
kaspersky
Bonjour,
Dans ce livre, tu apprendras les termes
les plus importants du monde virtuel.
Nous te dirons ce que tu peux y trouver d'utile
et quels sont les dangers qui s'y cachent.
Ouvre le livre et c'est parti !
kaspersky
L'abécédaire de
la cybersécurité

Ce livre appartient à _____

Chère amie, Cher ami,
Tu tiens entre tes mains l'abécédaire de la cybersécurité de Kaspersky.
As-tu déjà entendu parler du terme "cybersécurité" ? La cybersécurité nous aide à utiliser les technologies modernes - smartphone ou ordinateur - en toute sécurité et à explorer le monde en ligne sans se soucier des menaces éventuelles.

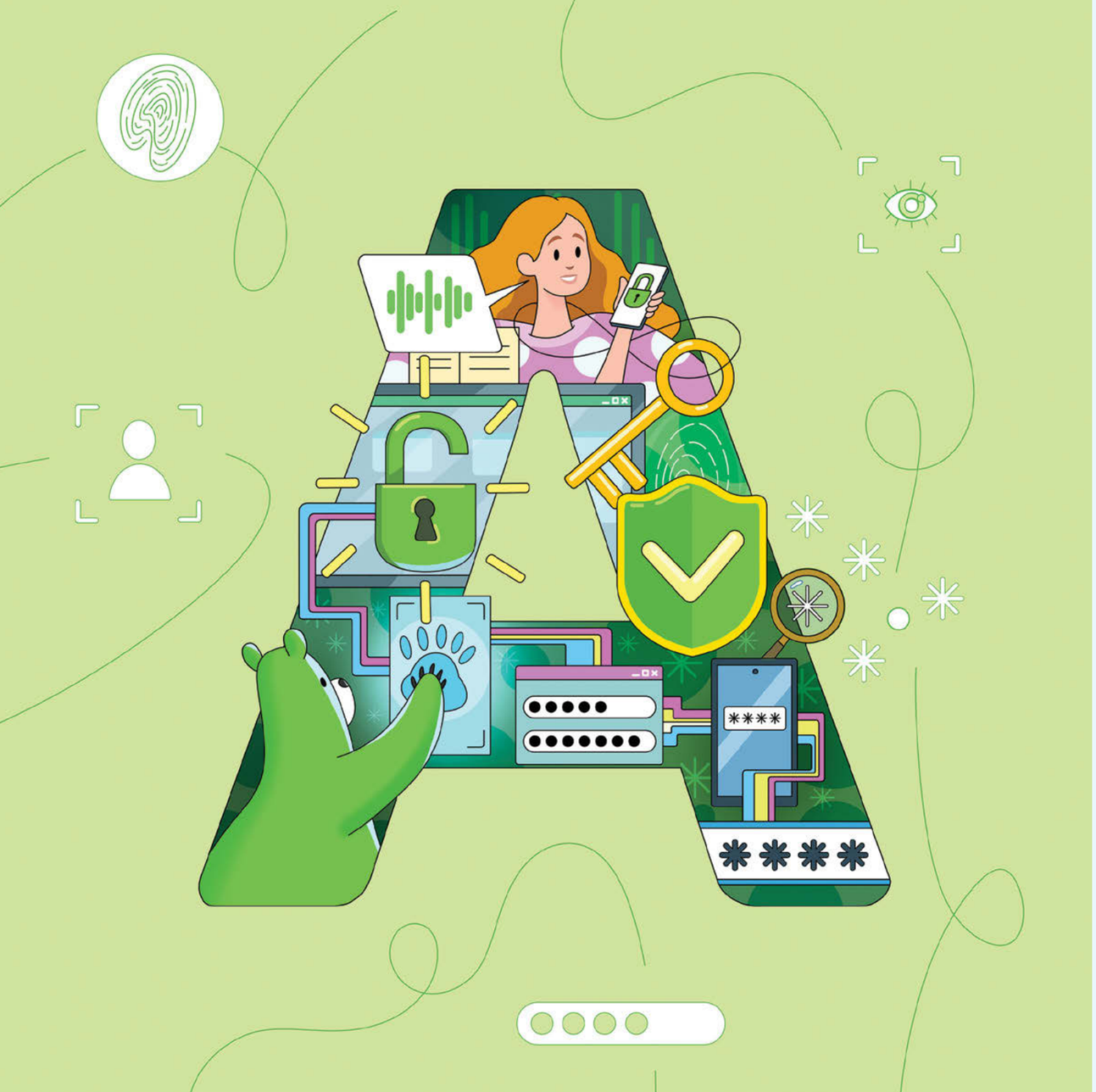
Le monde numérique est immense. Aujourd'hui, on peut faire beaucoup de choses en ligne telles que voyager sans sortir de chez soi ou étudier des langues étrangères. Et, bien sûr, tu peux jouer à des jeux, non seulement avec tes camarades de classe, mais aussi avec tes amis, même ceux qui sont loin de toi !

Mais à côté des possibilités infinies qu'il offre, Internet présente aussi des dangers, comme dans la vie réelle. Tu dois donc toujours être vigilant. Les actions imprudentes en ligne et la négligence des règles de cyberhygiène peuvent avoir de graves conséquences : tu peux infecter ta tablette ou ton smartphone avec des logiciels malveillants, exposant ainsi des informations importantes à des cybercriminels.

Grâce à ce livre, tu pourras te familiariser avec les nouvelles technologies, apprendre les principales règles de cyberhygiène, découvrir comment éviter les menaces en ligne et reconnaître les astuces des fraudeurs.

Pour que que ton aventure en ligne soit passionnante et sans mauvaises expériences, nous te recommandons de lire ce livre de A à Z !

Pour aider les enfants à explorer l'espace en ligne en toute sécurité, nous avons créé l'application Kaspersky Safe Kids.



