kaspersky

¡Hola!
En este libro aprenderás los términos más importantes del mundo virtual. Te contamos algunas de las cosas más útiles que podrás encontrar en Internet y algunos de los peligros con los que deberás tener cuidado. ¡Abre el libro y embárcate en un viaje de lo más emocionante!

kaspersky

Ciberseguridad

Este libro pertenece a _____

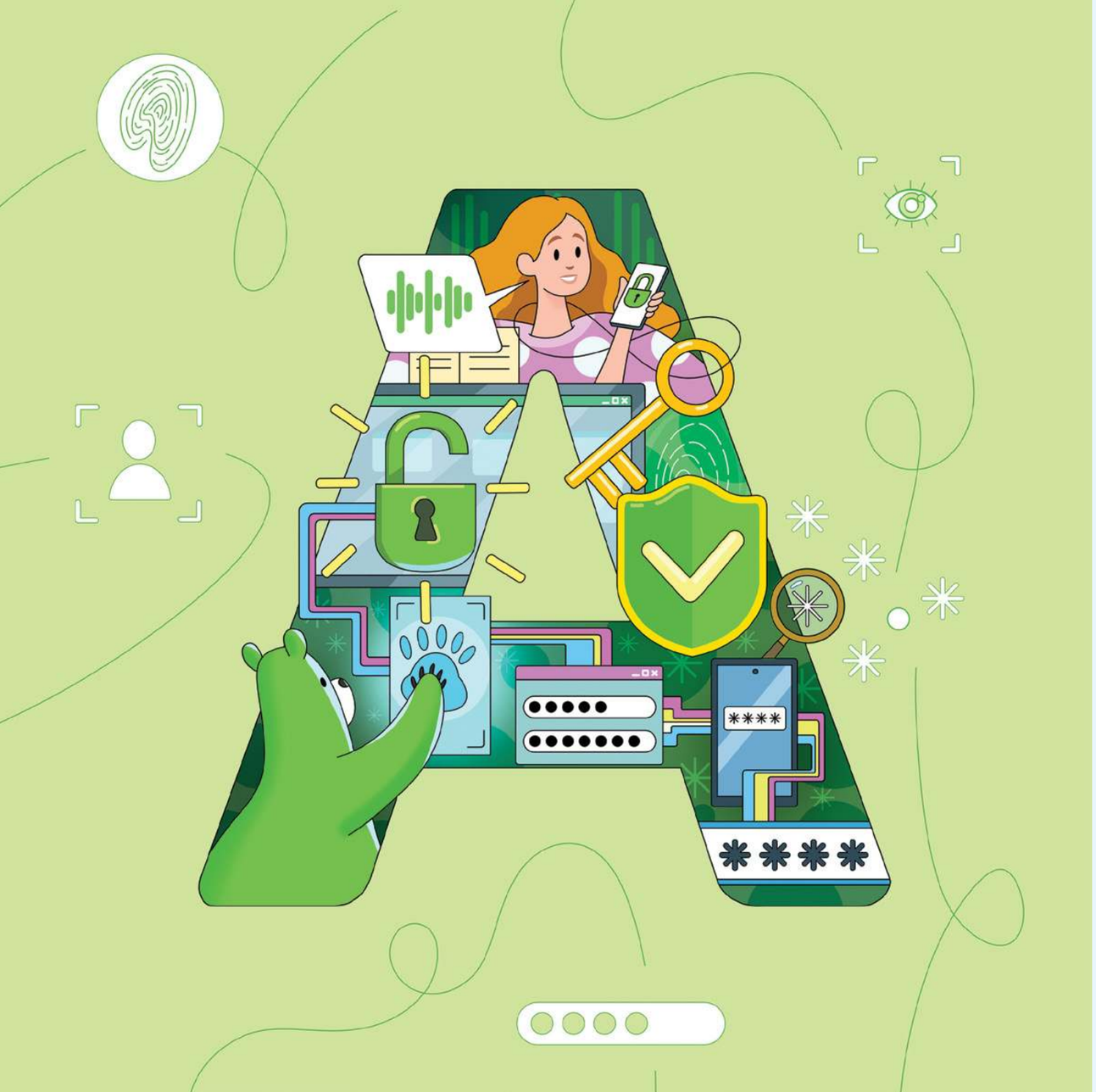
Querido amigo:
Tienes en tus manos el abecedario de Ciberseguridad de Kaspersky. ¿Habías escuchado alguna vez este término? La ciberseguridad nos ayuda a utilizar las tecnologías más modernas de forma segura, ya sea un smartphone o una computadora, y a explorar el mundo online sin tener que preocuparnos por posibles amenazas.

El mundo digital es enorme. Hoy en día, puedes hacer muchas cosas por Internet, como viajar sin salir de casa o estudiar otros idiomas hablando con gente que vive en otros países. Además, puedes jugar online, tanto con tus compañeros de clase como con tus amigos, ¡incluso con los que están lejos!

Sin embargo, además de estas infinitas oportunidades, y como sucede en la vida real, Internet también alberga algunos peligros. Por eso debes estar siempre alerta. Los descuidos en la red y el incumplimiento de ciertas normas pueden traer graves consecuencias como infectar tu tablet o smartphone con “malware”, exponiendo información importante a los ciberdelincuentes. También pueden robarte los logros y progresos que hayas conseguido en tu juego online favorito.

En este libro, conocerás las nuevas tecnologías, aprenderás las principales normas para hacer un uso seguro de Internet, descubrirás cómo evitar las amenazas online y reconocerás los trucos de los estafadores. Para que tu viaje por Internet sea emocionante y esté libre de malas experiencias, estudia este libro de la A a la Z.

Para ayudar a los niños a explorar el mundo online de forma segura, hemos creado una aplicación digital para padres: Kaspersky Safe Kids.



Autenticación

La autenticación es como tener un código o contraseña que te ayuda a entrar a tu computadora, teléfono o cuentas online.

Cuando quieres acceder a algo importante en tu teléfono o computadora, como a tus tareas de la escuela, ¡tu teléfono o computadora necesitan saber que eres realmente tú quien está intentando acceder! Gracias a la autenticación, podrás estár seguro de que solo quien tenga ese código especial o contraseña puede utilizar tus dispositivos.

Backup (copia de seguridad)

El backup es una copia digital de la información que no quieres perder.

¿Alguna vez has perdido tareas escolares o se te ha derramado un vaso de agua encima y has tenido que volver a hacerlas? ¿Alguna vez has olvidado guardar una partida en tu juego favorito y has tenido que volver a empezar? Estamos de acuerdo contigo en que es algo frustante. En el mundo virtual, los archivos también pueden borrarse o dañarse. Por este motivo existen las copias de seguridad, un lugar especial donde se pueden guardar todas las imágenes, videos y archivos importantes para que nunca se pierdan. Así que recuerda: ¡Ten una copia de seguridad y tus archivos digitales estarán siempre protegidos!

