kaspersky

Hello!
From this book you will learn the most important terms from the virtual world. We will tell you what useful things you can find in it and what dangers lurk in it.
Open the book and go on a journey!

kaspersky

Cybersecurity Alphabet

This book belongs to _____

Dear friend,
You're holding in your hands the Kaspersky Cybersecurity alphabet. Have you ever come across the term "cybersecurity" before? Cybersecurity helps us to use modern technologies — either a smartphone or a computer — safely and explore the online world without worrying about possible threats.

The digital world is huge. Nowadays, you can do a lot of things online: travel without leaving your home, or study foreign languages by talking to native speakers, for instance. And, of course, you can play games, not only with your classmates, but also with friends; even with those who are far away!

But along with the endless opportunities, there are some dangers on the internet, just like in real life. So you should always be alert. Careless actions online and the negligence of the cyber hygiene rules could lead to severe consequences: you can infect your tablet or smartphone with malware, exposing important information to cybercriminals or people could steal your awards and the progress you make in your favorite online game.

In this book, you'll get to know new technologies, learn the main cyber hygiene rules, find out how to avoid online threats, and recognize fraudsters' tricks. To make sure that your online journey is exciting and free from bad experiences, please study this book from A to Z.

To help children safely explore the online space, we have created a digital parenting app — Kaspersky Safe Kids
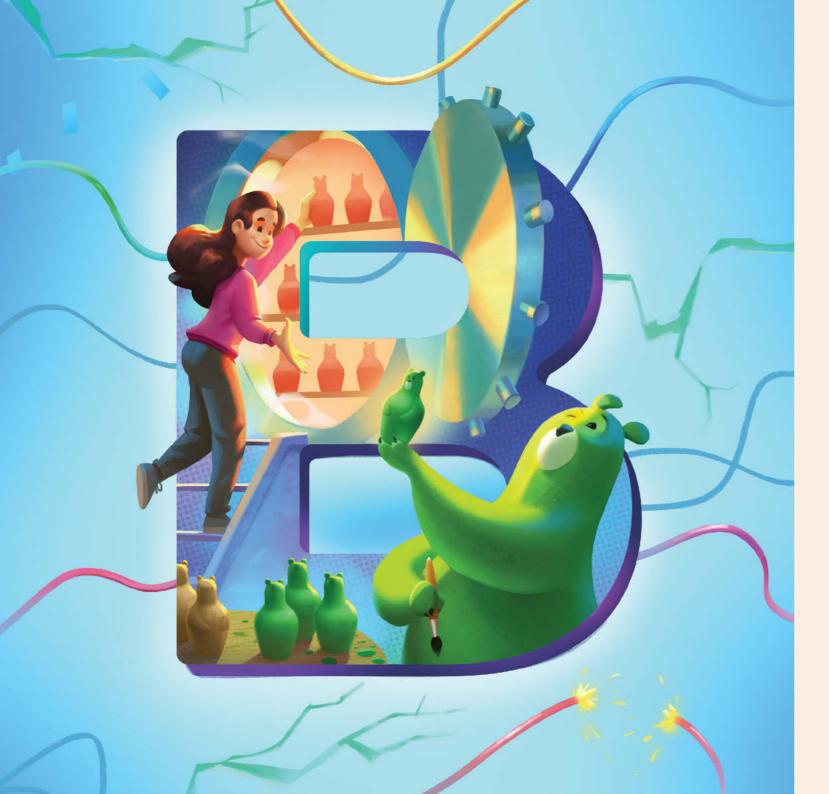
Authentication

Authentication is like having a special secret code or a password that helps you get into your computer, phone or online account.

When you want to get into something important like your phone or your school computer, you have to tell your computer that it's really you and that it can trust you. With this "authentication," you can make sure that only the right person is allowed to use or do something on your device. That's what authentication is all about: making sure only the right people can use special devices!

Backup

Backup is a copy of digital information that you really don't want to lose.

Just imagine: one of your favorite games got left behind when you were on vacation, but luckily your mom had exactly the same one put away in a special storage place. In the same way, a backup is a special place where all your pictures, videos, and important files can be put away, so they never get lost. Sometimes, accidents happen, or things go wrong with our devices; they can get lost or stop working. But with backup, we don't have to worry because all our favorite things are in a safe place. So remember, always have a backup, and your digital things will always be protected!

Captcha

Captcha is a special test to check
if you are a real person using a computer
or a robot pretending to be a person.

