

# CYBER SAFETY

STAYING SECURE IN THE DIGITAL WORLD

AN  
INTERACTIVE  
GUIDE



# *Introduction to the Cyber Safety Interactive Handbook*

The digital world is an exciting place where we can explore, learn and communicate with our friends! However, it is also important to learn to be safe in the digital world and not listen to strangers online.

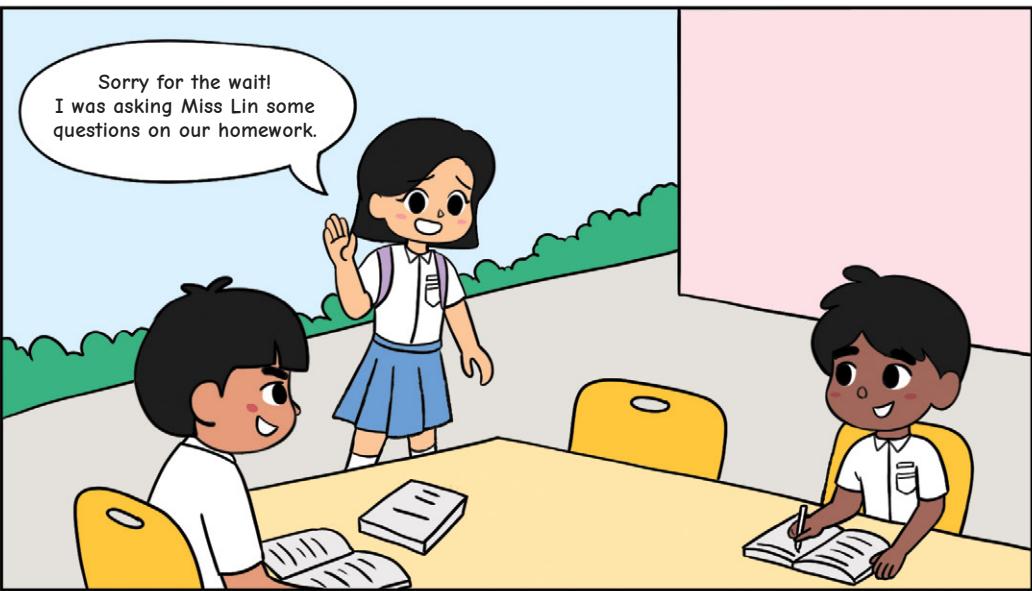
Join Dinesh, Fauzi and Kai Qi as they explore cyberspace with the help of the cyber defenders, Crypto and Synthia. Are you ready to discover more about how you can stay safe online?

**Let's get started!**

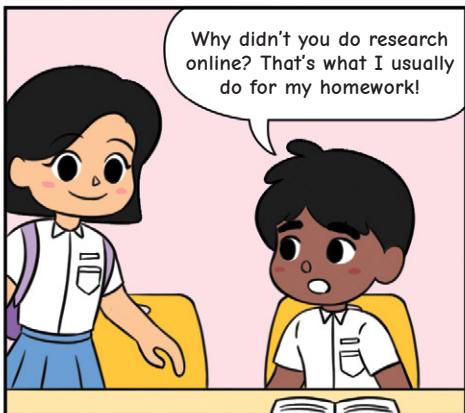
# *Contents*

● <b>Living in the Digital World .....</b>	04
Activity 1: Identify the Personal Information.....	07
● <b>Dangers in the Digital World.....</b>	09
Activity 2: Set a Strong Password.....	13
Activity 3: Spot Signs of Phishing.....	15
Activity 4: Avoid the Deepfakes.....	21
● <b>Steps to Stay Safe Online .....</b>	22
Case Scenario 1: The Online Stranger.....	23
Case Scenario 2: The Unknown Website.....	25
● <b>Conclusion: Final Tips &amp; Answer Key .....</b>	27

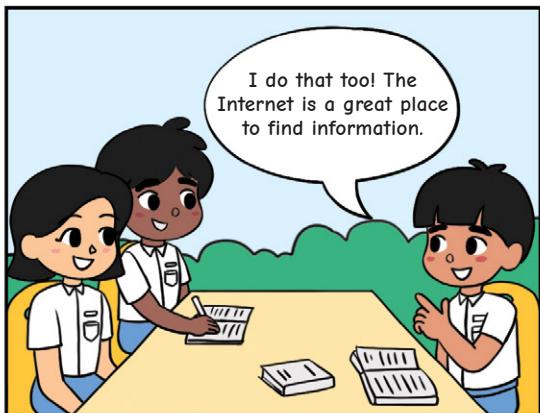
Sorry for the wait!  
I was asking Miss Lin some  
questions on our homework.



Why didn't you do research  
online? That's what I usually  
do for my homework!



I do that too! The  
Internet is a great place  
to find information.



There are so many possibilities  
with the Internet. You can...



... do research for  
your homework...



