LEARNING TOGETHER

CYBER SECURITY FOR TODDLERS

written by Elizabeth A. Quaglia
illustrated by Alex Thompson

LEARNING TOGETHER

CYBER SECURITY FOR TODDLERS

ELIZABETH A. QUAGLIA is Associate Professor in the Information Security Group at Royal Holloway, University of London. Her research area is Cyber Security, with a focus on Cryptography. She is a mum of two toddlers, Ale and Leo, who love eating cake.

ALEX THOMPSON is a digital product designer with a knack for illustration. When she isn't drawing dinosaurs, she's working to build international commerce and marketing tools in London.
Find her at @userologist.

This booklet has been created with the help of
DR. VALENTINA ZAMBON, psychologist,
and MICHELE VILLA, designer.

We also thank DR. JORGE BLASCO ALIS
and DR. JASSIM HAPPA for their advice and support.

HOW TO READ THIS BOOK

With this booklet we want to provide an opportunity for children and grown-ups to learn together about cyber security.

To help children understand the concepts, we suggest the grown-ups involve them in the description and discussion of the story in the following pages.

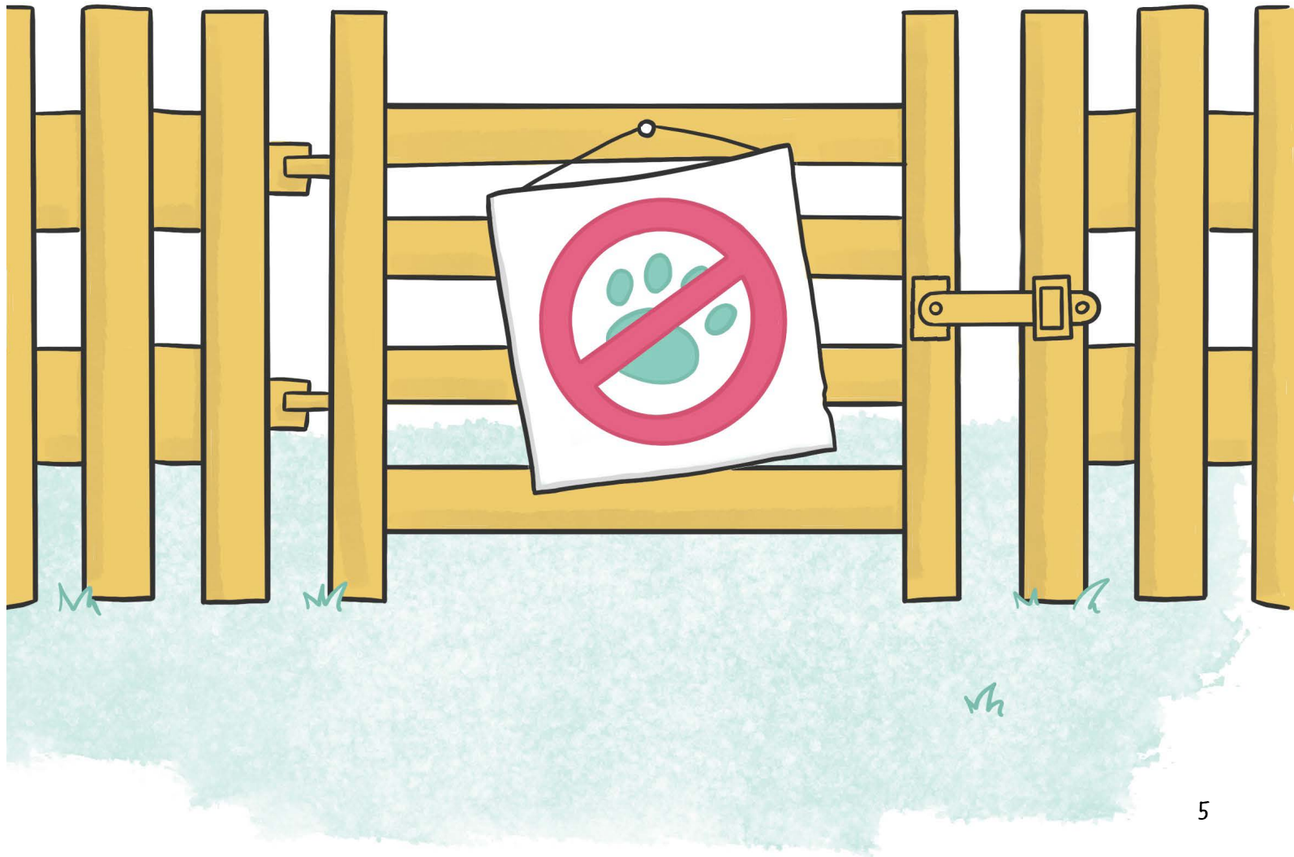
Questions like "Where is the dog?" or "What is the dog trying to do?" can be a useful way to engage the children. So… ask lots of questions!

