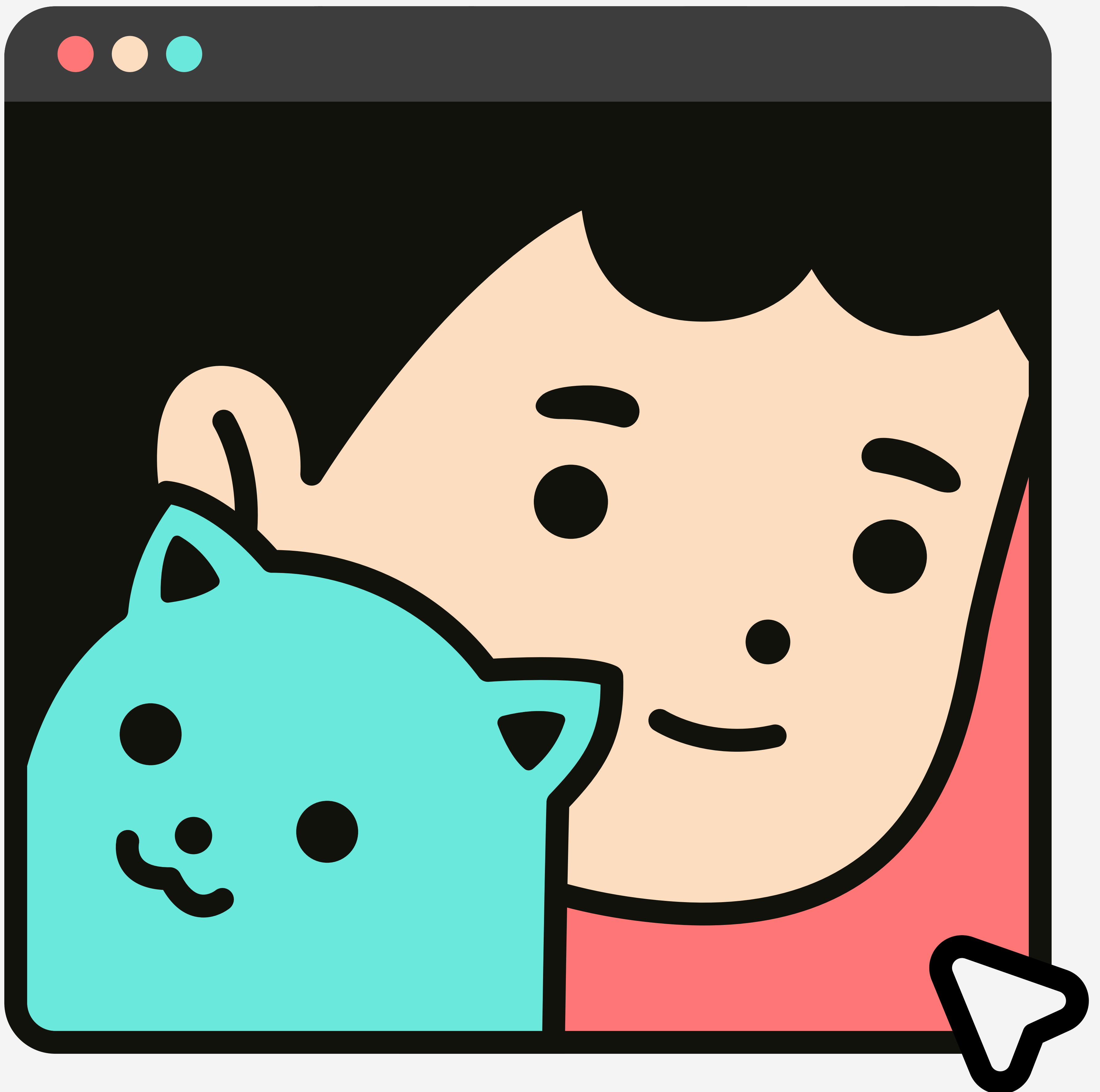


Internet safety for kids

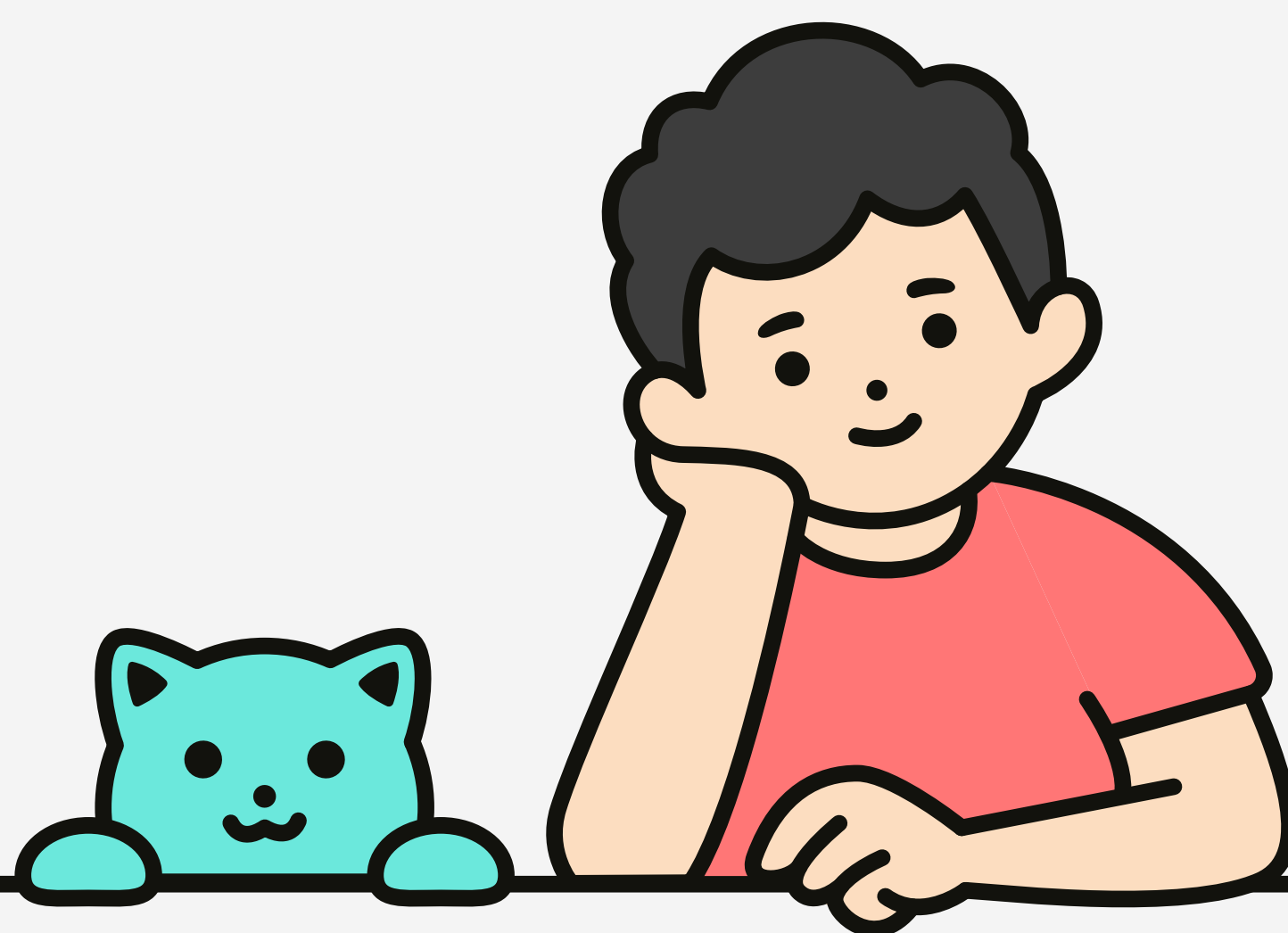
Learn to explore the
digital world safely



Contents

4

Top online threats



13

Social media safety for kids

17

Multiplayer games: Play online safely

19

Password security

21

Guard your identity: Protect personal information

24

Internet safety rules for kids: Take breaks for your brain

26

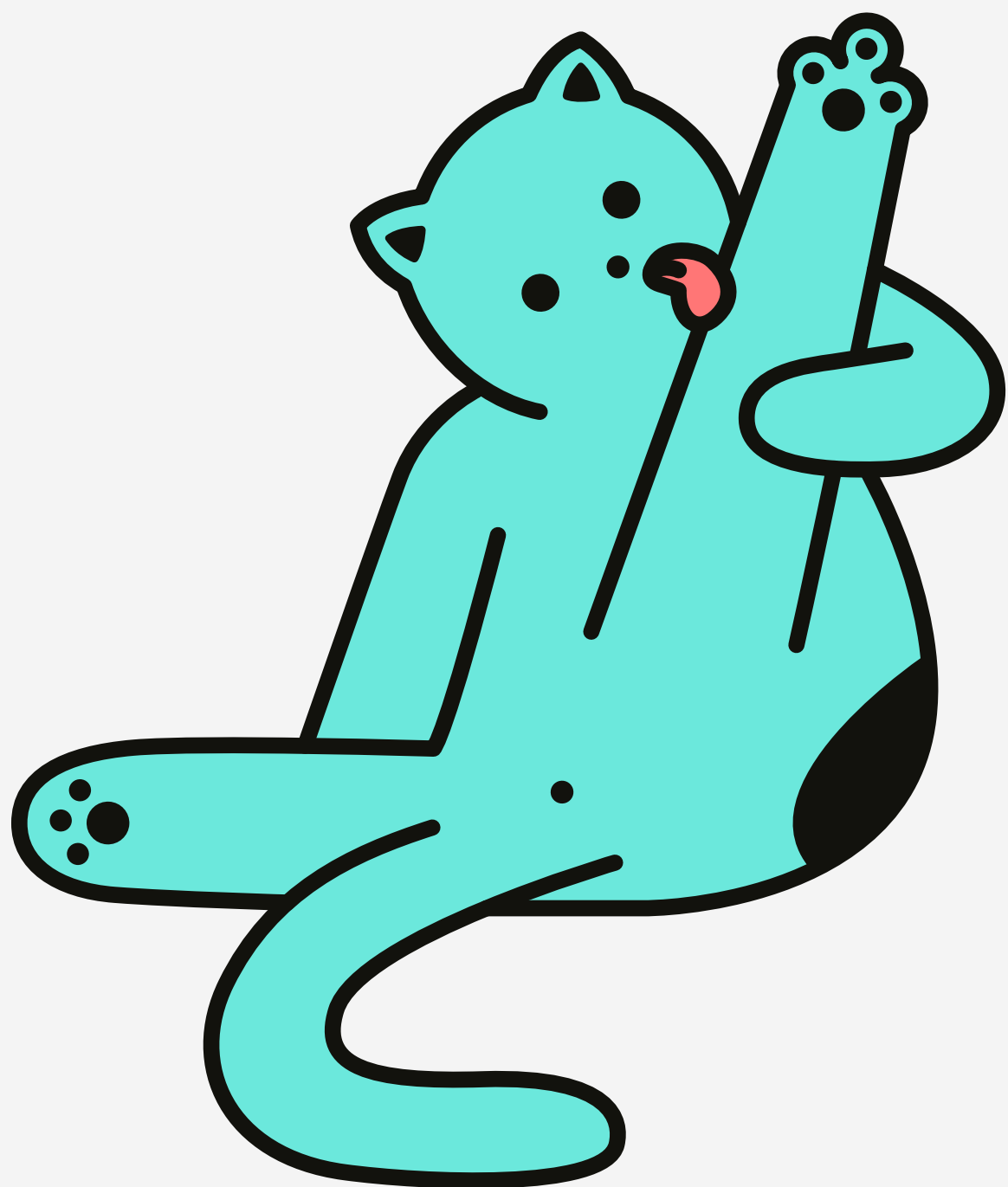
Test: What cyber animal are you?

29

Internet safety tips for parents

Welcome, digital explorer!

The internet is like an amazing playground, isn't it? Your parents probably let you play there every day. But, while your neighborhood playground is filled with kids you know, almost everyone you meet online is a stranger.



We've prepared this guide to help you learn how to navigate the internet safely and recognize when a stranger online is not who they say they are.

It'll be fun!

Stay curious. Stay safe.

The internet is full of amazing places to explore — but just like in any great adventure, there are a few tricky villains lurking around. In this section, we'll learn about common threats online, such as various scams and fake, AI-generated content.

Common scams you should know about



Email and DM scams

These scam messages usually contain a link or a file. The file may be infected with malware, while the link can lead to a fake lookalike website. Scammers hope to trick you into accidentally revealing your password.

Key to remember:

Use link checkers to recognize links to fake websites.

Fake websites

Fake websites look like popular platforms and shopping sites. Criminals build them to steal personal information, passwords, and payment details.

Key to remember:

Always double-check the website's address.

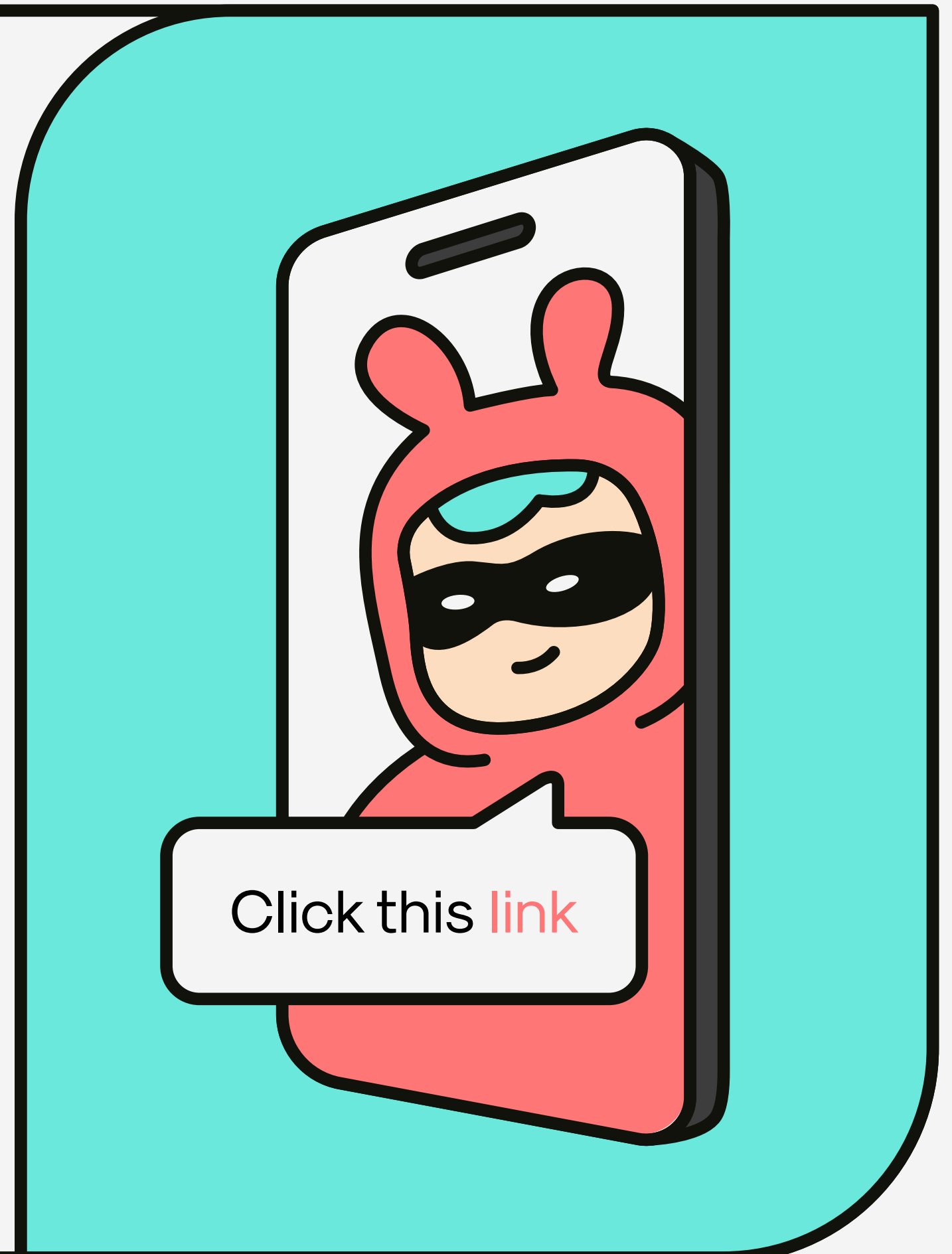


Phone scams

Scammers can call or text you pretending to be someone important — like a teacher, a company, or even someone you know. If they keep you talking long enough, they'll try to get personal information or money out of you. Some even send fake links by text message.