Have you ever been asked to solve a puzzle or pick out certain pictures before you can keep going onto a website or playing an online game? That's usually a Captcha! It asks you to do something that robots can't do very well, like clicking on boxes with cars or traffic lights or typing in tricky letters and numbers. It helps protect websites and apps from bad robots, also known as spambots, that might try to do something naughty.
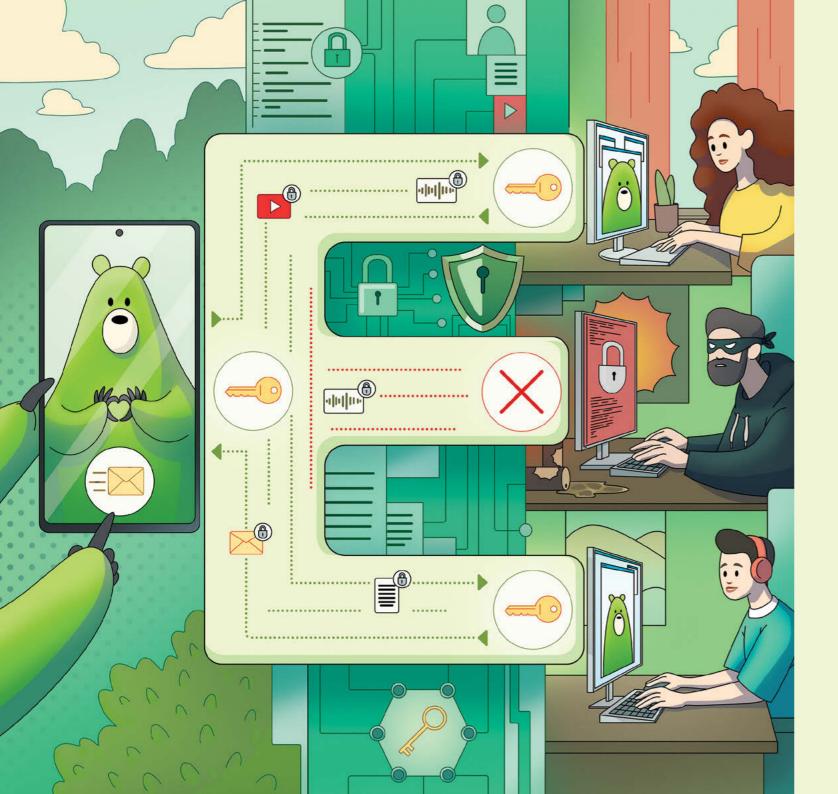
Digital footprint

A digital footprint is like a little trail of information that we leave behind whenever we do something on the internet. Just like leaving footprints in the sand when you walk on a beach.

Everything you do, like posting pictures, writing comments, or even liking posts, can be seen by other people online. It's important to remember that once something is online, it's there forever. That's why we need to be careful about what we do and say on the internet, because it can affect how other people see us.

Encryption

Encryption is like a special code that keeps things secret. When we want to send a message, we use encryption to scramble the words to keep our words inaccessible to strangers.

Encryption is really important because it helps protect our messages from people who shouldn't see them. It keeps our information safe, like our passwords and personal details. Apps and websites automatically use encryption tools to keep your information a secret.

In social media, like when we chat with our friends or send pictures, encryption is also used to keep our messages private. This way, if someone tries to take over your message and the app has encryption, the bad guy will only see scrambled letters.

Fraud

Fraud is when some people trick others into giving them their payment details, money or personal information.

Fraudsters pretend to be someone they're not, like a friend or someone you trust. They want you to tell them secrets or trick you into buying stuff that's not real so they can steal your money and do bad things with your information. Stay safe from fraudsters by not going on unknown websites, clicking on pop-ups, or on links that you don't know. Don't believe it when they say you won a PlayStation or money. And of course, don't chat online to or message people you don't know in real life. Also, if someone makes you feel weird or asks you to do bad stuff, tell an adult you trust.

Geolocation

Geolocation is a technology that tells our devices, like phones and computers, where we are in the world. Geolocation helps us go from one place to another, like finding the nearest ice cream shop or helping us to know how far away our friends are.

Geolocation is the biggest secret you have. So, you should always make sure you can trust the person you're sharing this information with. It's great when your mom and dad know where you are, but you shouldn't share your geolocation with strangers online. If an app asks for permission to have your geolocation, you should ask yourself: "Does this app really need to know where I am?". If not, you shouldn't give your geolocation to this app.

Honeypot

A honeypot is a trap set up by computer experts to catch bad people who try to do bad things on the internet.