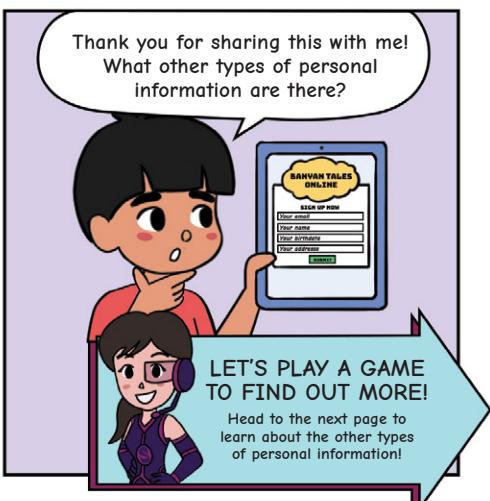
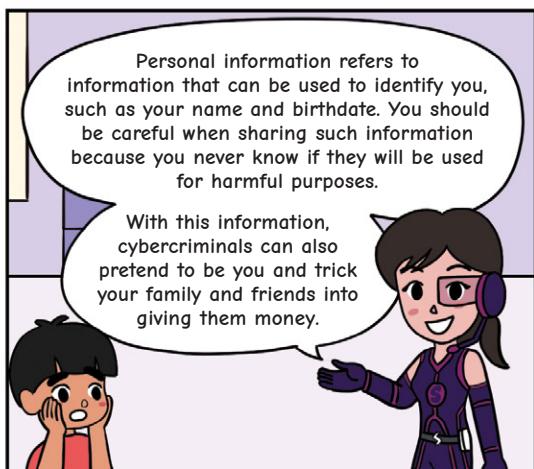
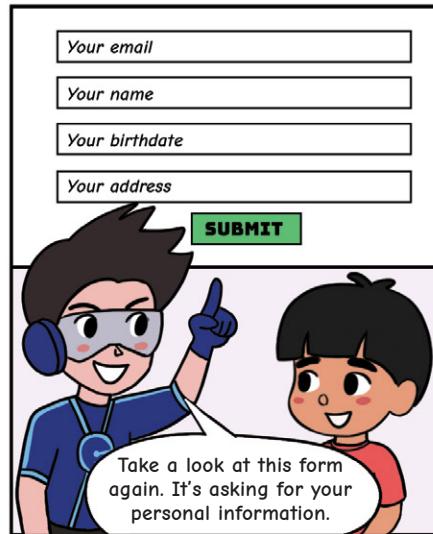
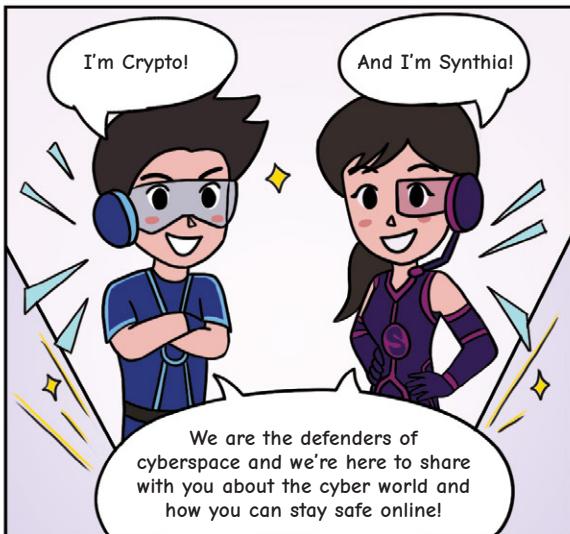
... watch videos  
and movies...



... or play  
online games!





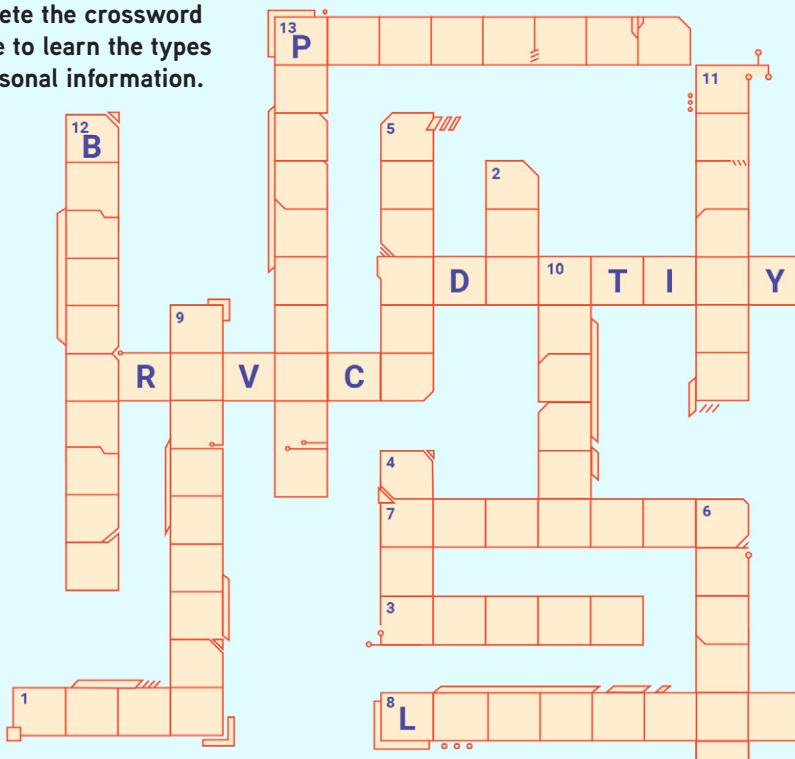


# ACTIVITY 1



Head to page 27  
for the answers!