Key to remember:

Always be wary whenever people call you and ask for personal information.

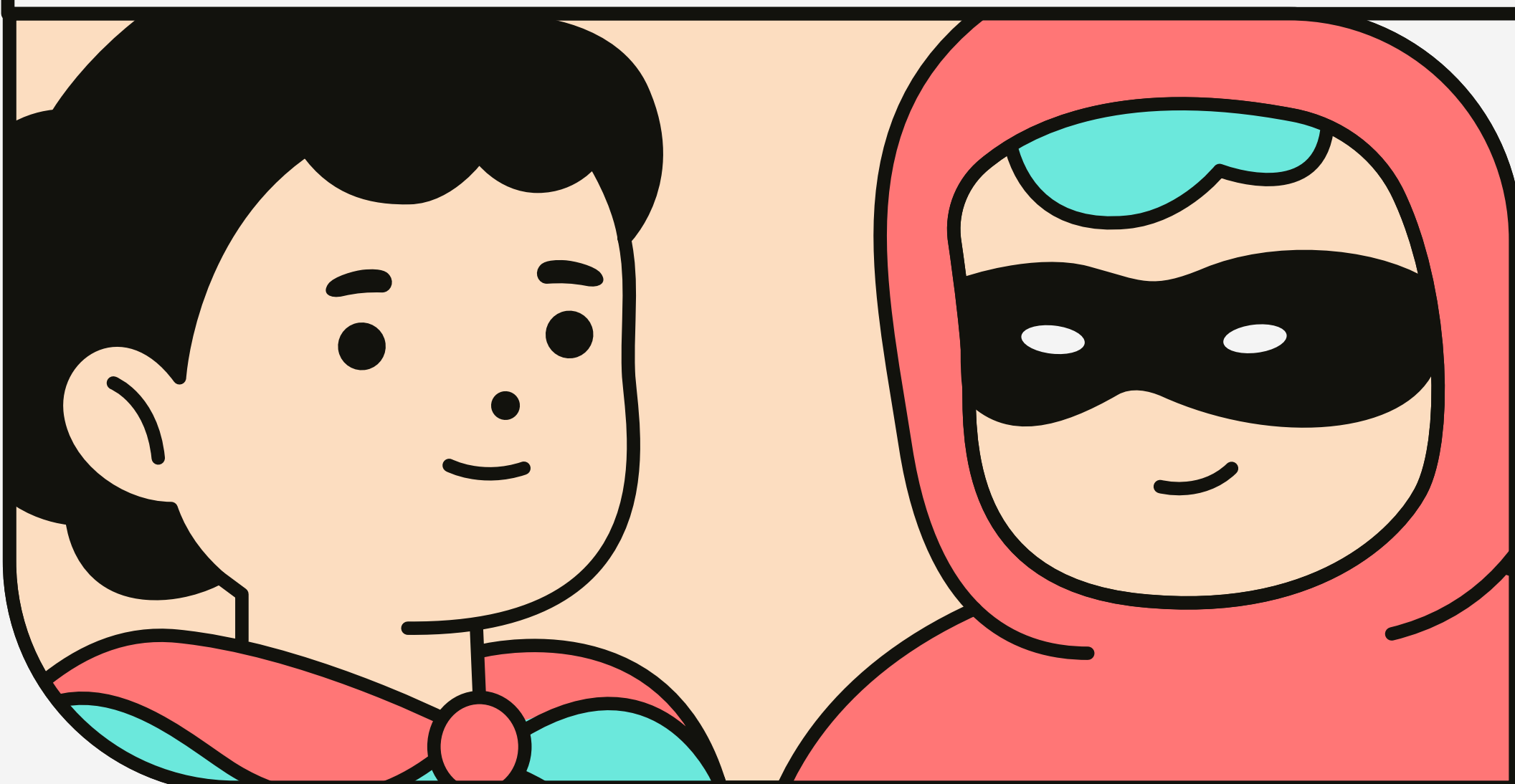


In-person scams

Be cautious when people approach you online. It could just be another kid. But it could also be a scammer. Instead of sending you links to fake websites, they pretend to be someone you'd likely trust, like a new player in your game. Eventually, they will start asking for personal details. These scammers are very good at recognizing and exploiting people's weak spots.

Key to remember:

Never share personal details with strangers online.



Next, let's take a look at a few threats, such as phishing, in more detail and learn how to recognize them.

Terms we'll learn

Phishing is a scam where someone online pretends to be a person or service you trust to steal your passwords or personal information.

Phishing

People exchange millions of emails every day. They also send SMS and direct messages (DMs) through social media. But hiding behind a screen name, random phone number, or an email address can make it easy for cybercriminals to pretend they're someone you should trust. That's called phishing.

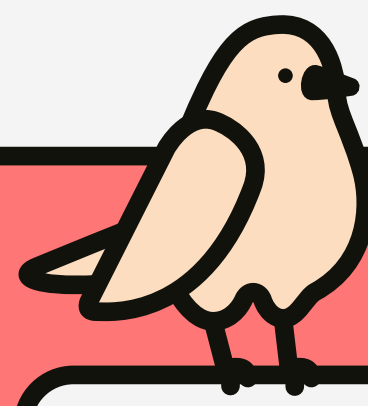
For example, a phishing email might look like this:



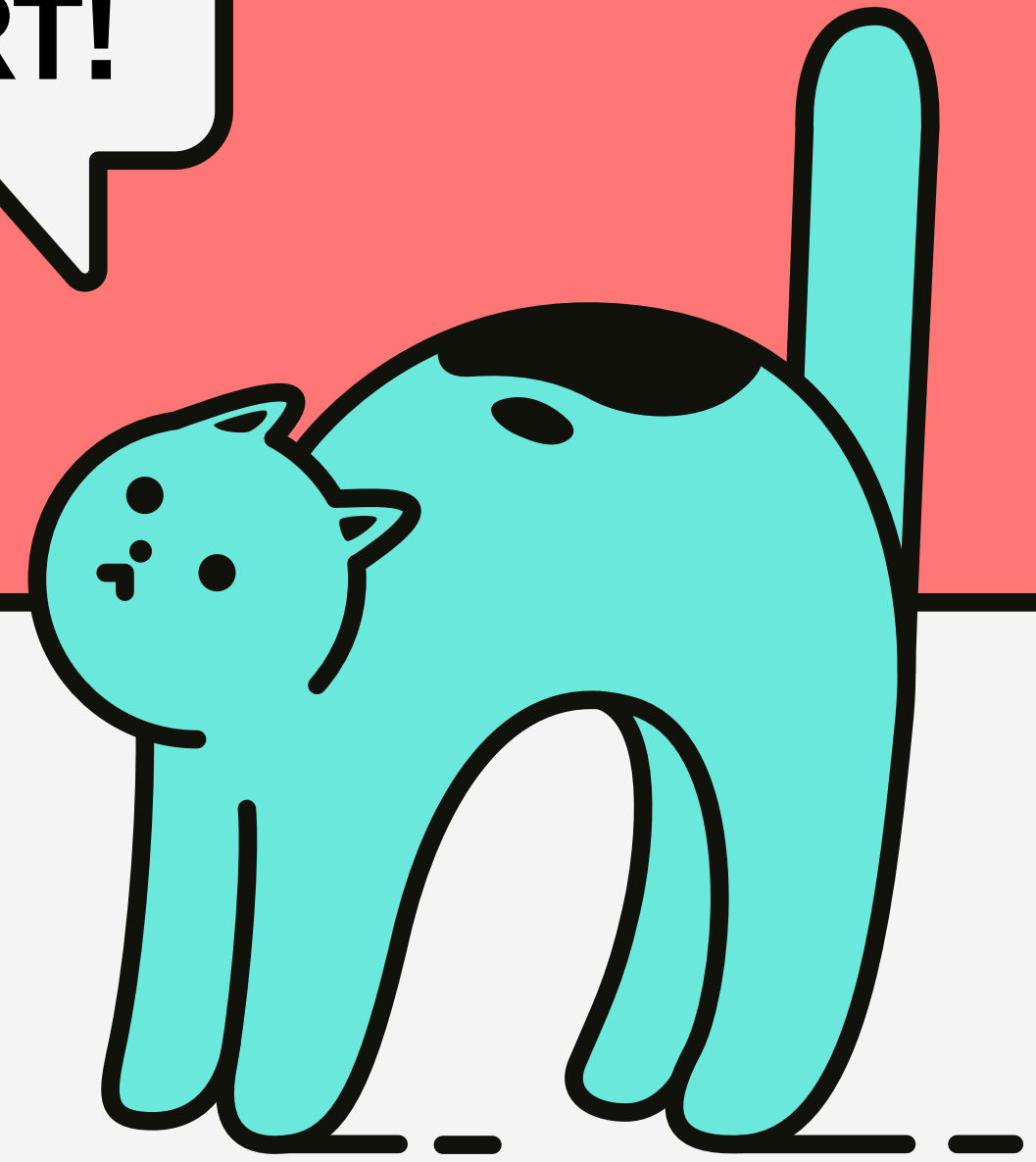
From: support@minecraft.t-support.com

"Urgent! Your Minecraft account has been suspended. **Click here** immediately to verify your details and restore access before it's deleted forever!"

Looks pretty alarming, right?
That's exactly the point. Here's what
you should pay extra attention to
recognize a fake message easily:



ALERT!



It creates panic

Words like "urgent," "immediately," and "deleted forever" are designed to rush you into clicking without thinking.

It asks for personal information

Legitimate companies will never ask for your password over email.

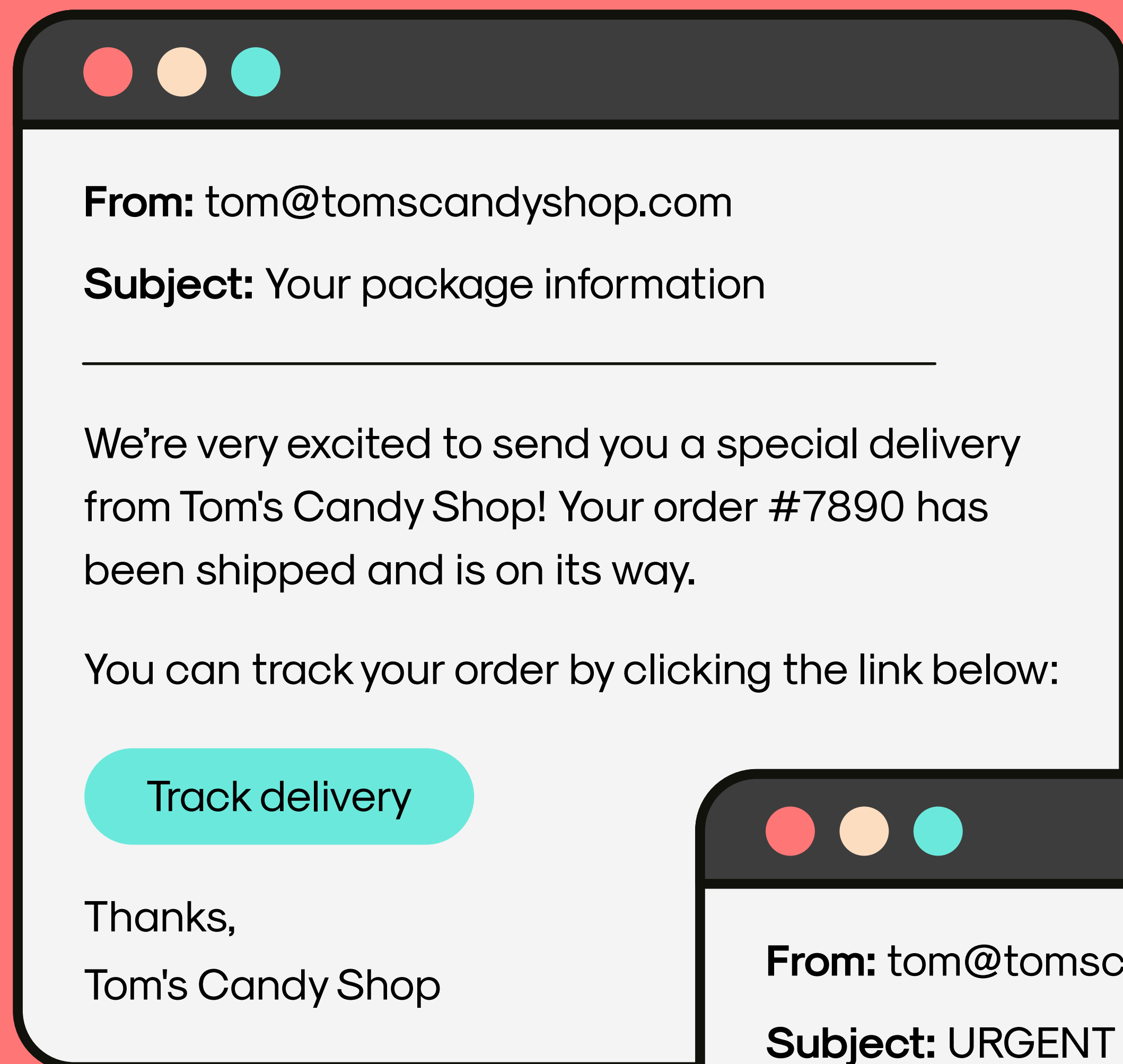
The links look slightly wrong

Instead of the real website, the email might say something like minecraft.t-support.com, instead of minecraft.com. Close enough to look real at first glance.