It might look like a real website or a game or something fun, but it's actually a trick to catch the bad guys. Computer experts watch everything the bad people do and learn about their tricks to keep us safe. So, honeypots are like "secret spy tools" that help protect us on the internet!
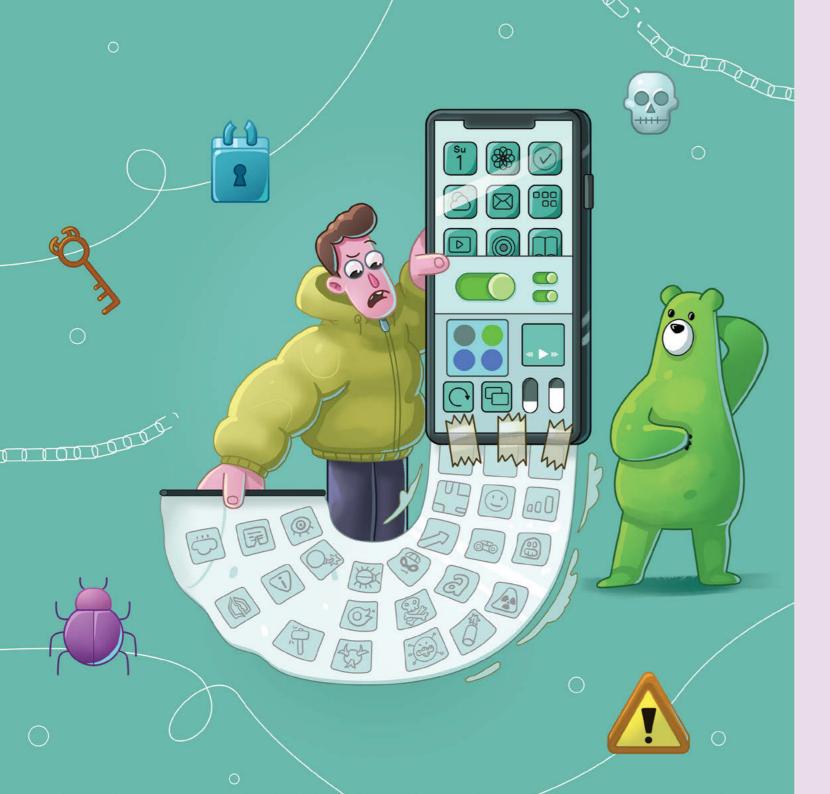
IP address

An IP address is a special address that connects you to the internet.

It helps the internet know where to send information when you're using the internet. It's like the way your home address tells the mailman where to bring your letters. Each internet connection point has its own unique IP address. If you are away from home traveling, and you take your device with you, your home IP address is not attached to the device. This is because the device will use a different network (Wi-Fi at a hotel, airport, cafe) to get on the internet.

Jailbreak

Jailbreak is when someone breaks the rules about the way how their phone works.

Normally, you can only download apps that the app store lets you use. But when you jailbreak, you can download and use all kinds of apps that are not normally allowed. It may sound fun, but it can get you into trouble. It can make the device not work well, or even let bad people do bad things with it. So, it's important to always follow the rules and not jailbreak our devices. It's much better to use our devices in the way they're meant to be used! And remember, there are plenty of fun apps and games that are safe and don't need to jailbreak.
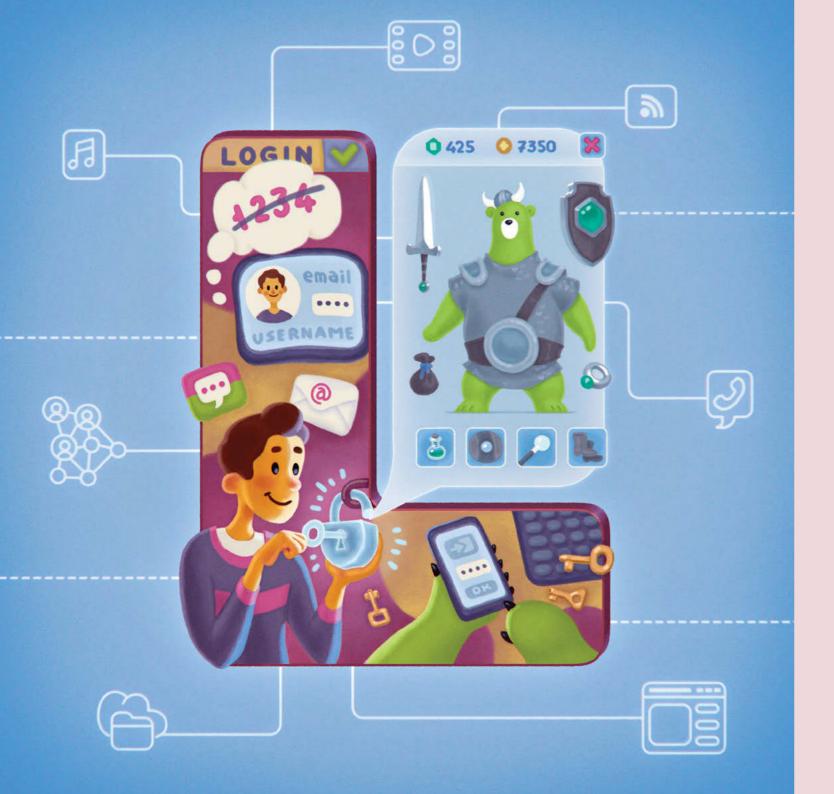
Keylogger

A keylogger is a special type of computer program that can secretly record everything you type on a computer.