Using the clues below,  
**complete the crossword  
puzzle to learn the types  
of personal information.**



## Across:

- 1 – You say this when you introduce yourself.
  - 3 – An electronic message you send to someone's inbox.
  - 7 – This information tells you where a person lives.
  - 8 – The place where something or someone is.
  - 13 – What you use to access your computer and/or online accounts.
- 2 – This number shows how old you are.
  - 4 – Regardless of \_\_\_\_, language, or religion.
  - 5 – The people you live with and love.
  - 6 – The place where you learn new knowledge from teachers and classmates.
  - 9 – The day, month and year when you were born.
  - 10 – When you call someone, you need their phone \_\_\_\_.
  - 11 – A land where people live together.
  - 12 – Where you were born.
  - 13 – A picture taken with a camera.

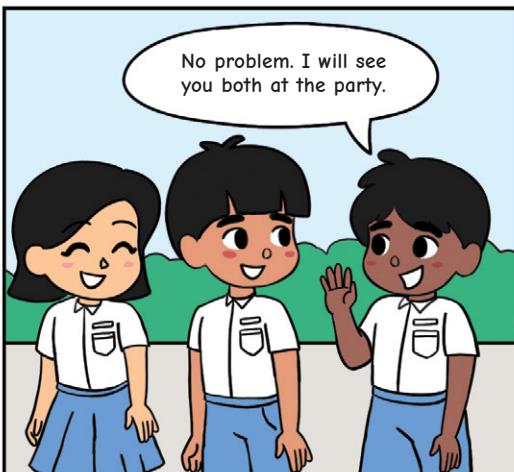
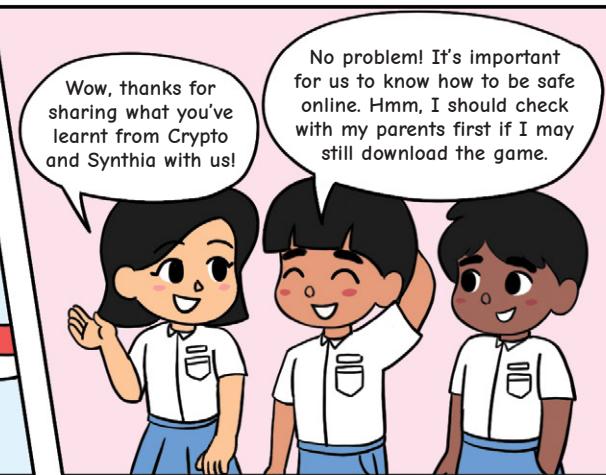


**Remember, it is important to keep your personal information safe as this protects your \_D\_ \_T\_I\_Y and \_R\_V\_C\_.**

Now that you know what personal information is, we hope that you will be more careful about what you share on the Internet!

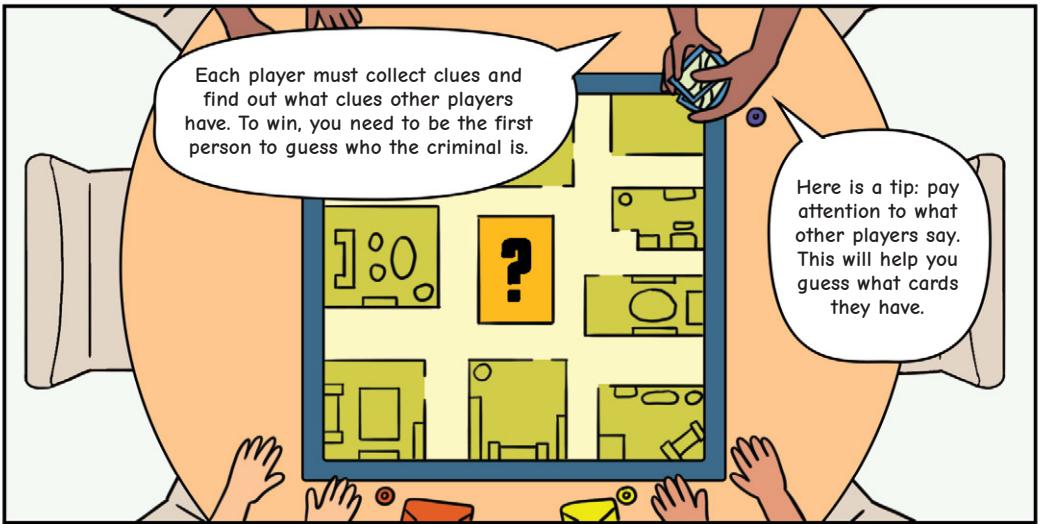
Thanks, Crypto and Synthia. I'll be sure to share what I've learnt with my friends.

You are welcome, Fauzi. Bye!



At Dinesh's house...





Each player must collect clues and find out what clues other players have. To win, you need to be the first person to guess who the criminal is.

Here is a tip: pay attention to what other players say. This will help you guess what cards they have.



This is going to be so fun.  
Let's start!



After a few rounds of the game...

I win.

Ugh, not again!



Wow, you are really good at this game!

Yes! How do you always know the answers so quickly?



Hmm... I guess it gets easier to find the clues if you know where to look.

You can also guess what the other players are thinking based on their questions and actions.