For example, on page 8, the dog is trying to get in the playground. In what ways can the dog do this? The drawings show it could jump over the fence or go through the gap. But what if someone left the gate open? Would that be another way in? Further, on page 15, the biscuit looks different from what expected. In what ways could this happen? Has it been replaced with a different biscuit? What if someone took a bite off it?

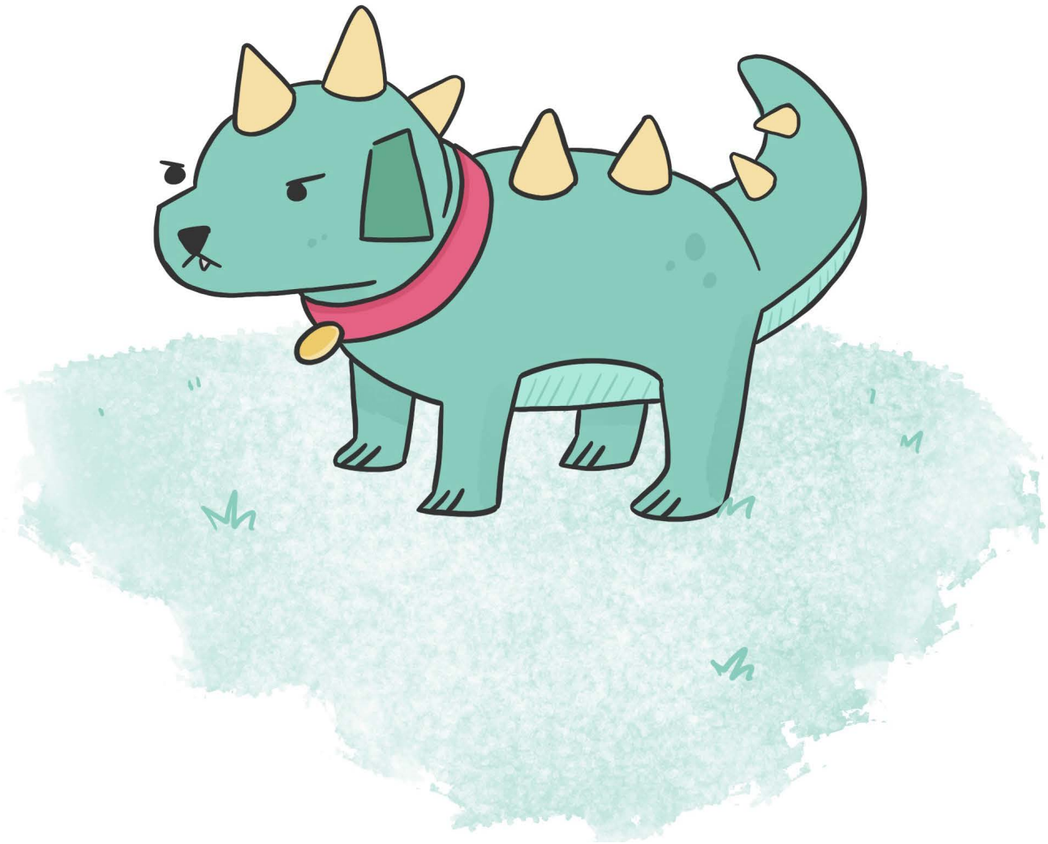
For the grown-ups, a glossary is provided at the end of the booklet, defining the cyber security terminology we capture in our story and providing links to additional resources for further learning on the topic.

Let's go to the PLAYGROUND!

This is a GATE.
It controls who can get into the playground.