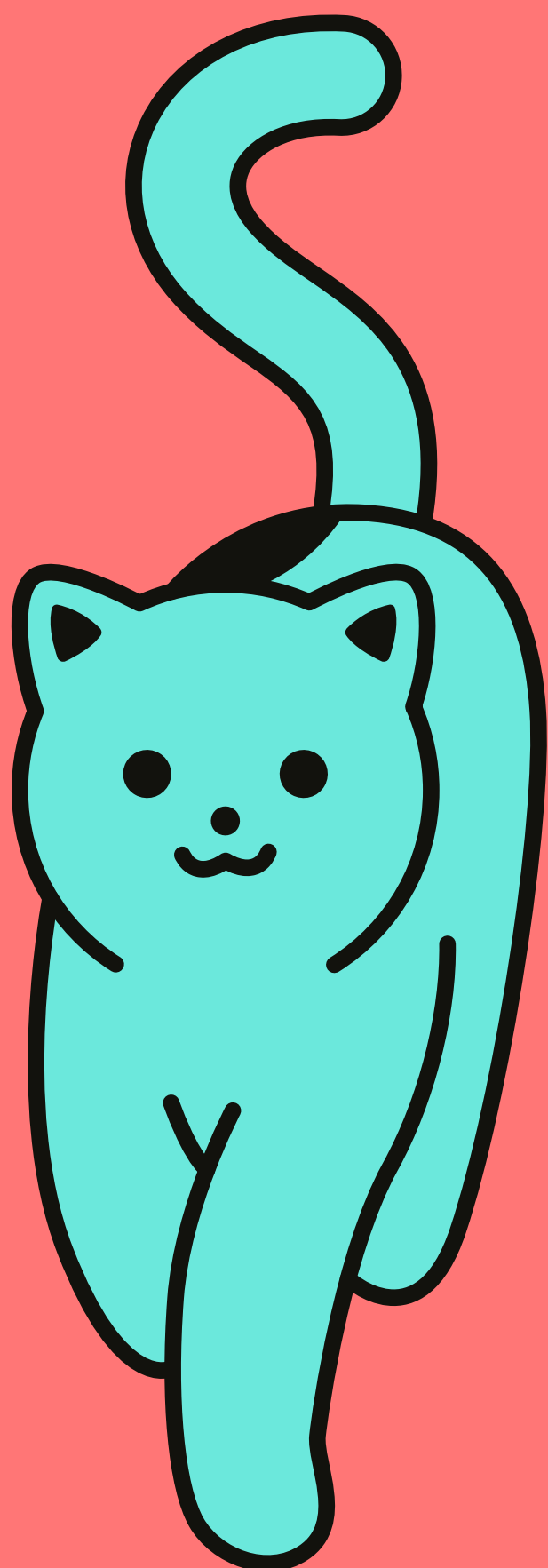
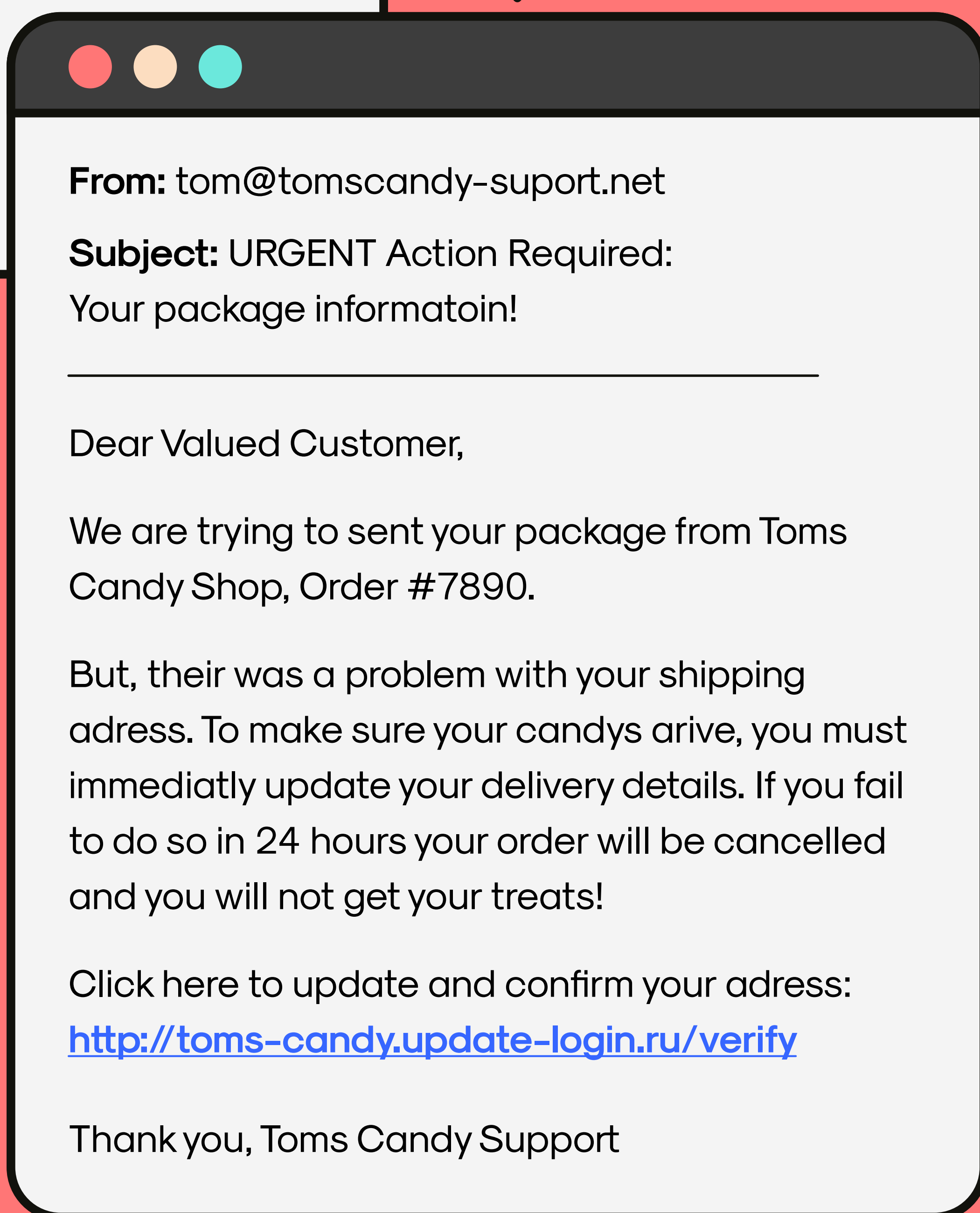
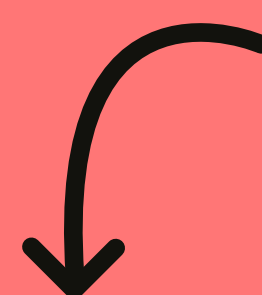
Activity

Let's practice. We'll go over two emails and learn how to recognize which one is real and which one is phishing.

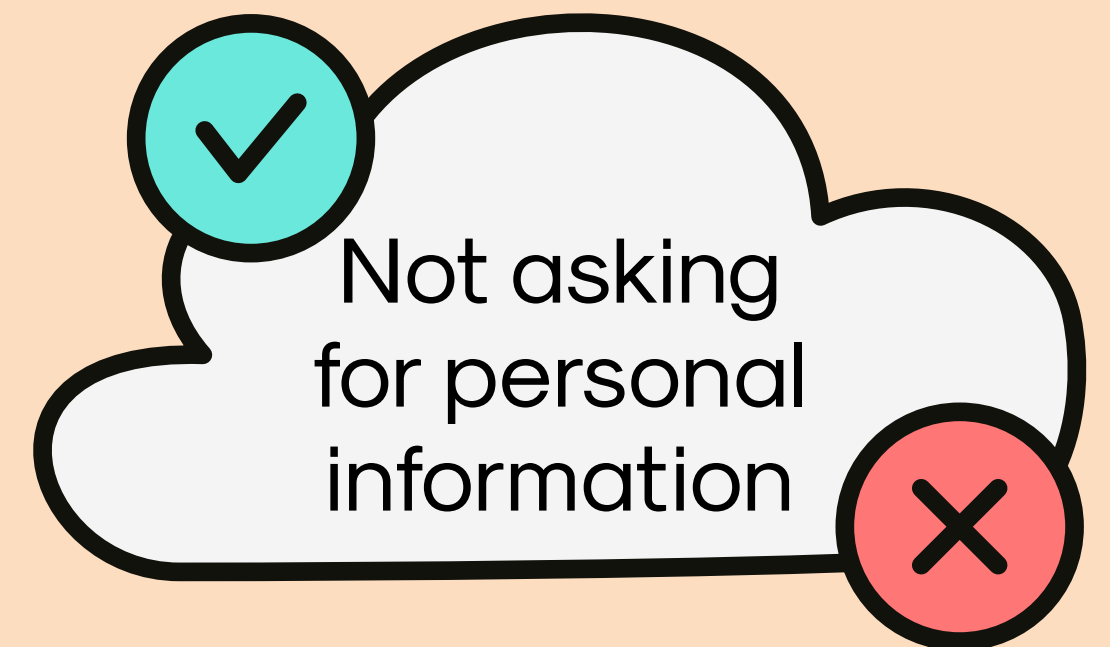
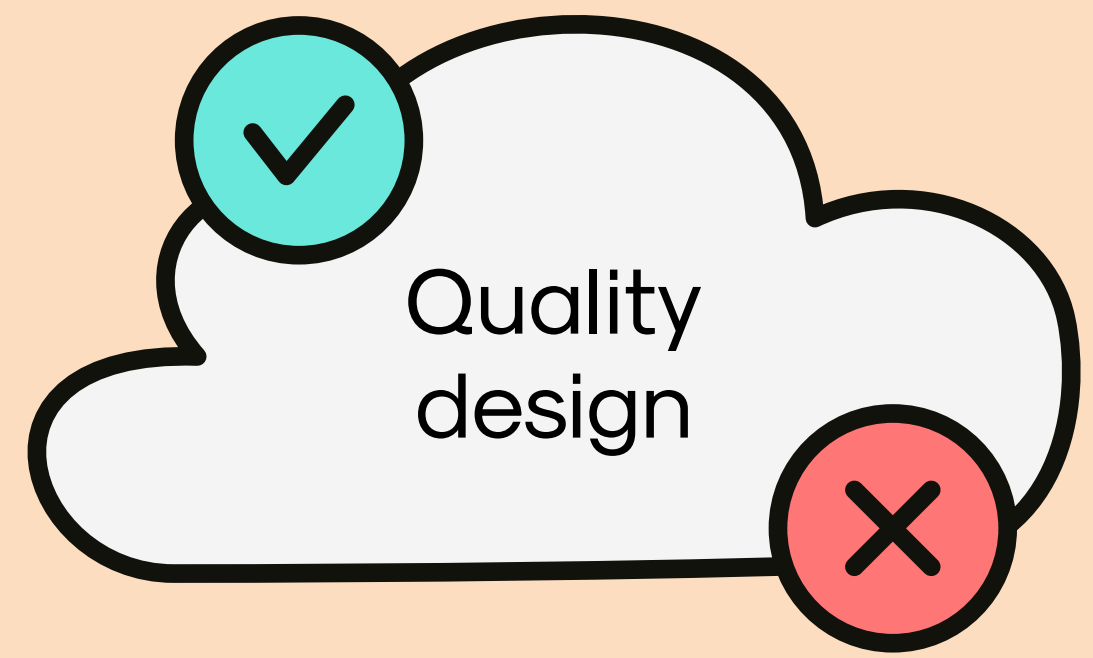
Example A



Example B



Here's what you should check first:



You should know!

Scams can look very real with AI

Sometimes cybercriminals use AI (artificial intelligence) tools to make their messages look exactly like the original — no grammatical errors or low-quality pictures. They may even use **deepfake** videos and clone voices to appear even more convincing.

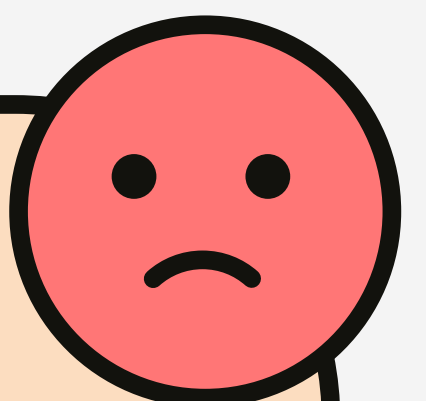
AI-related scams

Terms we'll learn

A deepfake is a fake photo, video, or voice recording made using AI to make it look or sound like a real person said or did something they never actually did.

Artificial intelligence (AI) tools can be used to create fake photos and videos, called “deepfakes”. Why would people create fake photos and videos? While it would be fun to imagine yourself riding a T-Rex or walking on the Moon, scammers often use deepfakes to trick people into giving away information they did not want to share.

Why deepfakes are dangerous:



Misinformation:

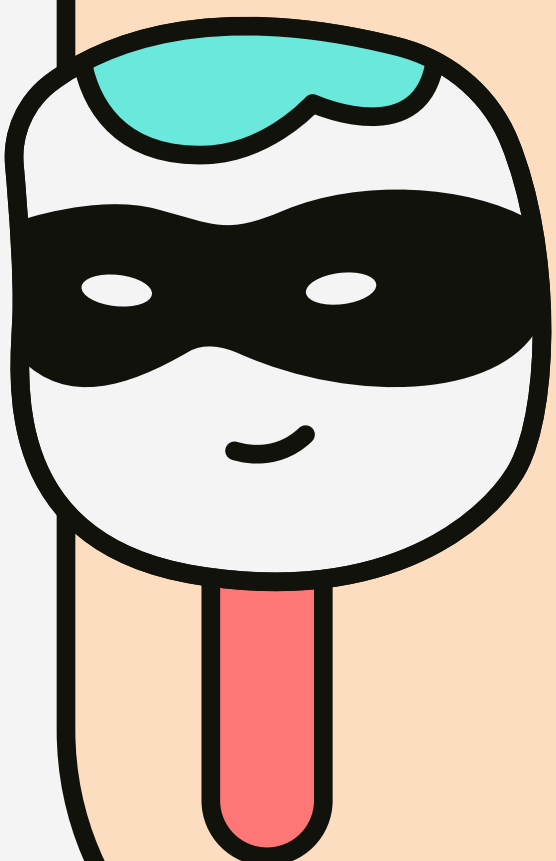
Deepfakes can be used to convince people that events happened when they never did.

Bullying:

Someone at school could use AI to create fake images or videos of a classmate to make fun of them.

Scams:

Scammers can clone someone's voice and pretend to be them. For example, they may pretend to be a parent to trick a child.



Activity

Recognizing deepfakes. Deepfakes can be easily mistaken for the real thing. It's smart to question anything that catches your attention online, especially if it's pushing you to buy something or evokes strong emotions. Here are a few pictures.

Can you guess which ones were generated by AI?



What to do next

Ask your parents if they know what deepfakes are or if they've ever gotten any phishing messages.

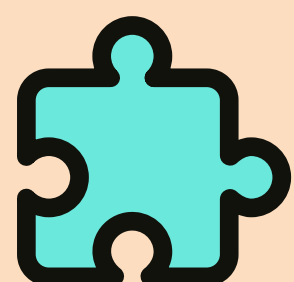
Fake news

Terms we'll learn

Fake news is lies spread online.

People have many reasons to lie online. Just remember that on the internet, most people are strangers — and strangers aren't always who they say they are. That's why we all need to stay vigilant online and check for truth, especially before we share it ourselves.

Activity



Checklist: How to recognize fake news? Recognizing lies on the internet can be difficult because they can easily blend into your social media feed. But if something has caught your eye and you think about sharing it, spare a minute to double-check.

Here's how:

Think about how it makes you feel

Lies online are often designed to evoke strong negative emotions, like fear or anger.