Authentification

L'authentification consiste à disposer d'un code secret spécial ou d'un mot de passe qui te permet d'accéder à ton ordinateur, ton téléphone ou ton compte en ligne.

Lorsque tu souhaites accéder à quelque chose d'important, comme ton téléphone ou l'ordinateur de ton école, tu dois dire à ton ordinateur que tu es vraiment toi et qu'il peut te faire confiance. Grâce à cette "authentification", tu peux t'assurer que seule la bonne personne est autorisée à utiliser ou à faire quelque chose sur ton appareil. C'est là tout l'intérêt de l'authentification : s'assurer que seules les bonnes personnes peuvent utiliser des appareils spéciaux !

Backup ou sauvegarde

La sauvegarde est une copie des informations numériques que tu ne veux absolument pas perdre.

Imagine : l'un de tes jeux préférés a été oublié pendant tes vacances, mais tes parents avaient heureusement rangé exactement le même dans un lieu de stockage spécial. De la même manière, une sauvegarde est un endroit spécial où toutes tes photos, vidéos et fichiers importants peuvent être conservés, afin qu'ils ne soient jamais perdus. Il arrive que des accidents se produisent ou que des problèmes surviennent avec nos appareils ; ils peuvent être perdus ou cesser de fonctionner. Mais avec la sauvegarde, tu n'as pas à t'inquiéter, car tous tes objets préférés sont en lieu sûr. Alors n'oublie pas, aie toujours une sauvegarde, et tes objets numériques seront toujours protégés !

Captcha

Le Captcha est un test spécial qui permet de vérifier si tu es une personne réelle utilisant un ordinateur ou un robot se faisant passer pour une personne.

As-tu déjà eu à résoudre un puzzle ou sélectionner certaines images avant de pouvoir continuer à accéder à un site web ou à jouer à un jeu en ligne ? Il s'agit généralement d'un Captcha ! Il te demande de faire quelque chose que les robots ne peuvent pas très bien faire, comme cliquer sur des cases avec des voitures ou des feux de circulation, ou taper des lettres et des chiffres compliqués. Il permet de protéger les sites web et les applications contre les robots malveillants, également connus sous le nom de "spambots", qui pourraient essayer de faire quelque chose de mauvais.

Deepfake

Le deepfake est une technologie spéciale qui permet de créer une image, une vidéo ou un fichier audio qui donne l'impression qu'une personne dit ou fait quelque chose qui ne s'est pas produit dans la réalité.

Si vous voyez une vidéo où le visage et la bouche d'une personne ne correspondent pas tout à fait aux mots qu'elle prononce, ou si sa tête et ses cheveux bougent de façon étrange, il peut s'agir d'un deepfake. Il est important d'être prudent et de ne pas croire tout ce que l'on voit en ligne, car certaines images ou vidéos peuvent être des "deepfakes".

E

Empreinte numérique

Une empreinte numérique est comme une petite traînée d'informations que nous laissons derrière nous chaque fois que nous faisons quelque chose sur Internet. C'est comme laisser des traces de pas dans le sable lorsque l'on marche sur une plage.

Tout ce que tu fais, comme poster des photos, écrire des commentaires ou même liker des messages, peut être vu par d'autres personnes qui utilisent également Internet. Une fois que quelque chose est sur le web, il y reste pour toujours. C'est comme écrire avec un stylo sur une feuille de papier: tu peux essayer de l'effacer, mais ce sera très difficile et, si tu y parviens, il restera peut-être une trace. C'est pourquoi il est important de faire attention à ce que tu fais et dis sur Internet.

Fraude

Il y a fraude lorsque des personnes incitent d'autres personnes à leur donner leurs coordonnées de paiement, de l'argent ou des informations personnelles.

Il est important de se méfier des escrocs sur Internet. Comme on ne sait pas qui est de l'autre côté de l'écran, ils se font passer pour des amis ou des personnes de confiance. Ils veulent que tu leur confies des secrets ou ils t'incitent à acheter des choses qui ne sont pas réelles, sous prétexte de t'offrir un cadeau vraiment sympa, comme une PlayStation. Mais méfie-toi, car leur but est de te voler ton argent et tes informations. S'ils te promettent des choses trop belles pour être vraies, ne les crois pas, car tu les paieras sans jamais les recevoir. Ne parle pas non plus à des inconnus sur Internet. Et si quelqu'un te met mal à l'aise ou te demande de faire des choses bizarres, dis-le à un adulte en qui tu as confiance : papa, maman, ton professeur...

Géolocalisation

La géolocalisation est une technologie qui permet à nos appareils, comme les téléphones et les ordinateurs, de savoir où nous nous trouvons : à la maison, à l'école, à la plage...

Elle est très utile parce qu'elle nous aide à aller d'un endroit à l'autre, à trouver le marchand de glaces le plus proche ou à savoir à quelle distance se trouvent nos amis, mais nous devons être prudents lorsque nous l'utilisons.

La géolocalisation est l'un de tes plus grands secrets. Tout comme le super-héros de ton film préféré ne révèle pas au méchant l'endroit où il se cache, il est important que tu ne révèles pas ta position à des inconnus sur Internet. C'est bien que tes parents sachent où tu es, mais pour ta sécurité, les inconnus ne doivent pas avoir accès à cette information. Si une application te demande la permission de te géolocaliser, dis-le à tes parents et pose-toi la question suivante : "Cette application a-t-elle vraiment besoin de savoir où je suis ?" Si ce n'est pas le cas, tu ne dois pas accepter de partager ta géolocalisation avec l'application.

Honeypot

Un honeypot est un piège mis en place par les experts en informatique pour attraper les personnes mal intentionnées qui tentent de faire de mauvaises choses sur Internet.

Savais-tu que certains ours aiment le miel ? Si tu veux attirer Winnie l'ourson, par exemple, un bon pot de cette délicieuse friandise suffira. Les informaticiens procèdent de la même manière : ils utilisent un pot de miel comme piège pour attirer non pas des ours, mais des personnes qui font de mauvaises choses sur Internet. Ils observent ainsi tout ce que font ces personnes et apprennent leurs astuces pour assurer notre sécurité.