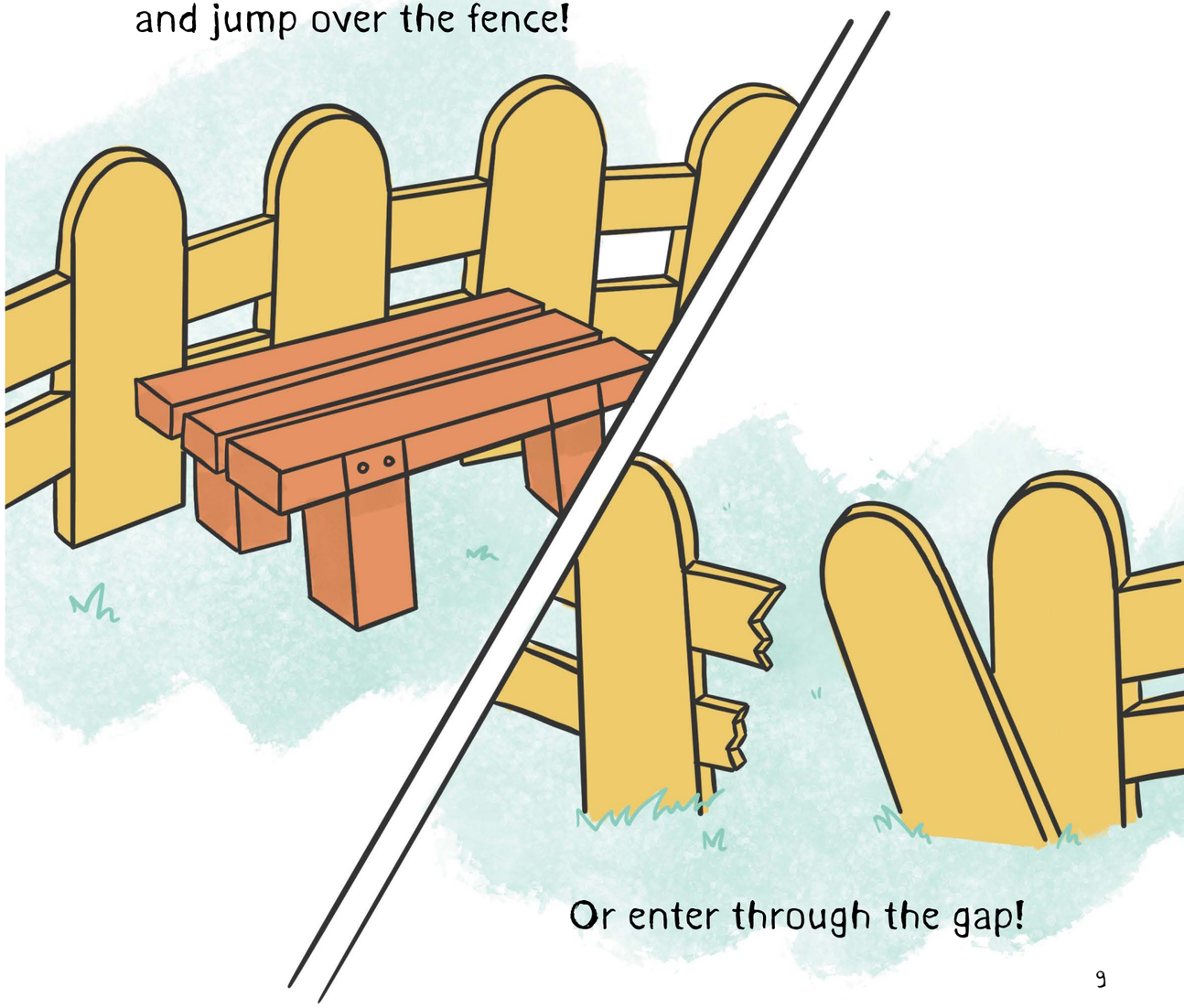
This is a dog.
The dog also wants to enter the playground.



But the dog is NOT ALLOWED
in the playground!

In what other ways could the dog get in?

It could climb onto the bench
and jump over the fence!



Or enter through the gap!