Check the source

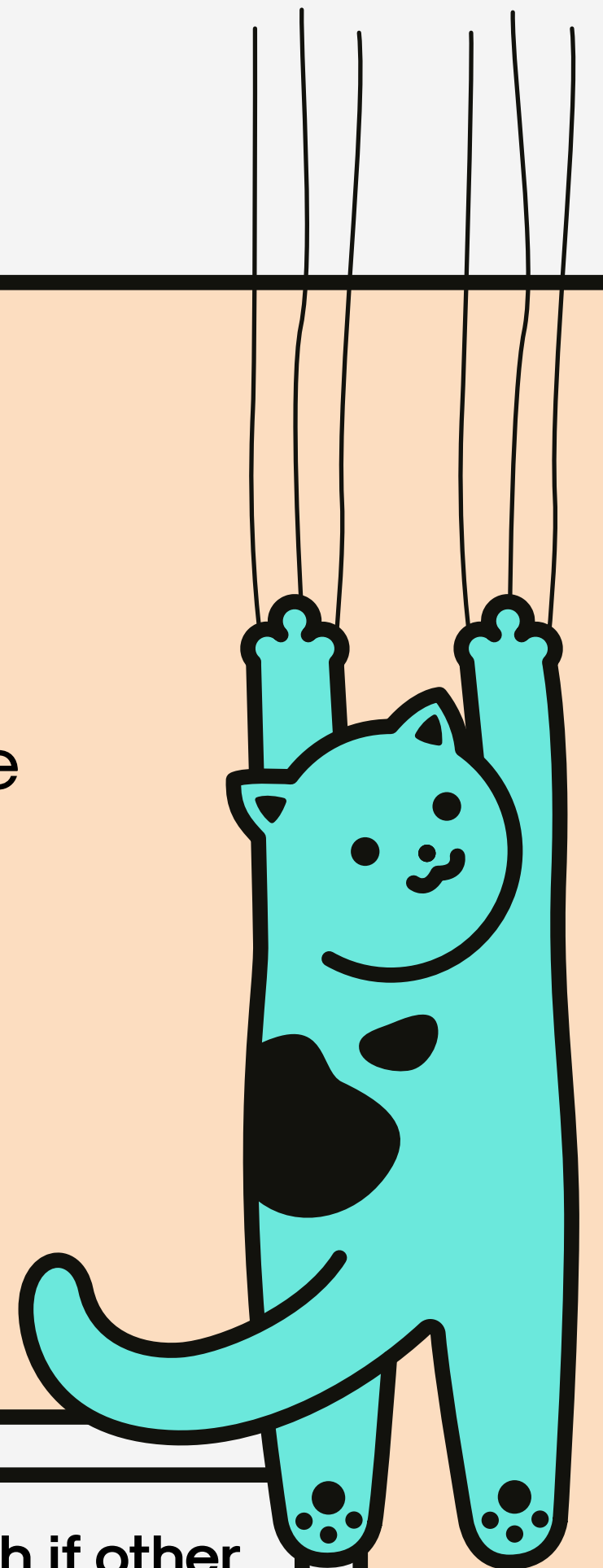
Who is saying it?
Is it a stranger?
A news organization?

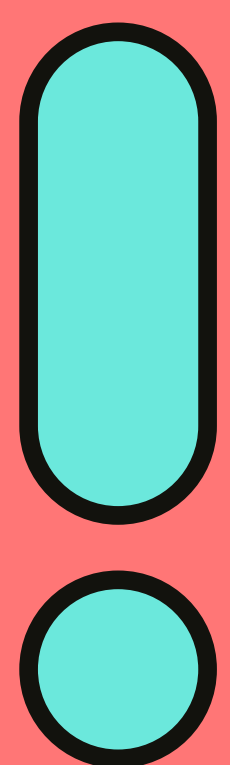
Consider its reputation

Have they ever been caught lying before?

Research if other sources are saying it too

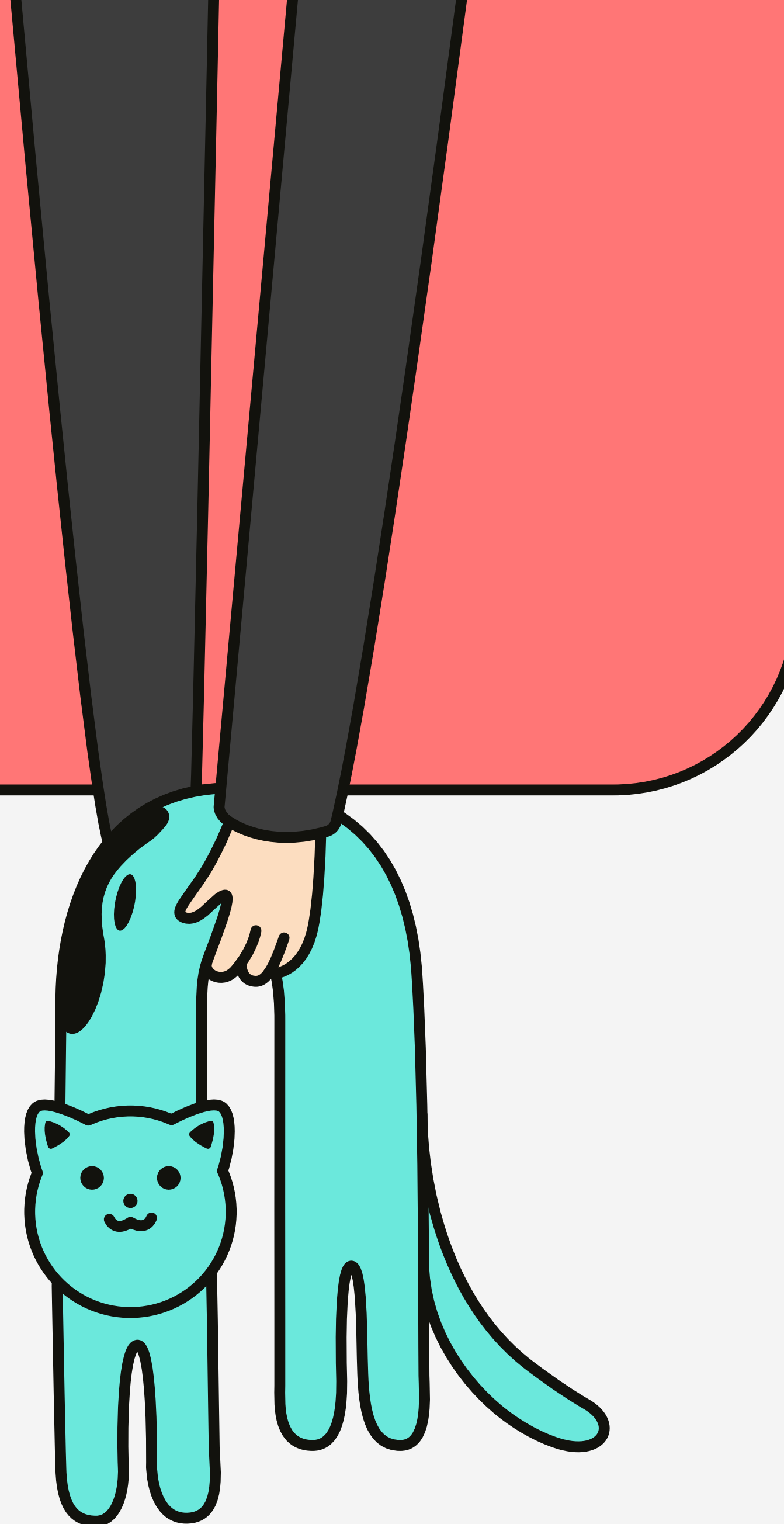
If something big is actually true, more than one source will be talking about it.





What to do next

Ask a parent to go through their social feed (or yours, if you have social media) and try to find three stories that might be fake. Check a credible source for confirmation.



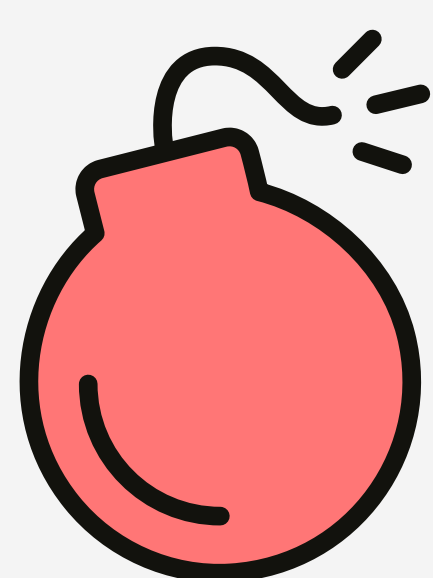
Social media safety for kids

What dangers lurk online

Terms we'll learn

Identity theft is a type of fraud where people pretend to be you to get something in your name.

If you already have a social media account, you'll know how great it can be to connect with friends and follow your favorite influencers. But sometimes social media can be strange. It can make you feel invisible as well as seen by the whole world. One thing you have to remember is that behind funny screen names and colorful avatars, there are real people. So whatever you read or post yourself can make a real impact on their lives.

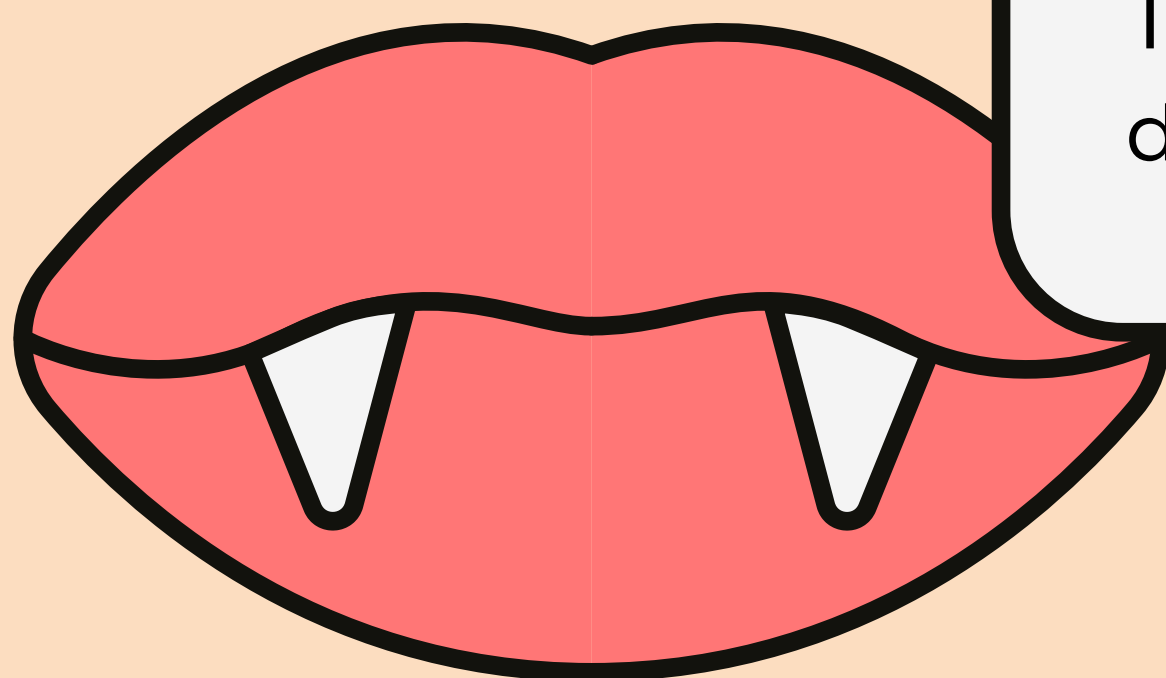


Dangers of social media

Online, crimes against children are especially frequent. Let's look at four main dangers of social media.



Adult content

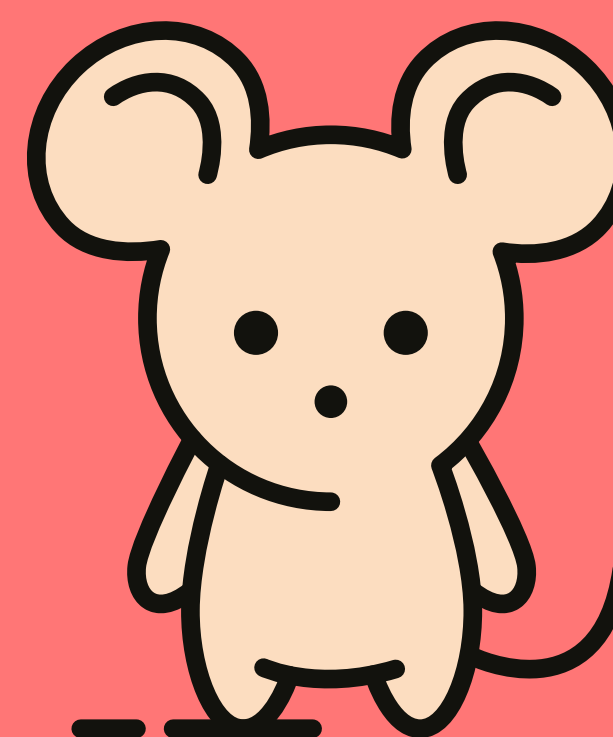


On social media, you might accidentally see videos, images, or messages meant for adults, not kids. This can include scary, violent, or sexual content. If you ever see something that makes you feel upset, confused, or “weird,” it is not your fault — and you should tell a trusted adult right away.

Child identity theft

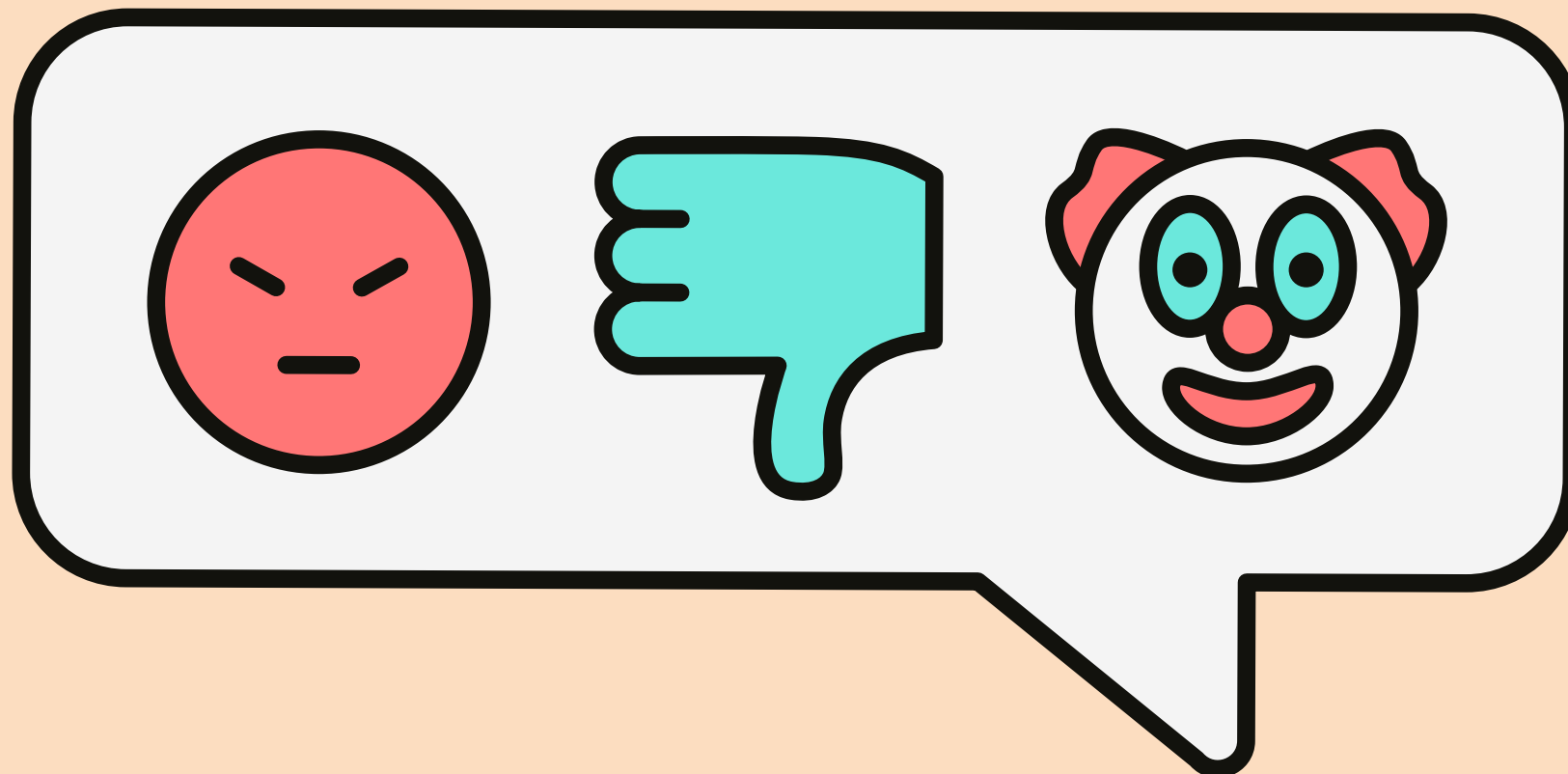


Some people try to collect bits of your information — like your full name, birthday, school, town, or even photos — to pretend to be you or use your identity for bad things (like opening accounts or tricking other people). That’s why it’s important not to share personal details in your profile, posts, or messages.



