National Cyber Security Centre
a part of GCHQ

internet matters.org

Story 3: Trojan Tales

a CyberSprinters adventure story

Press here to continue

CYBER SPRINTERS

Kids

Trojan Tales is the 3rd story in the CyberSprinters series - so get ready for another cyber spy adventure!

In this story you decide what happens on each page. Can you identify The Trojan?

There are some tricky choices and brain teasing puzzles along the way. You can read this story with your parent/carer, grandparent, aunt - any adult you trust - and swap ideas on what the right answers might be.

Adults

This is an adventure story families can read together. It is the final story in a series of 3. We recommend starting with the 1st story.

You can read this story several times, making different choices each time. You can read the story with your child/family member, and discuss the answers together. Or they can read the story and ask you when they want extra help with their choice.

This story contains important advice about cyber security. It's a great opportunity to talk about how to keep information secure online. For more advice for families, see our CyberAware webpages.

On each page you will see buttons to either 'continue' the story or decide what happens next. Choose 'Let's Go!' to begin your adventure.

Let's Go!

Another day, another dollar! You're on your way to GCHQ where you work as a cyber spy. On the way, you look at the group chat you share with colleagues Ross, Nila and Ollie. Ross has sent through another fun riddle. Can you solve it before your colleagues do?

I tell you something yet I am silent. I am real yet you cannot touch me. I have no home yet I have an address.

What am I?

Click here for a clue

Press 'Continue' to find out the answer.

Continue

Do you have an _____ address?

Go back

Just as you walk into the office, you realise the answer is ‘email’. Your colleague Nila is already at their desk.

“*Morning!*” you say.

You notice that Nila has posted a link in the group chat with the message ‘Sharing this with you as it’s a great way to earn some extra cash’. You’re about to ask Nila about it when Ollie walks in. His head is down so you can’t see his face clearly. He goes straight to his desk and sits down without saying anything. He seems upset.

Ask Nila about her message

Ask Ollie what’s wrong

Nila explains "*I'm investing in cryptocurrency! It's so exciting. You should try it too.*"

You don't look convinced.

"*It's all legitimate!*" she says. "*I transfer money to a company that mines for cryptocurrency for 24 hours. Then I get all my money back and more.*"
"*How do you know it's not a con?*" you ask.

"*Because I've already started making money!*" she beams.

Your conversation is interrupted by Ollie, who sighs heavily.

Ask Ollie what's wrong

"*I'm worried,*" Ollie says. "*You know SparJam games? Well, you can get paid for playing their games. The website says you can get £50 an hour and all you have to do is play beta games.*"

"*Beta games?*" you ask.

"*Games that haven't been finished yet. You test them by playing them, and tell SparJam if you find any problems,*" Ollie explains.

"*That sounds great. What went wrong?*" you ask.

"*They said I had to buy some equipment first, like a special mouse and keyboard. And pay for a training course. So I did all that, and then…*" his voice trails off.

"*Then?*" you prompt.

"*Nothing happened. I paid them a week ago. I've been emailing them but I've not heard back,*" says Ollie as he slumps back into his chair

Decide to investigate

"*Let me look into this*," you say. You ask Nila if she can help too. She doesn't know much about online investigations but you could explain what she needs to do.

"*Of course I'll help!*" says Nila. "*There are some bad people online! But it is possible to get good advice and make money. I've just done it myself.*"

You ask Ollie how he heard about being paid to play games.
"*I saw it online. Look*," he says as he brings up a video.

Watch the video

You watch the video. There are a few things that make you suspicious. You take a moment to think about them before sharing your concerns with Ollie. What makes you suspicious?

It sounds too good to be true

A billionaire is unlikely to be involved

You highlight that the video says you can make £400 a day playing games, which seems to good to be true – usually a warning sign. And using a celebrity's name could be dodgy too.