Captcha

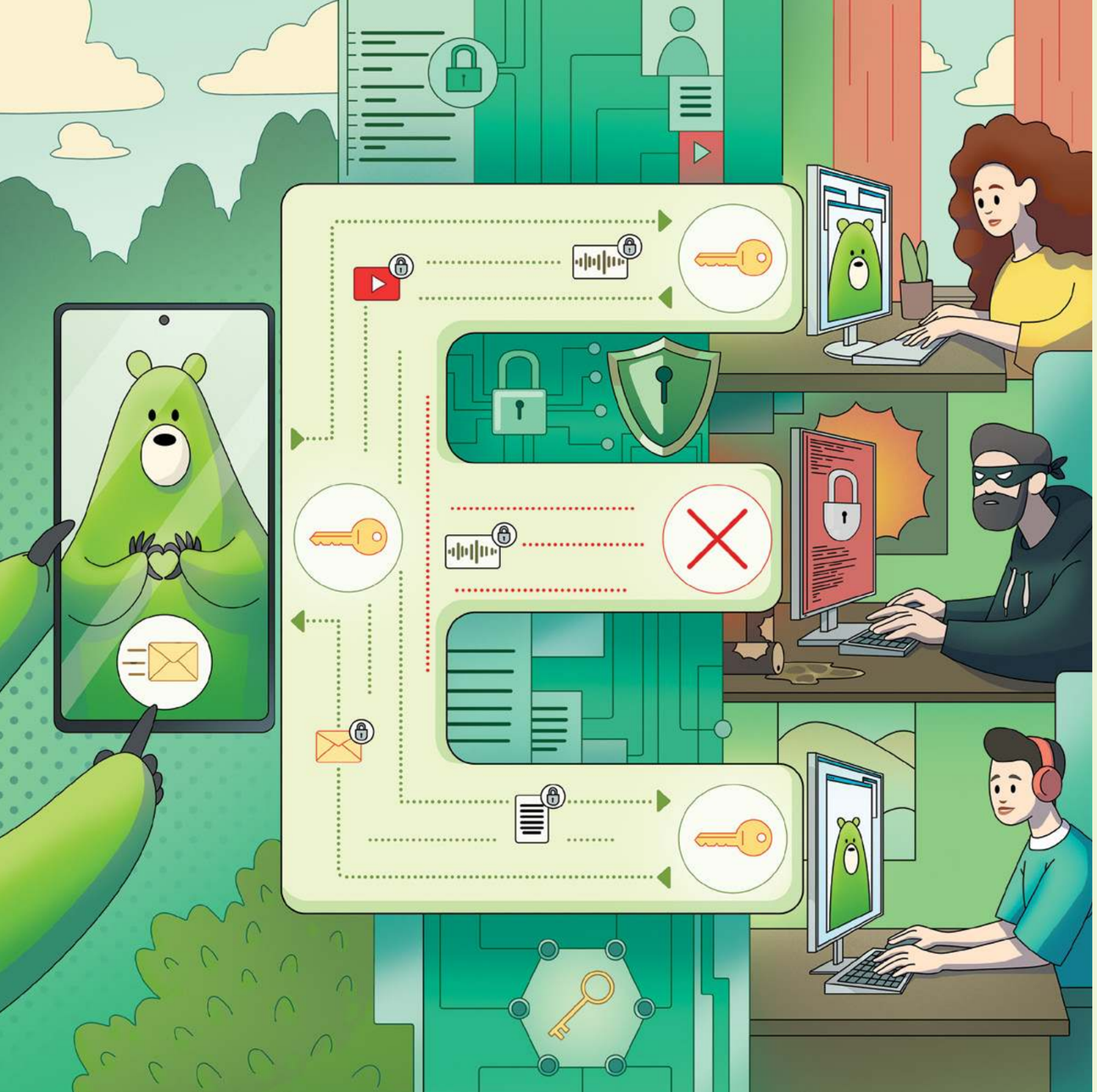
El captcha es una prueba para comprobar que eres alguien de carne y hueso y no un robot que se hace pasar por una persona.

¿Alguna vez te han pedido que resuelvas un rompecabezas o que elijas ciertas imágenes antes de poder entrar a un sitio web o un juego en línea? ¡Suele ser un captcha! Te pide que hagas algo que a los robots no se les da muy bien, como hacer clic en cuadros con automóviles o semáforos o escribir letras y números complicados. Esto ayuda a proteger las páginas web y aplicaciones de robots traviesos cuyas intenciones no suelen ser muy buenas, también conocidos como spambots.

Huella Digital

Una huella digital es como un pequeño rastro de información que dejamos cada vez que hacemos algo en Internet. Como las huellas que vas dejando en la arena cuando caminas por la playa.

Todo lo que haces, como publicar imágenes, escribir comentarios o, incluso, dar me gusta a publicaciones, puede ser visto por otras personas que también usan Internet. Una vez que algo está en la red, quedará ahí para siempre. Es como escribir con una pluma en un papel: puedes intentar borrarlo, pero será muy complicado y puede que si lo consigues, quede algo de rastro. Por eso es importante que seas precavido con lo que haces y dices en Internet.



Encriptación

La encriptación o el cifrado es parecido a un código especial que mantiene las cosas en secreto. Cuando vamos a enviar un mensaje y no queremos que ningún extraño pueda acceder a él, utilizamos la encriptación para codificar las palabras.

La encriptación es muy importante porque ayuda a proteger nuestros mensajes de personas que no deberían verlos. Mantiene segura nuestra información, como nuestras contraseñas y datos personales. Las aplicaciones y las páginas web, por ejemplo, utilizan automáticamente herramientas de cifrado para mantener la información en secreto.

En las redes sociales, cuando hablamos con nuestros amigos o enviamos fotos, el cifrado también se utiliza para mantener nuestros mensajes privados. De esta manera, si alguien intenta ver tu mensaje y la aplicación tiene cifrado, sólo podrá ver letras descolocadas que no tienen ningún significado. ¡Igual que si estuviera intentando leer una sopa de letras!

Fraude

El fraude se produce cuando algunas personas engañan a otras para conseguir información personal, datos de pago, etc.

Es importante que tengas cuidado con los estafadores en Internet. Como no sabes quién está al otro lado de la pantalla, fingen ser un amigo o alguien en quien confías. Quieren que les cuentes secretos o te engañan para que compres cosas que no son reales o con la excusa de hacerte un regalo muy lindo, como una PlaySation. Pero cuidado, porque su objetivo es robar tu dinero y tu información. Si te prometen cosas demasiado buenas para ser reales, no te lo creas, ya que pagarás por ello y nunca lo recibirás. Tampoco hables con desconocidos en Internet. Y, si alguien te hace sentir incómodo o te pide hacer cosas extrañas, díselo a un adulto en quien confíes: papá, mamá, tu profe...

Geolocalización

La geolocalización es una tecnología que permite saber a nuestros dispositivos, como teléfonos y computadoras, dónde estamos: en casa, en la escuela, en la playa... Es muy útil porque nos ayuda a ir de un lugar a otro, a encontrar la heladería más cercana o a saber a qué distancia están nuestros amigos, pero hay que ser cuidadoso al utilizarla.

La geolocalización es uno de tus mayores secretos. Al igual que el superhéroe de tu peli favorita no revela al villano dónde se esconde, es importante que tú no reveles tu ubicación a ningún desconocido en Internet. Es genial que tus padres sepan dónde estás, pero, por tu seguridad, los extraños no deberían tener esa información. Si una aplicación te pide permiso para tener tu geolocalización, coméntaselo a tus padres y pregúntate: "¿Esta aplicación realmente necesita saber dónde estoy?". Si no lo necesita, no deberías aceptar compartir tu geolocalización con esa app.

Honeypot

Un honeypot es una trampa que los expertos en informática utilizan para atrapar a personas que intentan hacer cosas malas en Internet.

¿Sabías que a algunos osos les encanta la miel? Si quisieras atraer a Winnie the Pooh, por ejemplo, bastaría con un buen tarro de este delicioso dulce. Algo parecido hacen los expertos en informática: utilizan un honeypot (que en español significa 'tarro de miel') a modo de trampa para atraer no a osos, sino a personas que hacen cosas malas en Internet. De este modo, observan todo lo que hacen esas personas y aprenden sobre sus trucos para mantenernos a salvo.