Adresse IP

Une adresse IP est une adresse spéciale qui te connecte à Internet.

L'adresse IP permet à Internet de savoir où envoyer les informations lorsque vous êtes connecté. C'est comme l'adresse de votre domicile, qui permet au facteur de savoir où livrer les lettres et les colis. Chaque point de connexion à Internet a une adresse IP unique. Vous aurez donc une adresse IP différente selon la connexion que vous utilisez : Internet sur votre téléphone portable, le Wi-Fi chez votre oncle et votre tante, le Wi-Fi à l'hôtel où vous passez vos vacances...

Jailbreak

On parle de jailbreak lorsque quelqu'un enfreint les règles de fonctionnement de son téléphone, en faisant quelque chose qui n'est pas autorisé.

Normalement, tu ne peux télécharger que les applications autorisées par les sites officiels. Lorsque tu débloques ton ordinateur, tu peux télécharger et utiliser toutes sortes d'applications qui ne sont normalement pas autorisées. Ça peut sembler amusant, mais tu risques d'avoir des problèmes, de provoquer des dysfonctionnements sur ton appareil, ou même de permettre à des personnes mal intentionnées de faire de mauvaises choses avec. Il est donc important de toujours respecter les règles et de te rappeler que les jeux et les applications les plus sûrs et les plus amusants n'ont pas besoin d'être jailbreakés.

Keylogger

Un keylogger (ou enregistreur de frappe) est un type particulier de programme informatique qui peut enregistrer secrètement tout ce que tu tapes sur un ordinateur.

Un enregistreur de frappe enregistre toutes les frappes que tu effectues et les sauvegarde. C'est très dangereux, car il peut découvrir les messages que tu tapes ou tes mots de passe. Le keylogger est généralement téléchargé sur tes appareils à ton insu, déguisé en éléments que tu télécharges sur Internet, comme la dernière version de ton jeu vidéo préféré. C'est pourquoi il est très important que tu ne télécharges des fichiers, des jeux, ou des applications qu'à partir de sites web sûrs, après en avoir discuté avec tes parents.

Login

Le login est ton nom d'utilisateur ou ton adresse électronique et un mot de passe qui te permet d'accéder à ton site web, jeu ou application préféré(e).

Le login est donc comme la clé qui ouvre la porte de ta maison.

Il permet au site web ou à l'application de savoir que c'est toi qui essaies de te connecter et te permet de faire des choses amusantes comme jouer à des jeux, regarder des vidéos ou discuter avec tes amis. Ton nom d'utilisateur et ton mot de passe forment une combinaison qui est comme ton propre code secret que tu es le seul à connaître pour entrer - Alohomora ! Sésame ouvre-toi !

N'oublie pas que lorsque tu crées ton nom d'utilisateur et ton mot de passe, il est déconseillé d'utiliser ton vrai nom ou ta date de naissance, car tu donnerais des indices à d'autres personnes. Utilise toute ton ingéniosité pour créer un login super sécurisé !

Logiciels Malveillants

Les logiciels malveillants sont des bogues informatiques sournois et malveillants qui peuvent infecter les ordinateurs, les tablettes et d'autres appareils.

Les logiciels malveillants peuvent se cacher dans différents trucs sur lesquels tu cliques ou que tu télécharges sur Internet, comme des jeux ou des images sympas, surtout si tu les télécharges à partir de sites web non fiables. Quand tu les laisses pénétrer par accident, ils peuvent endommager tes fichiers ou tenter de voler tes infos perso, comme tes mots de passe ou tes photos - mais ne t'inquiète pas ! Tout comme se laver les mains permet d'éloigner les germes, tu peux utiliser un logiciel de protection de la cybersécurité pour protéger tes appareils contre les logiciels malveillants.

Afin de protéger vos appareils contre les logiciels malveillants, n'oubliez pas d'installer et d'utiliser une solution de sécurité complète et fiable, telle que Kaspersky Premium.

NFT

Imagine que tu possèdes dans le monde virtuel un objet de grande valeur. Tu aimerais avoir un certificat qui prouve que cet objet n'appartient qu'à toi et à personne d'autre, n'est-ce pas ? C'est ce qu'on appelle un NFT.

Un NFT, c'est un peu comme un certificat qui prouve que tu possèdes quelque chose de spécial dans le monde numérique : des œuvres d'art, des vidéos, ou même des animaux de compagnie virtuels. Chaque NFT est unique et peut être acheté et vendu grâce à ce truc appelé la technologie blockchain, qui permet de s'assurer que personne ne peut tricher ou prétendre posséder un NFT qui n'est pas vraiment le sien.

OSINT

OSINT est l'abréviation de Open Source Intelligence, et c'est un peu comme si tu étais un détective, mais que tu utilisais des informations à la disposition de tout le monde.

Par exemple, si tu devais résoudre une enquête OSINT, on te demanderait peut-être de deviner l'endroit exact où une photo a été prise au hasard, même si tu n'y es jamais allé auparavant ! Mais les spécialistes de l'OSINT résolvent cette tâche comme s'ils assemblaient les pièces d'un puzzle pour en apprendre davantage sur différents lieux et différentes personnes. C'est pourquoi les spécialistes de l'OSINT peuvent recueillir des informations via Internet, les médias sociaux et les sites d'information pour les aider à comprendre où et comment certaines choses (et même certains mystères !) se sont produites dans le monde. Et, bien sûr, l'OSINT nous aide à apprendre et à mieux comprendre le monde qui nous entoure.

Phishing

Le phishing (ou hameçonnage) est la tentative des cybercriminels de te tromper et de voler tes informations - par exemple tes nom et prénom, ton nom de connexion ou ton numéro de compte bancaire (si toi ou tes parents les utilisez pour acheter quelque chose en ligne).