"*You're right,*" says Ollie. "*I ignored the warning signs because I was so excited by the idea.*"

"*But loads of people have liked and shared it,*" *says Nila "so it must be OK?*"

"*No. Other people can be fooled too,*" you explain. "*And sometimes fraudsters buy followers or bots to like and share their posts. So it looks like lots of people think something is OK when it's not true.*"

You also point out that this is an advert, but isn't labelled as one. All adverts should clearly show that they have been paid for. It should have the hashtag #ad or #advert. Although fraudsters might include the hashtag anyway. "*And there's another thing,*" you say. "*We should consider who posted the video.*"

Dig a little deeper

The video was posted by a user called *@trojan935*. You look at their profile. It was created 3 weeks ago and includes a picture. They have posted only 1 video but they have a lot of followers. You notice the profile also includes a link to a website.

@trojan935

Look at the website address

Search for the profile picture elsewhere

You open a website where you can search using a picture instead of words. It's called a 'reverse image search'. If the fraudster has stolen the picture from someone else, you might find the original online.

The only search result is the one you already have – for @trojan935.

"*So it must be her,*" Nila says.

"*Not necessarily,*" you explain. "*A fraudster could have taken the picture from a private message, so we wouldn't see it anywhere else online.*"

You don't think you can do anything else with the picture for now.

@trojan935

Look at the website address

You write the website address out in your notebook.

http://sparjam.playygames.com/getpaid

You look at it for a moment. What do you tell Nila and Ollie?

That isn't a secure website address

That isn't the SparJam website

“*That isn’t a secure web address.*” you explain. “*You want an address that is ‘https’ rather than ‘http’, especially if you make a payment on it or submit personal information. Even if it is a https address, you should also always make sure the address is genuine.*”

You get out some coloured pens to show Nila and Ollie a few more things about the address.

You explain that the SparJam website is sparjam.com. But this website is playygames.com.
We know this because it has the name (playygames) followed by
an extension (.com).

The sparjam bit before the name is just a section of the playygames.com website. It’s a trick to make you think it’s the SparJam website.

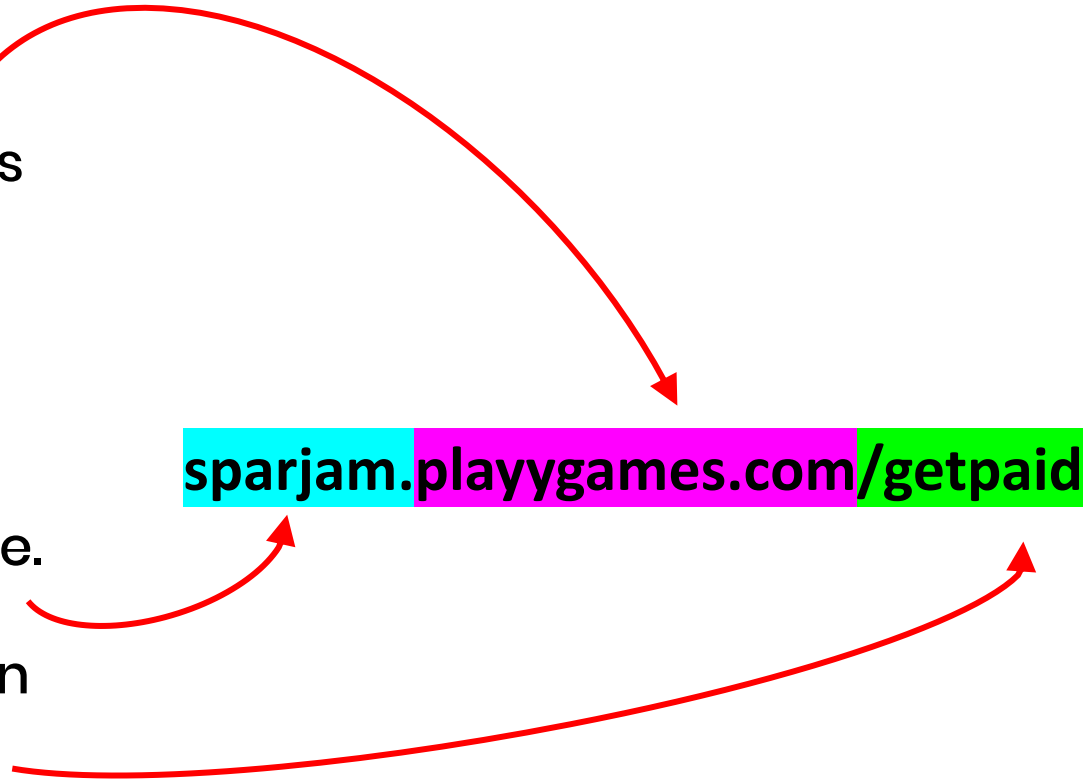
getpaid is the current page you’re looking at on the playygames.com website. It comes after the .com extension and a slash (/).

