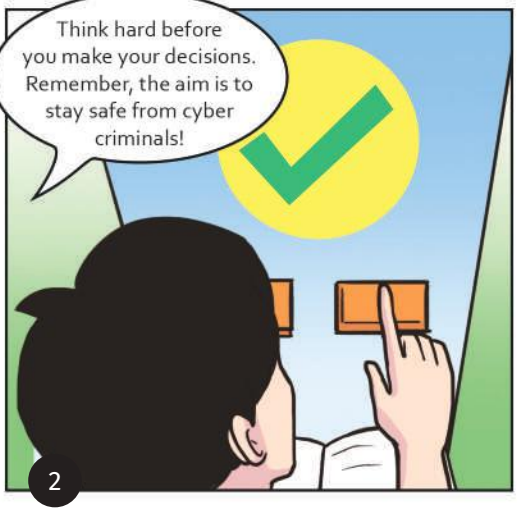
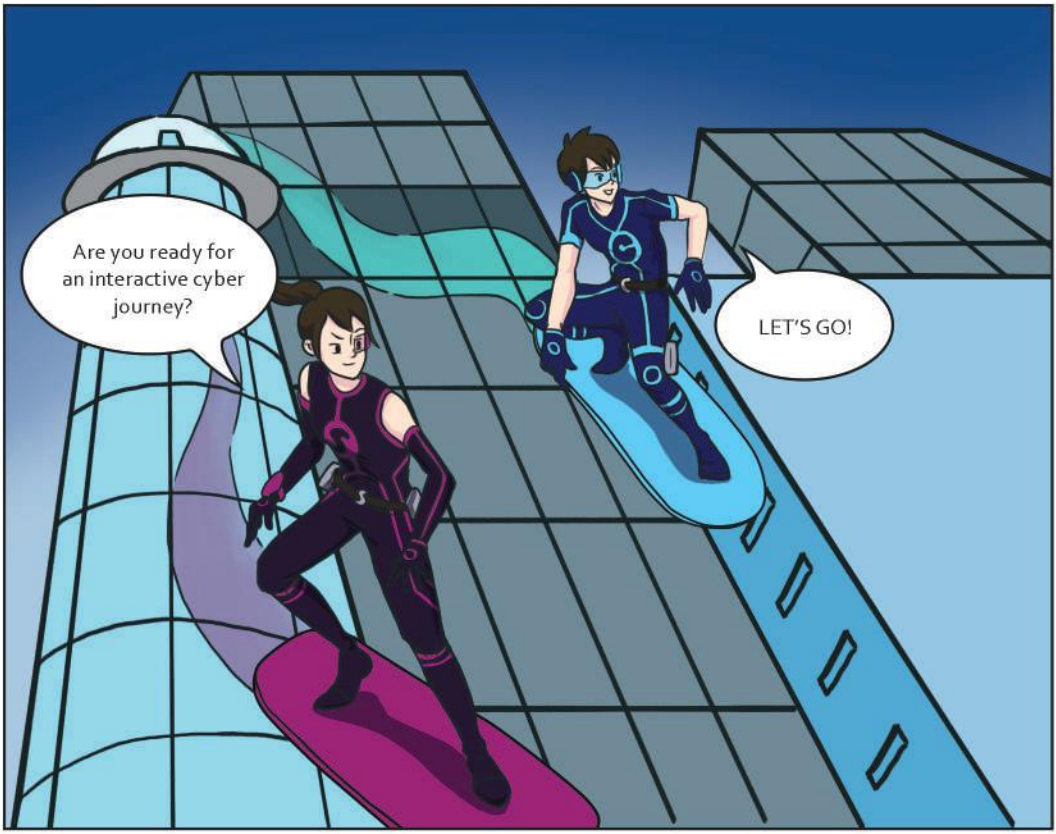
CYBER SAFETY