Il se peut que tu reçoives des courriels et des messages provenant de faux sites web qui ont l'air réels, mais qui essaient en réalité de voler tes informations. Il est important de veiller à ne pas partager d'informations personnelles avec qui que ce soit, à moins d'être absolument sûr qu'il s'agit d'un vrai site web.

Malheureusement, toutes les personnes que tu rencontres en ligne ne sont pas forcément de bonnes personnes, et il est très important de faire attention à qui tu donnes ton adresse électronique. Parfois, ils essaient de nous inciter à révéler des informations personnelles en étant très gentils ou en offrant des choses merveilleuses, mais tu ne dois jamais donner des détails tels que ton nom complet, ton adresse, ton numéro de téléphone, tes mots de passe, tes numéros de carte bancaire... à qui que ce soit, à moins qu'un adulte de confiance ne te dise que tu peux le faire.

QR code

Le terme code QR vient des mots “Quick Respone” ou “Quick Response”. Il ressemble à une image carrée composée de nombreux petits carrés noirs et blancs à l’intérieur d’une boîte plus grande qui te renvoie à un autre fichier contenant plus d’informations.

Bien qu’il ait l’air d’une image amusante, composée de carrés noirs et blancs, un code QR est en fait comme une clé magique qui ouvre une porte secrète. Pour l’ouvrir, tu dois le prendre en photo avec l’appareil photo de ton téléphone ou utiliser une application spéciale et cliquer. Soudain, c’est comme une carte au trésor qui t’emmène dans des endroits spéciaux. Au zoo, tu peux scanner le code QR et un site web apparaîtra avec des infos intéressantes sur l’animal que tu regardes. Dans un livre, le code QR peut te conduire à un site web amusant qui te donne plus d’infos sur l’histoire.

Malheureusement, les cybercriminels savent aussi comment utiliser les codes QR et s’en servir à des fins malveillantes. Heureusement, il existe un programme spécial qui te dit si le code QR est sûr. N’oublie pas de ne jamais télécharger une app à partir d’un code QR, mais toujours à partir de l’App Store ou de Google Play.

Ransomware

Un ransomware est un programme informatique capable de crypter tous les fichiers de ton appareil et d'exiger une rançon pour y accéder.

Le ransomware s'infiltre dans ton ordinateur et prend en otage tous tes fichiers importants : images, vidéos, et documents. Les malfaiteurs qui ont créé le ransomware les emportent ensuite et laissent une note en demandant de l'argent pour les récupérer, sous la forme d'une rançon. Mais n'oublie pas de ne jamais te fier à ce qu'ils disent ! Ils peuvent tout simplement disparaître et te laisser avec un appareil cassé, même si tu as payé. Il faut alors prévenir un adulte pour qu'il répare l'appareil. Fais également une sauvegarde : c'est comme sauvegarder un niveau dans un jeu. Ainsi, en cas de problème, tout ne disparaîtra pas.

Spam

Le spam est comme un courrier indésirable, mais pour ton courrier électronique.

Tout comme nous recevons parfois par la poste des lettres ou des prospectus dont nous ne voulons pas ou dont nous n'avons pas besoin, il en va de même pour les courriers électroniques. Ces courriels peuvent être commerciaux, porter sur des choses que nous ne voulons pas acheter, ou même être des escroqueries qui tentent de nous faire révéler nos infos personnelles. Il est important de se méfier des courriels indésirables et de ne pas cliquer dessus ni d'y répondre, tout comme nous le faisons avec le courrier indésirable dans la boîte aux lettres de notre domicile. La meilleure façon d'éviter les courriels indésirables est de ne pas révéler ton adresse électronique, sauf si tu en as vraiment besoin.

Chevaux de Troie

Les chevaux de Troie sont des programmes informatiques qui peuvent prendre le contrôle de ton ordinateur et l'utiliser pour faire de mauvaises choses.

Un cheval de Troie peut ressembler à un jeu vidéo ou à un programme inoffensif, mais il s'agit en réalité d'un petit personnage maléfique qui veut s'introduire dans ton ordinateur, voler tes données et détruire tes fichiers. Les chevaux de Troie se cachent souvent dans des sites web non sécurisés et ont de nombreuses astuces pour te tromper : ils te disent que tu peux télécharger gratuitement des jeux coûteux ou regarder sur ton ordinateur un film qui n'est projeté que dans les cinémas... Ne prête pas attention à ces faux cadeaux et n'utilise que des sites web vérifiés, ceux qui portent une grosse coche verte. N'oublie pas que, de même que tu ne laisses pas entrer des inconnus chez toi, fais attention à ce que tu télécharges, car il peut s'agir d'un astucieux cheval de Troie. Demande toujours la permission à tes parents avant de télécharger quoi que ce soit sur tes appareils.

URL

L'URL est une adresse que tous les éléments en ligne possèdent - sites web, images, livres en ligne, etc.

Tout comme ta maison a une adresse pour que les gens sachent comment la trouver, une URL indique au navigateur web où trouver un site web. Il s'agit d'une combinaison de lettres, de chiffres et de symboles qui te permet de te connecter au bon site web. Tu trouveras l'URL d'une page dans la barre d'adresse située en haut de ton navigateur. Prête attention à l'URL et compare-la avec le nom officiel d'une entreprise, organisation, boutique, ou autre. Si l'URL semble étrange ou suspecte, il se peut que tu sois sur un faux site web ou un site d'hameçonnage.

VPN

Un VPN (Virtual Private Network) est un outil qui rend la navigation sur internet plus sûre.

C'est comme un tunnel secret sur Internet qui préserve la confidentialité de tout ce que tu fais en ligne - comme une cachette secrète à laquelle tu es le seul à pouvoir accéder ! Un VPN déplace tes données vers un endroit spécialement protégé et fonctionne comme un masque : les sites web que tu visites n'obtiendront pas tes infos, ils ne verront que le masque que le service VPN leur montre. Tout comme tu n'aimerais pas qu'un étranger vienne bavarder dans ton journal intime ou dans ta chambre à coucher, un VPN t'aide à protéger tes activités en ligne contre les étrangers qui pourraient essayer de consulter tes données personnelles.