Dirección IP

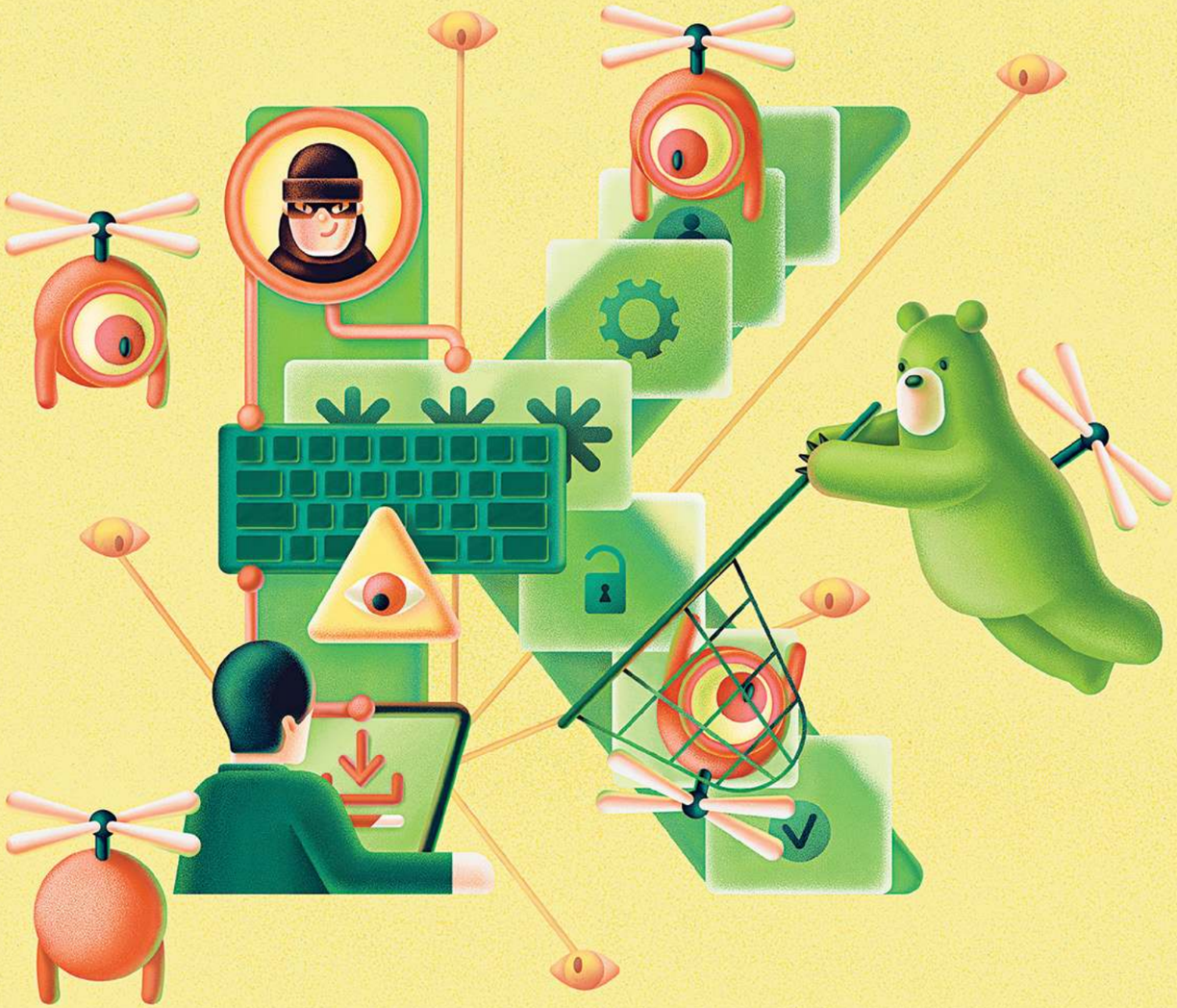
Una IP es una dirección especial que te conecta a Internet.

Una dirección IP ayuda a Internet a saber dónde enviar la información cuando estás conectado. Es como la dirección de tu casa para que el cartero sepa dónde entregar las cartas y los paquetes. Cada punto de conexión a Internet tiene una dirección IP única. Por ello, tendrás una IP diferente dependiendo de qué conexión estés usando: el Internet de tu móvil, la Wi-Fi de casa de tus tíos, la Wi-Fi del hotel en el que pasas las vacaciones...

Jailbreak

Jailbreak, que en español significa ‘fuga’, es cuando alguien rompe las reglas sobre el funcionamiento de su teléfono, haciendo algo que no está permitido.

Normalmente, solo puedes descargar las aplicaciones permitidas por los sitios oficiales. Cuando haces jailbreak, puedes descargar y usar todo tipo de aplicaciones que normalmente no están permitidas. Quizás suene divertido, pero puede meterte en problemas, provocando que el dispositivo no funcione bien o, incluso, permitiendo que gente mala haga cosas malas con él. Por lo tanto, es importante seguir siempre las normas y recordar que los juegos y aplicaciones más seguros y divertidos no necesitan jailbreak.



Keylogger

El keylogger es un registrador de teclas. Se llama así porque es un programa que puede saber todo lo que escribes en tus dispositivos y guardarlo con objetivos no muy buenos.

Un keylogger registra cada tecla que presionas y luego la guarda. Es muy peligroso, ya que puede saber qué mensajes escribes o cuáles son tus contraseñas. Por lo general, el keylogger se descarga en tus dispositivos sin que tú lo sepas, escondido en cosas que descargas de Internet, como el último lanzamiento de tu videojuego favorito. Por este motivo es muy importante que solo descargues archivos, juegos o aplicaciones de sitios web seguros tras haberlo consultado antes con tus padres.

Login
(Inicio de Sesión)

Para que solo tú puedas acceder a tu juego preferido o a otras aplicaciones, hay que iniciar sesión introduciendo un nombre de usuario y contraseña. De este modo, el login es como la llave que abre la puerta de tu casa.

Permite que la página web o la aplicación sepan que eres tú quien está intentando acceder y te permite hacer cosas divertidas como jugar, ver videos, o chatear con tus amigos. Tu nombre de usuario y contraseña forman una combinación que es como tu propio código secreto y que sólo tú debes conocer para poder entrar. ¡Alohomora! ¡Ábrete Sésamo!

Recuerda que para crear tu nombre de usuario y contraseña no es recomendable usar tu nombre real ni tu fecha de cumpleaños, ya que estarías dando pistas a otras personas. ¡Utiliza todo tu ingenio para crear un login súper seguro!

Malware

El malware es un gusano informático escurridizo y malo que puede infectar a computadoras, tablets y otros dispositivos.

El malware puede esconderse en diferentes cosas en las que haces clic o que descargas de Internet, como juegos o fotos, sobre todo si las descargas de sitios web que no son de confianza. Cuando lo dejas entrar accidentalmente, puede estropear tus archivos o intentar robar tu información personal, como tus contraseñas o fotos. ¡Pero no te preocupes! Al igual que lavarse las manos ayuda a mantener alejados los gérmenes, puedes utilizar programas de protección de ciberseguridad para mantener tus dispositivos a salvo del malware.

NFT

Estas 3 letras significan en inglés Non Fungible Token o en español Token no fungible. ¡Uf! parece complicado, así que usaremos simplemente NFT.

Imagina que posees algo en el mundo virtual que para ti tiene mucho valor. Te gustaría tener un certificado que demuestre que esa cosa es solo tuya y de nadie más, ¿verdad? Eso es un NFT.

Un NFT es una especie de certificado que prueba que posees algo especial en el mundo digital: obras de arte, videos, o hasta mascotas virtuales. Cada NFT es único y se pueden comprar y vender utilizando algo llamado tecnología blockchain, que ayuda a garantizar que nadie pueda hacer trampas o pretender tener un NFT que en realidad no es suyo.

Oversharing

Oversharing es cuando compartimos demasiada información en Internet, más de la que deberíamos.

Compartir con desconocidos ciertos datos personales en Internet puede ser peligroso. Por ejemplo, decir a alguien nuestro nombre completo, la dirección de casa o la escuela a la que vamos. ¿Crees que Batman revelaría a un desconocido la ubicación de su baticueva?

Facilitar datos como la fecha de tu cumpleaños o el nombre de tu mascota también puede dar pistas sobre tus contraseñas. No cuentes a ningún extaño en Internet lo que no le contarías a un desconocido en la calle.

P

Phishing

Los ciberdelincuentes lo usan para intentar engañarte y robar tu información, como tu nombre y apellido, nombre de usuario o número de cuenta bancaria (si tú o tus padres los usan para comprar algo online).