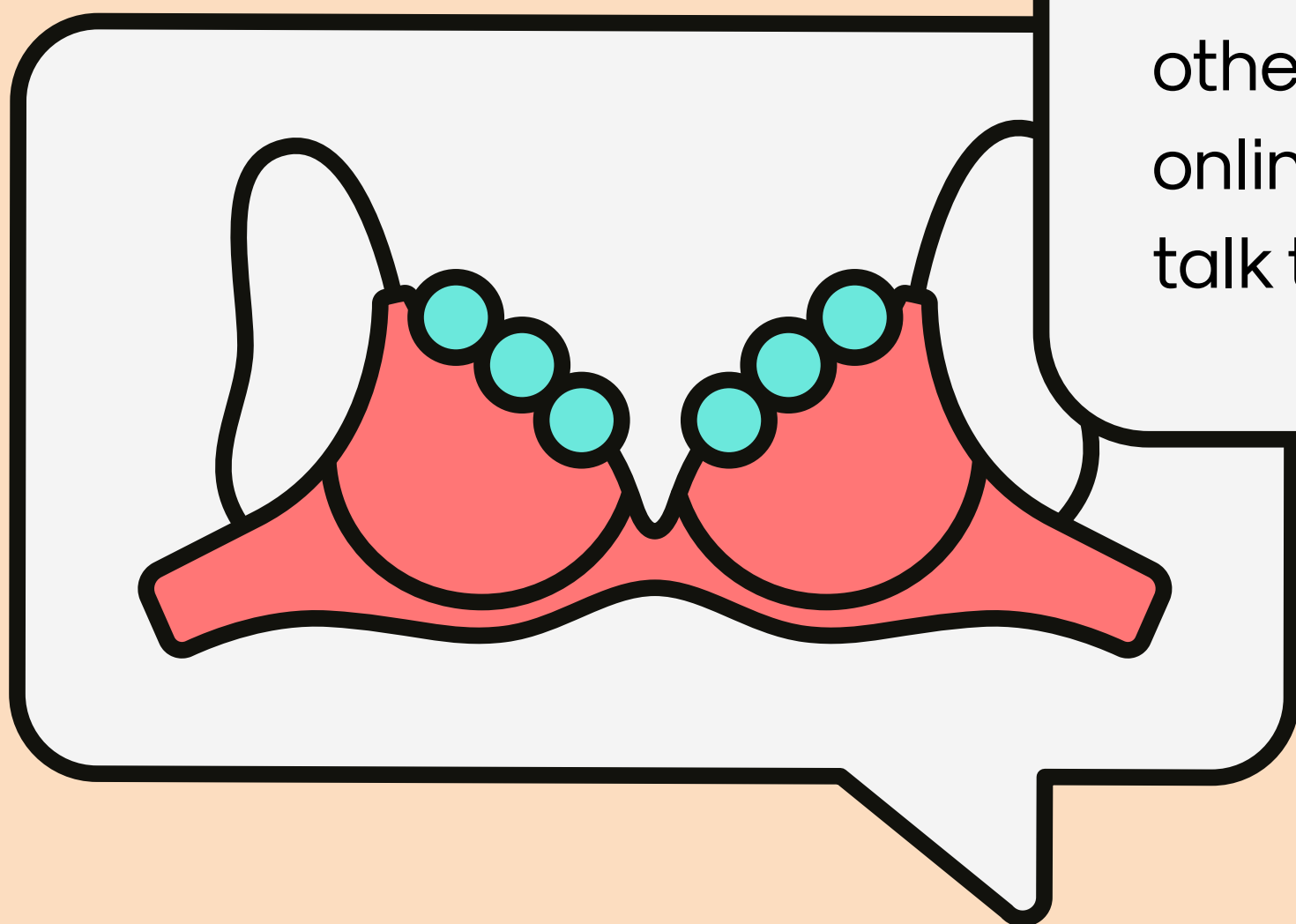


Cyberbullying

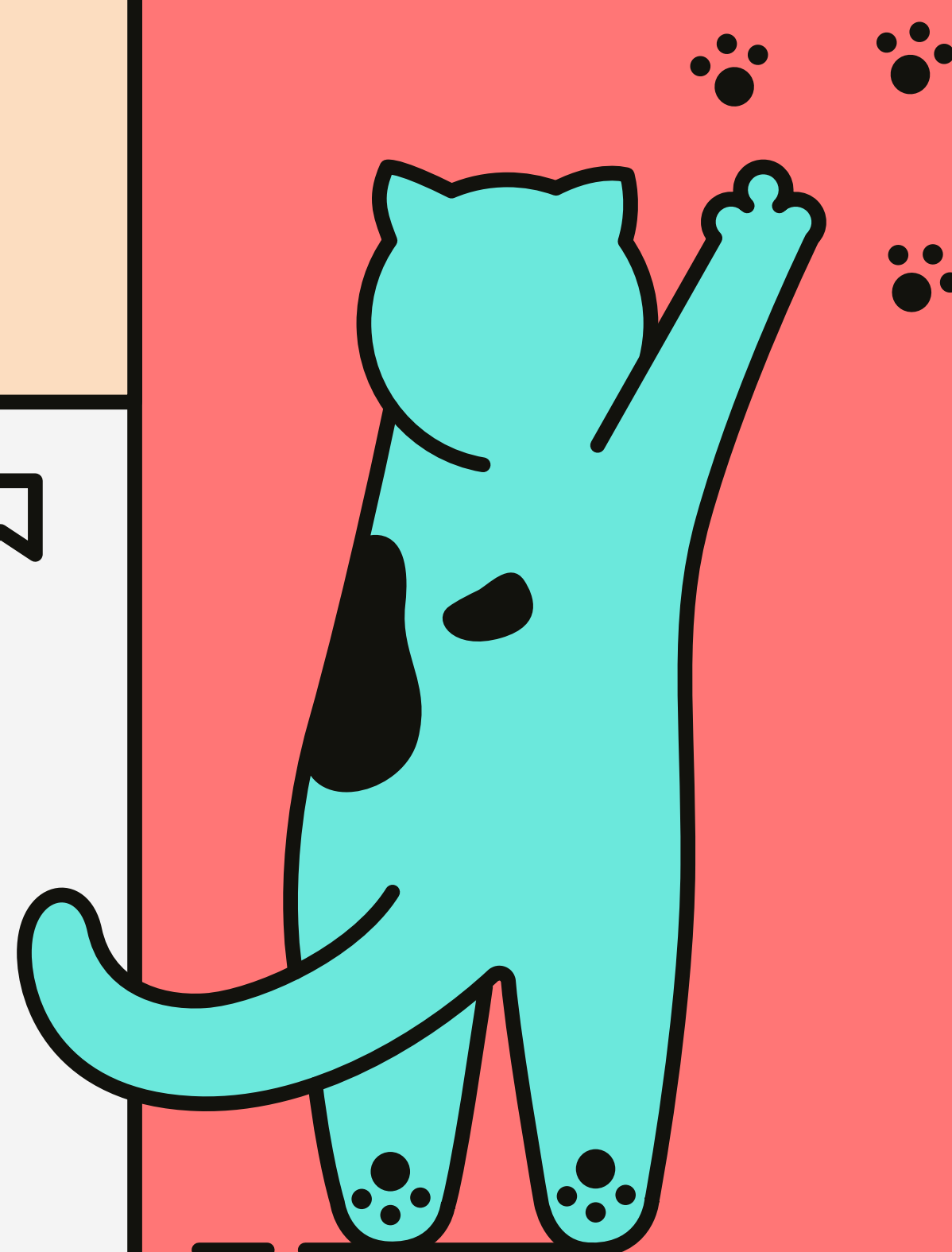


Cyberbullying is when people use social media to be mean. They can post hurtful comments or share embarrassing photos. Remember that there is a real person with real feelings on the other side of the screen. If someone is unkind online, it's okay to block them, report them, and talk to an adult.

Sexting



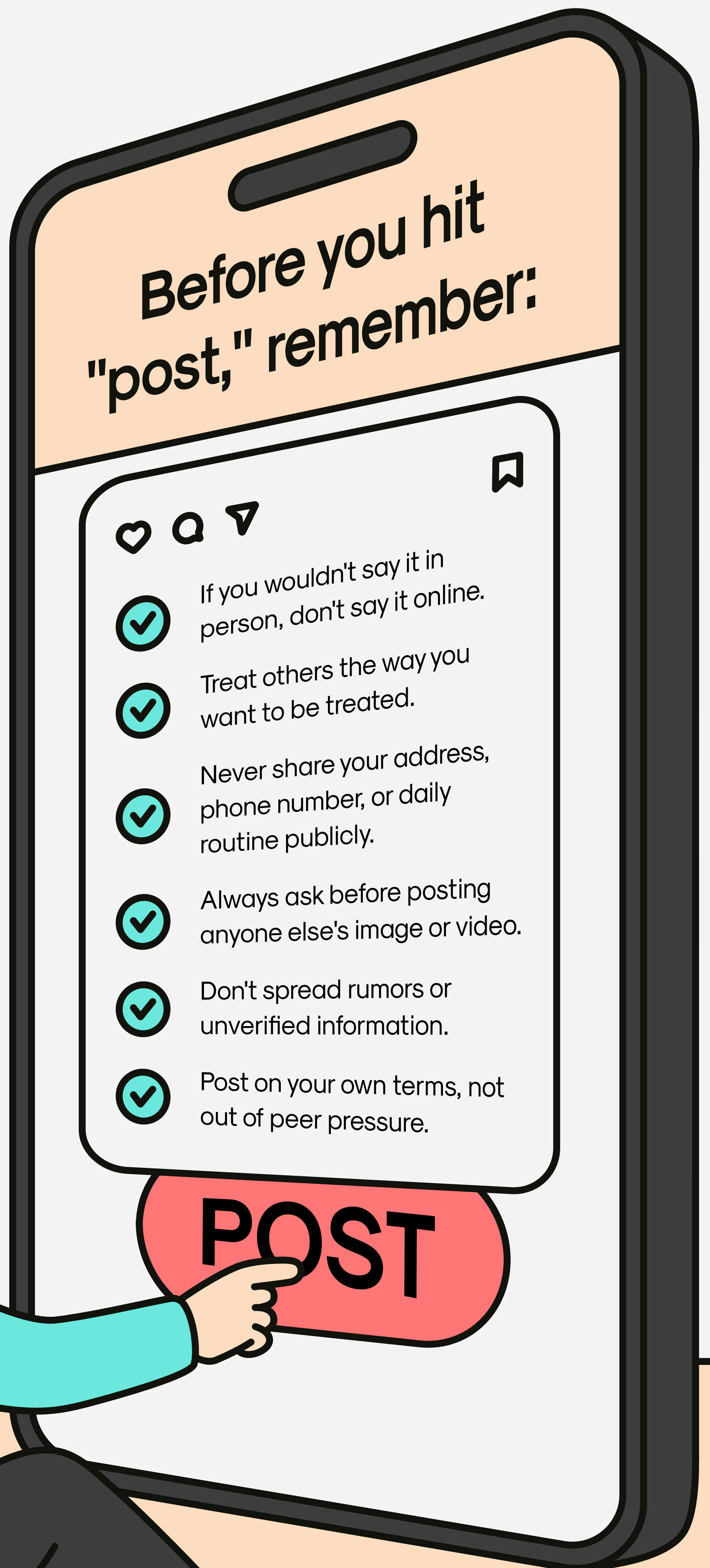
Sexting means sending or asking for sexual pictures, videos, or messages. If anyone asks you for a “secret picture” or anything that makes you feel uncomfortable, it is not okay. You never have to send or share anything private. Tell a trusted adult right away — you are not in trouble for speaking up.

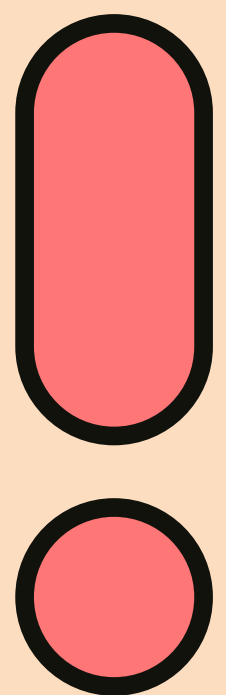


Activity

Rules of posting

Social media can make us eager to join the conversation, but you should follow a few rules when you want to share something online:



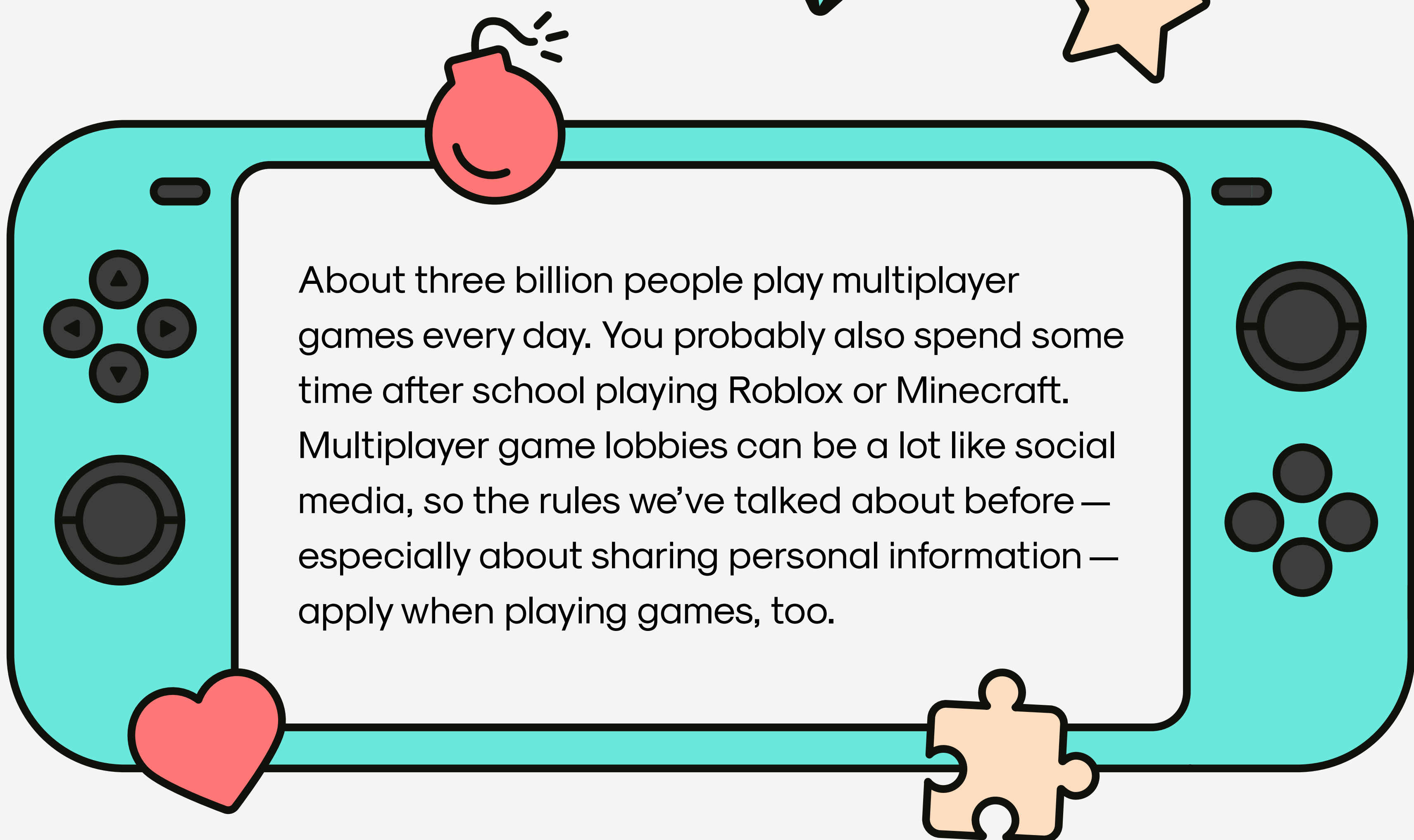


What to do next

If you ever see someone being bullied online, try to stand up for that person or send them a kind message. Even a few words of support sent to the person being bullied can make a huge difference.