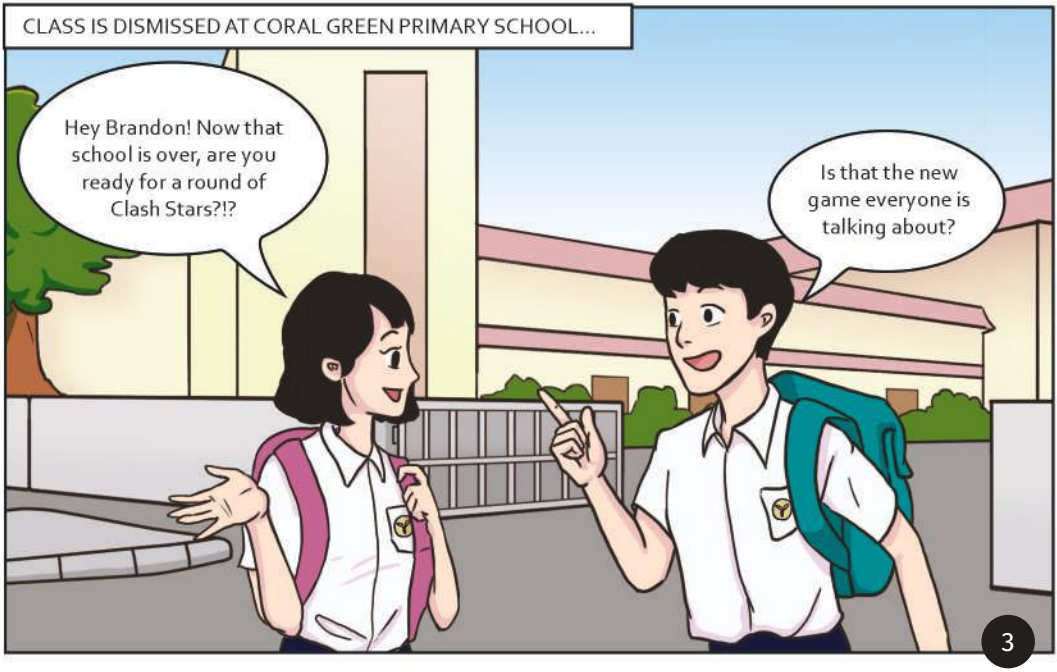
THE INTERACTIVE HANDBOOK

AIDEM

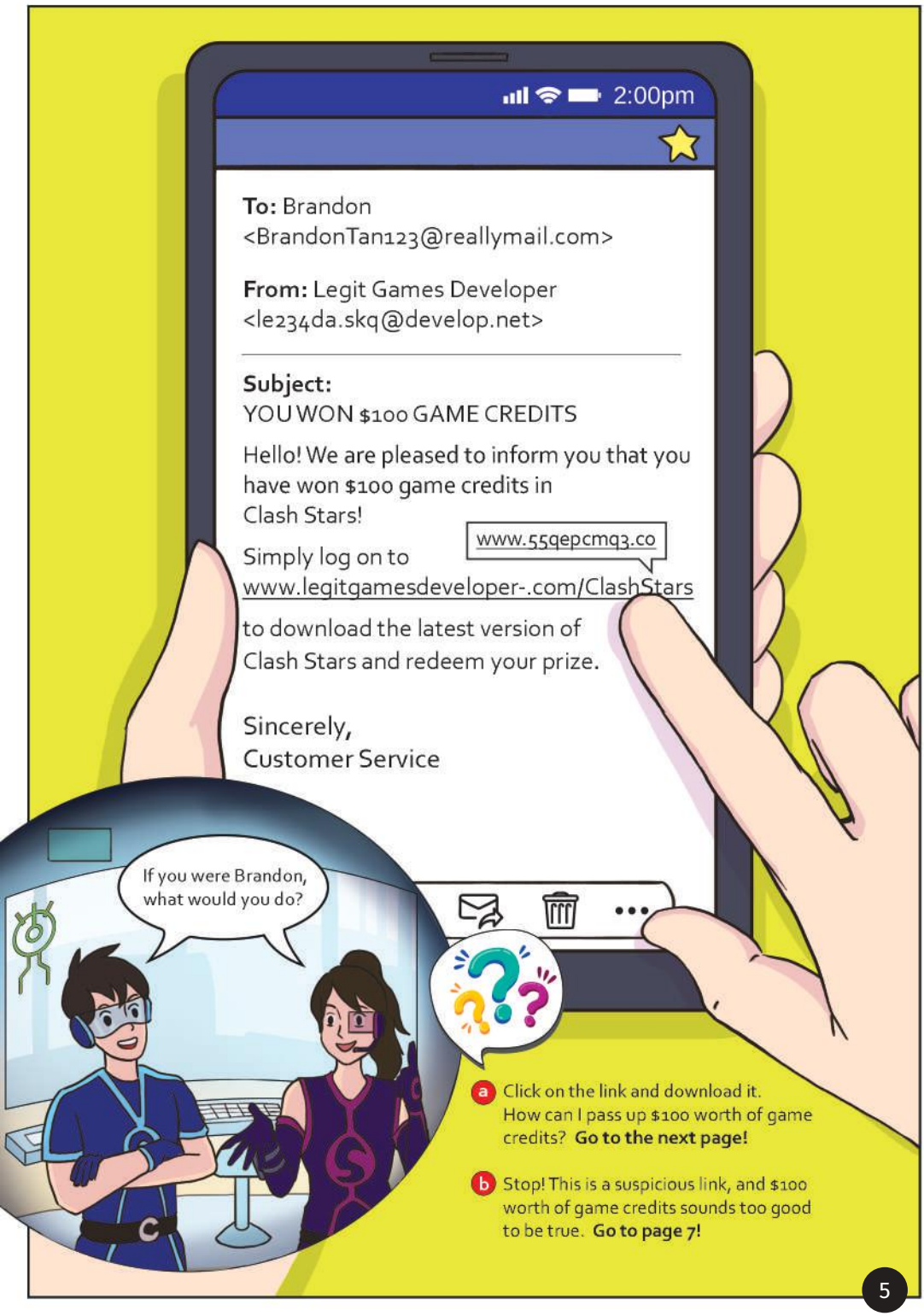
ARTIFICIAL INTELLIGENCE DEFENSE MECHANISM

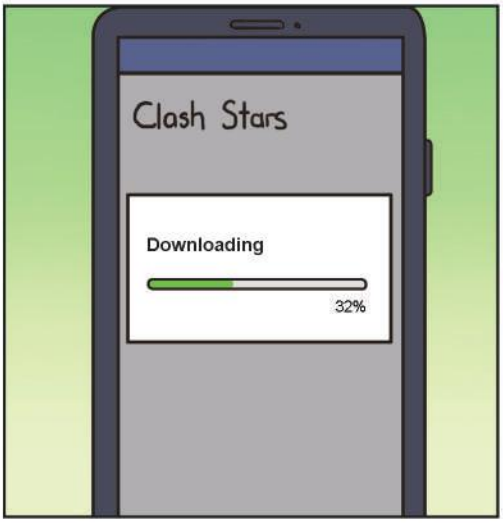



Are you ready for an interactive cyber journey?
LET'S GO!


CLASS IS DISMISSED AT CORAL GREEN PRIMARY SCHOOL...
Hey Brandon! Now that school is over, are you ready for a round of Clash Stars?!?
Is that the new game everyone is talking about?


You mean you haven't tried it out yet? You can try it out on my phone.
5 MINUTES LATER...
Remember to join the Clash Stars forum for more tips!
Thanks for the tips on Clash Stars, Alexia! It's getting late, we should head home.
See you tomorrow!
LATER THAT WEEK...
Oh an email. I wonder who it is from.
Ping!
Oh wow! That's amazing!


2:00pm
To: Brandon
<BrandonTan123@reallymail.com>
From: Legit Games Developer
<le234da.skq@develop.net>
Subject:
YOU WON $100 GAME CREDITS
Hello! We are pleased to inform you that you have won $100 game credits in Clash Stars!
Simply log on to
www.55qepcmq3.co
www.legitgamesdeveloper-.com/ClashStars
to download the latest version of Clash Stars and redeem your prize.
Sincerely,
Customer Service
If you were Brandon, what would you do?
a Click on the link and download it. How can I pass up $100 worth of game credits? Go to the next page!
b Stop! This is a suspicious link, and $100 worth of game credits sounds too good to be true. Go to page 7!

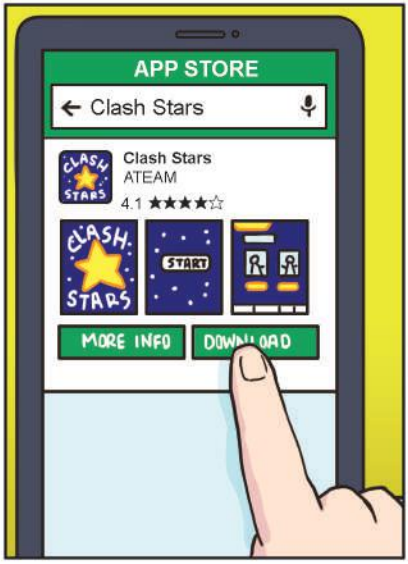


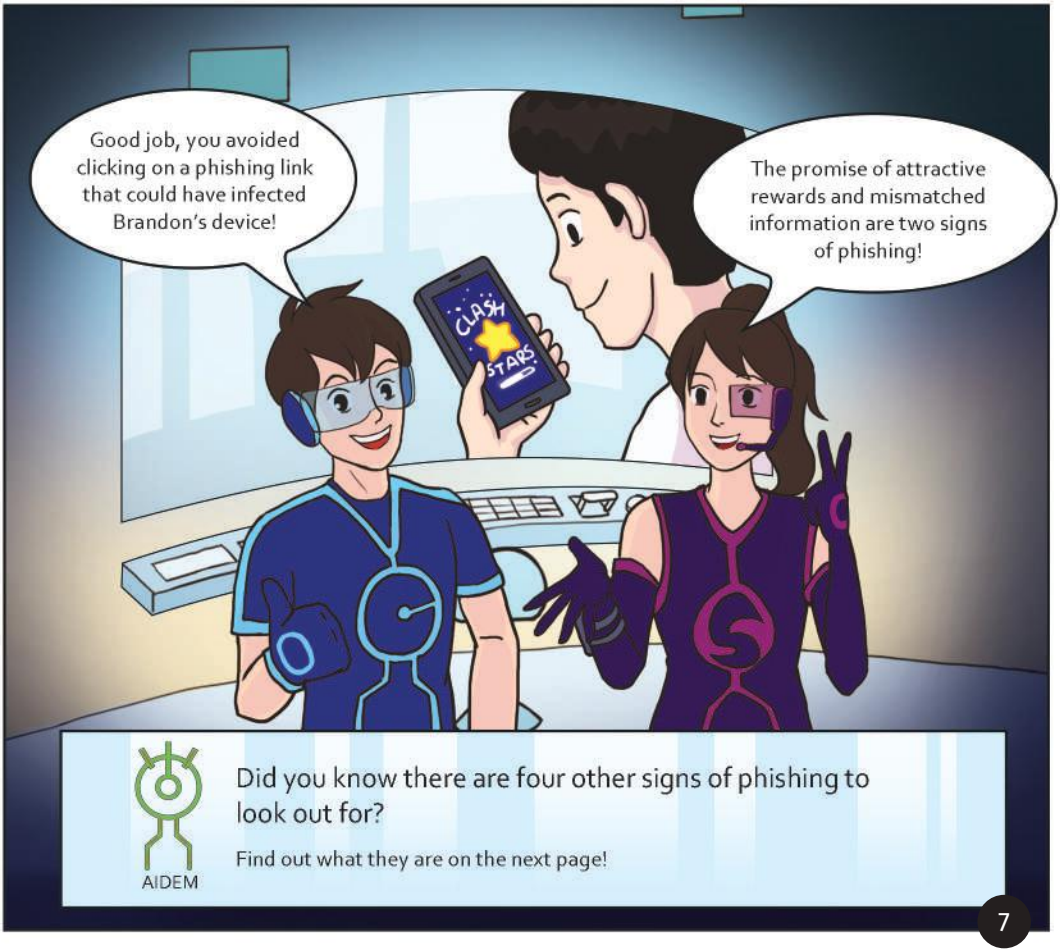
AIDEM

- Always look out for signs of phishing
- Look out for mismatched or misleading information, such as website links
- Be wary of promises of attractive rewards
- Remember to only download apps from official app stores

Head to page 8 to learn how to spot signs of phishing!