Seguro que te llegan correos electrónicos y mensajes de sitios web falsos que parecen reales, pero en realidad están intentando robar tu información. Es importante tener cuidado y no compartir información personal con nadie a menos que estés absolutamente seguro de que es una página web real.

Desafortunadamente, no todas las personas que conoces online son buenas y es muy importante cuidar a quién le das tu dirección de email. A veces intentan engañarnos para que revelemos información personal siendo muy amables u ofreciendo cosas maravillosas, pero nunca debes facilitar datos como tu nombre completo, dirección, número de teléfono o contraseñas, números de tarjeta bancaria... a nadie, a menos que un adulto de confianza te diga que puedes hacerlo.

Código QR

El término código QR viene de las palabras “Quick Response” o “Respuesta Rápida”. Es una imagen cuadrada formada por muchos cuadrados pequeños de color blanco y negro, dentro de una caja más grande que te enlaza con otro archivo con más información.

Aunque parezca una imagen divertida, formada por cuadrados blancos y negros, un código QR es en realidad como una llave mágica que abre una puerta secreta. Para abrirlo, tienes que tomarle una foto con la cámara del móvil o usar una app especial y hacer clic. Al momento, es como un mapa del tesoro que te lleva a lugares especiales. En el zoológico, puedes escanear el código QR y aparecerá un sitio web con datos interesantes sobre el animal que estás mirando. En un libro, puede llevarte a un sitio web divertido que te brinda más información sobre la historia.

Lamentablemente, los ciberdelincuentes también saben cómo utilizar los códigos QR y los usan para hacer maldades. Pero por suerte, existe un programa especial que te indica si el código QR es seguro. Recuerda que no debes descargar una aplicación desde un código QR, hazlo siempre desde la App Store o Google Play.

Ransomware

El ransomware es un programa informático que puede cifrar o encriptar todos los archivos del dispositivo y luego pide un rescate para acceder a ellos.

El ransomware se cuela en el ordenador y secuestra todos los archivos importantes: imágenes, videos y documentos. Luego, los malvados que crearon el ransomware los secuentran y dejan una nota pidiendo dinero para poder recuperarlos, a modo de rescate. Pero recuerda, ¡nunca te fíes de lo que dicen! Es posible que simplemente desaparezcan y te dejen con un dispositivo dañado aunque hayas pagado. Lo que debes hacer es decírselo a un adulto para que pueda arreglar el equipo. Además, haz una copia de seguridad: es como guardar un nivel en un juego. De esa manera, si algo sale mal, no todo desaparecerá de tu dispositivo.

Spam

El spam es como la basura que nos dejan en nuestro buzón (folletos, publicidad...), pero en nuestro email.

Igual que a veces nos envían por correo cartas o folletos que no queremos ni necesitamos, también sucede con los correos electrónicos. Estos emails pueden ser comerciales, de cosas que no queremos comprar, incluso estafas que intentan engañarnos para que revelemos nuestra información personal. Es importante tener cuidado con los correos electrónicos no deseados y no hacer clic en ellos ni responderlos, igual que hacemos con el correo basura del buzón de casa. La mejor manera de evitar los correos electrónicos no deseados es no revelando nuestra dirección de email a menos que realmente lo necesitemos.

Troyano

Los troyanos son programas informáticos que se apoderan del ordenador para hacer cosas malas.

Un troyano puede tener la apariencia de un juego de computadora o un programa inofensivo, pero en realidad es un pequeño personaje malvado que quiere entrar en el equipo, robar la información y destruir los archivos. Los troyanos suelen esconderse en sitios web no seguros y tienen muchos trucos para engañarnos: te dicen que puedes descargar juegos caros gratis o ver en tu ordenador una película que sólo se proyecta en los cines. No hagas ni caso a esos regalos falsos y utiliza sólo páginas web verificadas, las que tienen una gran marca de verificación verde. Recuerda, así como no dejas que entren extraños en casa, ten cuidado con lo que descargas porque podría ser un troyano astuto. Sin duda, pide permiso a tus padres antes de descargar algo en los dispositivos.

URL

URL es una dirección que tienen todos los elementos online: sitios web, imágenes, un libro en línea, etc.

Igual que tu casa tiene una dirección para que la gente sepa cómo encontrarla o el cartero sepa dónde dejar las cartas, una URL le dice al navegador de Internet dónde encontrar un sitio web. Es una combinación de letras, números y símbolos que ayudan a conectarse al sitio web correcto. Puedes encontrar la URL de una página en la barra de direcciones en la parte de arriba del navegador. Presta mucha atención a la dirección URL y compárala con el nombre oficial de una empresa/organización/tienda o cualquier otra cosa. Si la URL parece rara o sospechosa, igual es porque estás en un sitio web falso o de phishing.

VPN

Una VPN (Virtual Private Network), en español, Red Pivada Virtual, es una herramienta que te ayuda a navegar seguro.

Es como un túnel secreto en Internet por el que pasa todo lo que haces cuando te conectas en privado. ¡Como un escondite secreto al que solo puedes acceder tú! Una VPN mueve tus datos a un lugar especialmente protegido y funciona como una máscara: los sitios web que visites no obtendrán tu información, sino que verán solo la máscara que les muestre el servicio VPN. Igual que no te gusta que un extraño revise tu diario o tu habitación, una VPN te ayuda a proteger tus actividades en línea de extraños que puedan intentar mirar tus cosas personales.

Router Wi-Fi

El router Wi-FI es lo que te ayuda a conectarte a Internet.

Sin Wi-Fi no podrás acceder a Internet. El router es la caja que está casi siempre cerca de la tele y te permite conectar a Internet los dispositivos de casa: tele, tablet, teléfono móvil, etc. Es lo que está justo en medio, entre Internet y tú, y trasmite los datos desde tu dispositivo a Internet. Por eso, y para evitar que alguien robe tus fotografías u otros archivos, debes proteger tu Wi-Fi con una contraseña. Pon una contraseña que sea difícil de adivinar con tu familia y dísela solo a personas de confianza.

Por muy interesante que parezca, no te conectes al wi-fi “gratuito” de tiendas o restaurantes, porque podría no ser seguro. Al menos, no te conectes sin proteger tu dispositivo.