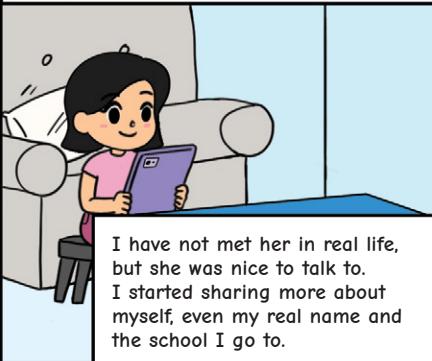
Hmm, speaking of spotting clues, this reminds me of a conversation that I had with an online friend. It made me wonder if she was really who she claimed to be.



Which online friend is this?



During the June holidays, I met a girl through an online game. She said that she was one year older than me and we had many things in common, such as our favourite songs and cartoons.



I have not met her in real life, but she was nice to talk to. I started sharing more about myself, even my real name and the school I go to.

But after a while, I started to notice that she would say things that didn't match what she said previously. Once, she even forgot her own username!

**SilverArc3**

Oh, your birthday is coming soon? Mine too! I cannot wait to find out what my birthday cake will look like. Last year, I had a white birthday cake with the number 12 written in bright pink icing.

That is weird. Last month, she told me that she was 10 years old...

She also kept asking me to share my personal information, such as my birthdate and account password!

**SilverArc3**

By the way, when is your birthday?

**Kai1806**

18 June, why?

**SilverArc3**

I have a present for you. If you give me your password, I'll leave it in your character's bag on your birthday! :)

**Kai1806**

Is there another way you can transfer the present to me?

**SilverArc3**

The item is very precious and I don't want you to lose it! I think it's better if I log in to your account to put it in your character's bag.

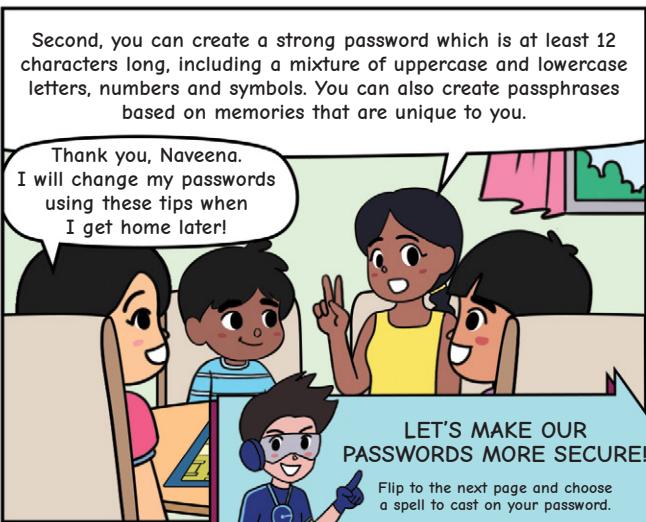
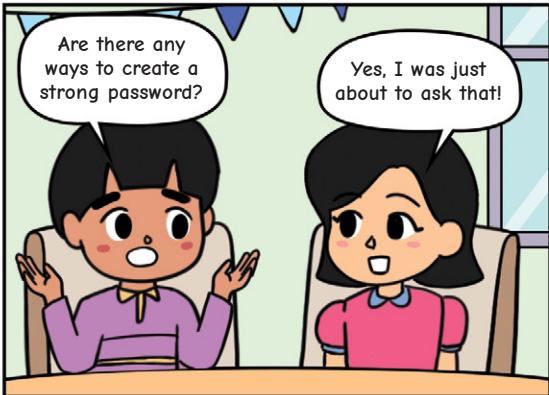
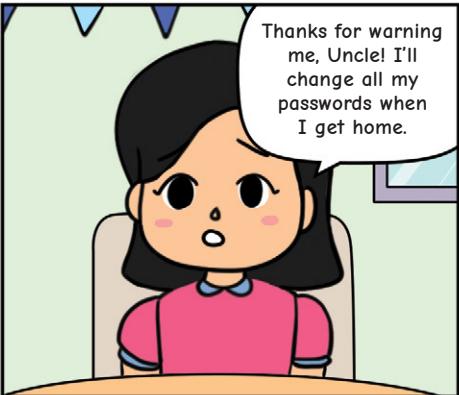
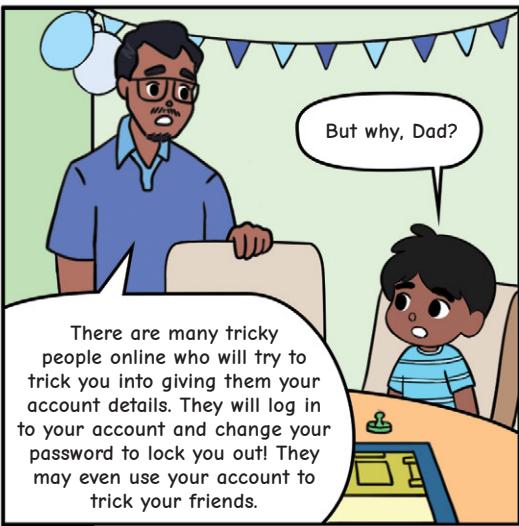
What did you do?



I remembered that our teacher said we should avoid talking to strangers online as we do not know their intentions. When I started to find her requests weird, I blocked her.

Kai Qi, I could not help but listen to your story. I am glad that you stopped talking to her, but you should be more careful in future.