Router Wi-Fi

Le routeur Wi-FI te permet de te connecter à Internet.

Sans Wi-Fi, tu ne pourras pas accéder à Internet. Le routeur est le boîtier qui se trouve presque toujours à côté de la télévision et qui te permet de connecter tes appareils domestiques au Web : télévision, tablette, téléphone portable, etc. C'est lui qui se trouve au milieu, entre toi et le réseau, et qui transmet les données de ton appareil à Internet. Pour éviter que quelqu'un ne vole tes photos ou d'autres fichiers, tu dois donc protéger ton Wi-Fi par un mot de passe. Définis un mot de passe difficile à deviner avec ta famille et ne le donne qu'aux personnes en qui tu as confiance.

Aussi intéressant que cela puisse paraître, ne te connecte pas au Wi-Fi "gratuit" dans les magasins ou les restaurants, car il n'est peut-être pas sécurisé. Tout du moins, ne te connecte pas sans protéger ton appareil.

eXploit

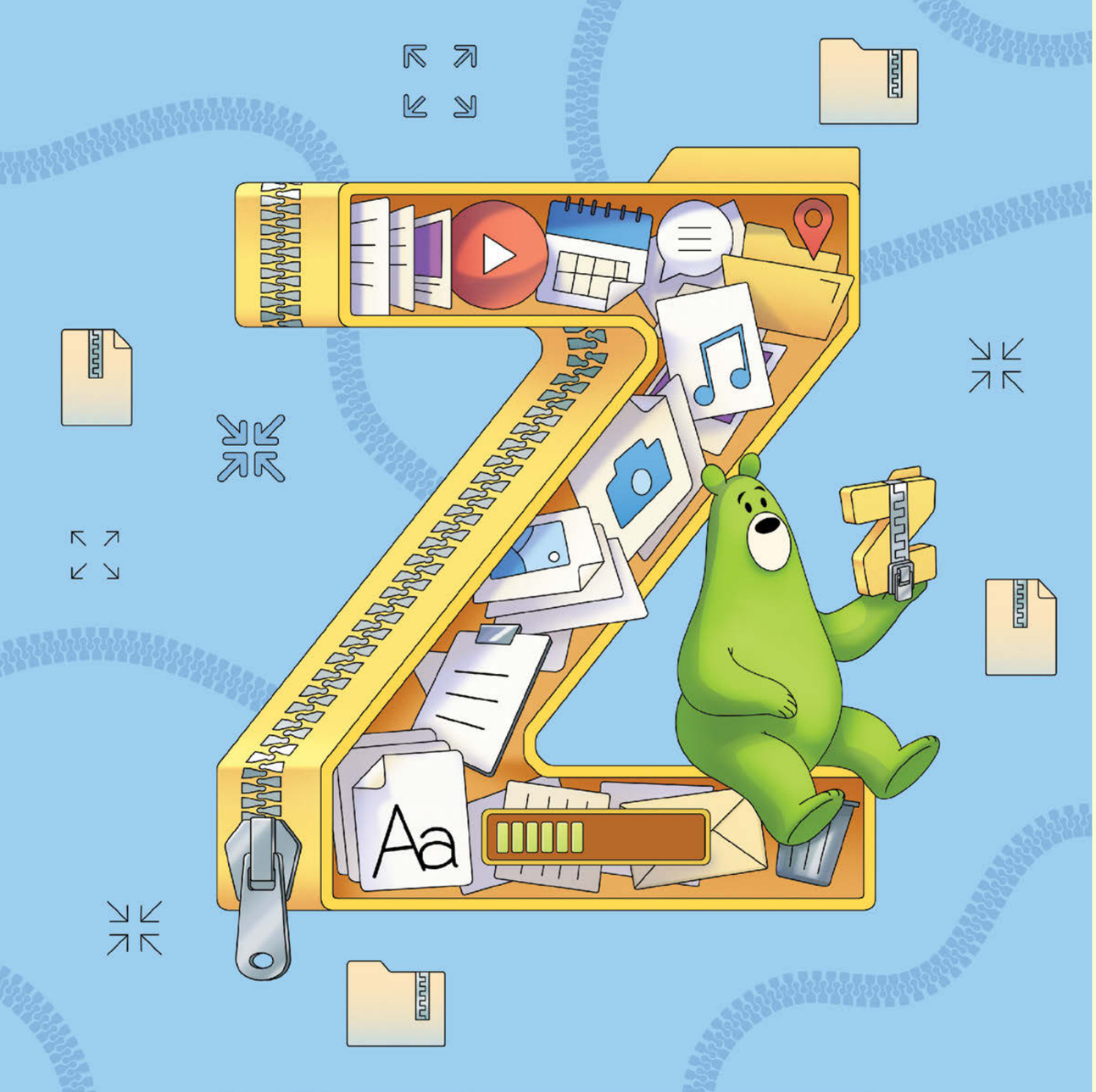
Un exploit est une sorte de faille dans ton appareil qui permet aux cybercriminels de s'y introduire, de l'infecter avec un programme malveillant et de lui dire ce qu'il doit faire sans ta permission.

C'est comme un cheat code dans un jeu en ligne - en connaissant ces cheat codes, les cybercriminels peuvent enfreindre les règles et faire ce qu'ils veulent avec ton appareil.

cYber-harcélement

On parle de cyber-harcélement lorsqu'une personne est méchante ou blessante à l'égard d'autres personnes en ligne.