eXploit

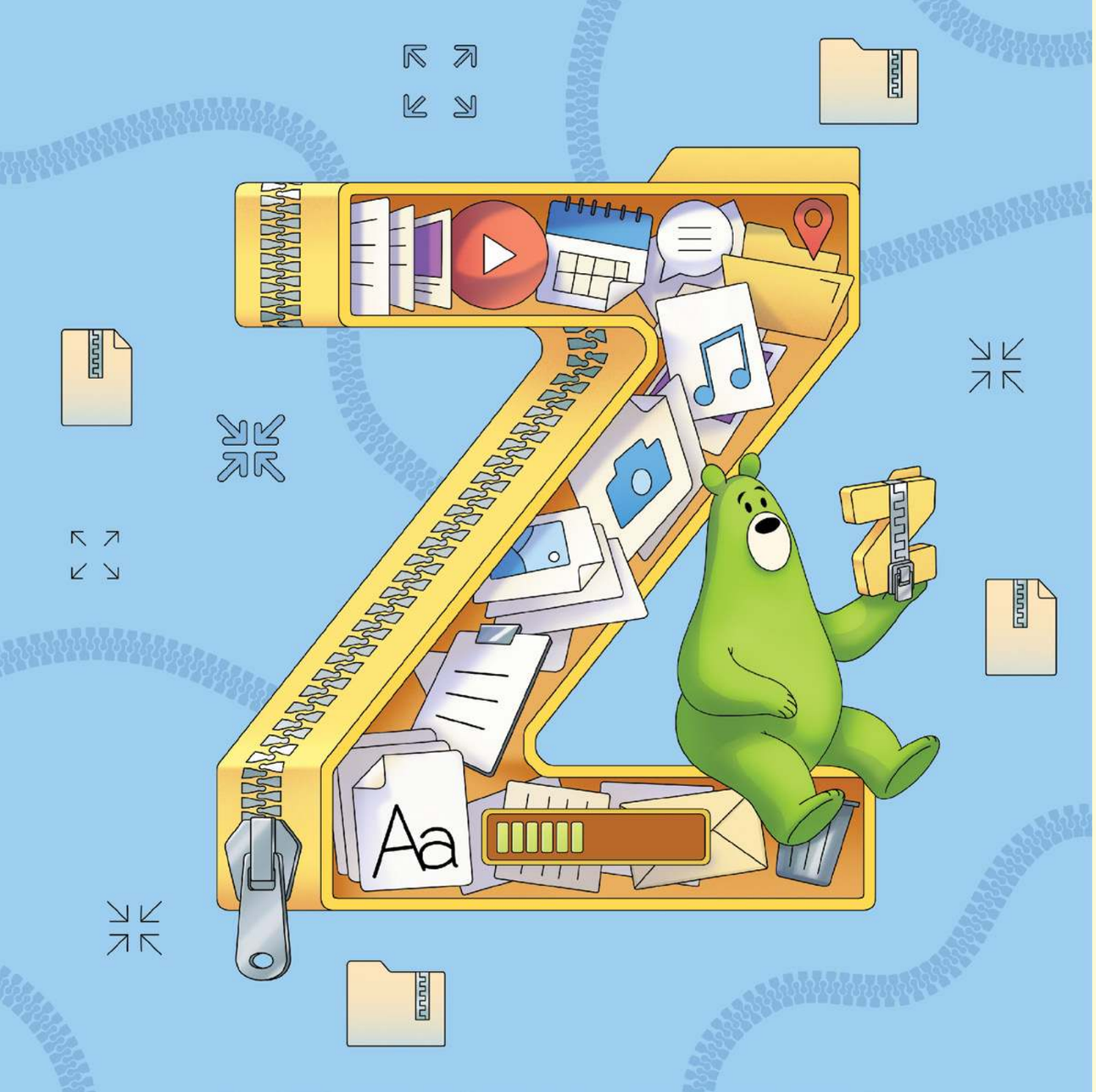
Un exploit es una especie de agujero en tu dispositivo que ayuda a los ciberdelincuentes a entrar, infectarlo con un programa malicioso y decirle a tu dispositivo qué hacer sin tu permiso.

Es como un código de trucos en un juego online: conociendo estos trucos, los ciberdelincuentes pueden romper las reglas y hacer lo que quieran con tu dispositivo.

Ciberbullying

El Ciberbullying se produce cuando alguien se porta mal o intenta hacer daño a otras personas en Internet.

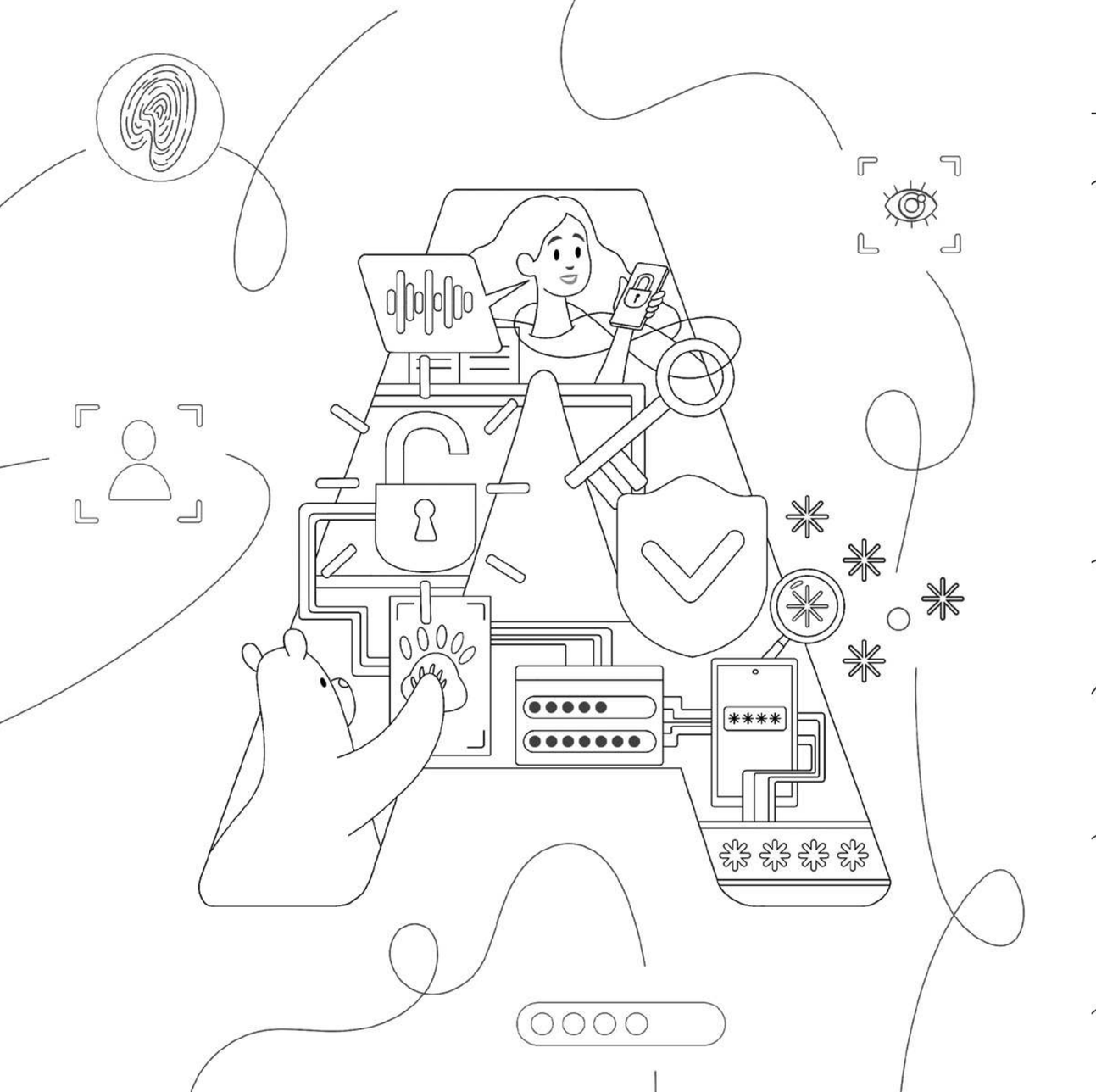
Puede pasar de muchas formas, como enviar mensajes desagradables o difundir rumores sobre alguien en Internet. El ciberacoso o ciberbullying hace que las personas que lo sufren se sientan tristes, avergonzadas o asustadas. Es importante ser amable con los demás en Internet, igual que en la vida real. Si crees que alguien te está acosando online, comparte tus sentimientos con adultos en quienes confíes. Lo que un acosador dice sobre ti no tiene nada que ver con quién eres realmente. Por lo tanto, nunca tomes en serio sus palabras. No intentes devolver el acoso, porque a menudo esto puede empeorar las cosas. Toma capturas de pantalla de tu chat, bloquea a quien te está acosando/molestando y habla con un adulto.