## ACTIVITY 2



Passphrases are passwords made up of a string of words. A strong passphrase is one that is easy for you to remember, but difficult for cybercriminals to guess. However, you should avoid using common words or patterns as these are both easy to remember and guess.

There are a few methods to create a strong password. Take a look at the spell cards below and **cast the right spell to make your password more secure.**

**CHARACTER WIZARD**

Use a combination of letters, numbers and symbols to make your passphrase more unique.

**GO TO PAGE 14**

**PERSONAL DETAILS**

Use personal information such as your name, birthdate or your pet's name to make your passphrase easier to remember.

**GO TO TIP 1 ON PAGE 27**

Later at Kai Qi's home...

Have you completed your chores?

Yup!

Okay, you can use the tablet for 30 minutes.

**CHANGE YOUR  
PASSWORD**

YOUR OLD PASSWORD  
kaiqi1234

YOUR NEW PASSWORD  
Spark1e@mer360!  
**SUBMIT**

Hmm, what is this? I won a phone? I don't remember signing up for any giveaway...

**YOUR PASSWORD HAS BEEN  
CHANGED SUCCESSFULLY!**

We will send you a confirmation email shortly.

New email alert  
**Banyan Tales ONLINE**  
Hello, Congratulations on winning...

So, I just click here and submit my contact details? This is great!

From: Banyan Tales ONLINE GIVEAWAY  
<BanyanTalesOnline@onlineemail.com>  
Sent: Tuesday, January 27, 2025 11:43 AM  
Subject: Winner of Encode Phone Giveaway  
Attached: Terms&Conditions.exe

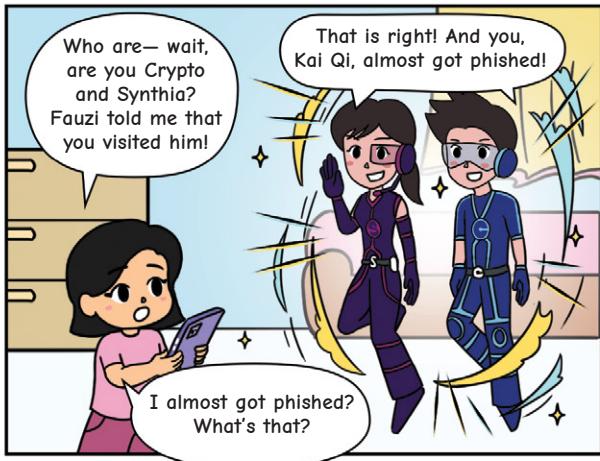
Hello,  
Congratulations on winning a brand new Encode Phone!  
Submit your details and claim your prize!

**CLICK HERE**

If you do not respond within 24 hours, your prize will be given to another winner.

Regards,  
Banyan Tales ONLINE

Stop!



Phishing is when cybercriminals pretend to be trustworthy individuals or organisations to trick you into providing personal information or giving them access to your accounts. Let us take a closer look at that email.

## ACTIVITY 3

**From:** Banyan Tales ONLINE GIVEAWAY  
**<BanyanTalesOnline@onlinemail.com>** ①

**Sent:** Tuesday, January 21, 2025 11:43 AM

**Subject:** Winner of Encode Phone Giveaway ②

**Attached:** Terms&Conditions.exe ③

Hello,  
**Congratulations on winning a brand new Encode Phone!** ④

**Submit your details and claim your prize!**

**CLICK HERE** ⑤

If you do not respond within 24 hours, your prize will be given to another winner. ⑥

Regards,  
 Banyan Tales ONLINE

This email looks suspicious. Can you spot the signs of phishing? Try matching the highlighted parts of the email to the six signs of phishing.

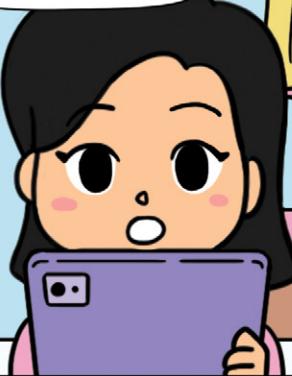


### Signs of Phishing

- A. Use of urgent or threatening language
- B. Promises of attractive rewards
- C. Requests for personal information
- D. Unexpected emails or messages
- E. Suspicious attachments
- F. Mismatched and misleading information

Head to page 27 for the answers!

But why would Banyan Tales ONLINE try to trick me?



Similar to fishing, cybercriminals use a bait to trick victims into doing something. In this situation, a cybercriminal is pretending to be Banyan Tales ONLINE to trick you.



When you believe that an email is from an official source, you are more likely to do what the email asks you to do, such as clicking on links or giving away your personal information.

From: Banyan Tales ONLINE GIVEAWAY <BanyanTalesOnline@onlinemail.com>  
Sent: Tuesday, January 21, 2025 11:43 AM  
Subject: Winner of Encode Phone Giveaway  
Attached: Terms&Conditions.exe

Hello,  
Congratulations on winning a brand new Encode Phone!  
Submit your details and claim your prize!

[CLICK HERE](#)

If you do not respond within 24 hours, your prize will be given to another winner.

Regards,  
Banyan Tales ONLINE



Once they have your personal information, they can use it to steal your accounts, or even your identity!



