È come schiacciare tutto insieme e quando si desidera utilizzare di nuovo questi file, si può aprire la cartella ZIP ed estrarre tutto il contenuto.










Aa

Appunti

Caro cyber-esploratore,

che incredibile avventura abbiamo vissuto! Dalla A alla Z, hai scoperto tutti i segreti della cybersicurezza. Ricorda che essere sicuri online è proprio come esserlo nel mondo reale. Come i supereroi, hai il potere di prendere decisioni intelligenti online: scegliere password sicure, mantenere private le informazioni personali e pensarci due volte prima di cliccare su link sconosciuti.

La tua avventura non finisce qui. Il mondo digitale è in continua evoluzione e c'è ancora molto da imparare. Sii curioso, fai domande e aggiorna continuamente le tue conoscenze informatiche. Insegna ai tuoi amici e alla tua famiglia l'ABC della sicurezza online. Insieme, costruirete un mondo online più sicuro.

Progettazione grafica, layout e illustrazioni a cura dell'agenzia Thoughtform: www.behance.net/Thoughtform