A keylogger remembers every key you press and then saves it. This way, it can keep stuff like your messages and passwords. To stay away from a keylogger, don't download anything from websites you aren't sure about… some online places are dangerous, just like in the real world! Some websites try to trick people into downloading bad things like keyloggers, so only save things from trusted websites and get your parents' permission.

Login

Login is your username or email address and a password that allows you to go onto your favorite website, game, or app. It's like a special key to the door!

It helps the website or app know who you are and lets you do fun things like playing games, watching videos, or chatting with friends. Your login is like your own secret code that only you should know, so you can keep your things safe and have lots of fun in your own special space!

Create your own unique username that only you will have. Remember, it should not include your real name or your birthday. Try to create something special!

Malware

Malware is like a sneaky and bad computer bug that can make your computer or tablet sick.

It can hide in different things you click or download, like games or cool pictures, especially if you download them from websites that can't be trusted. When you accidentally let it in, it can mess up your files or try to steal your personal information, like your passwords or pictures. But don't worry! Just like washing your hands helps keep germs away, you can use cybersecurity protection programs to keep your computer safe from malware.

In order to protect your devices from malware, don't forget to install and use a comprehensive and reliable security solution, such as Kaspersky Premium.
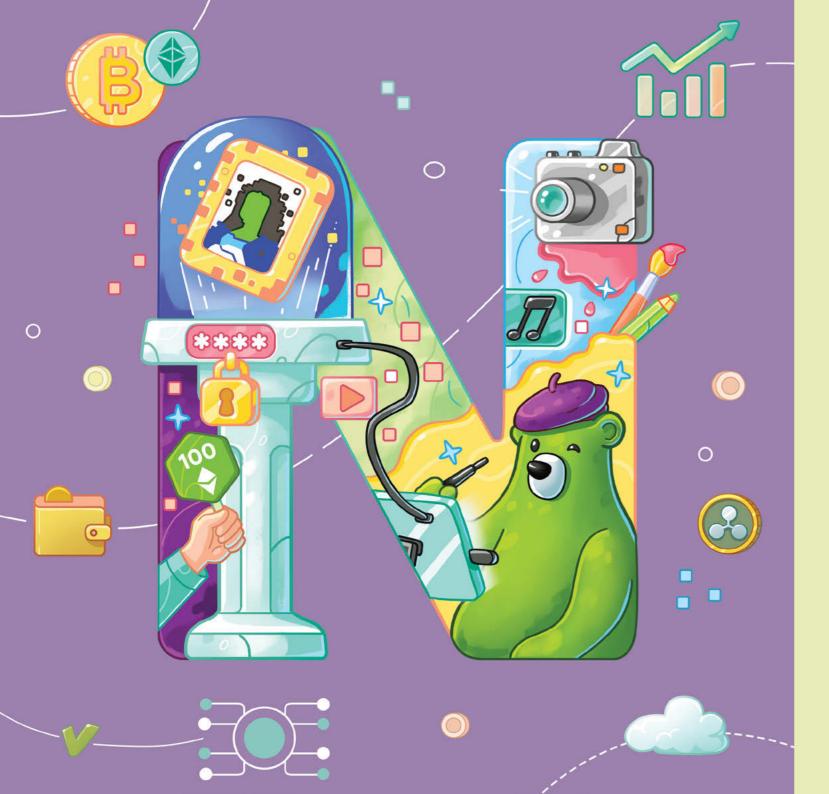
NFT

Imagine you have a special trading card that everyone loves. It's not just any trading card, though; it's a one-of-a-kind card and can only belong to you. This trading card is called a Non-Fungible Token, or NFT for short.

An NFT is a special digital thing that can stand for things like artwork, music, videos, or even virtual pets. It's different from something like money or regular trading cards because each NFT is unique, just like you are! It can't be swapped for something else of the same value.

NFTs are like having a certificate or a proof that you own something special in the digital world. People can buy and sell NFTs using something called blockchain technology. That's like having a special computer network that keeps a record of who owns each NFT. It helps make sure that nobody can cheat or pretend to have an NFT that is not really theirs.

Oversharing

Oversharing is when we tell someone more about ourselves online than we should.

Always be careful about telling people you don't really know something personal about yourself: things that are unique only to you and can help someone tell you apart from others (your name, birthday, contact details, school, location, and etc.). Also be careful about some facts that don't seem so important, like your pet's birthday. Your personal information or any facts that you tell someone about yourself and your life online can be used by strangers to get your trust. Before sharing or publishing any information about yourself online, ask yourself if you would tell these things to a stranger on the street.

Phishing

Phishing is when cybercriminals try to fool you and steal your information – things like your first and last name, login name, or bank account number (if you or your parents use those to buy something online).