Oh no! Thank you so much for warning me! I shall delete this email right now.



Glad that you learnt something about phishing!

Remember to stay vigilant!

Goodbye!



At Cyber Safety HQ...

It has been a while since the last time we warned the students about the dangers in the digital world.

That is true! They seem to be more careful now!



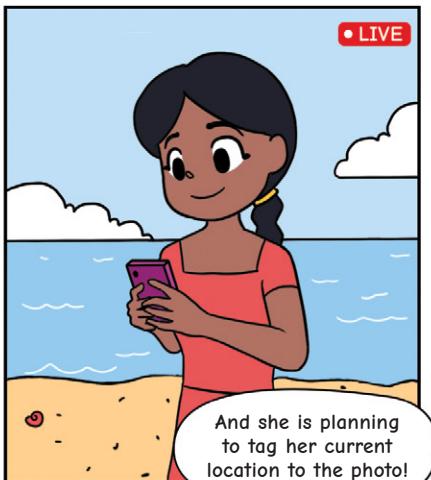
What is going on?

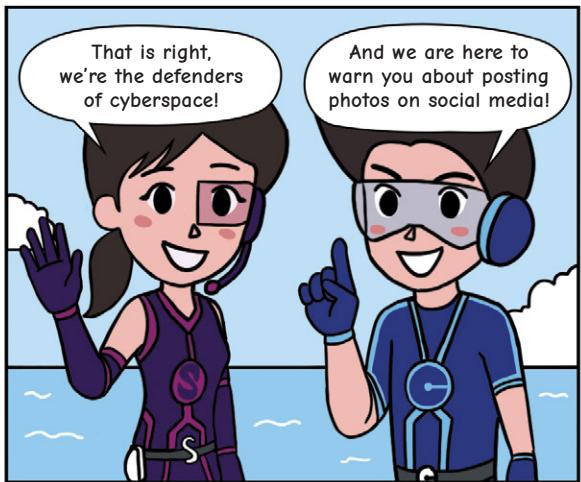
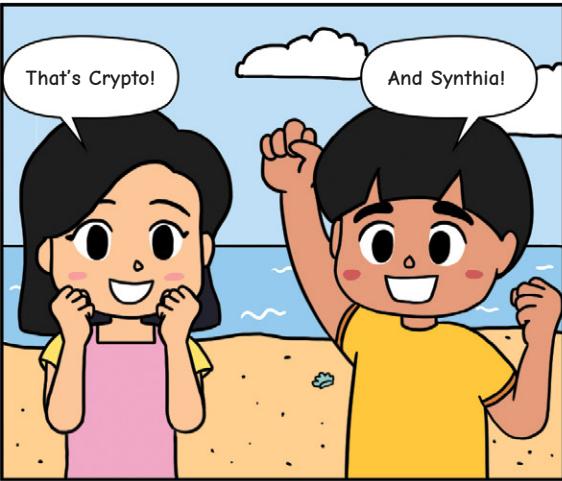
It appears that Naveena is planning to post a photo of them on social media!

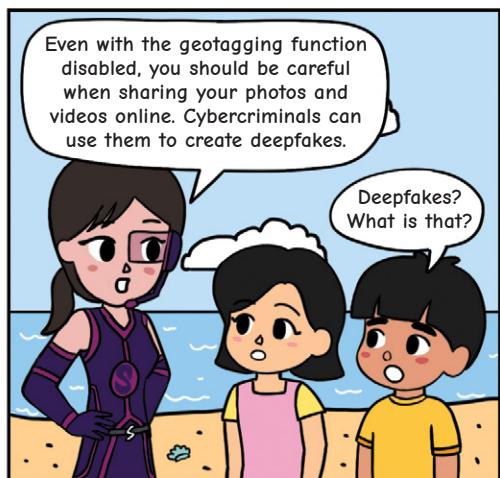
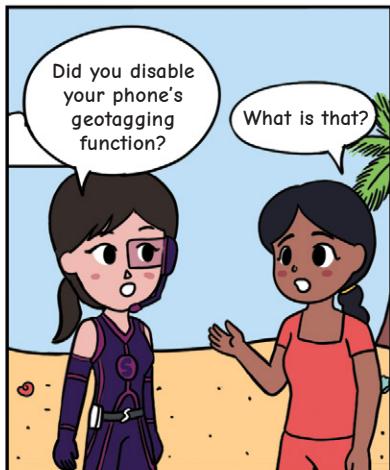
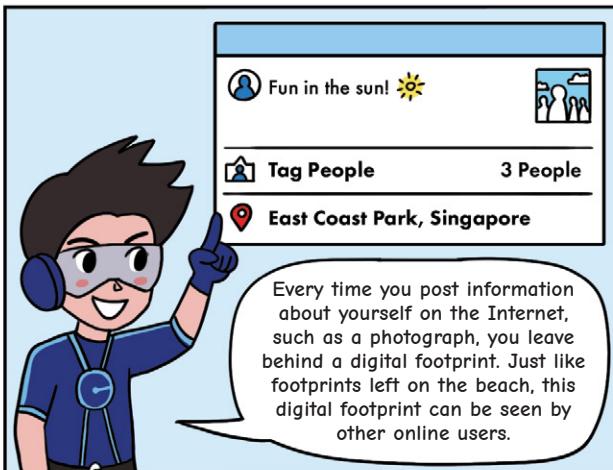


And she is planning to tag her current location to the photo!