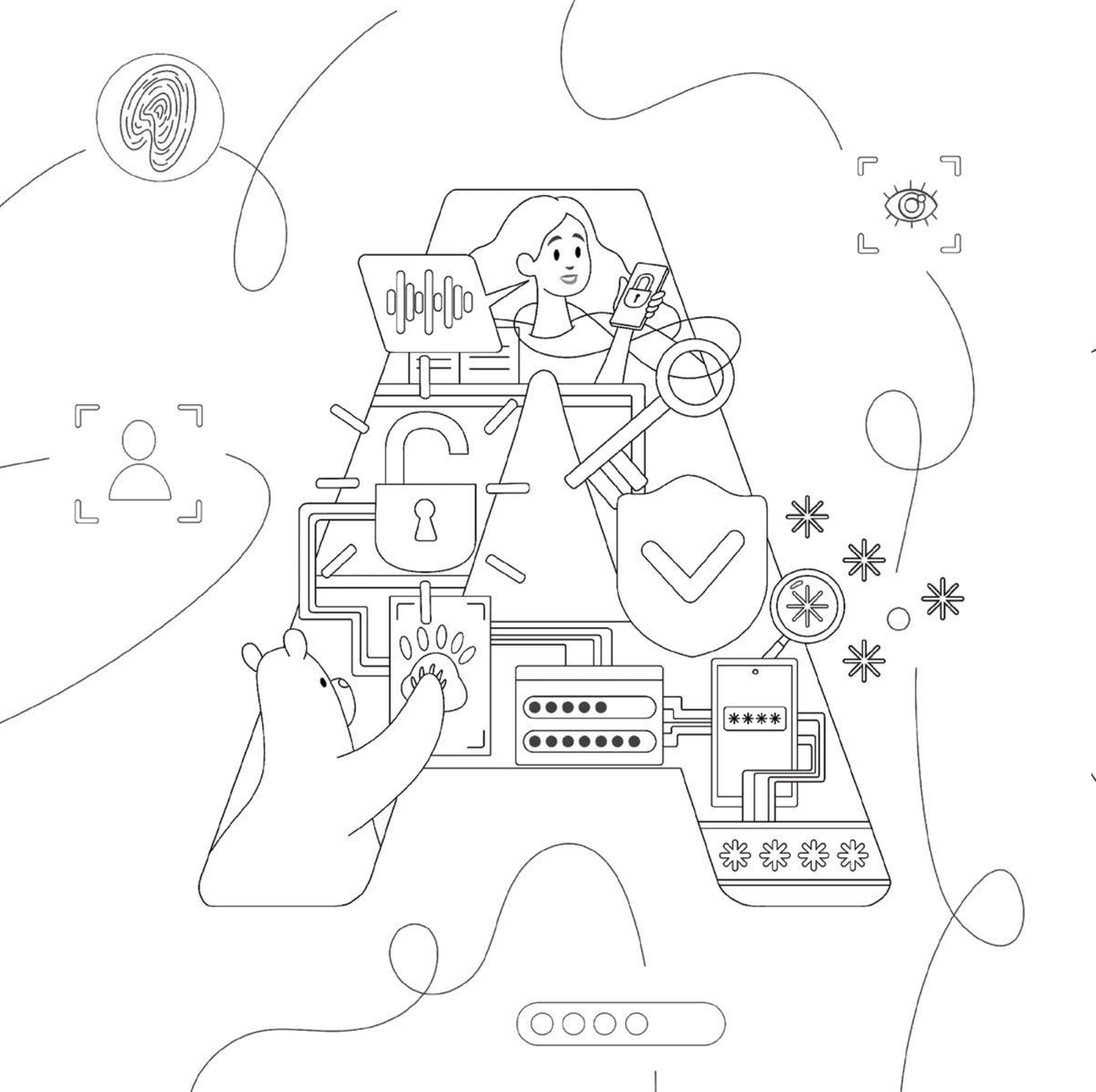
Le cyber-harcélement peut prendre de nombreuses formes, comme l'envoi de messages méchants ou la diffusion de rumeurs sur une personne sur Internet. La cyberintimidation rend les personnes qui en sont victimes tristes, honteuses ou effrayées. Il est important d'être gentil avec les autres en ligne, tout comme dans la vie réelle. Si tu penses que quelqu'un te harcèle en ligne, fais part de tes sentiments à des adultes en qui tu as confiance. Ce qu'un harceleur dit de toi n'a rien à voir avec ce que tu es vraiment. Ne prends donc jamais ses paroles au sérieux. N'essaie pas de riposter, car cela risque souvent d'aggraver la situation. Fais des captures d'écran de ton chat, bloque la personne et parle à un adulte.