They might send you emails and messages, or even make fake websites that look real, but they are actually trying to steal your information. So, it's important to be careful and never share your personal information with anyone unless you are absolutely sure it's safe. Unfortunately, not everyone you meet online is a good person, and it's really important to be careful who you give your email address to. Sometimes people may try to trick you into giving away your personal information by being really nice, but you should never give things like your full name, address, phone number, or passwords to anyone online unless a trusted adult says you can.

QR code

The term QR code comes from the words "quick response." It looks like a square picture made up of lots of little black and white squares inside a bigger box.

Although it looks like a funny picture made up of black and white squares, a QR code is actually like a magic key unlocking a secret door. To open it, you can point the camera on your phone or a special gadget and click. Suddenly, it's like a treasure map taking you to special places. At the zoo, you can scan the QR code, and a website with interesting facts about the animal you're looking at will pop up. In a book, it can take you to a fun website telling you more about the story.

Sadly, cybercriminals also know how to use QR codes and they use them to do bad things. But luckily, there is a special program that tells you if the QR code is safe. Also remember to never upload an app from a QR code, only get safe ones from the App Store or Google Play.

Ransomware

Ransomware is a computer program that can encrypt all the files on your device.

Ransomware sneaks into your computer and kidnaps all your important files: pictures, videos, and documents. Then, the bad guys who made the ransomware take them away, leaving a note telling you to give them money so you can get them back. But remember, never trust what they say! They might just disappear leaving you with a broken device even though you paid. What you need to do is tell a grown-up so they can fix the machine and keep you safe. Also, make a backup – it's like saving a level in a game. That way if anything goes wrong, everything will not be gone.

Spam

Spam is like junk mail but for your email.

Just like sometimes people send us mail that we don't want or need, people also send us emails that we don't want or need. These emails can be commercials for things we don't want to buy or even scams trying to trick us into giving away our personal information. It's important to be careful with spam emails and not click on them or reply to them, just like we would throw away junk mail without reading it. The best way to avoid spam emails is not to give away your email unless you really need to and not to leave it on strange websites.

Trojan

Trojans are computer programs that can take over your computer and use it to do bad things.

A Trojan pretends to be a computer game or a harmless program, but it's really a sneaky little character who wants to get into your computer, steal your information, and wreck your files. Trojans usually hide in unsafe websites, and they have lots of tricks – they say you can download expensive games for free or see a film on your computer that is only on at the cinemas... Ignore those pretend giveaways and use only verified sites – the ones with a big green checkmark on them. Remember, just like you can't let strangers into your house, be careful what you download because it could be a sneaky Trojan. To be sure, ask your parents for permission before you let anything into your computer.

URL

URL is an address that all the online items have – websites, pictures, an online book, etc.

Just like your house has an address that tells people where to find it, a URL tells your internet browser where to find a website. It's a combination of letters, numbers, and symbols that help connect you to the right website. You can find the URL of a website in the address bar at the top of your browser. Always pay attention to the URL address and compare it with the official name of a company/organization/shop or anything else. If the URL looks weird or suspicious, it could mean that you're on a phishing or a fake website.

VPN

VPN (Virtual Private Network) is a tool that makes surfing the internet safer.

It is like a secret tunnel on the internet that keeps your online activities private and safe. Just like a secret hideout that only you can get to. The VPN tool moves your data to a special protected place and works as a mask: the websites that you'll be visiting won't get your information, they'll see the mask that the VPN service will be showing to them instead. Just like you wouldn't want a stranger peeking into your diary or bedroom, a VPN helps protect your online activities from strangers who may try to look at your personal things.

Wi-Fi

Wi-Fi is like a walkie talkie which helps you to communicate with the internet.

Wi-Fi is the box in the corner of the room that helps you surf the internet. You tell it what you want to do – go on a website or listen to music – and the Wi-Fi will answer. Without it, you can't go on the internet. To stop someone from stealing your pictures or other files, protect your Wi-Fi with a password. Together with your family, make the password hard to guess and only tell people you trust. Also, the safest Wi-Fi is in your home. No matter how exciting it seems, don't connect to the "free" one in shops or restaurants, because it might not be safe.

eXploit

An exploit is a hole in your computer or device that helps cybercriminals to get into it, infect it with a bad program, and tell your device what to do without your permission.