Oh no, we've got to warn her!







Deepfakes are fake voice messages, photos or videos that are created using smart computer systems. Cybercriminals can edit real photos and videos to make them look and sound as if they are from the actual person.



Original Video



Deepfake

Cybercriminals can use deepfakes to trick people into believing fake news, giving away their personal information or even their money.



Yes! Always be careful if the person in the audio or video is saying something strange, or is trying to get you to share your personal information. You should not share your personal information with strangers online.



And if the person in the video is telling you to do something urgent or suspicious, such as downloading an app or clicking on an unknown link, always ask a trusted adult for help.



THE DIGITAL WORLD CAN BE DANGEROUS BECAUSE OF ONLINE DANGERS SUCH AS DEEPFAKES.

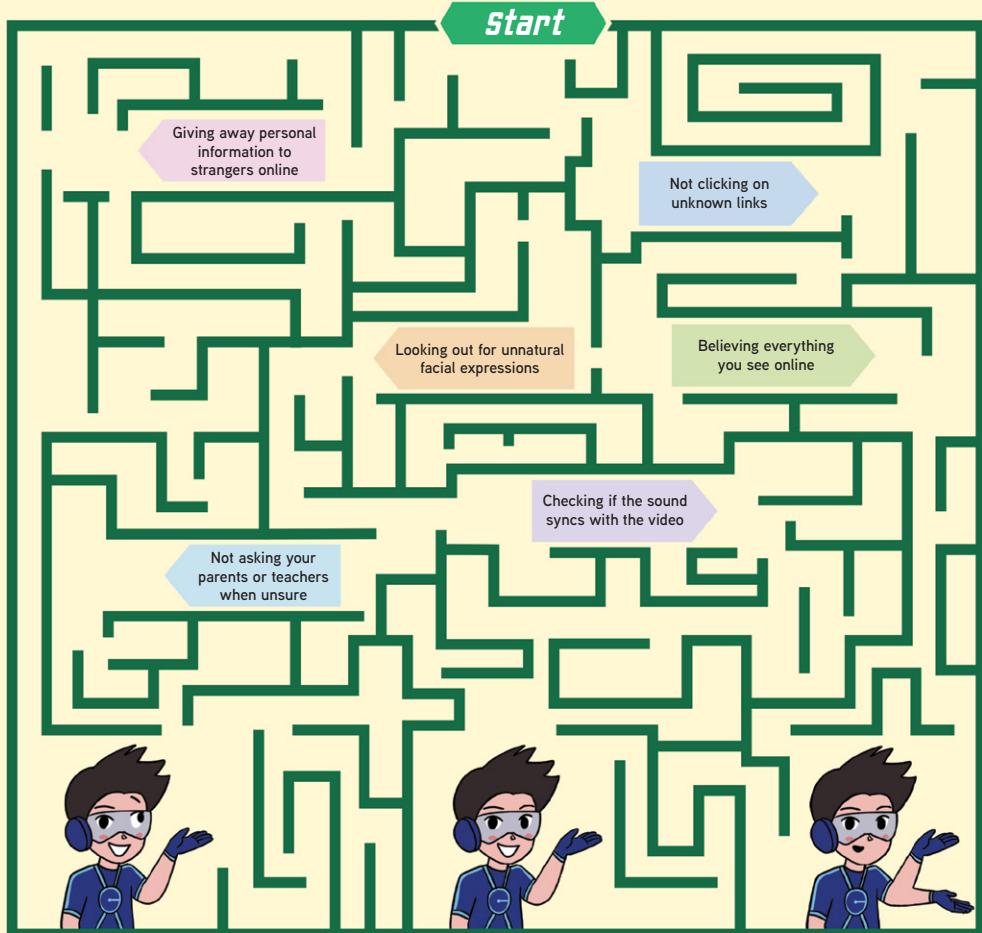
Try the activity in the next page and find your way out of the maze by avoiding online dangers to stay cyber safe!

# ACTIVITY 4



Escape the maze and find the real Crypto by following the path with the correct cyber tips! Watch out for the other two versions of Crypto, which are deepfakes created by cybercriminals.

Hint: Some of these tips have been shared by Crypto and Synthia



Do not believe everything that you see online! If the content looks suspicious, check with a trusted adult. Do not talk to strangers online and do not share your personal information!

Head to page 27 for the answers!

## Steps to Stay

# CYBER SAFE

Now that you have read about the dangers in the online world, let us take a moment to recap the cyber tips highlighted in the story.



Avoid sharing your personal information online.



Avoid talking to strangers online and do not meet them in person.



Do not click on unknown links that tell you to download apps or share your personal information.



Seek advice from a trusted adult when you are unsure.



Disable the geotagging function when taking photos or videos.



Be wary of deepfakes and do not believe everything that you see online!

In the next few pages, you will find two scenarios about people who did not practise the steps to stay cyber safe. As you read the stories, try to spot the mistakes made by the victims and reflect on what you can do to avoid making the same mistakes.

## CASE SCENARIO #1

# DANGERS in the Digital World

Shaun was at home. After completing his homework, he logged in to his favourite online game, Banyan Tales ONLINE.

Just then, one of his online friends logged in.