The website links do not match... obviously a phishing email! I should only download games from the official app store.


APP STORE
Clash Stars
Clash Stars
ATEAM
4.1
START
MORE INFO
DOWNLOAD

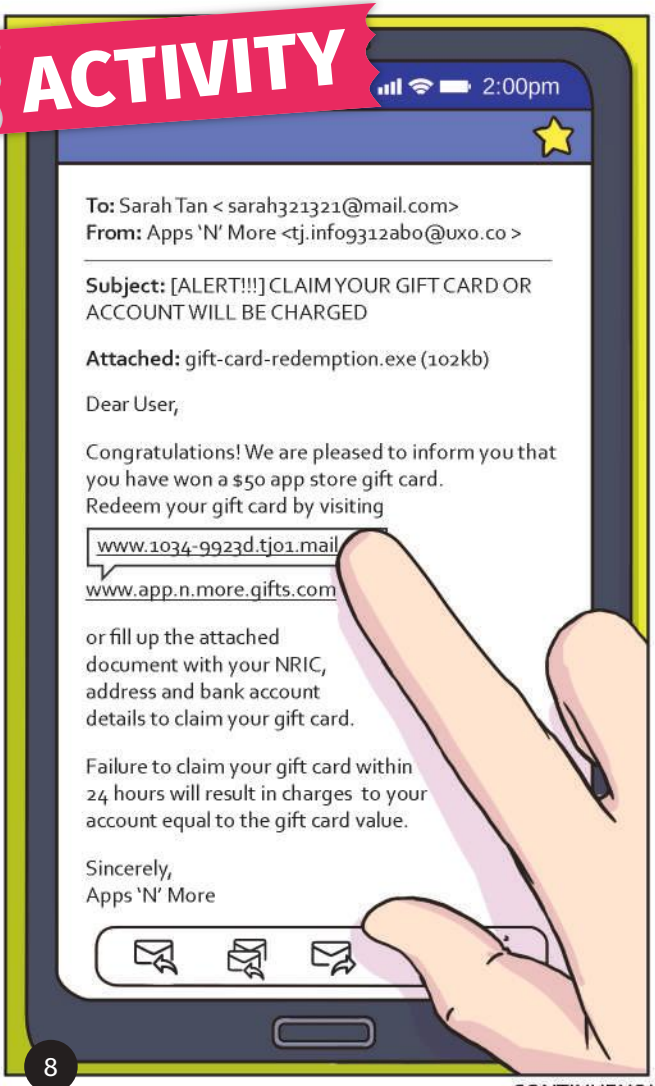

Good job, you avoided clicking on a phishing link that could have infected Brandon's device!
The promise of attractive rewards and mismatched information are two signs of phishing!
CLASH
STARS
AIDEM
Did you know there are four other signs of phishing to look out for?
Find out what they are on the next page!

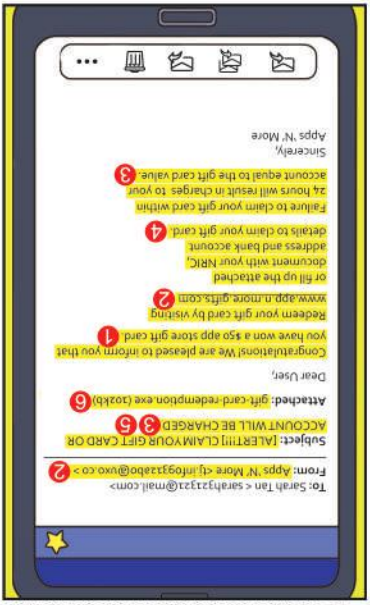
AIDEM ALERT

Six signs of a phish!

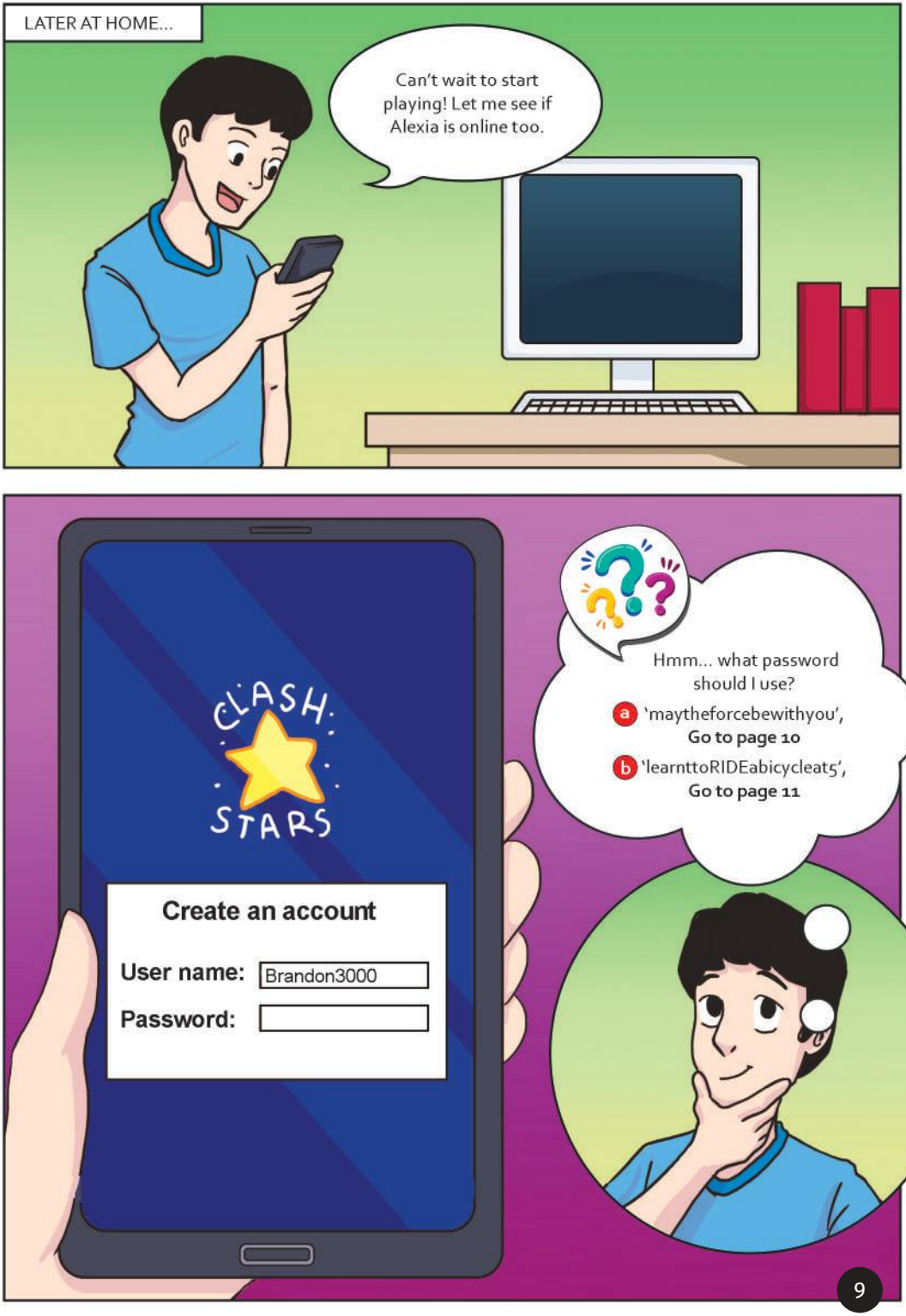
1. Promise of attractive rewards
2. Mismatched and misleading information
3. Use of urgent or threatening language
4. Requests for confidential information
5. Unexpected emails
6. Suspicious attachments

ACTIVITY





CONTINUE YOUR CYBER JOURNEY ON THE NEXT PAGE...