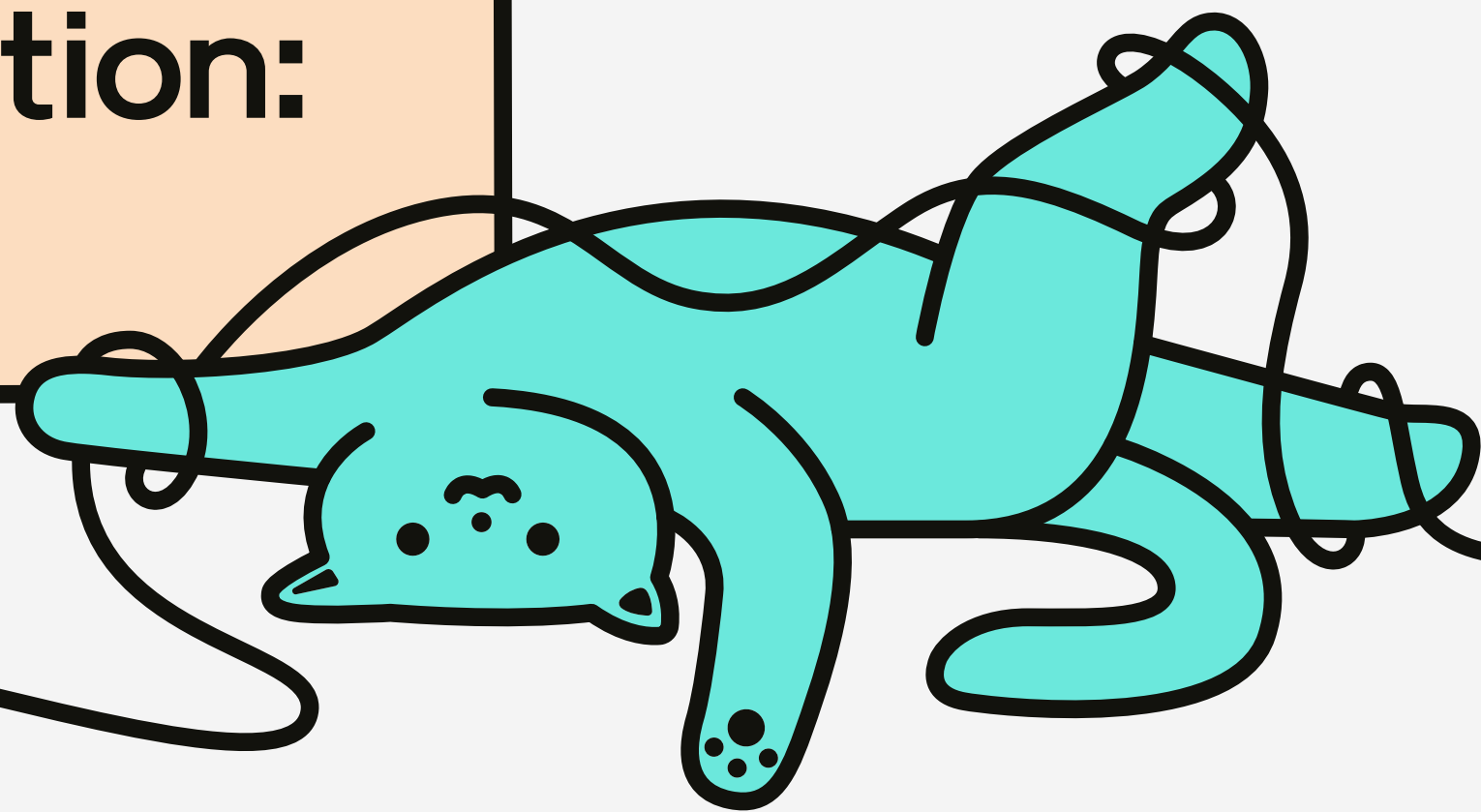
Multiplayer games

Play online safely



About three billion people play multiplayer games every day. You probably also spend some time after school playing Roblox or Minecraft. Multiplayer game lobbies can be a lot like social media, so the rules we've talked about before — especially about sharing personal information — apply when playing games, too.

But games are also very unique. Here's where you should pay extra attention:



Using your microphone and camera when playing



Not everyone in a game lobby is who they say they are. Keep your camera off with strangers and be careful about what you share in the heat of the moment.

Spending money on in-app purchases



Modern games are designed to make purchases feel exciting and urgent, but even small amounts can add up fast. Take a breath and think twice before you buy.

Trading game items between other players



If someone is offering you something that seems too good to be true, it usually is. Never trade anything valuable with someone you have just met.

Downloading game updates and mods



New mods can make your favorite game even better — but only download them from official, trusted sources. Fake mods are one of the sneakiest ways hackers get onto your device.

Winning and losing



Winning and losing are two sides of the same coin — you can't have one without the other. Enjoy your wins and try to learn from your losses. But if losing ever makes you so frustrated that you still can't stop playing, remember that as your brain telling you it's time for a break.

Activity



Next time you play, invite your parents and show them your favorite games, characters, and items you're saving up for. Parents love to hear about all the friends you meet online and can help you decide if they are trustworthy.

Password security

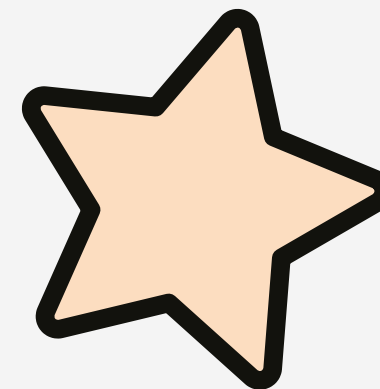
Passwords are important. In your life, you'll create hundreds of accounts. You'll need passwords for email accounts, social media, banking apps, online stores, and game platforms. Your password will determine how protected your account is.



If you only spend a second to enter “123456” as your password, anybody could guess it and steal your account. Even worse, if you reuse the same password, all your accounts could be stolen.

@Online!Hero#+1

Here's what you should know about account security:



Complex passwords

A strong password is long and mixes uppercase letters (ABC), lowercase letters (abc), numbers (123), and special characters (!@#). A password using 12 or more symbols, alternating between letters, numbers, and special characters, would be very hard to crack. Make it as complex as **#P1nkUn1C0rn\$!**

Passphrases

A passphrase is just a long password made of words, but that is its superpower. A short, jumbled password like **X!9fsfkPt@** is hard to crack but also hard to remember. A long phrase, such as **pizzarocketdolphin** is memorable and is even harder to guess than a short but complex password. Come up with your own crazy passphrase!

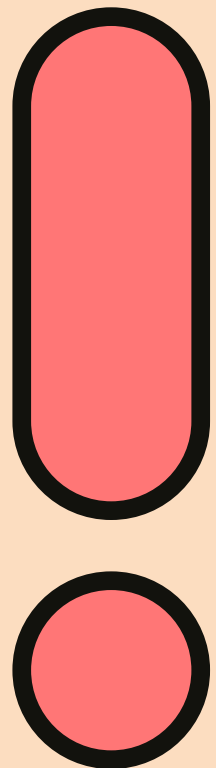
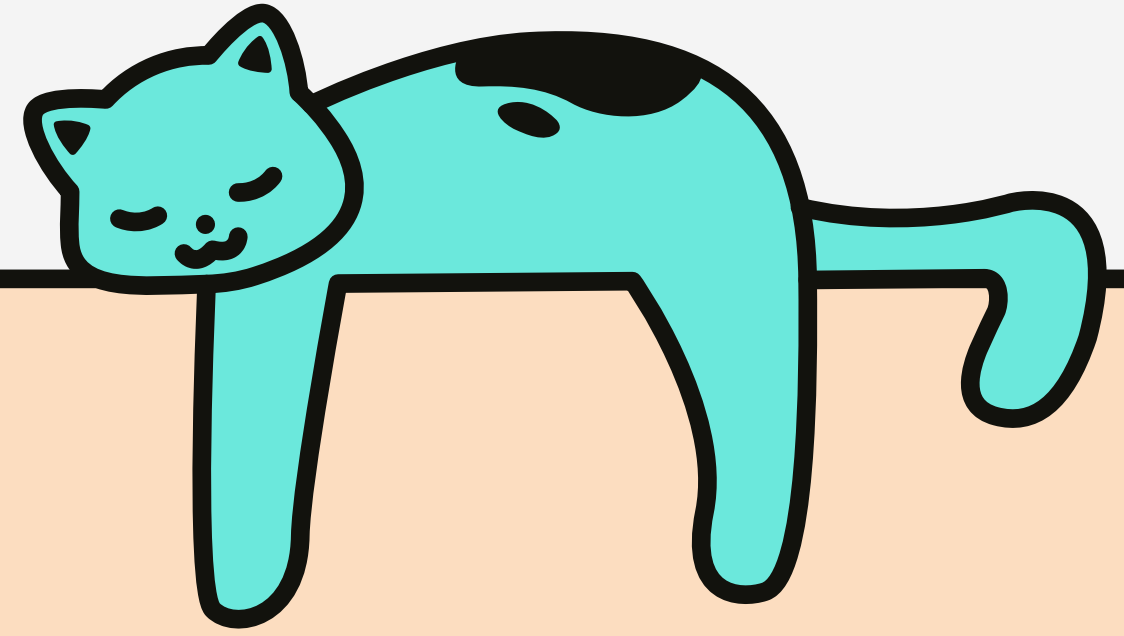
Two-factor and multi-factor authentication

Whatever password method you choose, you can make it twice as strong by having a second lock — like on your door. Even if someone has your password, they still can't get in without a second check — like a code sent to your phone or email. Turn two-factor authentication on wherever you can — it's a powerful way to be safer online.

Activity

Weak password challenge!

Challenge your parents to go through the [200 most common passwords](#) together and count how many you've used for your accounts. Be honest! You can also visit [this page](#) to check how strong your passwords are and even know how many times they've been found in leaks before.



What to do next

If you find that creating strong passwords is difficult, ask your parents to install a good password manager for you. This way, you'll only need to remember one strong password for your password vault.

Guard your identity

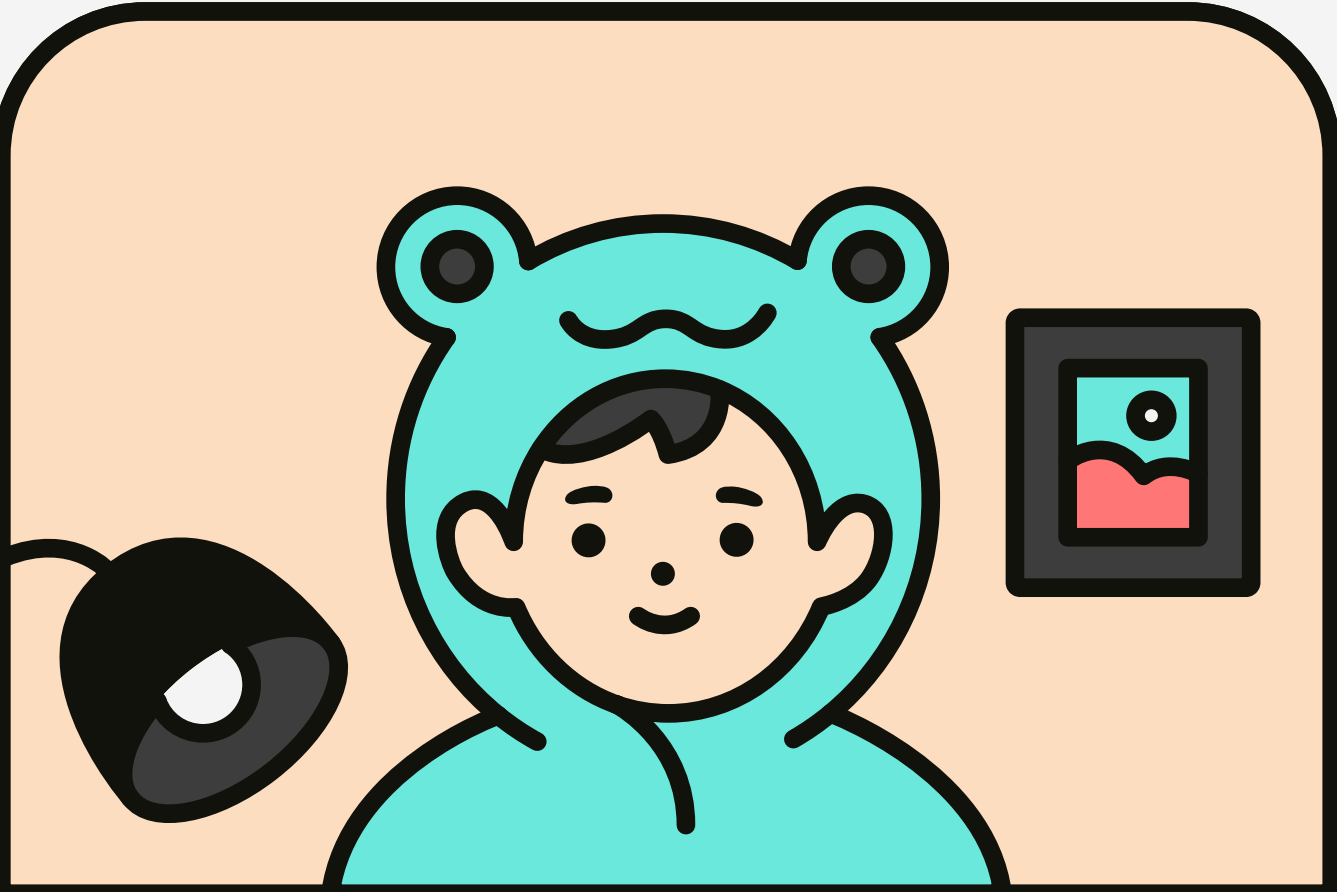
Protect personal information

When you walk on snow or sand, you leave footprints. It's the same online. Whenever you visit websites, create accounts, like pictures, and share posts, you leave digital footprints someone could use to follow you online.

Terms we'll learn

A digital footprint is a trail of data you leave behind every time you use the internet.

What does a digital footprint actually look like?