Continue

You explain that the SparJam website is sparjam.com. But this website is playygames.com. We know this because it has the name (playygames) followed by an extension (.com).

The sparjam bit before the name is just a section of the playygames.com website. It's a trick to make you think it's the SparJam website.

getpaid is the current page you're looking at on the playygames.com website. It comes after the .com extension and a slash (/).



"*And that isn't a secure web address.*" you explain. "*You want an address that is 'https' rather than 'http', especially if you make a payment on it or submit personal information.*"

Continue

You tell Ollie that people can report a suspicious website to the National Cyber Security Centre. You can also report scam phone calls, text messages and emails to them. And you can report scam adverts to the Advertising Standards Authority. "*I'll get right on it*," he says, and thanks you for your help.

For your own investigation, you need to find out more about the person who posted the video and the link to the website.

You send the profile photo to your colleague Ross, GCHQ's tech whizz, to see if he has any ideas about how to identify who it is.

While you wait, you search for more clues.

Search for @trojan935 online

As you are about to start your search for the username @trojan935 online, a notification from your social media app pops up on your phone. Your boss Jess has just posted something. You also see a message from Ross on the group chat.

You ask Nila to do the search of @trojan935 while you check these out.

What do you do first?

Check the group chat

Check what Jess has posted online

You look at the message Ross has shared. Lots of people in the chat are posting about it. But you are suspicious again – what should you tell the group?

You don't know who made the keyboard or where it is downloaded from

It's only available for 24 hours

There is a sense of urgency as you have only 24 hours to download it. This is a common scam tactic.

But you're also suspicious because you don't know who made the keyboard or where it is downloaded from. You can't be sure that you would download a keyboard or something else, like a virus.

You message the group and tell everyone you don't think it's trustworthy.

Just then, Nila shouts over to you. "*Found something!*"

Go to Nila's desk

Jess is on holiday this week. She's just put this on social media. It's a public post, so anyone can see it.

Jess Perkins is in Madrid, Spain
14 July at 10:19

MY LITTLE MUNCHKIN IS A TEENAGER!
HAPPY BIRTHDAY GRACE.
#FUNINTHESUN
#BACKINTWOWEEKS

Ask Jess why she posted the message

Ask Jess if she has a burglar alarm

You explain to Jess that she is sharing information that could be used to steal Grace's identity when she turns 18. All that's needed is her name, address and date of birth. Jess has shared two of these in her social media post. You advise her to check what else she's posted about Grace and talk to Grace about what she's happy for Jess to share about her online.

You go on to say "*It can be helpful to reflect on why we post the things we do.*"

"Why did you post that?"

After a minute, Jess replies. *"I've never really thought about why I post things online. I wanted to celebrate Grace's birthday. I love being a mum and I wanted to show people we're a happy family. I didn't really think about who would see it. And I didn't think about what Grace would say about it either. I'll be careful about oversharing online in future."*

You suggest to Grace that she also checks her privacy settings on social media, so that only friends can see her personal information.

Ask Jess if she has a burglar alarm

You message Jess "*Do you have a burglar alarm?*"
"*Weird question!*" she replies. "*Why do you ask?*"

You explain that Jess has just told the world she's in Spain for two weeks. Thieves can target people using information they find on social media. And they now know her house will be empty. You add that her home insurance may not pay out if they know she posted online that the house was empty.