LATER AT HOME...
Can't wait to start playing! Let me see if Alexia is online too.
CLASH STARS
Create an account
User name: Brandon3000
Password:
Hmm... what password should I use?
a 'maytheforcebewithyou', Go to page 10
b 'learnttoRIDEabicycleat5', Go to page 11


STAR WARS
STARS
Create an account
User name: Brandon3000
Password: maytheforcebewithyou
New user 'Brandon3000'? Says here on his Clash Stars profile that he is a fan of Star Wars.
Let me guess, his password is 'may the force...'
CLASH STARS
Login Successful !
Wahaha! When users choose a password that is predictable, it makes my job so easy!
Bad choice! While the password is long (at least 12 characters), it needs to be unpredictable and random.
This means that it would be difficult for others to guess, even with password cracking tools!
CLASH STARS
In addition, remember to enable Two-Factor Authentication (2FA) for your accounts for an additional layer of security. Also, use different passwords for different accounts. Commit it to memory and don't write it down!
Hey! Why am I logged out of my account? I can't sign in anymore!
CLASH STARS Game Logout
AIDEM
Head to page 12 to learn how to create a strong password!

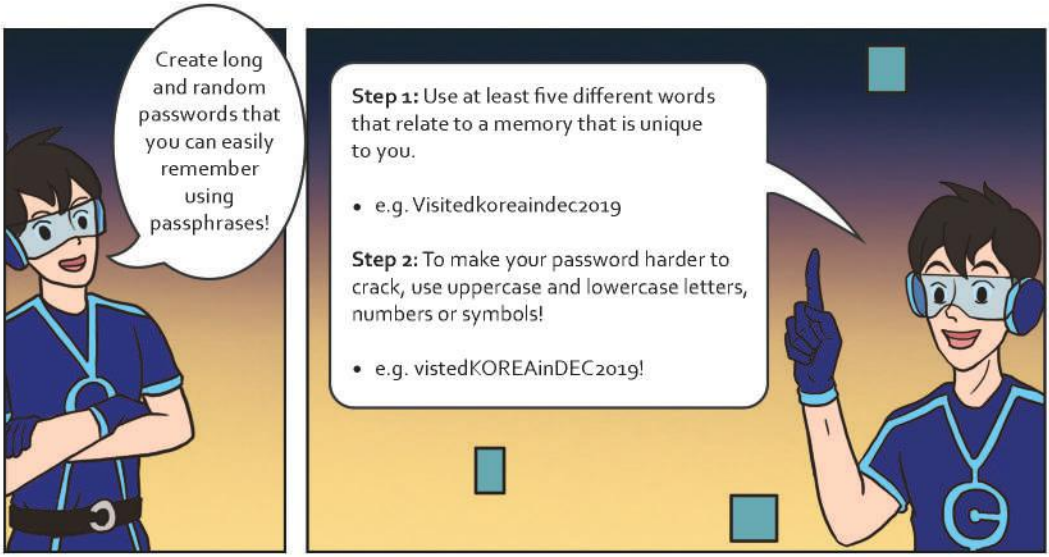

STARS
Create an account
User name:
Brandon3000
Password:
learnttoRIDEabicycleat5


New user 'Brandon3000' ? Heh heh heh! I wonder if I can guess his password...


CLASH STARS
Login Unsuccessful !
Argh! I can't hack into this account! His password is strong!


Good job! In addition to creating strong passwords, enable Two-Factor Authentication (2FA) where available.
CLASH STARS
You should also use different passwords for different accounts, and don't write it down!


Yes! Another victory!
Level up
AIDEM
Head to the next page to learn how to create a strong password, just like Brandon's!



AIDEM

TIP 1

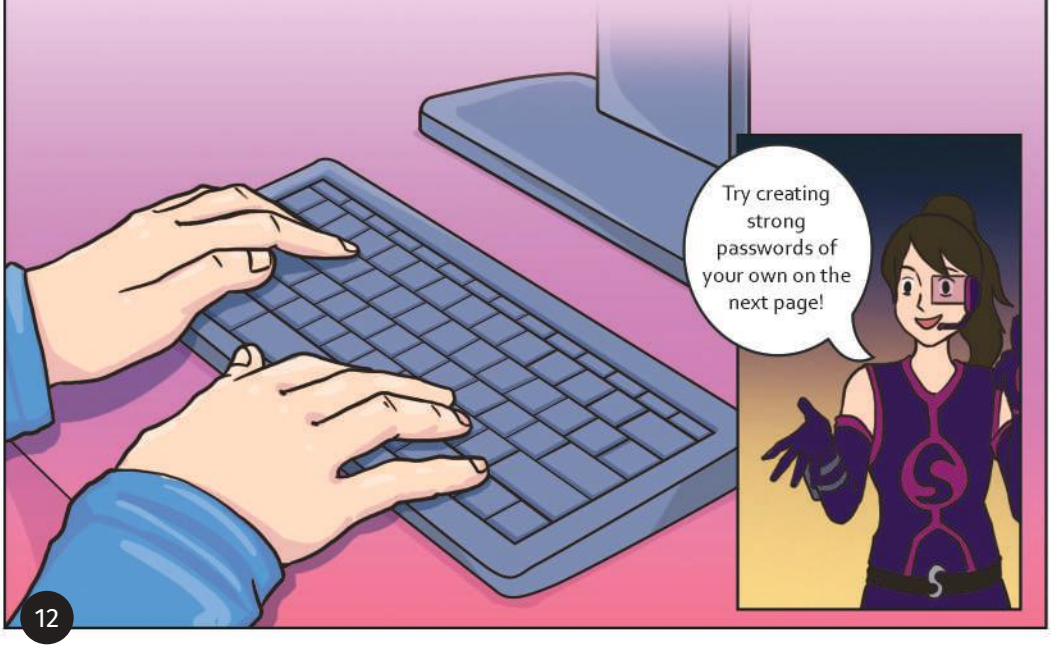
Passwords should be at least 12 characters long.

The shorter and less complex your password is, the quicker it is for cyber criminals to guess it. For example, the password '123456' can hacked in less than one second.

TIP 2

Never use personal information when creating a password.

Your name, NRIC, birthdate, or any other information that can be obtained easily, for instance by doing a search online, should never be used as your password.



ACTIVITY

Practise creating strong passwords using the suggested topics below!

	Topic	Write at least five words	Suggested passphrase
1	Food	Toast and tea at 8am	TOAST+teaAT8am
2	Holidays	Chinese New Year in Kuala Lumpur 2020	CNYinKL2020!
3	Songs	Sang 'Let It Go' 50 times	sangLETITGO!50times
4	Games	Number one player on FIFA 20	#1playeronFIFA20
5	Pets	Clean fish tank on Friday	CleanFISHTANKon#FRI