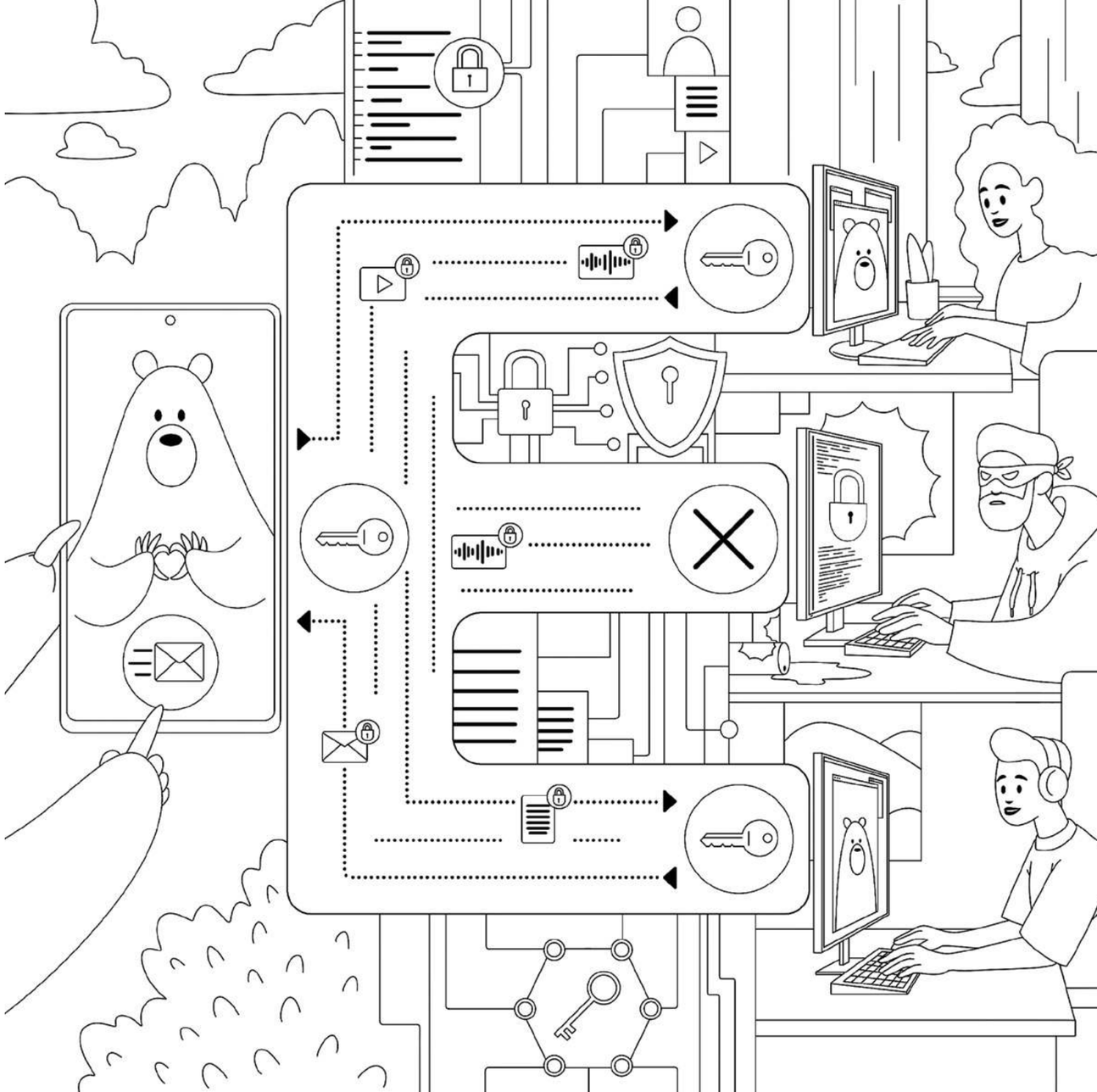


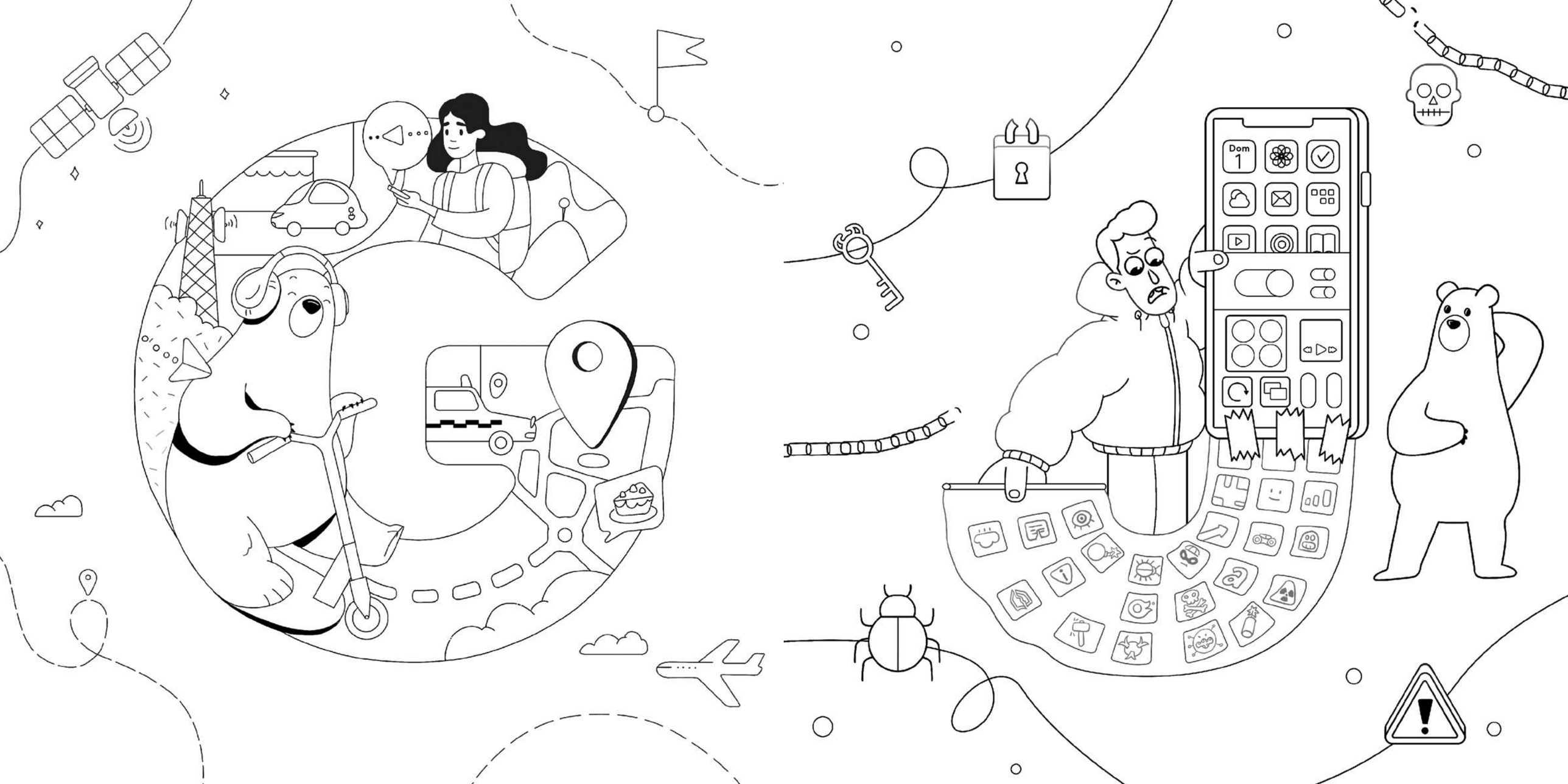
ZIP

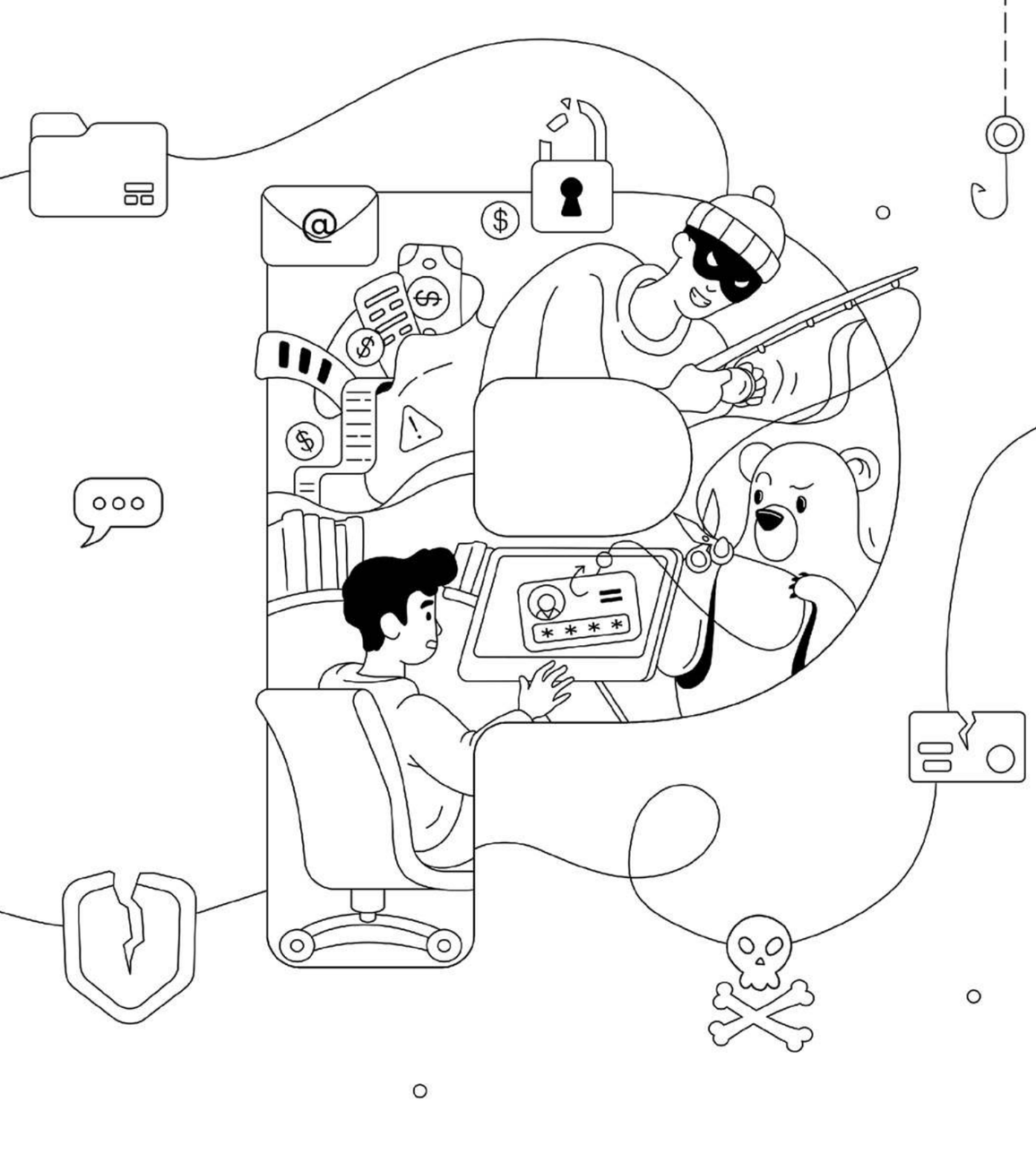
Un archivo zip es como una bolsa en la que puedes guardar muchas cosas.

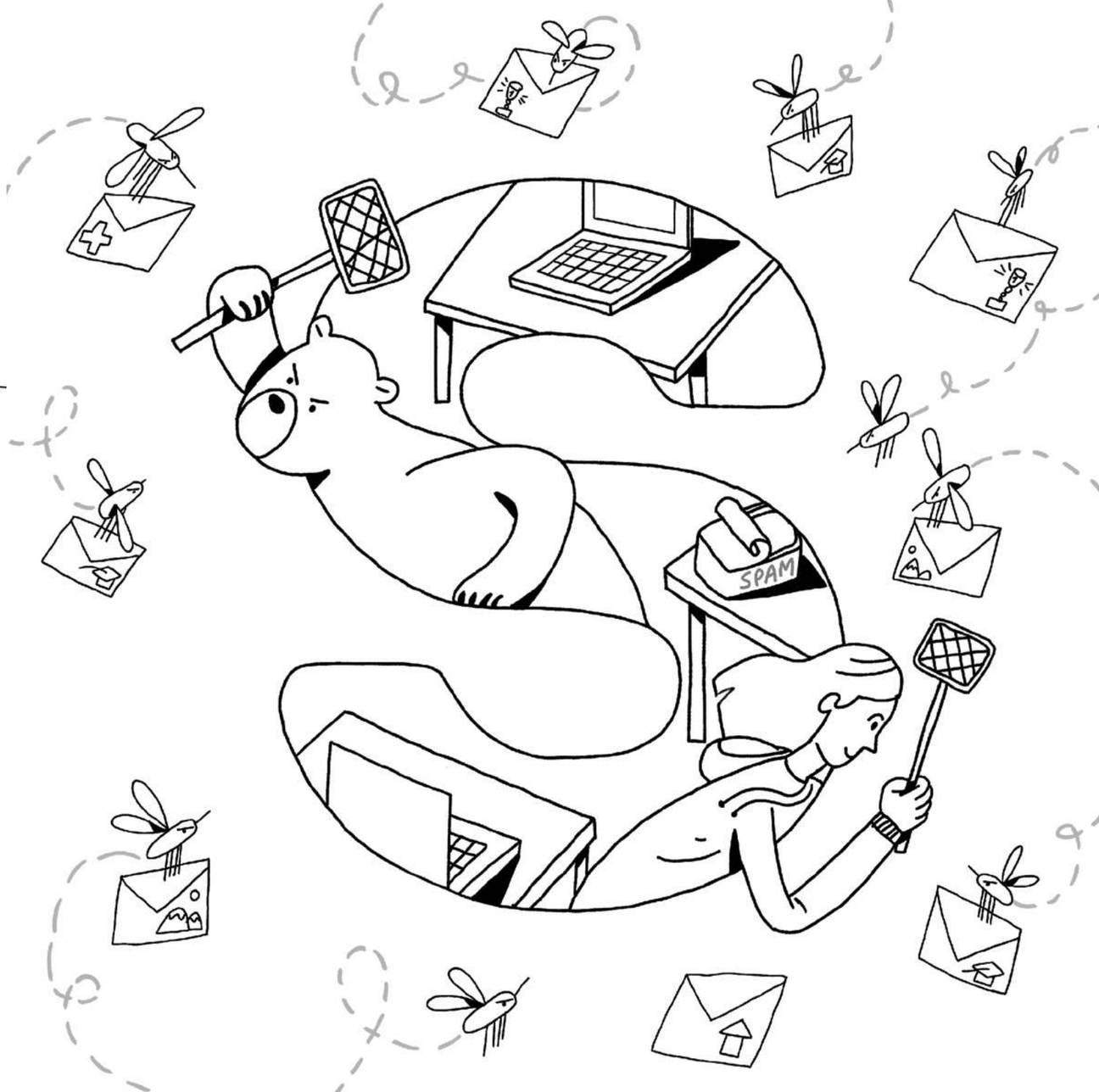
Ayuda a mantener todas las imágenes, archivos y carpetas juntos en un solo lugar. Cuando usas un archivo zip, puedes reducir o "comprimir" todas esas cosas, haciéndolas pequeñas para que ocupen menos espacio en tu equipo o computadora. Y cuando quieras volver a utilizar esas cosas, puedes abrir esa bolsa con cierre y sacar todo lo que hay dentro.