"*Eep! Thanks!*" messages Jess. "*I'll delete the social media post.* I'll put my holiday *pictures online once I'm back home. I'll also go through my old posts to check what else I've shared*."

"*Great stuff!*" You message and add a suggestion to regularly check the privacy and security settings on her account.

Ask Jess why she posted the message

"*Weird question! Why do you ask?*" Jess messages back

You explain that Jess has just told the world she's in Spain for two weeks. Thieves can target people using information they find on social media. And they now know her house will be empty. You add that her home insurance may not pay out if they know she posted online that the house was empty.

"*Eep! Thanks!*" messages Jess. "*I'll delete the social media post.* I'll put my holiday *pictures online once I'm back home. I'll also go through my old posts to check what else I've shared*."

"*Great stuff!*" You message and add a suggestion to regularly check the privacy and security settings on her account.

Just then, Nila shouts over to you. "*Found something!*"

Go to Nila's desk

You explain to Jess that she is sharing information that could be used to steal Grace's identity when she turns 18. All that's needed is her name, address and date of birth. Jess has shared two of these in her social media post. You advise her to check what else she's posted about Grace and talk to Grace about what she's happy for Jess to share about her online.

You go on to say "*It can be helpful to reflect on why we post the things we do. Why did you post that?*"

After a minute, Jess replies. "*I've never really thought about why I post things online. I wanted to celebrate Grace's birthday. I love being a mum and I wanted to show people we're a happy family. I didn't really think about who would see it. And I didn't think about what Grace would say about it either. I'll be careful about oversharing online in future.*"

Just then, Nila shouts over to you. "*Found something!*"

Go to Nila's desk

"*You asked me to search for @trojan935 online. It's an unusual username,*" Nila says. "*I found it in two other places. On a shopping website, and on the social media site Chitterflix.*"

Look at the shopping website

Look at Chitterflix

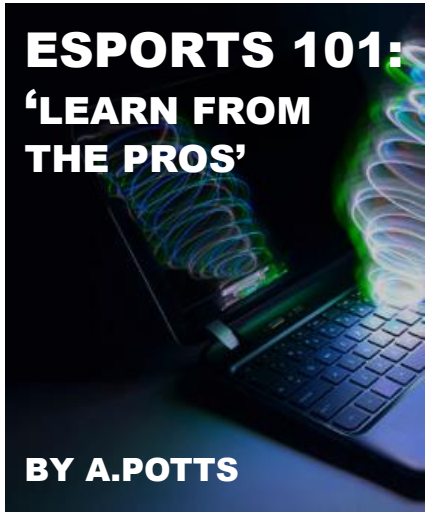
Nila brings up the shopping website. "*Someone with the same username bought a book about esports 3 weeks ago. They left a review*," she explains.

You wonder if this is the same person. Are they interested in esports?

You can't see any other useful information here so decide to look at Chitterflix.

Esports 101: Learn from the Pros

By A.Potts



£7.99

@trojan935

★★★☆☆

What a waste of money.

Look at Chitterflix

Nila shows you the post on Chitterflix. You take a close look. What information has been shared?

When did @trojan935 go for lunch?

Can you work out the street name from the post?

@trojan935
5 October at 12:03

afk for lunch #BackAt1

Continue

Hmm yes, you can work out that @trojan935 went for lunch at 12:03 on 5th October.

You can't work out the name of the street from the post though.

Could this be the same person you wonder? You send the picture to Ross. You ask if he can work out where it was taken.

"*A phone box, bus stop, bridge, cycle path and some traffic lights are all in the photo. That's an unusual combination,*" he replies. "*I'm sure I can find it*".

@trojan935
5 October at 12:03

afk for lunch #BackAt1

Thank Ross

Nila shows you the post on Chitterflix. You take a close look. What information has been shared?

When did @trojan935 go for lunch?

Can you work out the street name from the post?