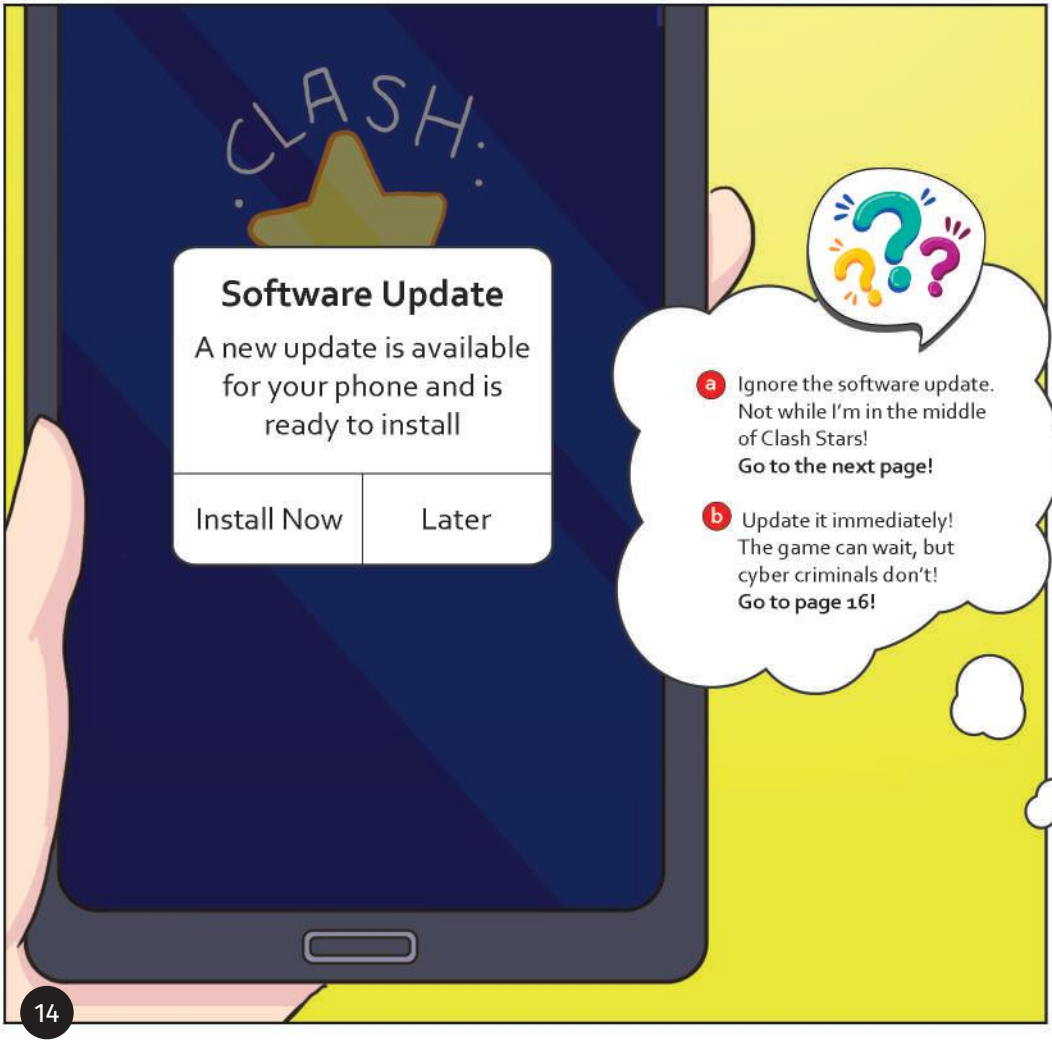
Try it out!

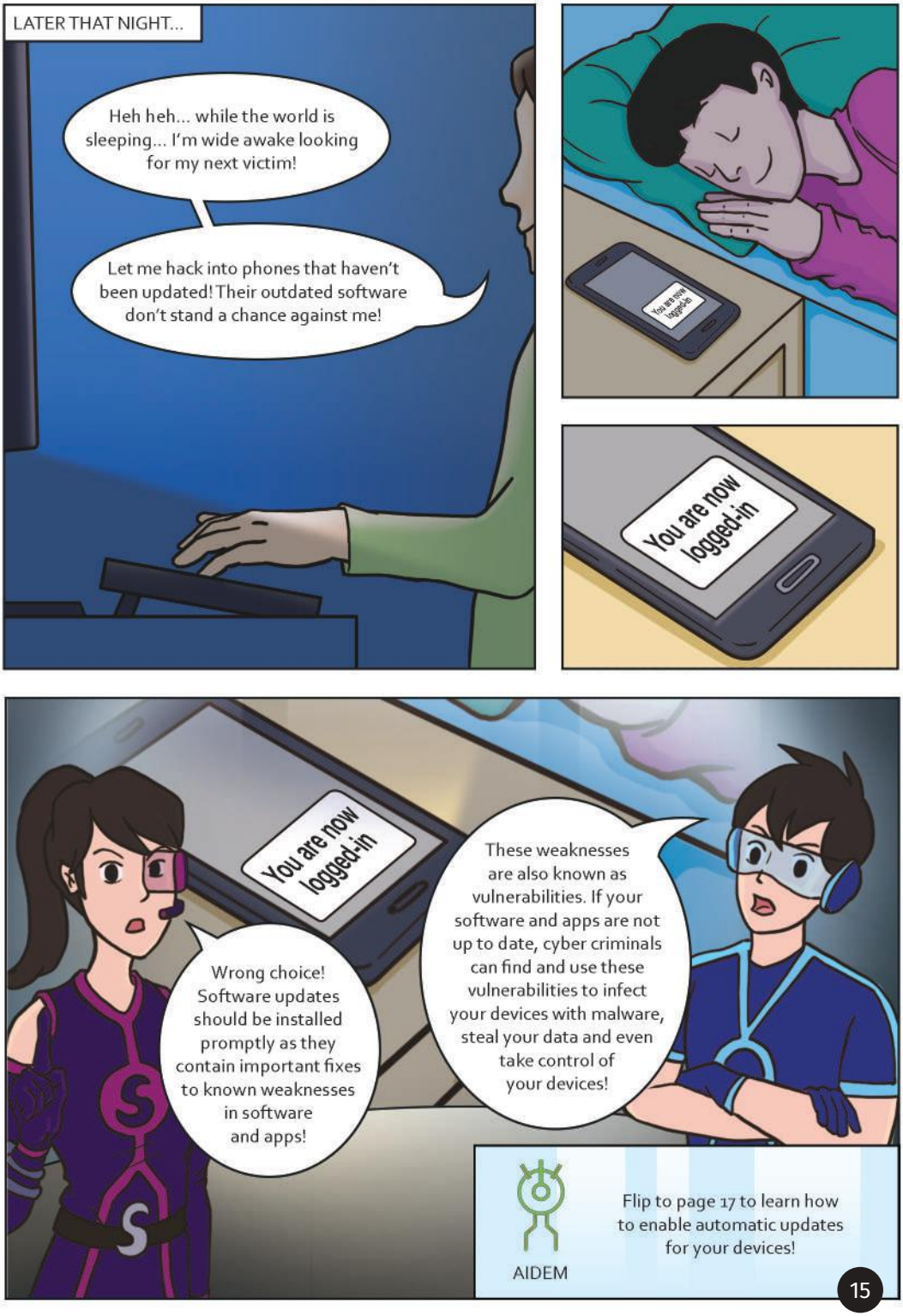
	Write at least five words	My passphrase
1		
2		
3		
4		
5		