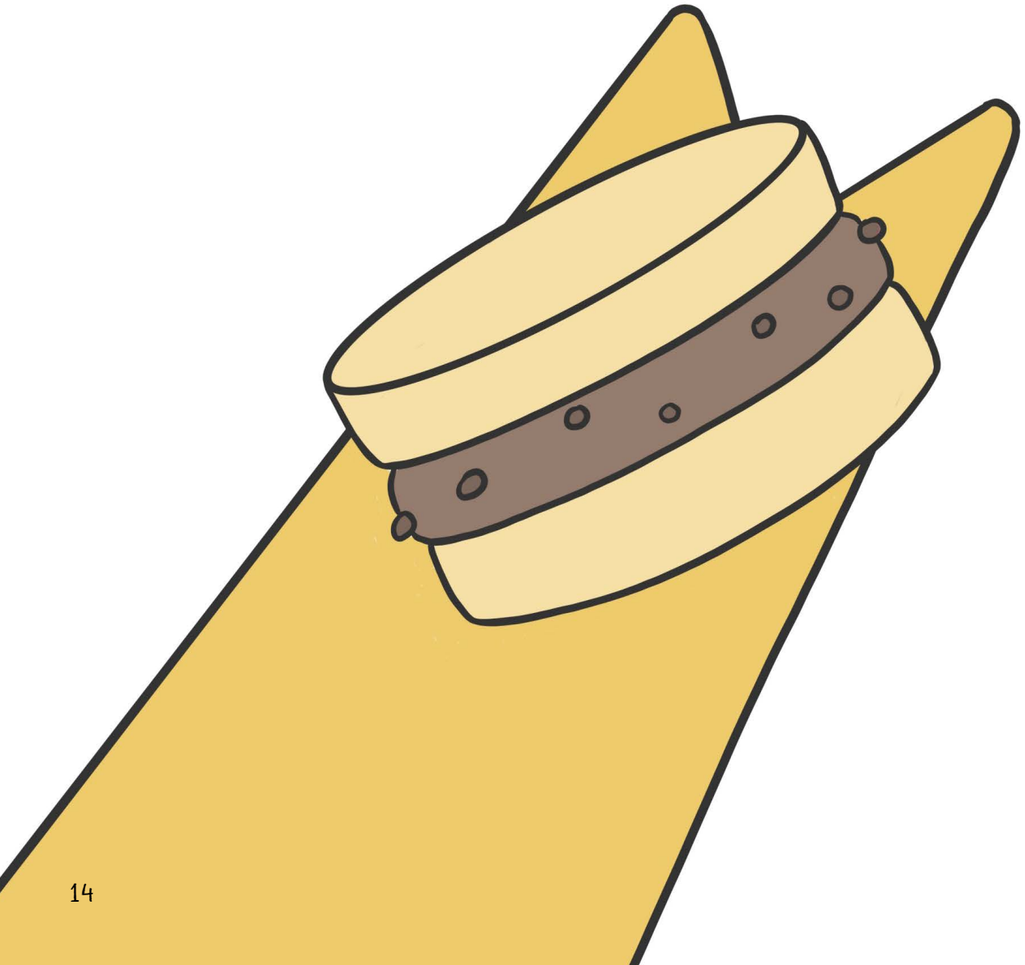
There is a PAWPRINT in the mud!

The dog must have found
A WAY INTO the playground!

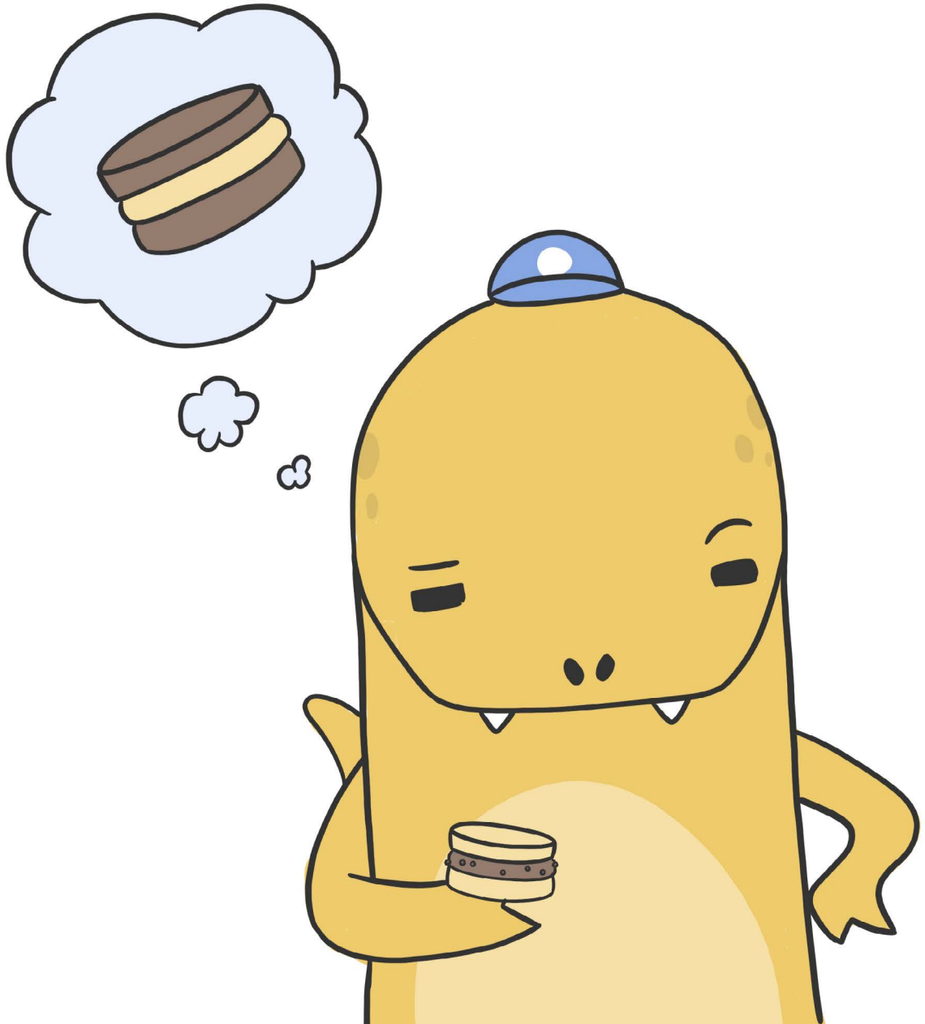
I'm hungry now.
Let's have a biscuit!