@trojan935
5 October at 12:03

afk for lunch #BackAt1

Continue

Hmm yes, you can work out that @trojan935 went for lunch at 12:03 on 5th October.

You can't work out the name of the street from the post though.

Could this be the same person you wonder? You send the picture to Ross. You ask if he can work out where it was taken.
"*A phone box, bus stop, bridge, cycle path and some traffic lights are all in the photo. That's an unusual combination,*" he replies. "*I'm sure I can find it*".

You message Ross to thank him.

@trojan935
5 October at 12:03

afk for lunch #BackAt1

Look at the shopping website

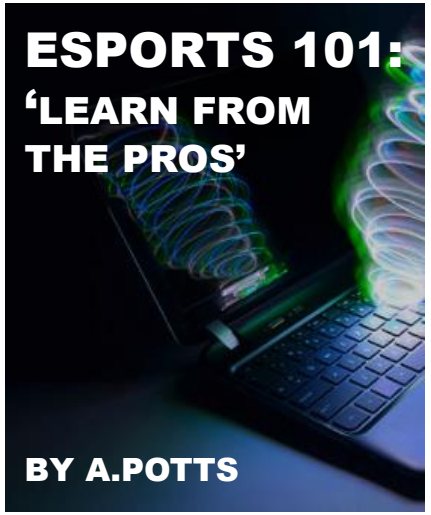
Nila brings up the shopping website. "*Someone with the same username bought a book about esports 3 weeks ago. They left a review*," she explains.

You wonder if this is the same person. Are they interested in esports?

You can't see any other useful information here.

Esports 101: Learn from the Pros

By A.Potts



£7.99

@trojan935

★★★☆☆

What a waste of money.

A new message pings on your screen

You see there's another message from Ross. "*By the way, the profile picture you sent me earlier is a fake.*"

You look closely at the picture and realise something is not quite right.

@trojan935

Show Nila

You show the picture to Nila.

"*Oh I see!*" she says "*The colours behind her head are all wrong. And her ears are different.*"

You agree that it's a fake picture. You remember there are websites that use Artificial Intelligence (AI) to create fake pictures of people. Sometimes they make mistakes and you can spot them!

@trojan935

Ding what's that noise?

Nila has just been sent a text.
"*Oh no!*" she exclaims. "*It says someone has tried to hack into my bank account. They're trying to transfer money out of my account. The bank have sent a text to warn me.*"

"*They've sent me my password to prove they are my bank,*" she adds. "*They are going to send me a verification code and then phone me. I need to tell them the code so they know they're talking to me and not the hacker.*"

Nila receives the code in a text message. Her phone starts to ring.

Advise Nila to answer the phone

Tell Nila not to answer the phone

Nila answers the phone.

You suddenly realise it's a scam.

Shout "Stop!"

"*It's a scam!*" You say. "*No bank would ever text someone their password. A fraudster is trying to break into your bank account. They have probably cracked your password and just need the two step verification (2SV) code to get in. You mustn't give it to them!*"

Nila reports the attempted fraud to her bank immediately and she changes her password. She also reports it to the Police via Action Fraud UK (if she were in Scotland she would report to Police Scotland).

You remind Nila that a fraudster can phone, email or text pretending to be a genuine organisation. If she's suspicious of an email or text, she shouldn't click links that are sent to her. She can forward suspicious emails to report@phishing.gov.uk. And she can report suspicious texts by forwarding them to 7726.

buzz-buzz

You have a message! You check your phone. "*I know the street name*," says Ross' text. "*It's Old College Lane*."

There is still a college on that street, you look it up online. You wonder if @trojan935 is a student or works there.

On the website front page there is an article about the College's Esports Club. There's a quote from the Club President which says "*If you love esports, the club at Bringham is fantastic. You can get involved in esports at any age. I started when I was 11 and I've never looked back.*" The article includes a link to an esports chat forum.

Ask Nila for help

Join the esports chat

You join the chat forum. It says there are over 600 members. You're sure one of them is the fraudster. You post that you're short of cash and looking for ways to make money.