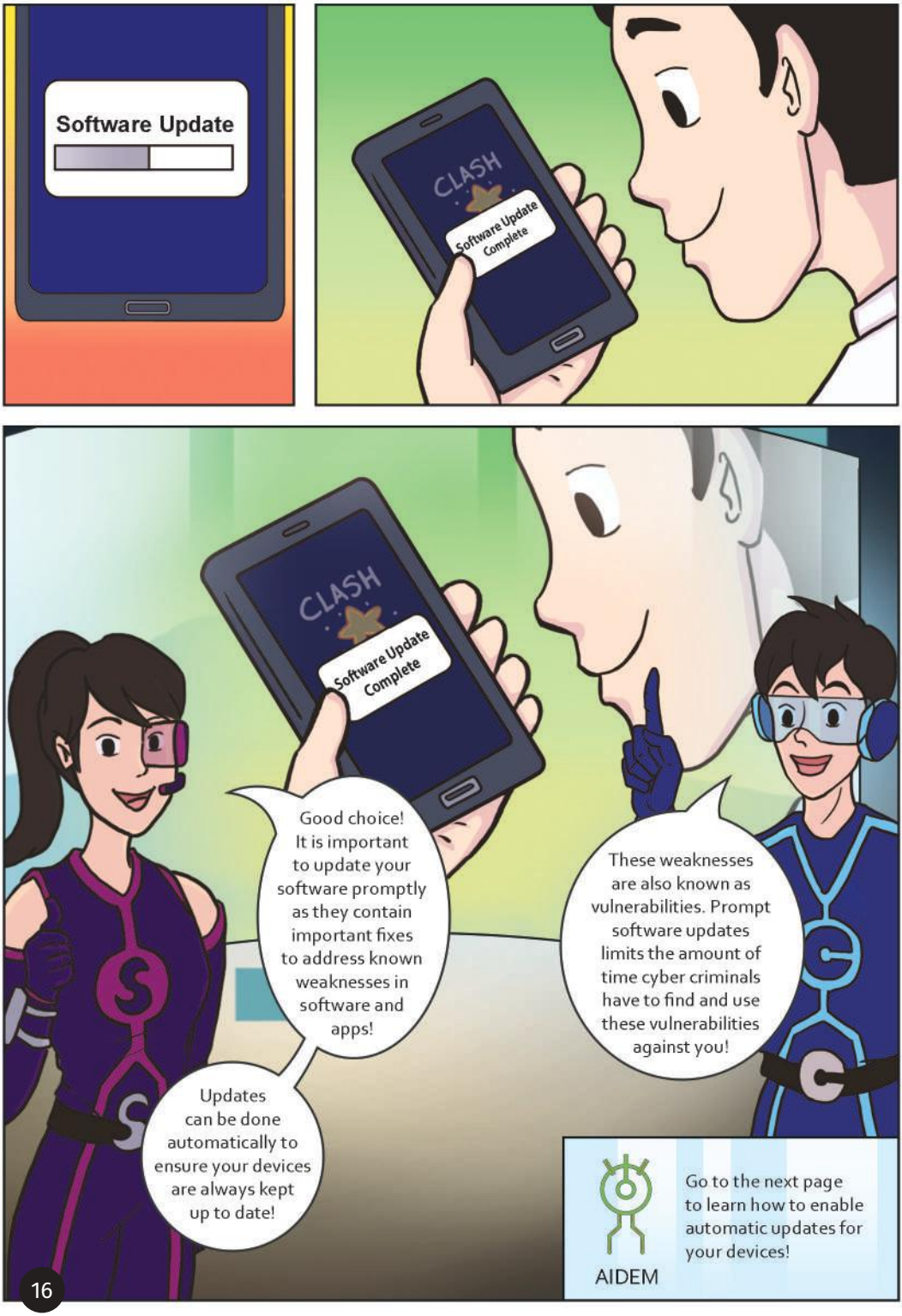
CONTINUE YOUR CYBER JOURNEY ON THE NEXT PAGE...


BACK IN SCHOOL...
One last round of Clash Stars!
Yes, let's start!


What's this?


CLASH
Software Update
A new update is available for your phone and is ready to install
Install Now
Later
a Ignore the software update. Not while I'm in the middle of Clash Stars!
Go to the next page!
b Update it immediately! The game can wait, but cyber criminals don't!
Go to page 16!

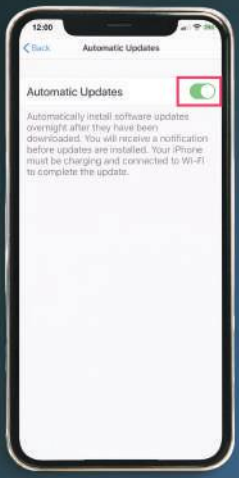

LATER THAT NIGHT...
Heh heh... while the world is sleeping... I'm wide awake looking for my next victim!
Let me hack into phones that haven't been updated! Their outdated software don't stand a chance against me!
You are now logged-in
You are now logged-in
Wrong choice! Software updates should be installed promptly as they contain important fixes to known weaknesses in software and apps!
These weaknesses are also known as vulnerabilities. If your software and apps are not up to date, cyber criminals can find and use these vulnerabilities to infect your devices with malware, steal your data and even take control of your devices!
AIDEM
Flip to page 17 to learn how to enable automatic updates for your devices!


Software Update
CLASH
Software Update Complete
CLASH
Software Update Complete
Good choice! It is important to update your software promptly as they contain important fixes to address known weaknesses in software and apps!
These weaknesses are also known as vulnerabilities. Prompt software updates limits the amount of time cyber criminals have to find and use these vulnerabilities against you!
Updates can be done automatically to ensure your devices are always kept up to date!
AIDEM
Go to the next page to learn how to enable automatic updates for your devices!

ACTIVITY:

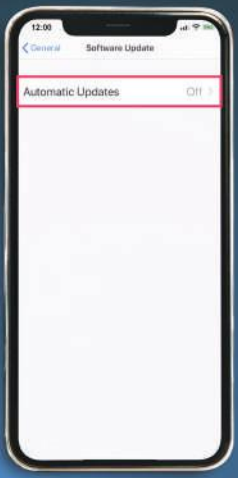
Do you know how to enable automatic software and app updates on Android and iOS devices? Indicate the correct sequence in the boxes below!