I can't wait to eat my favourite biscuit!

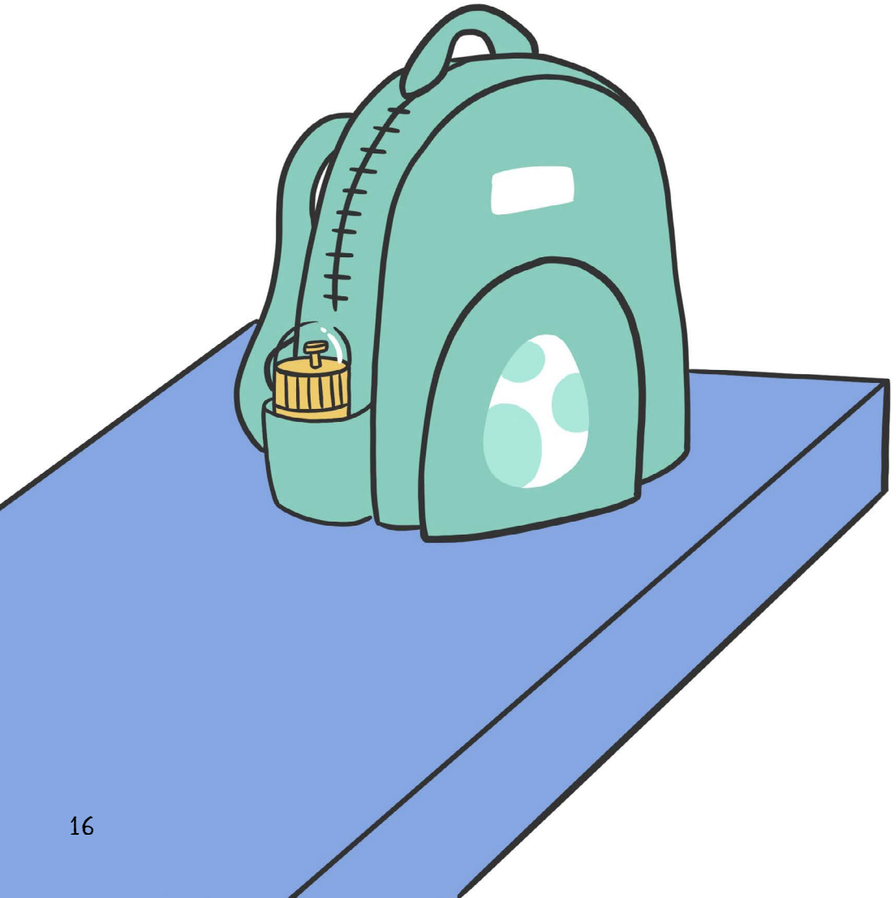
But something looks different...