♥ 💬 ▼

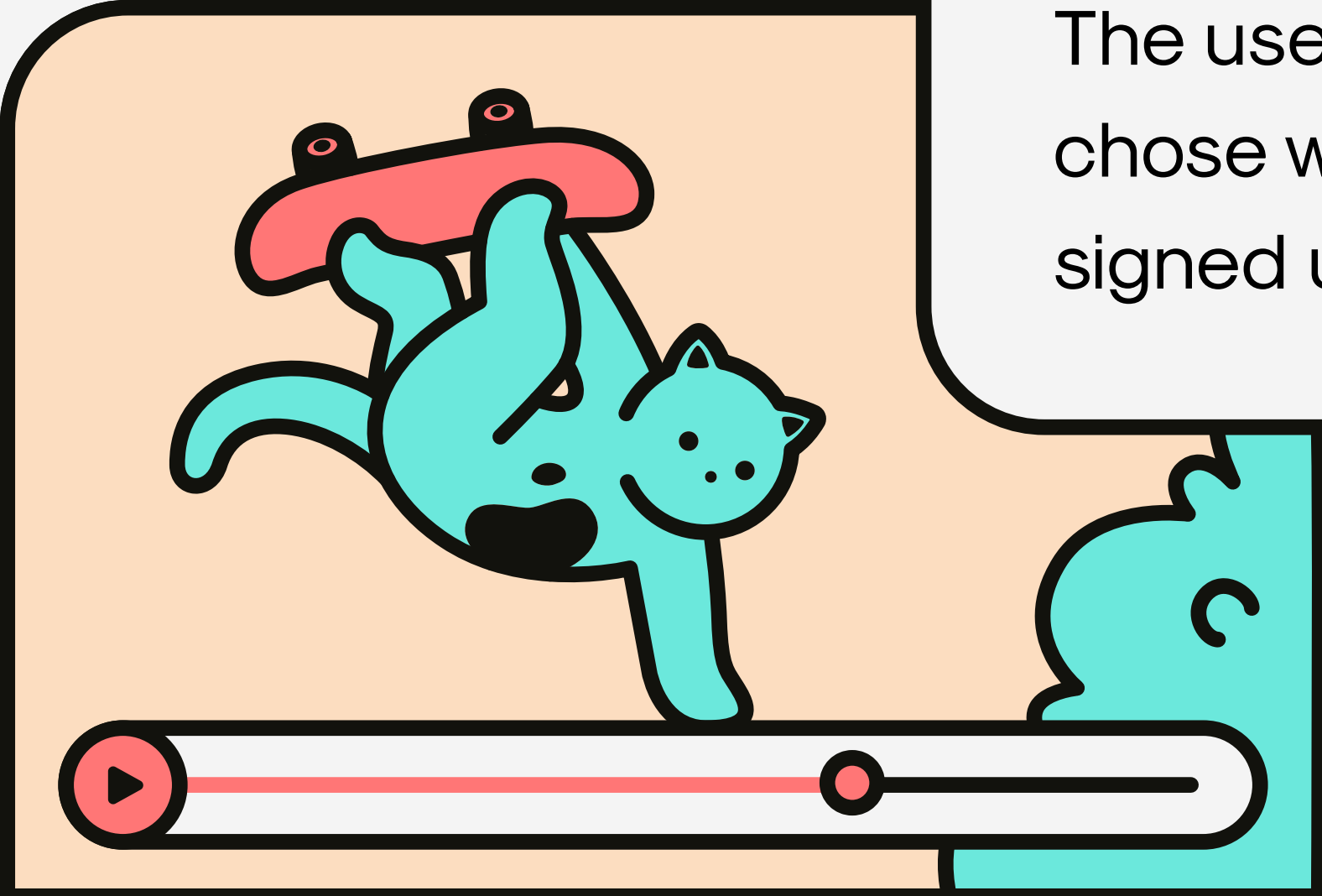
A photo you posted on a gaming profile.



Online-Hero

Sign Up

The username you chose when you signed up for an app.

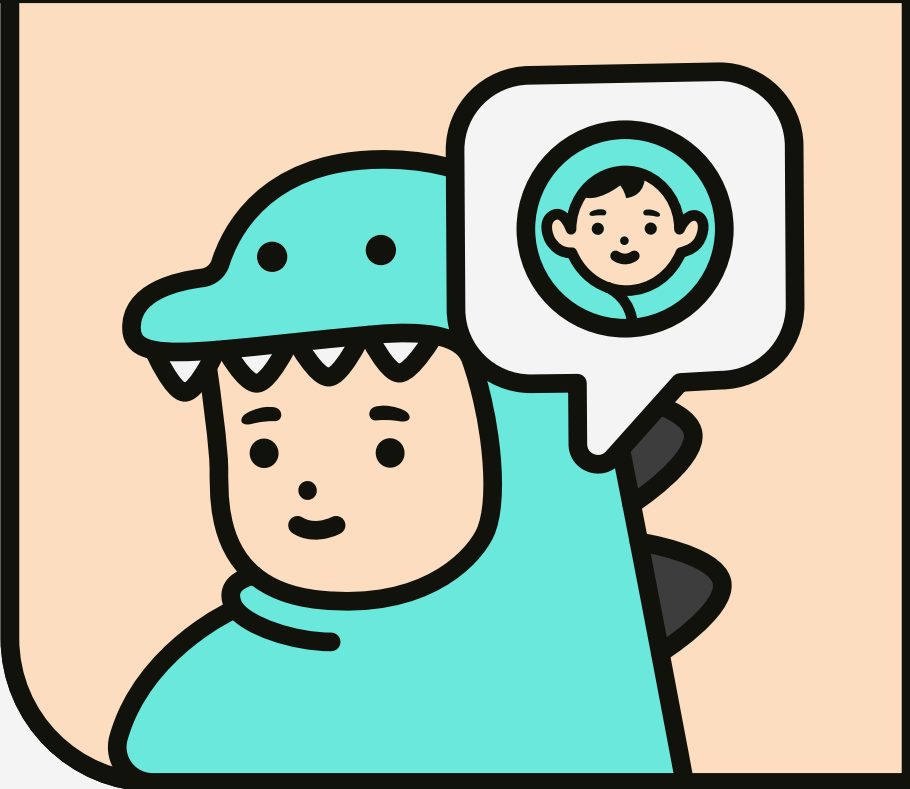


A comment you left under a YouTube video.





Your location if an app was tracking it in the background.



A post a friend tagged you in — even if you didn't post it yourself.

Why privacy matters

You may be thinking why would anybody need your old email account or the town you live in. What's the big deal? Well, privacy is a big deal because even a small piece of information about you can reveal a lot, if it's added to all of the other pieces. Determined scammers can take a lot of time putting pieces together just to ensure their attack is successful.

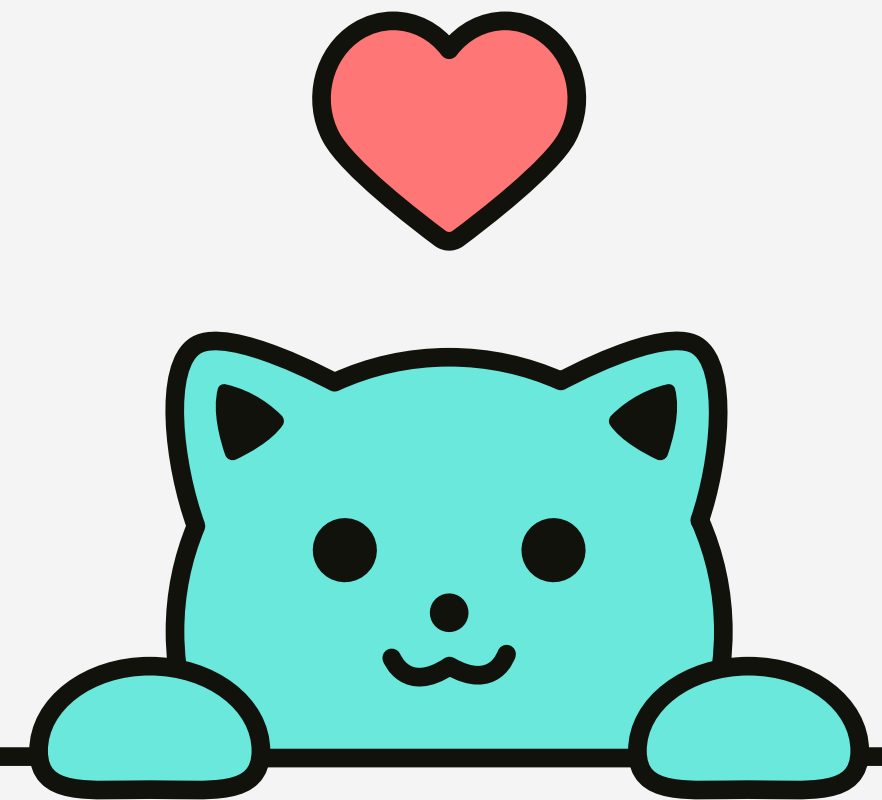


Activity

Do you have any accounts you don't use anymore? Apps on your phone or tablet you haven't used in months? Delete these accounts, then the apps.

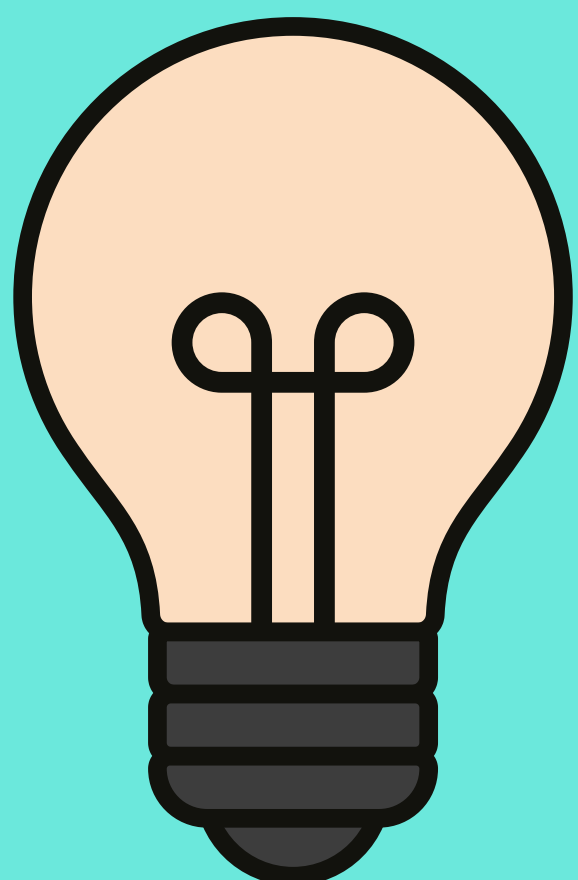
Internet safety rules for kids

Take breaks for your brain



The internet is a fascinating place — full of games, videos, friends, and endless things to discover. Sometimes, too many things. Adults and kids alike end up spending way more time online than they planned. And honestly? That's not entirely your fault. Companies design apps and games to keep people scrolling, making purchases, and wanting to spend just a little bit more time and money on them. That's why taking breaks is not just a rule grownups made up, it's actually really important for your brain.

Did you know?



Boredom is good for you

When you're bored, your brain doesn't just switch off. It actually gets to work. Boredom helps your imagination grow, it gives your mind time to rest, and it improves your focus when you do come back to something. In other words, those quiet moments away from the screen are secretly doing a lot for you.

So how do you know when it's time to take a break?

Use a digital timer.

Set a limit before you start playing — and actually stick to it when it goes off.

Ask an adult for help.

If you find it really hard to stop on your own, ask for help. Talk to a parent so they can help you set up boundaries that work for you.

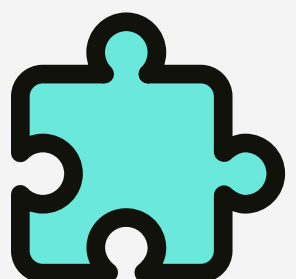
Notice if fun has turned into a habit.

If you're playing but not really enjoying it anymore, it's definitely time to stop.

Check in with how you feel.

Are your eyes tired? Are you grumpy or frustrated? That's your body telling you it needs a break.

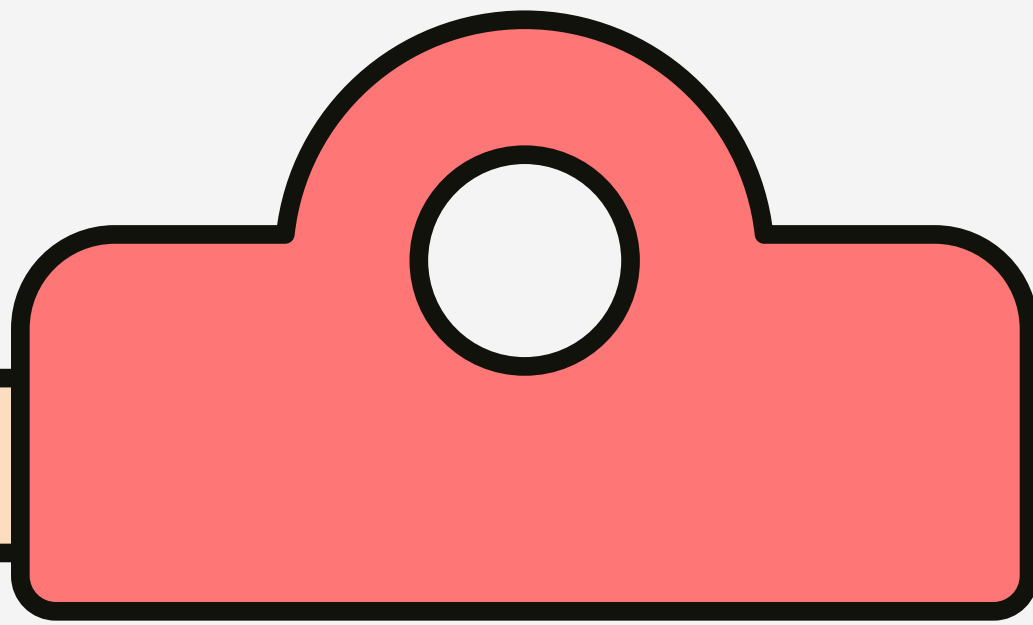
Activity



Track your time! For one week, mark the time you spend on your devices and how much time you spend on breaks. You can also track if breaks improve your mood.

Test

What cyber animal are you?



Q1

You're setting up a new gaming account. It asks for your real name and birthday. What do you do?

- A** You fill in your name and birthday. That's what you were asked for, weren't you?
 - B** You fill in some details but skip the birthday, just in case.
 - C** You use a fun username instead and leave personal details out completely.
-

Q2

Another player sends you a vague DM. It only says "Check this out" with a link to click on. What do you do?

- A** You click it — it looks interesting and they seem friendly enough.
 - B** You click it just to see where it goes, but close it quickly if it looks weird.
 - C** You don't click it. Show it to a trusted adult and report or block the sender.
-

Q3

You get an email saying you've won a free gaming headset. It asks you to enter your home address to claim it. What do you do?

- A** You fill in your address right away. How cool will it be to have a new headset?
 - B** You're not sure what to do because you don't remember entering any competition recently.
 - C** You don't fill in anything. Instead, you show the email to your parents.
-

Q4

You see a funny video of a celebrity doing something shocking. It seems fake, but you're not sure. What do you do?

- A** You share it immediately — it's hilarious whether it's real or not!
 - B** You share it with your closest friends only, just in a private group.
 - C** You don't share it. You check the comments to make sure it's not fake.
-

Q5

Someone sends you a friend request on social media. You have three mutual friends, but you've never met them in real life. What do you do?