iOS Software Update

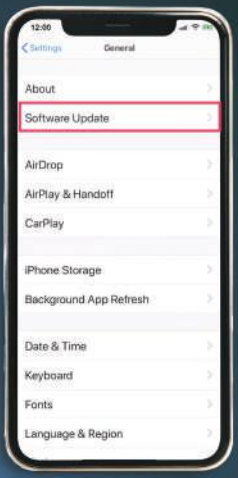


Step ⬤

Step ⬤



Step ⬤



Step ⬤

iOS App Update

Step ⬤

Step ⬤

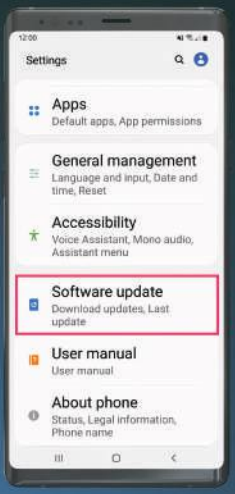
Step ⬤

Answers:
iOS Software: 4, 1, 3, 2
iOS App: 3, 2, 1

Android Software Update

Step

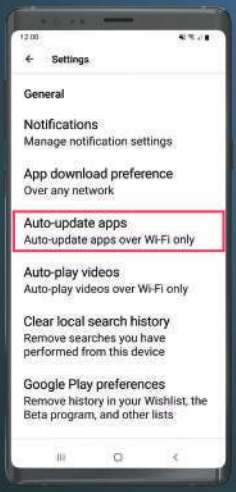
Step



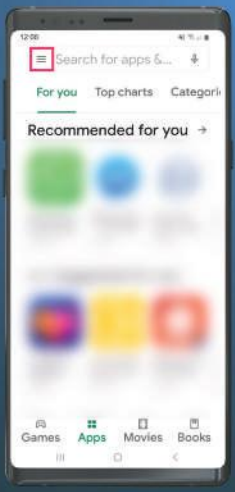
Step

Answers:
Android Software: 2, 3, 1
Android App: 3, 1, 2, 4

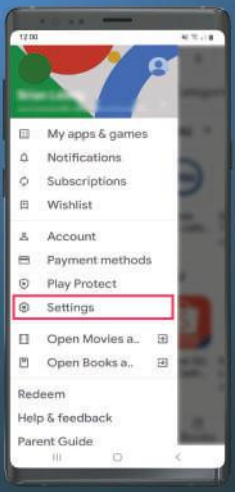
Android App Update



Step



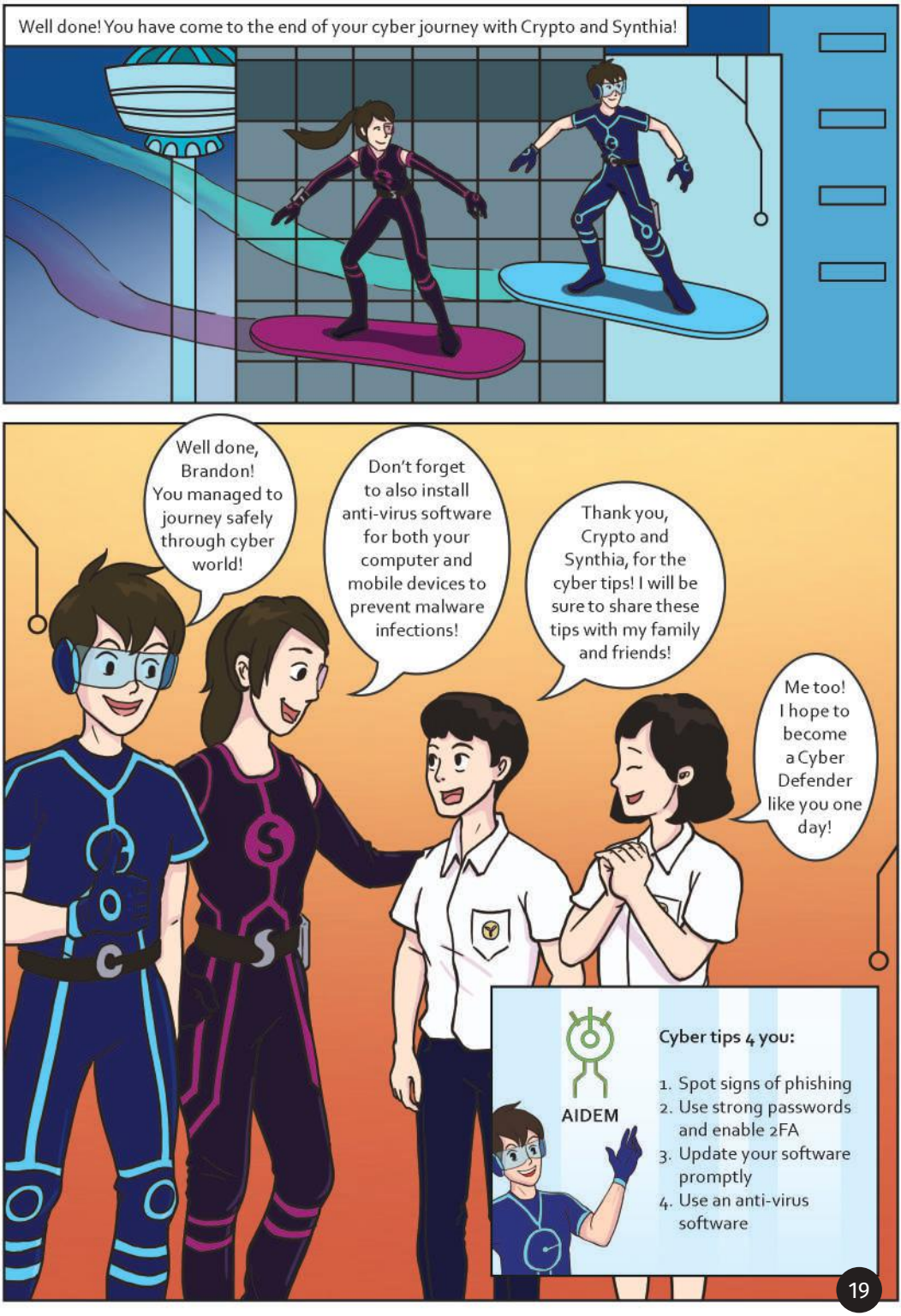
Step



Step

Step

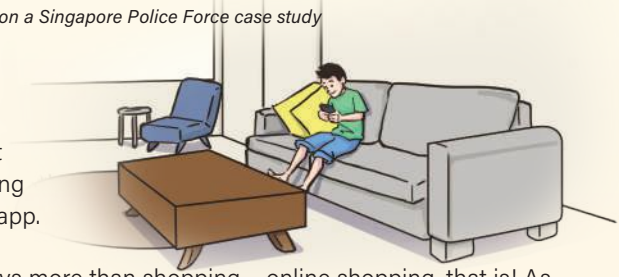
CONTINUE YOUR CYBER JOURNEY
ON THE NEXT PAGE...


Well done! You have come to the end of your cyber journey with Crypto and Synthia!
Well done, Brandon! You managed to journey safely through cyber world!
Don't forget to also install anti-virus software for both your computer and mobile devices to prevent malware infections!
Thank you, Crypto and Synthia, for the cyber tips! I will be sure to share these tips with my family and friends!
Me too! I hope to become a Cyber Defender like you one day!
AIDEM
Cyber tips 4 you:
1. Spot signs of phishing
2. Use strong passwords and enable 2FA
3. Update your software promptly
4. Use an anti-virus software

CASE STUDY: ONLINE SCAM

Based on a Singapore Police Force case study

One night



Peter (not his real name) was at his grandparents' house browsing through his favourite shopping app.

There is nothing that Peter enjoys more than shopping – online shopping, that is! As usual, Peter opened his favourite app and was soon engrossed in comparing prices, reading user reviews and searching for the best deals.

When he saw the product listing, Peter almost dropped his phone in shock.

A brand new mobile phone going for only $800!

With his interest in the latest tech devices, Peter knew it was worth more than $1,200. He had to make his move – fast!

Peter_2009

Hello, is this phone still available?

His heart was pounding with trepidation at the thought that the phone may already have been sold. Who could resist such a good deal? Thankfully, the seller, 'Bestseller78' replied almost immediately with the good news.

Bestseller78

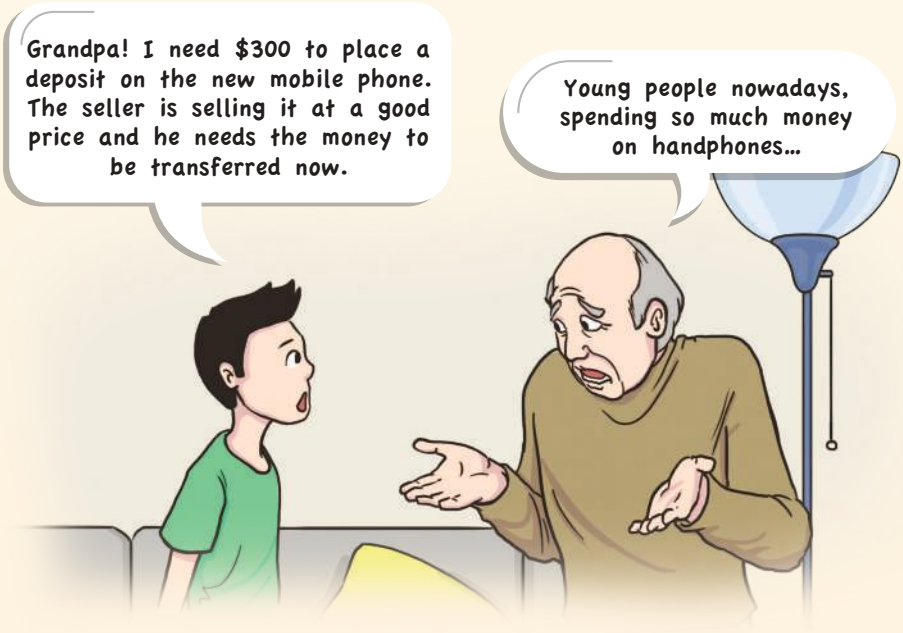
Hi, yes still available. Please make deposit to confirm the order. There are many buyers interested.

Of course! Peter knew that there had to be many others keen on this unbelievable offer. He replied without hesitation.

Peter_2009

Ok, what is your bank account number? I'll transfer the money now.

After the seller replied with his bank account details, Peter approached his grandfather for help to transfer the money.



After Grandpa made the deposit, Bestseller78 messaged Peter an hour later.

Bestseller78

I have another interested buyer. Transfer $400 to me to confirm this deal.

Peter's eyes almost popped out of his head. Sweat dripped down his brow as he clutched his phone. He couldn't let this amazing deal slip away! Taking a deep breath, he yelled, "**GRANDPA!!!**"

At first, Grandpa was hesitant to make the transfer a second time.

"**Another few hundred dollars again?**" Grandpa shook his head, then looked concerned. "**Ah boy, are you sure that this is not a scam? I just saw on the news last week that...**"

"Of course not, Grandpa!" Peter interrupted.

He just couldn't help himself. As precious seconds slipped by, Peter grew more and more worried that the phone would be snapped up by another astute buyer.

Look, I even have the seller's home address here, and a picture of his NRIC. Nothing can go wrong!

Grandpa sighed. He had a weak spot for his one-and-only grandson, and could not bear to disappoint him.