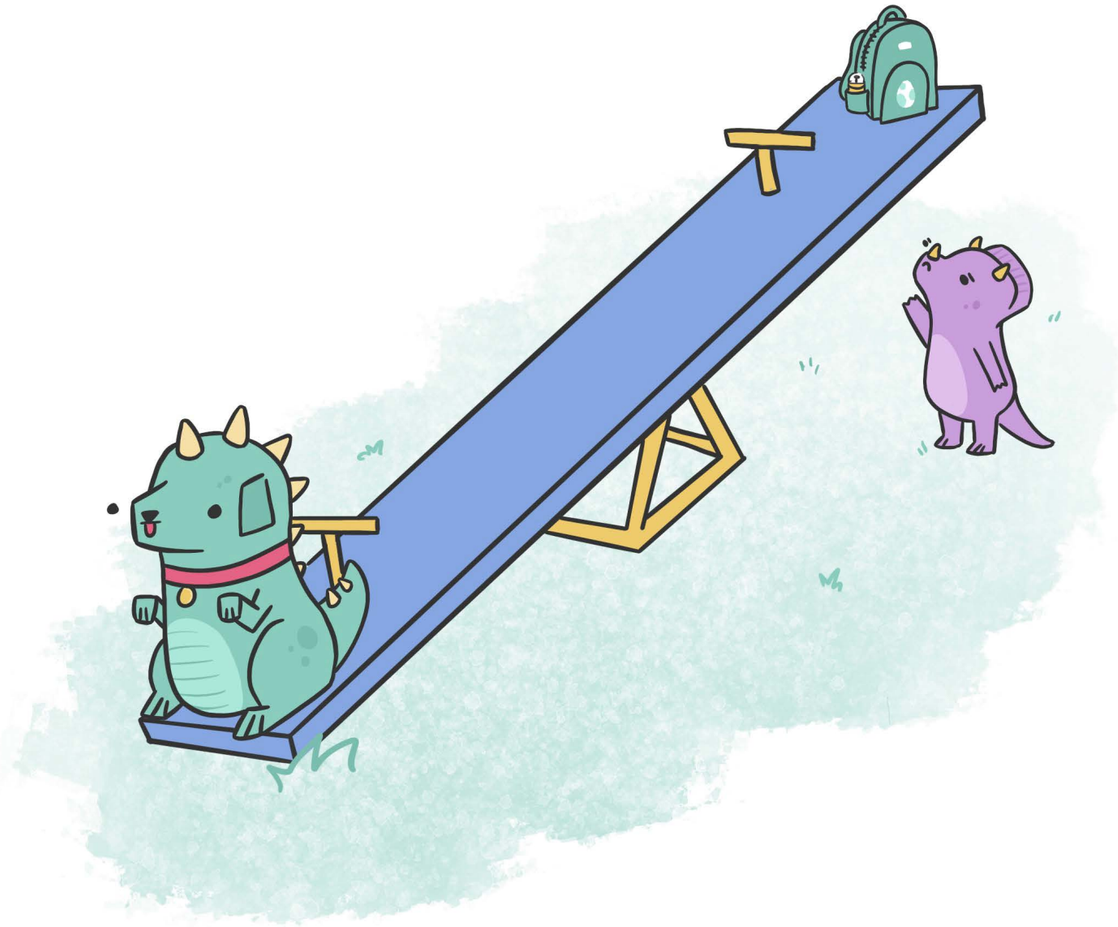
The biscuit has been CHANGED!



It's time to drink some water.



But the water bottle is OUT OF REACH!



Better HIDE the food and drinks from the dog.