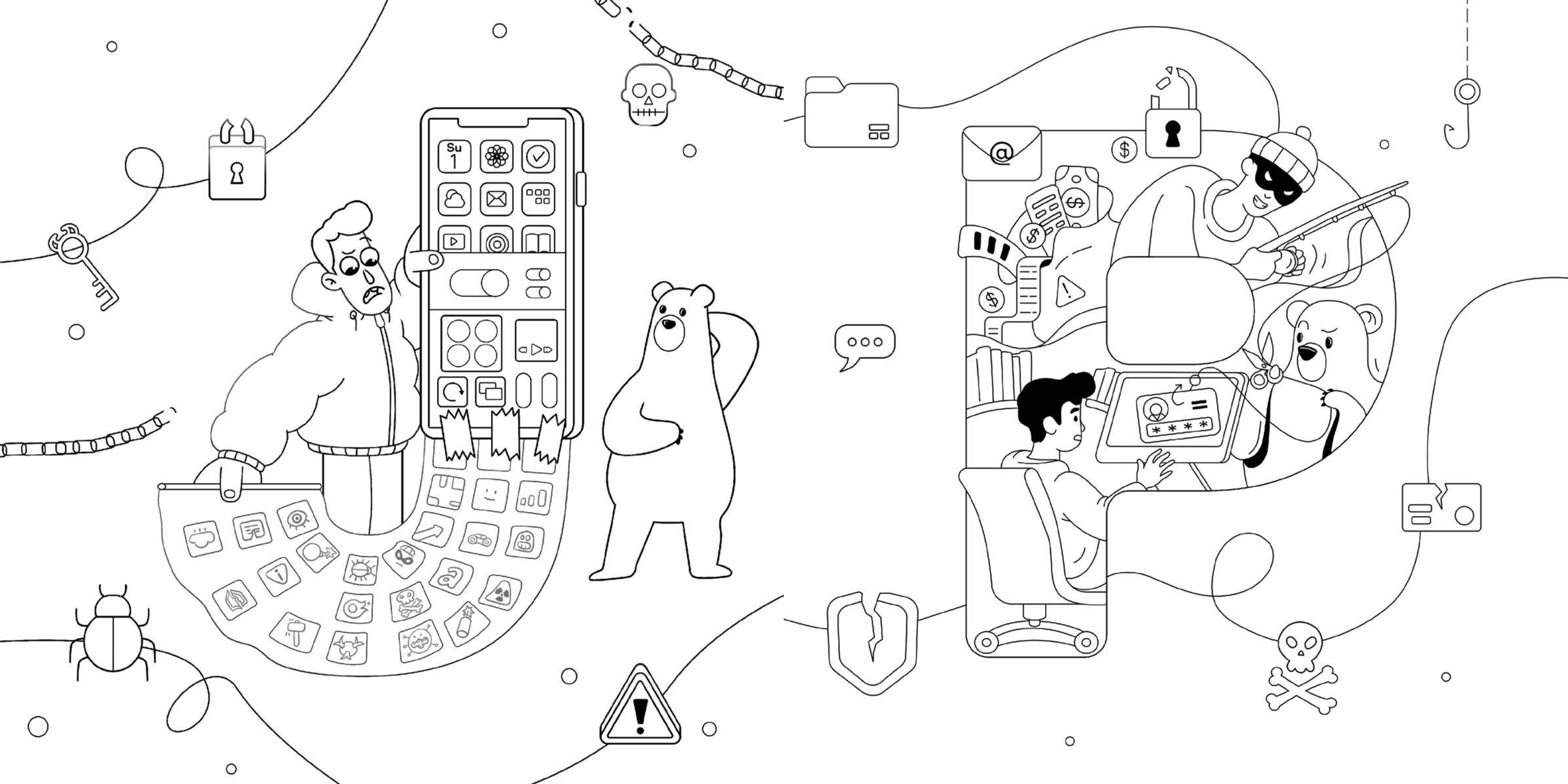


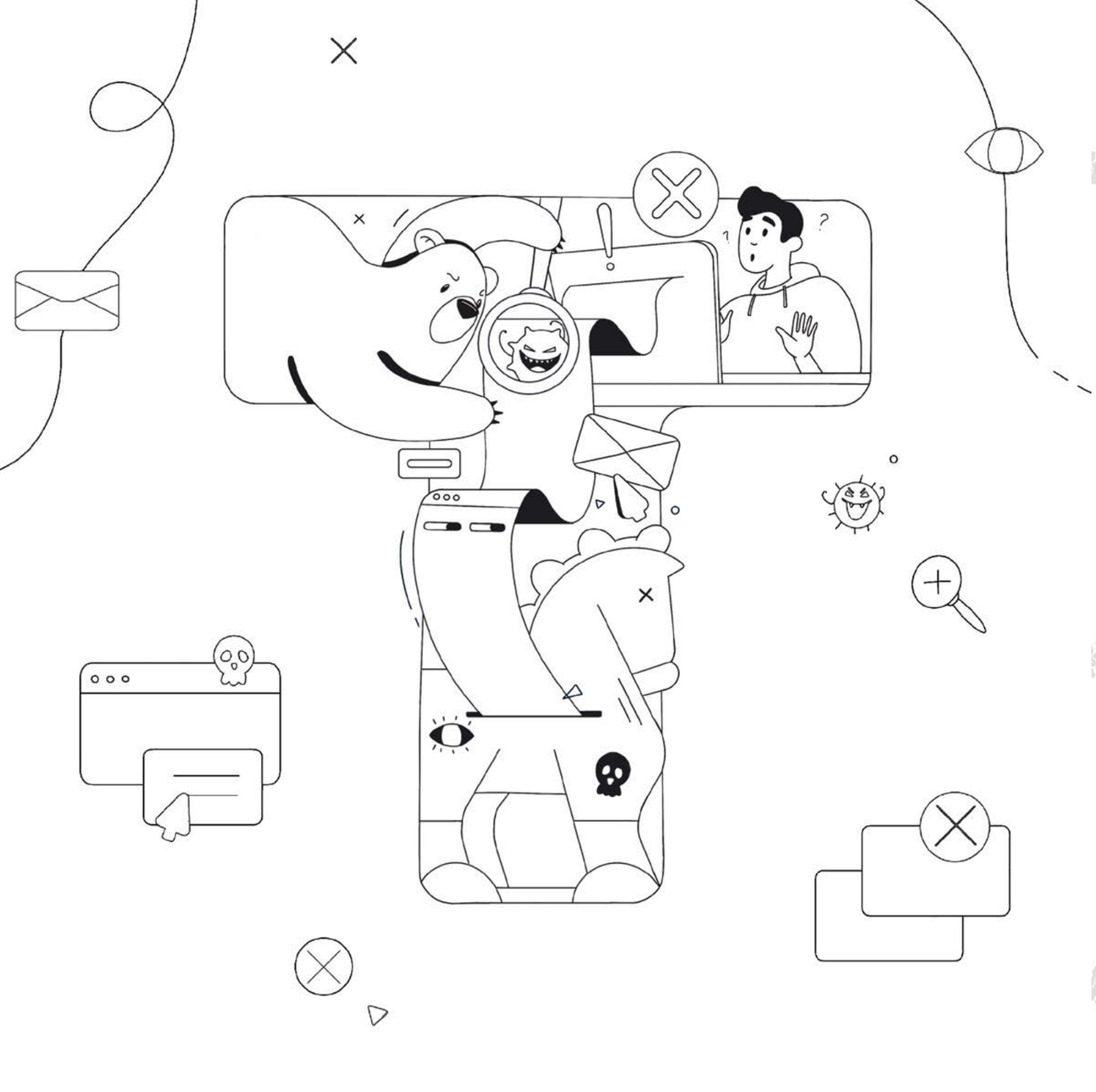
Fichier ZIP

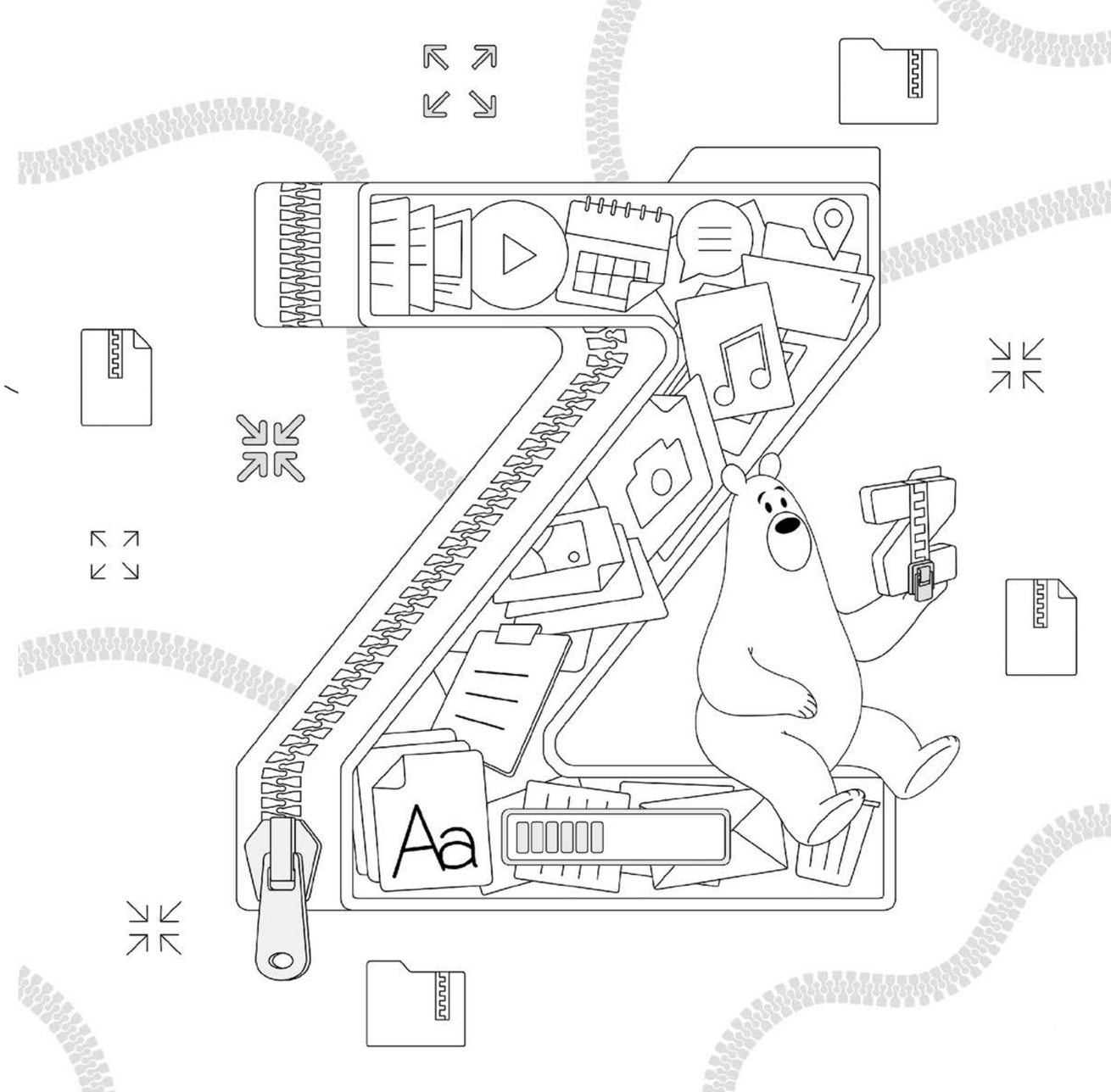
Un fichier zip est comme un sac dans lequel on peut mettre beaucoup de choses.

Il permet de conserver toutes les images, tous les fichiers et tous les dossiers au même endroit. Lorsque tu utilises un fichier zip, tu peux rétrécir ou “compresser” tous ces éléments, en les rendant plus petits pour qu’ils occupent moins d’espace sur ton ordinateur. Et lorsque tu souhaites réutiliser ces éléments, tu peux ouvrir le sac zip et en extraire tout ce qu’il contient.




Su
1
@
$
$
$
$
* * * *




Aa

Remarques

Chère cyber-exploratrice, cher cyber-explorateur,

Quelle incroyable aventure nous avons vécue ! De A à Z, tu as parcouru les méandres de la cybersécurité. Mais n'oublie pas que la sécurité en ligne, c'est comme dans le monde réel. Comme les super-héros, tu as le pouvoir de faire des choix intelligents en ligne - choisir des mots de passe forts, protéger tes infos perso et réfléchir à deux fois avant de cliquer sur des liens inconnus.

L'aventure ne s'arrête pas là. Le monde numérique est en constante évolution, et il y a encore beaucoup à apprendre. Reste curieux, pose des questions et mets à jour tes connaissances en ligne. Enseigne à tes amis et à ta famille l'abécédaire de la cybersécurité. Ensemble, vous construirez un monde en ligne plus sûr.

Conception graphique, mise en page et illustrations par Thoughtform agence: www.behance.net/Thoughtform