"Ok..." he muttered.

Success! Peter was over the moon. The brand new phone would soon be his!
But little did he know...

Bestseller78 had promised to hand-deliver the phone to his house at 1pm the next day. All Peter had to do was wait...

The next day...

Peter paced up and down in the living room. He was nervous. It was already 3pm and Bestseller78 was nowhere in sight.

Could it be that the seller was lost? A million possible scenarios flashed through his mind.

Just at this moment, he received a message from the seller.
Bestseller78 asked for an additional $436 for VAT and delivery insurance.
Peter ran to Grandpa and urged him to make a transfer one last time as the seller was already on his way. Afraid of disappointing his grandson, Grandpa transferred the money.

Soon after, the seller requested for a sum of money for the fourth time. At this moment, Peter started to feel something was amiss.

It didn't help that Grandpa had decided to tell his mother about the bank transfers and how the seller was requesting for yet another sum of money. Peter's mother rushed back home from work and demanded that Peter explain what happened.

"You did what?!" Mother screamed in disbelief. **"I can't believe you gave money to a stranger just like that! And not once or twice, but three times!"**

Peter tried to convince his mother that the phone will be delivered soon, and checked his phone for what felt like the hundredth time that day.

The seller's response was immediate this time. But the contents of his message had Peter boiling with rage.

Mom huffed when Peter showed her the latest message.

Mom was furious! Her eyes flashed angrily, and she grabbed her keys off the coffee table...

The victim never got his money back. When they showed up at the address provided by the offender, the victim and his mother found that no such person lived there. Instead of getting a good deal, the victim lost a total of $1,136.

Tempted by a deal that seemed too good to be true, the victim had fallen prey to an online scam.

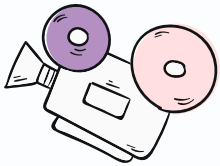
To avoid making the same mistake, here's what you can do:

- Stranger Danger! Don't believe everything you see online, as scammers can use an identification card or driver's licence that does not belong to them to gain your trust.
- Don't assume that just because the seller uses a local bank account, it is safe. The owner of the account may not be the person you are communicating with online.
- Where possible, insist to pay cash on delivery. If the seller insists that you pay in advance, use shopping platforms that only release your payment to the seller after you receive the item.
- Before performing a transaction on an online shopping site, find out how the website safeguards your interest in the event of a dispute with the seller.

For more information about combating scams, visit **scamalert.sg** or call the anti-scam helpline at **1800-722-6688**.

SCREENPLAY

Free Wi-Fi? Are you S.U.R.E ?



Act out this scene with your classmates. Find out what happens when Student K and L connect to an unsecured public Wi-Fi network and encounter a fake news article!

Character List:

Student K Student L Café staff Crypto Synthia

Scene: Two students, K and L, are in a café to complete their project work over the weekend.

Student K: I need to connect to the Internet to download a file for my project but I have exceeded the data limit for my mobile phone. Let me check with the café staff if I can tap on their free Wi-Fi...

Student K to café staff: Hey! Can I have your Wi-Fi network name and password please?

Café staff: I'm sorry but we do not have a Wi-Fi network here... you will have to use your mobile data.

Student K speaks to Student L: How can that be? I'm sure every café has Wi-Fi.

Student K: A-ha! I found a Wi-Fi network and it isn't password protected. Let's connect to it!

Student L: Great! I will connect to it too and login to my Facebook account before getting started on my project.

Student L to Student K: Wow, did you read about this? All schools in Singapore will be closed for a week due to the haze!

Student K: Are you serious? Share the good news with our classmates immediately!

Scene: Enter café staff, who happens to be cleaning the table beside them, and overhears their conversation.

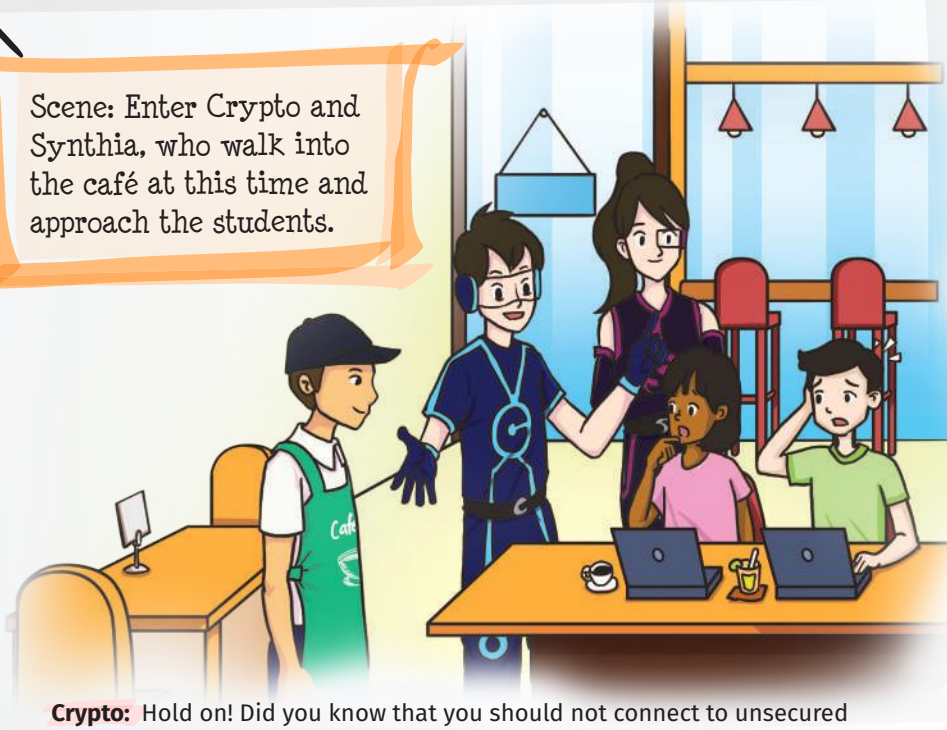
Café staff: Are you sure? Did you check with your teacher if this is true?

Student L: Of course it is true! I saw this on my friend's Facebook post.

Student K: Why should we listen to you anyway? You lied about your Wi-Fi network.

Café staff: What do you mean? We really don't have a Wi-Fi network here!

Scene: Enter Crypto and Synthia, who walk into the café at this time and approach the students.



Crypto: Hold on! Did you know that you should not connect to unsecured Wi-Fi networks? Your personal information such as your account login details could be stolen by cyber criminals!

Synthia: Cyber criminals can eavesdrop on what you are browsing, and steal sensitive information such as your usernames and passwords!

Student K: Oh no, I didn't know that it could be so serious!

Crypto: You should also avoid spreading fake news. The article you came across is fake!

Student L: But how do I know whether it is fake?

Synthia: Always be **S.U.R.E.** before sharing news articles. Firstly, look at the 'Source', is it trustworthy? You must ensure that the source of information is credible and reliable.

Crypto: Secondly, do you 'Understand' what you're reading? Search for clarity and look for facts rather than opinions.

Synthia: Thirdly, always do your 'Research'! Do not rely on one source. Always investigate thoroughly before making a conclusion by checking and comparing the information with multiple reliable sources.

Crypto: And finally, 'Evaluate' the article and exercise fair judgement. Look at the article from different angles. There are at least two sides to every story.

Student L: I'm sorry, I didn't mean to spread fake news. What should I do now?

Crypto: You should delete your post and inform your friends that the article is fake!

Student K: What about our online accounts? Is it safe?

Synthia: You should change your passwords for your accounts immediately. Always remember that nothing is private on unsecured public Wi-Fi networks. You should only use it for general Internet surfing.

Crypto: Remember, we need to guard against threats online. As part of Digital Defence, we must be secure, alert and responsible online!

Café staff: Thanks for saving the day, Crypto and Synthia! Let's take a photo together to remember this eventful day and we can safely share this photo on Facebook!

In support of

Brought to you by

In partnership with

Special thanks to the Ministry of Education and National Library Board

Copyright 2020 All Rights Reserved