It's like a cheat code in an online game – knowing these cheat codes, cybercriminals can break the rules and do whatever they want with your device.
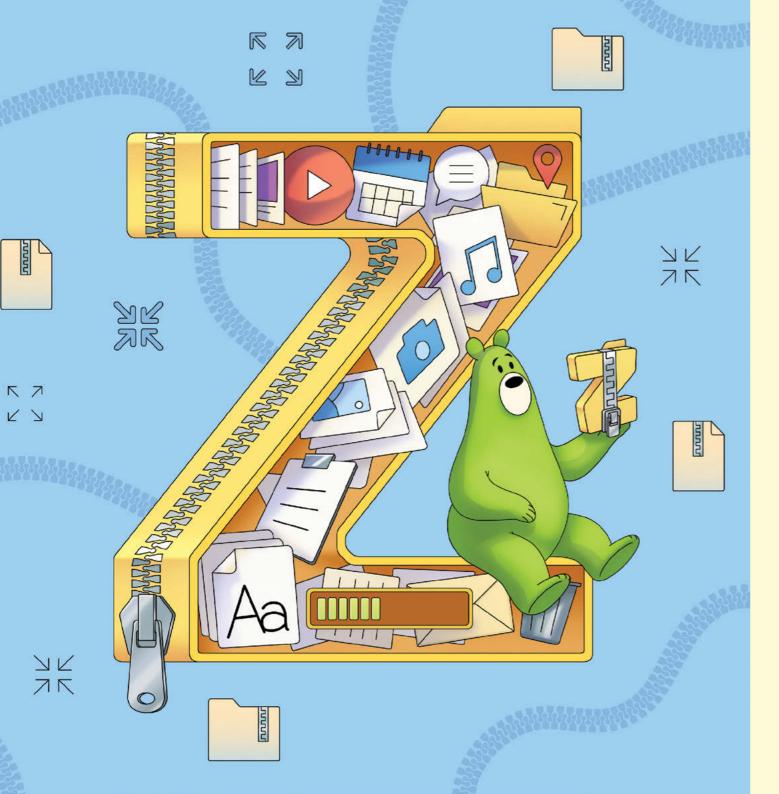
cyberbull**Y**ing

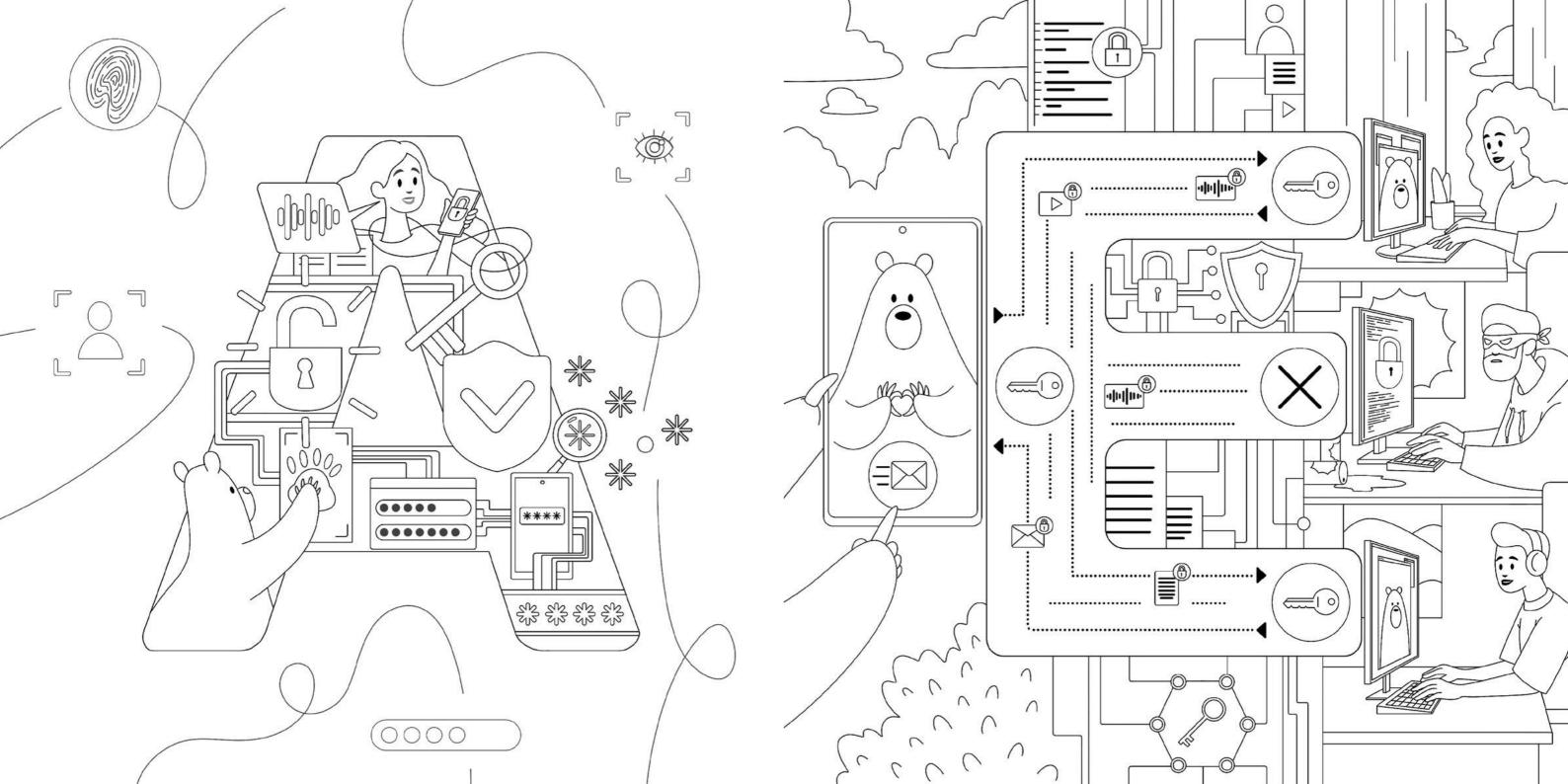## Cyberbullying is when someone is mean or hurtful to other people online.