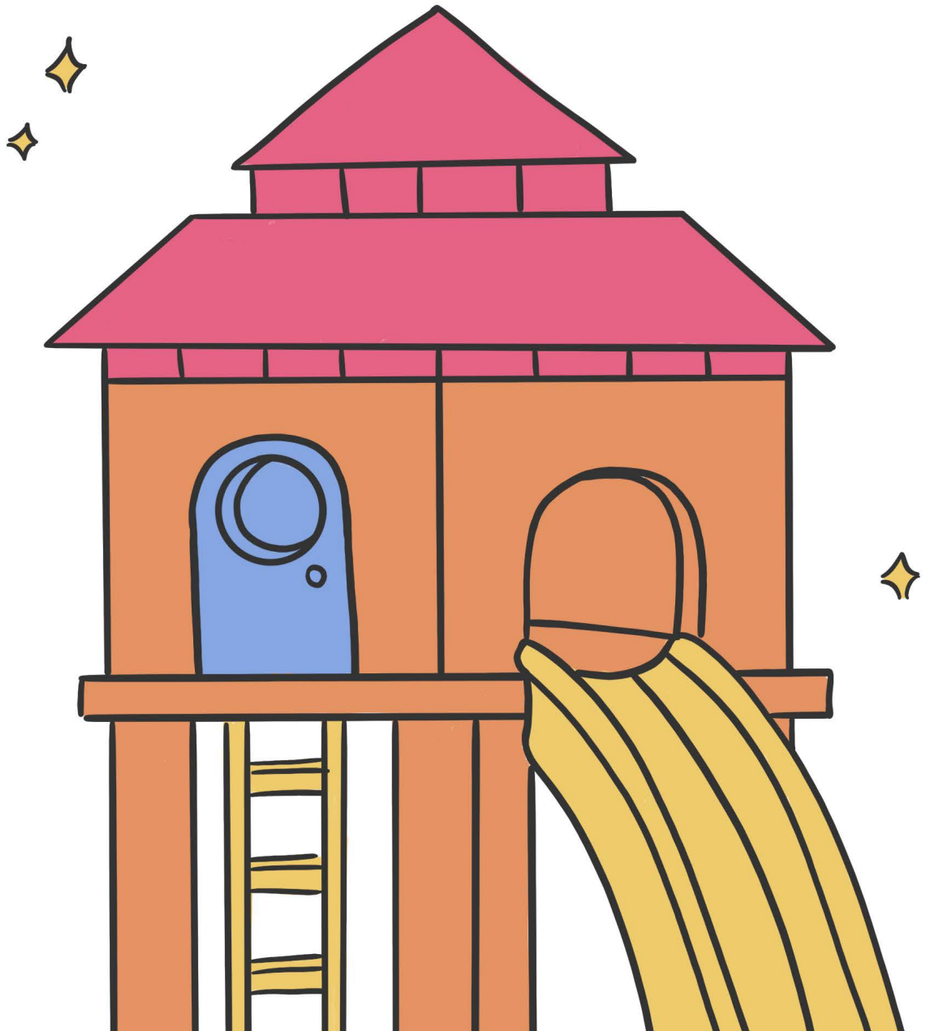
Let's SECURE our bags!

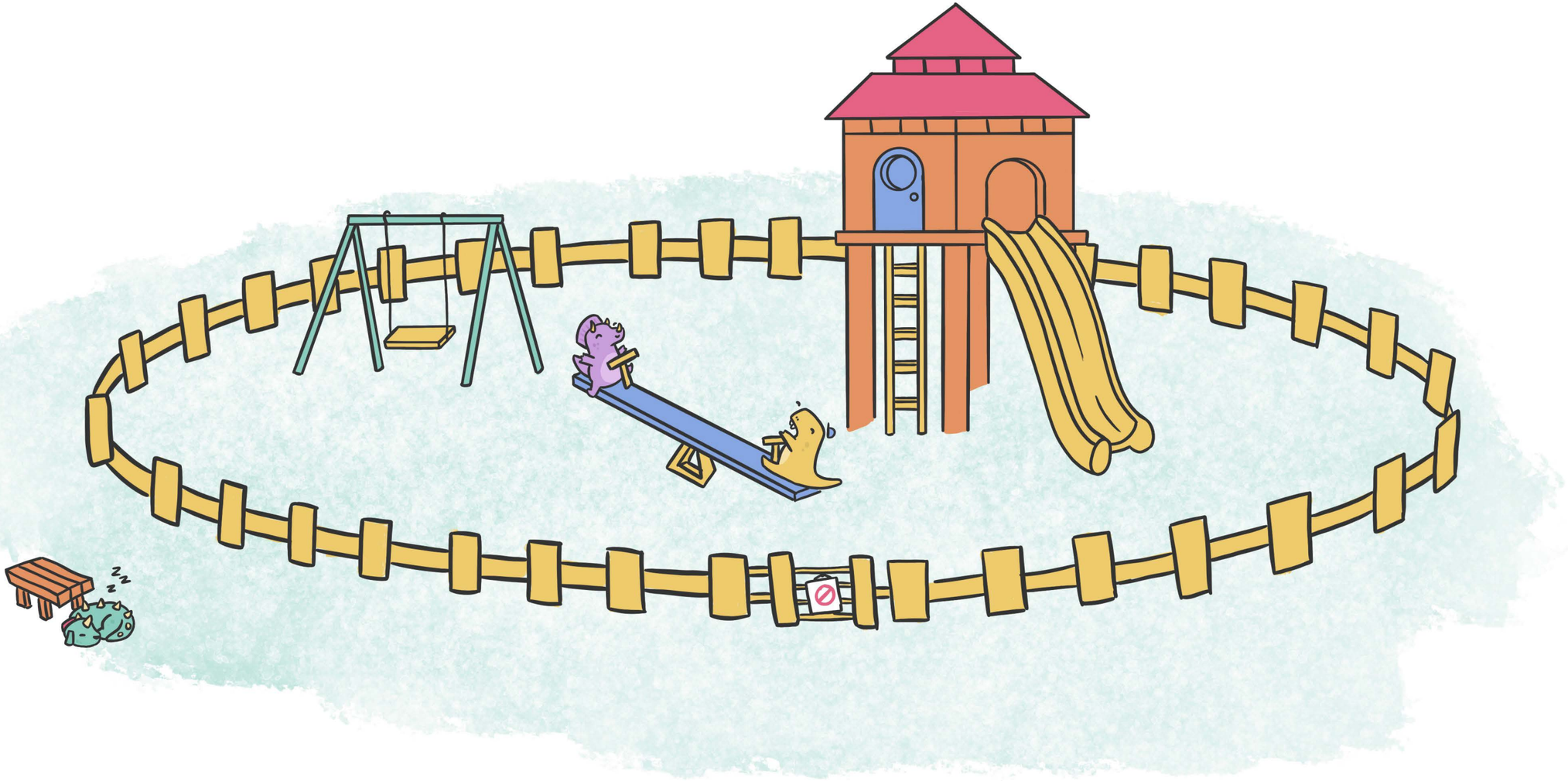
Let's go on the slide now.
We need to climb the steps to reach it.