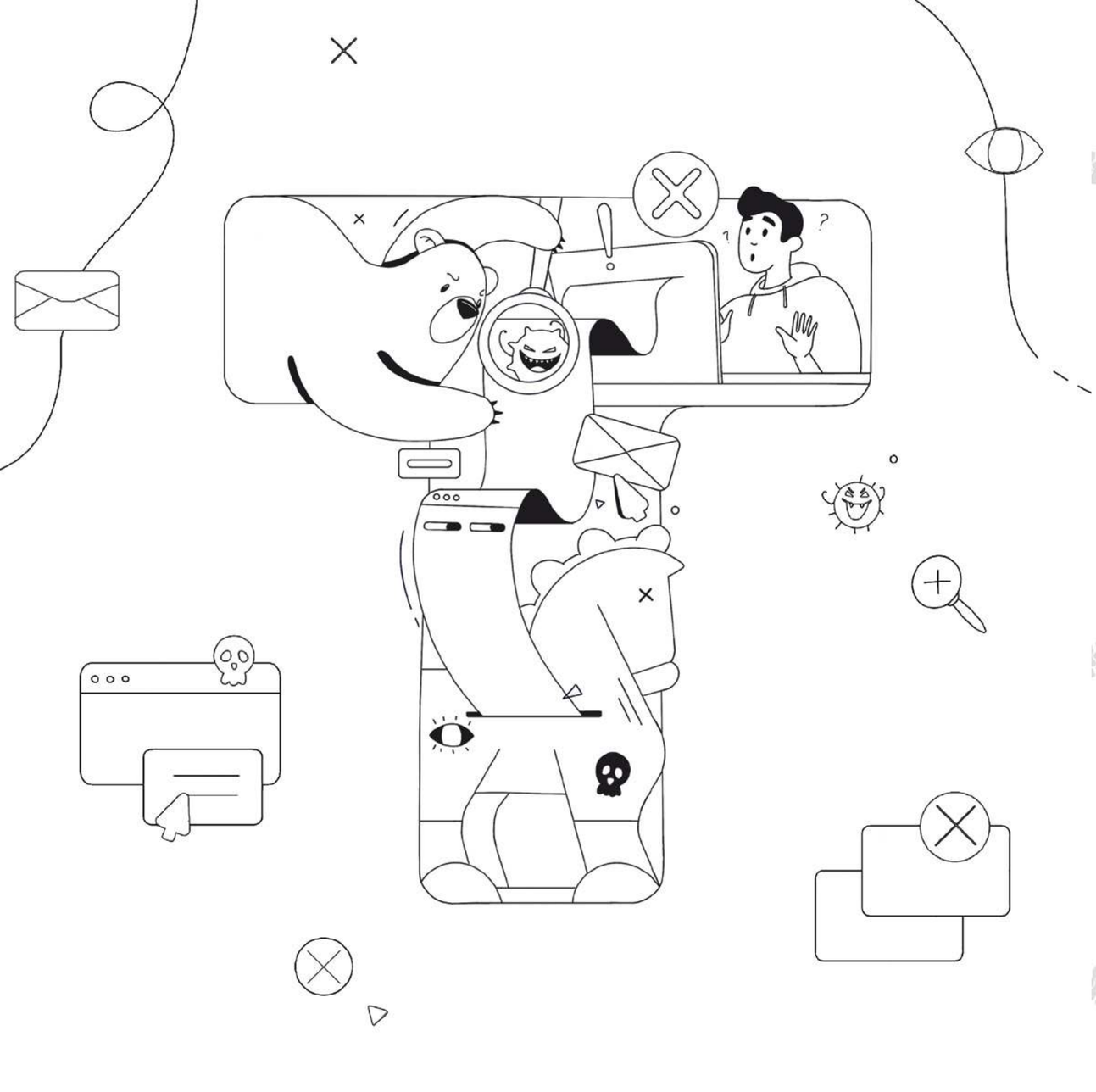


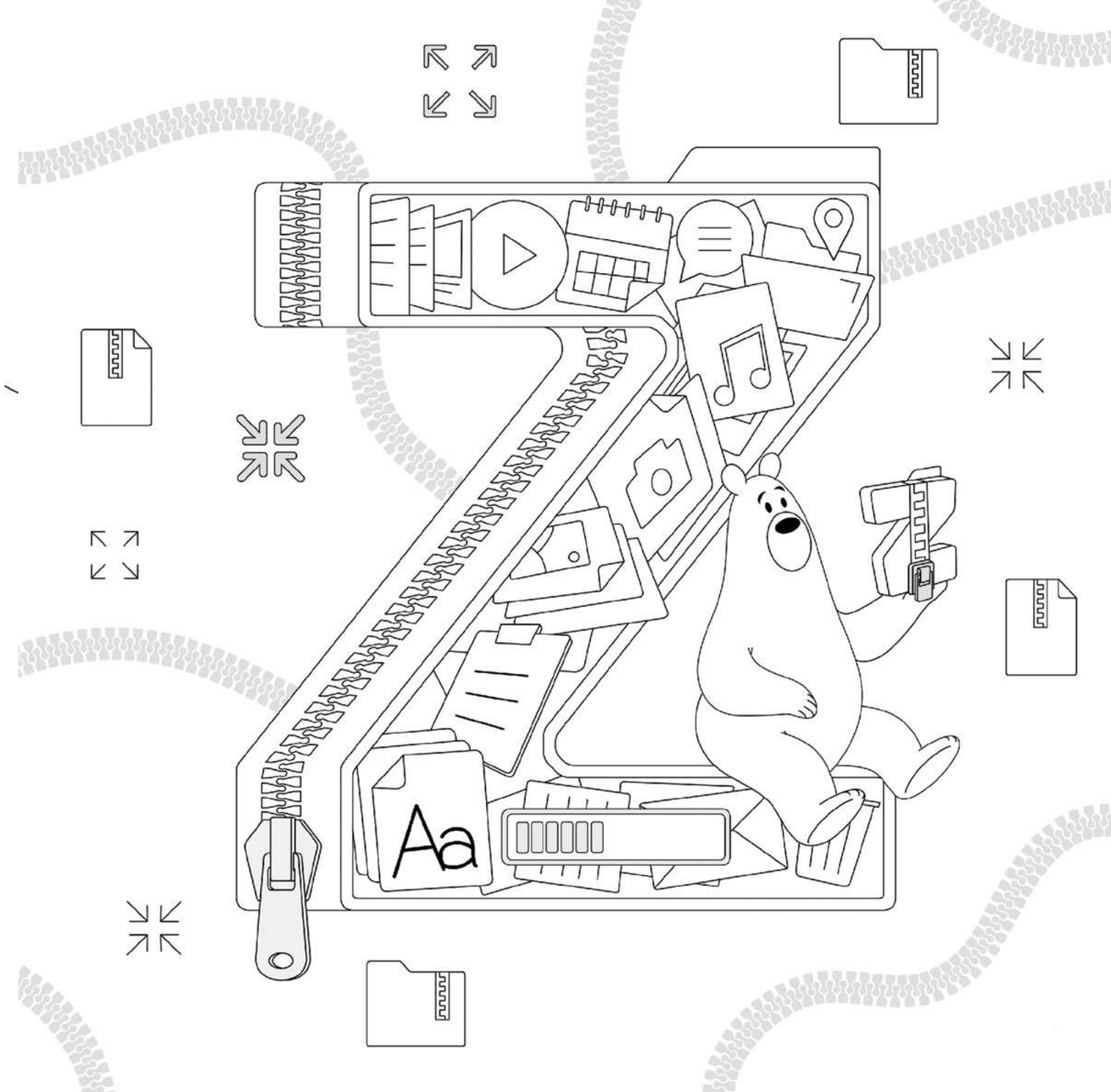



Dom
1


@
$
$
$
$
$
!
* * * *


SPAM




Aa

Notas

Querido ciberexplorador:

¡Qué increíble aventura hemos vivido! De la A a la Z, has recorrido todos los senderos de la ciberseguridad. Recuerda que estar seguro en Internet es igual de importante que estarlo en el mundo real. Como los superhéroes, tienes el poder de tomar decisiones inteligentes en Internet: elegir contraseñas seguras, mantener la privacidad de la información personal y pensártelo dos veces antes de acceder a enlaces desconocidos.

Tu aventura no acaba aquí. El mundo digital está en constante cambio y aún queda mucho por aprender. Mantén la curiosidad, haz preguntas y sigue actualizando tus conocimientos cibernéticos. Enseña a tus amigos y familiares el abecedario de la seguridad en Internet. Juntos ayudarán a construir un mundo online más seguro.

Diseño gráfico, maquetación e ilustraciones de la agencia Thoughtform: www.behance.net/Thoughtform