It can happen in different ways, like sending mean messages or spreading rumors about someone online. Cyberbullying makes people feel sad, embarrassed, or scared. It's important to be kind to others online, just as in real life. If you think that you're being bullied online, share your feelings with adults you trust. What a bully says about you has nothing to do with who you really are. Therefore, never take their words seriously. Do not try to get bully back, because it can often make things worse. Take screenshots of your chat with the bully and block them on the platform.
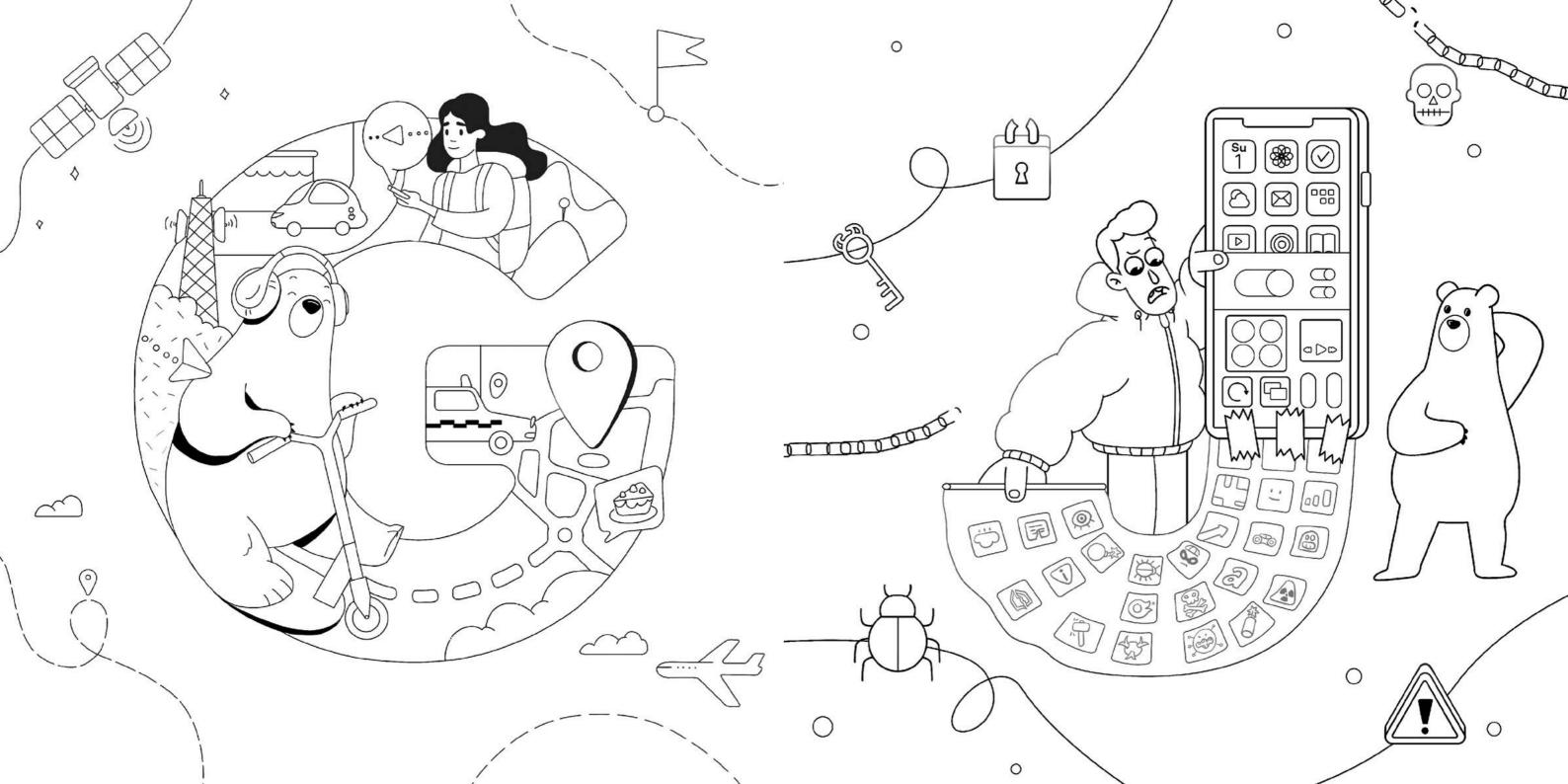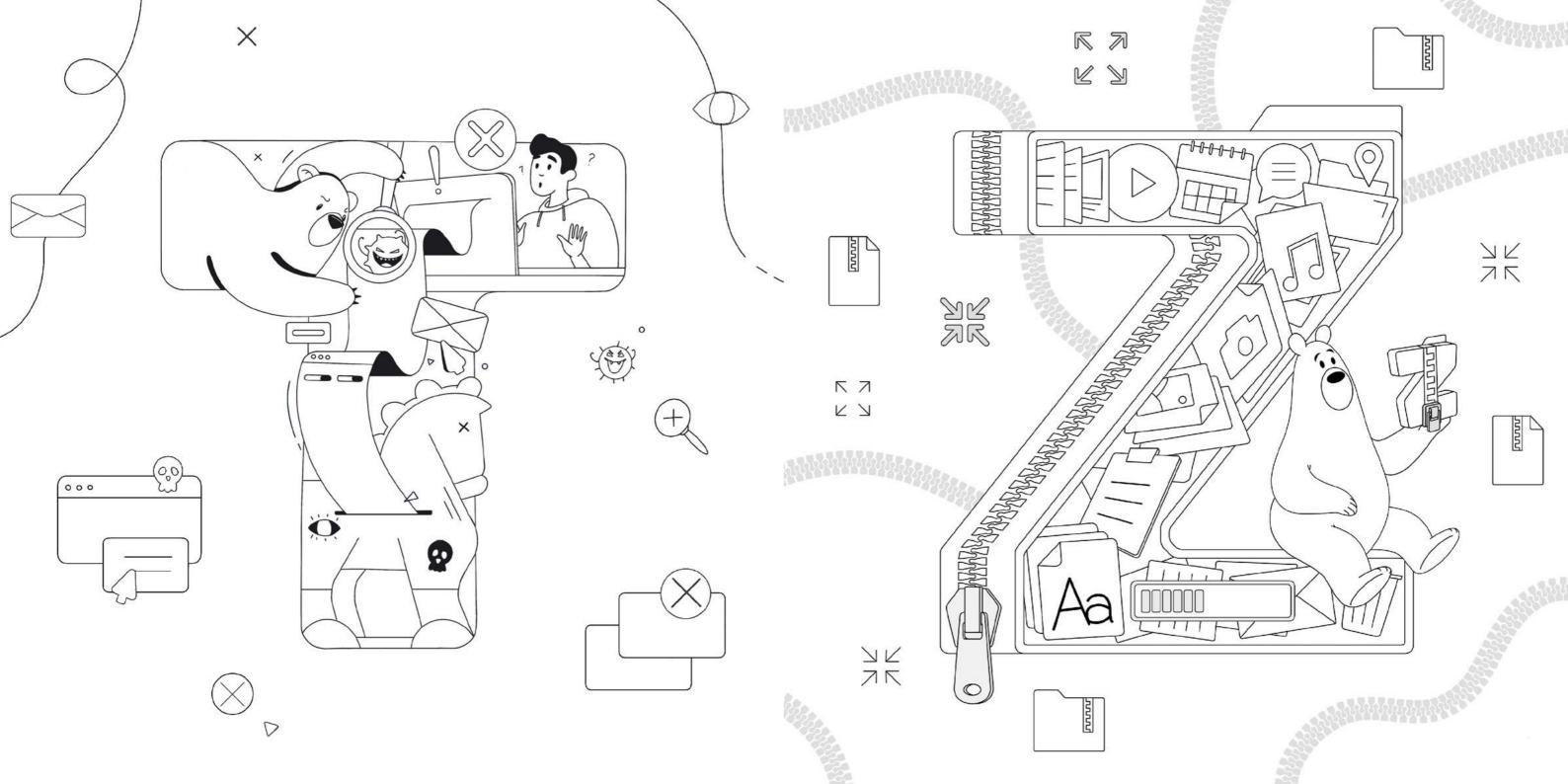
ZIP file

A zip file is like a bag that
you can put many things into.

It helps to keep all the pictures, files and folders together in one
place. When you use a zip file, you can shrink or "compress" all
those things, making them small so they take up less space on the
computer. It's like squishing everything together tightly. And when
you want to use those things again, you can open the zip bag
and take out all the stuff inside.

Notes

Dear cyber explorer,

What an incredible adventure we've had! From A to Z, you've journeyed through the twists and turns of cybersecurity. But remember, being safe online is just like being safe in the real world. Like superheroes, you have the power to make smart choices online — choosing strong passwords, keeping personal information private, and thinking twice before clicking on unknown links.

Your adventure doesn't end here. The digital world is always changing, and there's so much more to learn. Stay curious, ask questions, and keep updating your cyber-smarts. Teach your friends and family the ABCs of staying safe online. Together, you'll build a safer online world.