- A** You accept the request. Having mutual friends means they must be trustworthy.
 - B** You check the person's profile before accepting the request.
 - C** You don't accept the request because you don't know that person.
-

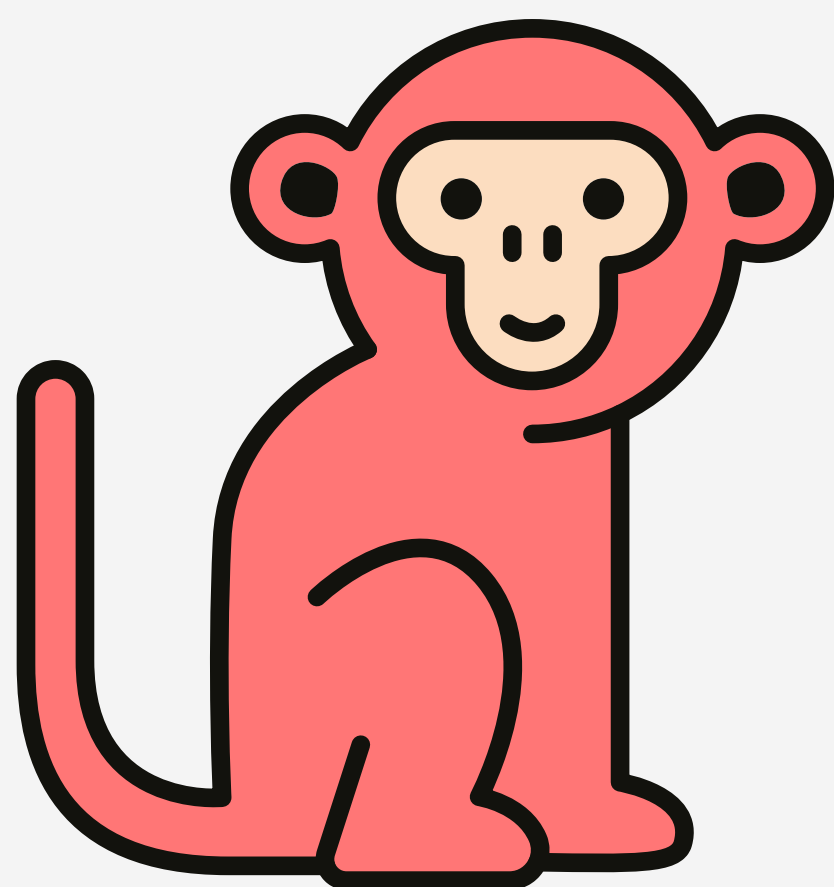
Q6

A game wants permission to access your location, camera, and contacts. What do you do?

- A** You allow all permissions — the game says it needs them.
- B** You grant access to location but not to your camera and contacts.
- C** You deny all permissions.



Now, count your answers and find out what kind of **cyber animal** you are.



**If you answered A the most,
you're an Adventurous Monkey.**

You are enthusiastic, friendly, and you always see the best in people. You make online spaces more fun and welcoming for everyone around you. But watch out — your big, trusting heart can sometimes get you into trouble. Not everyone online is as kind as you are. Before you click on links or talk to strangers, remember that things aren't always what they seem on the internet.



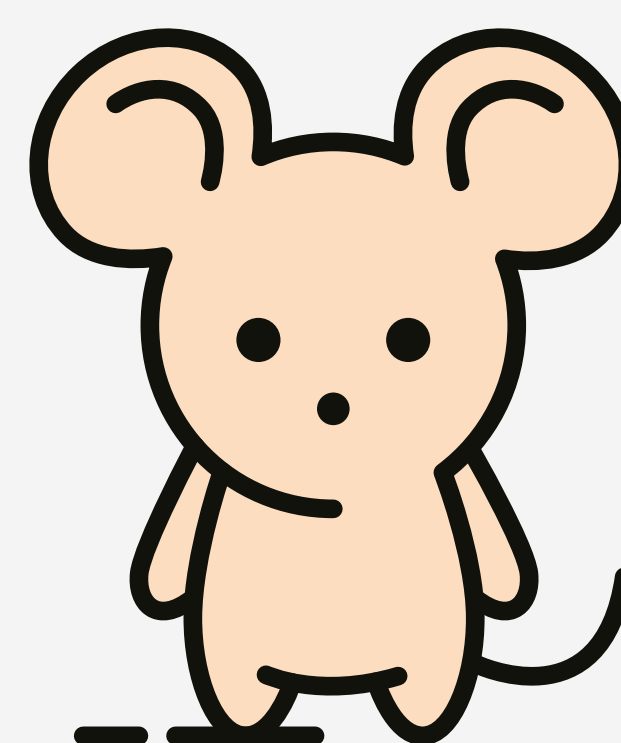
**If you answered B the most,
you're a Curious Cat.**

You are clever, independent, and love exploring new things. You figure out new apps in five minutes flat and always find the coolest corners of the internet. But while curiosity is amazing, it can sometimes lead you somewhere you didn't want to go. Even a quick peek at a dodgy link can cause problems. When something feels even slightly "off," trust that instinct and check with an adult before exploring further.



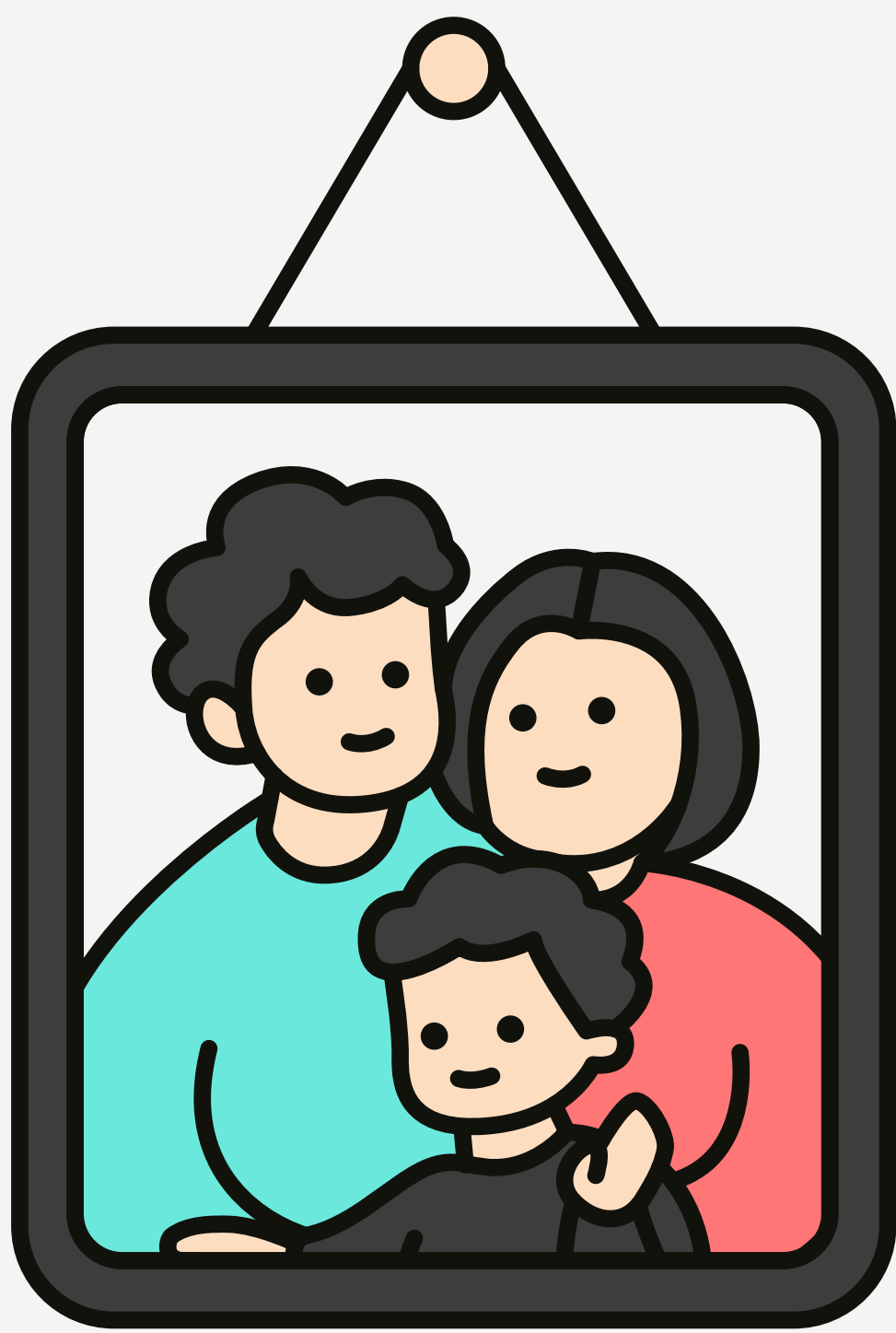
**If you answered C the most,
you're a Cautious Mouse.**

You are calm, smart, and you don't let excitement cloud your judgment. You think before you act, and you're already one of the most safety-savvy animals online. Just watch out for one thing — sometimes being too cautious can make you feel like the internet is a scary place. It's not! Keep your wise instincts, but don't forget to have fun and enjoy your adventures online too.



Activity

Do you like to color? You've learned so much here, so to help you remember all of it, we've created a coloring book for you. Here's where you can [download it](#). And don't worry, this link is safe!



Internet safety tips for parents

Knowing your child is safe online starts with one simple thing — conversation. But not many know how to talk with their child about online safety. The more natural and regular these conversations are, the more likely your child is to come to you when something doesn't feel right. Here are a few important topics to talk about with your children:

Online privacy

Many apps and games collect more information than most people realize. Go through the privacy settings on every app and game your children regularly use. Check who can see their profiles, whether their location is being shared, and who is allowed to contact them.



People they meet online

You and your children can never know who is hiding behind the avatar in the game lobby. Encourage your child to question people's motives and think before sharing anything personal or clicking on a link from a stranger.



Tip

If you notice your child becomes withdrawn or irritable after using their device, it could be a sign of cyberbullying. Check in with them and, if needed, review their recent messages or activity together.

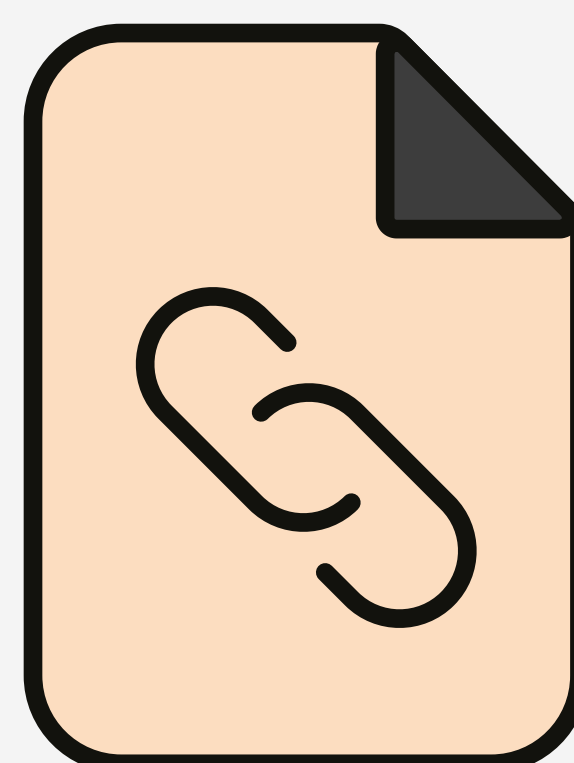


Downloads

Being online, your kids are bound to download something, whether it's a mod for a game, an app, or a shared file. Ask them how they know if a download is safe.

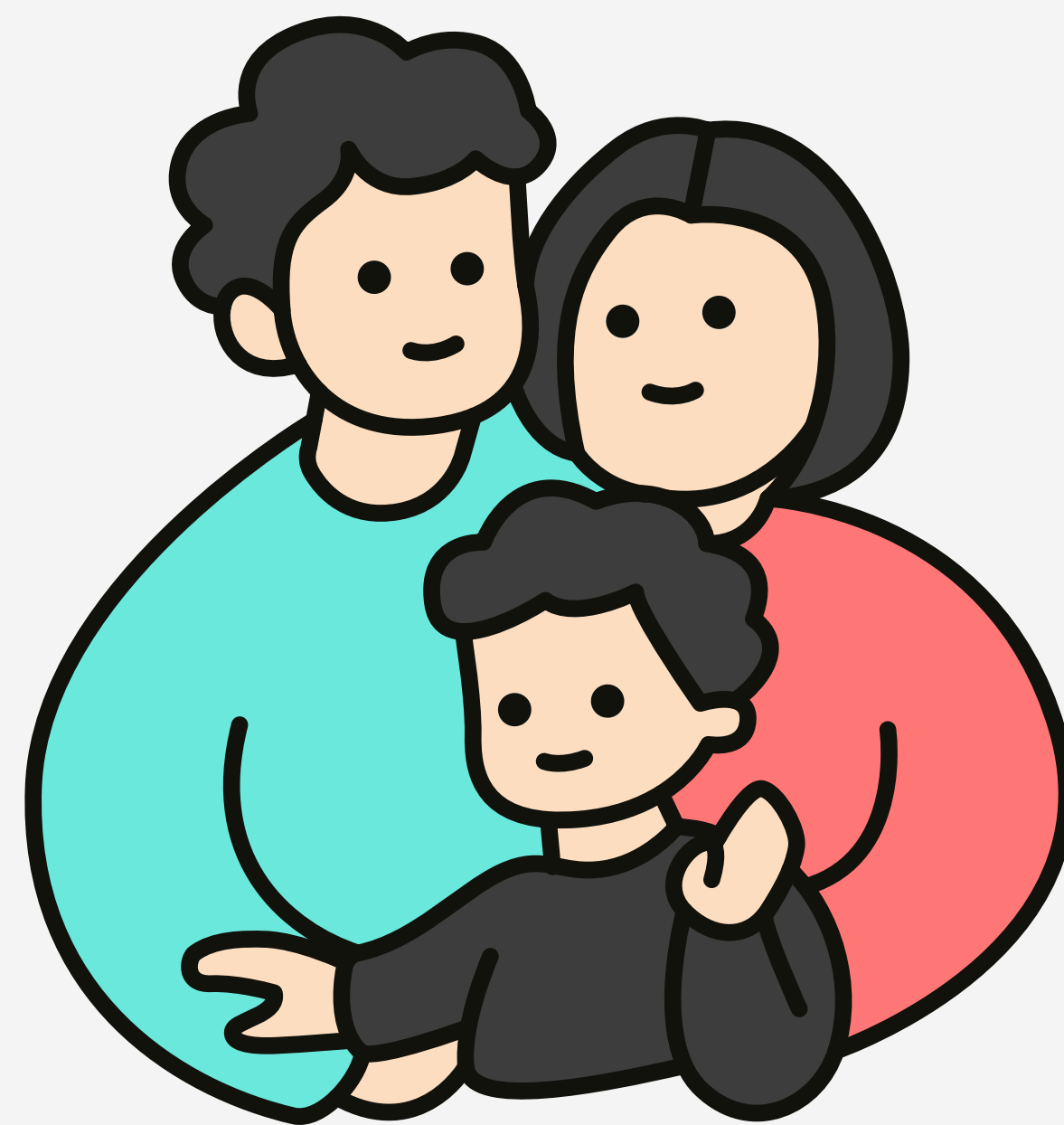
Tools for online safety

Show your child how to use tools such as the [link checker](#) or [file checker](#). These are easy ways to make sure that any dubious link or file is safe to click on.



Keep the conversation going

The goal isn't to monitor your child's every move or **lock the screen to protect your kids**. It's to build enough trust that they feel comfortable coming to you with problems. Ask about the games they play, the people they talk to online, and how things make them feel. The more involved and informed you are, the safer they'll be.



Activity

Of course, we've got an activity for you too! And this one's all about understanding your kids' online behavior. Without any judgement, ask your child what their favorite activity online, who they talk to online most often, or if anything has made them uncomfortable online. You can also ask about hypothetical scenarios about recognizing malicious links or fake news. But remember, no judgement, just curiosity.

Additional resources

If you're interested in more information about cybersecurity, here are a few extra resources:



Cybersecurity awareness hub



NordVPN's YouTube channel



Cybersecurity quiz for kids