But the last step is out of position.
This is dangerous - someone could fall.

The step can be put safely back into position.

Now it is SAFE to play in the playground!

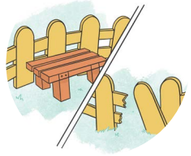




GLOSSARY

CYBER SECURITY deals with the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse (whether intentional or accidental). In our booklet we view the playground, and the activities that happen within it, as a system that needs protection from unauthorised access and misuse.

ACCESS CONTROL is about selectively restricting access to a resource. It involves both authentication (the act of verifying who you claim to be) and authorization (the act of granting access to the resource). In our story, the gate controls the access to the playground, preventing the dog, i.e., an unauthorised entity, from entering.



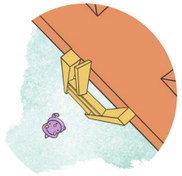
A **VULNERABILITY** is a flaw that can be exploited to gain unauthorised access to a (computer) system. In our story, the gap in the fence can be viewed as a weakness the dog can exploit to enter the playground.

INTRUSION DETECTION is the ability to monitor and react to (computer) misuse. In our story, the pawprints in the playground reveal that an intruder has entered the system (i.e., the playground) and following them could help monitor the situation.

DATA INTEGRITY enables the detection of unauthorised modification of information. We capture this concept representing information as a biscuit, and showing how a modification to the original (i.e., the flavours have been swapped) can be detected. Similarly, one could detect if a chunk of biscuit had been bitten off, or it had been substituted altogether with a fruit.

DATA AVAILABILITY is the prevention of unauthorised withholding of information or resources. In our story, the dog makes the water bottle unavailable by putting it out of reach.

DATA CONFIDENTIALITY is the prevention of unauthorised disclosure of information. We capture this representing the bag with food and drinks as information the dog wants access to, and tying the bags with some string prevents the dog from opening them and finding out what the bags' contents are.



RISK (ANALYSIS) involves not just listing possible threats, but also assessing the likelihood of their being realised, and the potential cost to the system users if they are realised. In our story, we capture this concept by observing there is a risk to climb the steps as the last one is broken, and fixing it allows to continue to play safely.

For more information on these concepts, and on
cyber security as a whole, please visit https://www.cybok.org.

ADDITIONAL RESOURCES

An introduction to cyber security and its knowledge areas

An introduction to cyber security: Stay safe online - A free course

Online safety videos for parents, teachers and children