**W4RR10R:** I didn't see you online during the limited time event. Did you get the luminous blade?

**Shaun03:** No 😞 I was doing my homework.

**W4RR10R:** 😞

**W4RR10R:** There is another way to get it.

**Shaun03:** How?

**W4RR10R:** There is a secret area. You need to defeat the monsters there to get the luminous blade.

**Shaun03:** Why haven't I heard about this before?

**W4RR10R:** There is a problem with that place.

**Shaun03:** ???

**W4RR10R:** Anyone who goes there will lose all items in their inventory in exchange for the luminous blade. A lot of players got upset and stopped telling others about the secret area. That is why nobody talks about it.

**Shaun03:** Then there is no point going.

**W4RR10R:** Not true. I can hold your items for you. You can take them back when you're done.

**Shaun03:** Really? You are the best!

|





Determined to get the luminous blade, Shaun transferred all his in-game items to W4RR10R and set off to the secret area. He searched high and low but he could not find the place. Finally, he approached a group of players for directions.

**BlueMage82:** I have never heard of that place before.

**Shaun03:** It is the place where you can get the luminous blade!

**BlueMage82:** I have been playing this game since it was first released, but I have no idea what you are talking about.

**Shaun03:** Let me try asking my friend...

**Shaun03 » W4RR10R:** Hey, I can't find the place. Could you come here and show me where it is?

[Game Notice: You are unable to message user W4RR10R]

**Shaun03:** This is strange! I can't seem to message my friend anymore.

**LuckyStarz:** Sounds like he blocked you. What is his username?

**Shaun03:** W4RR10R

**LuckyStarz:** Oh no, I heard that he is a tricky person! He tricked many players into giving their items away!

|



That was when Shaun found out that his new “friend” had scammed him. After that experience, he became more careful about befriending online strangers.

### What can you do to avoid making the same mistake as Shaun?

- Do not listen to strangers. If something seems too good to be true, it probably is.
- If someone asks you to make a decision that seems urgent, be careful and do not act immediately. Check with a trusted adult before taking any action.



## CASE SCENARIO #2

### BEWARE of Unknown Websites and Apps



Natasha has been looking forward to watching the latest blockbuster movie. However, it was only available on a paid streaming service that her family does not subscribe to.

When her classmates talked about the movie, Natasha realised she was the only one who had not watched it. Feeling left out, she decided to find a way to watch it for free.

When she was at home, she searched for the movie on the Internet. She found a link to download the movie on a free movie website.



After clicking on the link to download, she was prompted to install an app from an unknown website.



After following the instructions on the website to install the app, Natasha was prompted to sign up for an account and fill in her personal details such as her name, birthdate and address.



Natasha was reminded of her teacher's warning about cybercriminals being on the lookout to trick people into giving away their personal information. If something seems too good to be true, it probably is.

Natasha decided to delete the app and inform her parents. Her parents reminded her to seek their permission before downloading mobile apps and they installed an anti-virus app, which can protect the tablet from malware. She promised to be more careful in future.



### DID YOU KNOW?

**Apps that are downloaded from unknown sources can be dangerous, as they may contain malware.**

Malware, or malicious software, is a program created by cybercriminals to harm a device. Cybercriminals can use malware to gain access to your online accounts, then use your account to send false messages to trick your family and friends into believing them!



### What can you do to avoid making the same mistake as Natasha?

- Be careful when clicking on unknown links. If unsure, check with a trusted adult.
- Only download apps from official app stores, such as Google Play Store and Apple App Store.

# Final Tips Before You Go

## Tip 1: Use Strong Passwords

Setting a password with uppercase and lowercase letters, numbers and symbols will make it harder for cybercriminals to guess. Do not use personal information such as your name and birthdate in your password.



Learnt how to set a strong password?  
Continue on your cyber journey on **page 14**.

## Tip 2: Spot Signs of Phishing

Look out for these six signs:

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

### Remember: Be wary of deepfakes too!

If you are unsure if a photo or video is real, ask a trusted adult for help.  
Do not share your personal information with strangers online.

## Tip 3: Use Anti-virus Apps

Use an anti-virus app to keep your device safe from harmful apps, viruses and phishing messages.

## Tip 4: Install Software Updates Promptly

Install software updates to protect your devices from harmful content.

## Answer Key

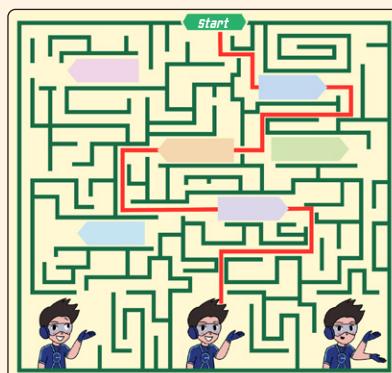
### Activity 1:

- Down:  
2 - Age  
4 - Race  
5 - Family  
6 - School  
9 - Birthdate  
10 - Number  
11 - Country  
12 - Birthplace  
13 - Photograph

- Across:  
1 - Name  
3 - Email  
7 - Address  
8 - Location  
13 - Password

 Identity, Privacy

### Activity 4:



### Activity 3:

A-6, B-4, C-5, D-2, E-3, F-1



In support of



Brought to you by



Cyber Security Agency of Singapore

Special thanks to the Ministry of Education