Within two minutes, you receive a direct message from @trojan935. It says you can get paid for playing games, and gives you a link to the fraudulent website.

Reply "What's your real name?"

Reply "Do you know Ollie?"

You ask the fraudster what his real name is. He ignores your question and says you can make a lot of money fast. You realise he's not going to tell you anything useful.

Ask Nila for help

You ask @trojan935 if they know Ollie.

There is no reply. You've spooked @trojan935! He's blocked you. You realise you can't solve this crime on your own... **your *story doesn't have to end here.***

Change your last decision

"*Oh sorry,*" says Nila. "*I can't help at the moment, I'm expecting to hear back about my latest investment any minute.*"

"*Who are you investing with?*" you ask. "*I met someone called Phil through gaming. He's teaching me about cryptocurrency.*" Nila explains.

"*Is he trustworthy?*" you ask. Nila frowns. "*Phil? Of course! I've made money already. He's a great guy. We talk online all the time. Look, here he is.*" She brings up his profile on Chitterflix. Phil's username is @innvestforfun. His profile picture shows a handsome man in his mid-20s.

"*How much money have you spent?*" you ask.

"*My first investment was £50 and I got £80 back straight away. So I'm putting more money in now.*" Nila says.

Ask for more details

"*Hmm, how much more are you putting in this time?*" you ask.
"*I've put in £200 this time,*" Nila says. "*I should get all that back and make a nice profit. Phil said he bought his house with money he made this way.*"

You ask Nila to show you her conversation with Phil. Looking through the messages, you recognise tactics that fraudsters use.

Explain the tactics

"*Look at this message,*" you say to Nila. "*He says you'll make a lot of money but only if you act now. He's trying to get you to make a decision quickly so you don't have enough time to think about it properly. And he's acting like he's doing you a favour.*"

"*But that's just how it is!*" Nila replies.

Keep talking to Nila

"*And he's been flattering you,*" you point out. " *And I see he's been asking for personal information.*"
"*We're friends!*" *exclaim*s Nila. "*It's nice when someone takes an interest in you. Phil knows I could really do with some extra money at the moment. He's helping me out.*"

What do you do next?

Try one more time to get Nila to listen

Head back to your desk

"*The signs are all here.*" you say to Nila "*Phil is a fraudster.*"

Nila replies "*I'm not talking to you about this anymore. Just mind your own business!*"

You've run out of ideas to help Nila but you might be able to do more to identity Ollie's fraudster... **your story doesn't have to end here.**

Change your last decision

You head back to your desk and think about what to do next . You remember the Wayback Machine from your cyber spy training. It is a web archive. It began to keep copies of webpages in 1996. There are now 588 billion web pages in the Wayback Machine. You can take almost any web page and see what it looked like last week, last month or years ago!

You copy and paste the web address listed in the @innvestforfun profile into the Wayback Machine. You see that last year @innvestforfun had a different profile picture. It's a picture you recognise.

Show the picture to Nila

“*Why are you showing me @trojan935?*” Nila says.

“*Last year @innvestforfun was using this picture and a woman’s name,*” you say. “*It changed 6 months ago to use a picture of the man you think is Phil. But Phil isn’t real. It’s all fake. You’ve been talking to a fraudster.*”

@trojan935

Keep talking

"*But, I made money. I invested £50 and I got £80 back!*" Nila mutters, confused.

"*That's how they do it,*" you explain. "*First, they pretend your investment is making money. They give you more money back than you've put in. So you feel good and invest more next time, and tell other people to invest too. But when you put a lot of money in, you will get nothing back.*"

"*Who would do this to me?*" Nila asks.
"*And Ollie!*" you add.

You know it is the same person. But you don't know who it is yet.

Think through the clues you've found

"*I think I'm close to working it out Nila,*" you say. "*I think the fraudster is involved in esports at Bringham College. I think they are a student there. Can you think of anything they told you when you were messaging? Any tiny thing that they shared about themselves?*"

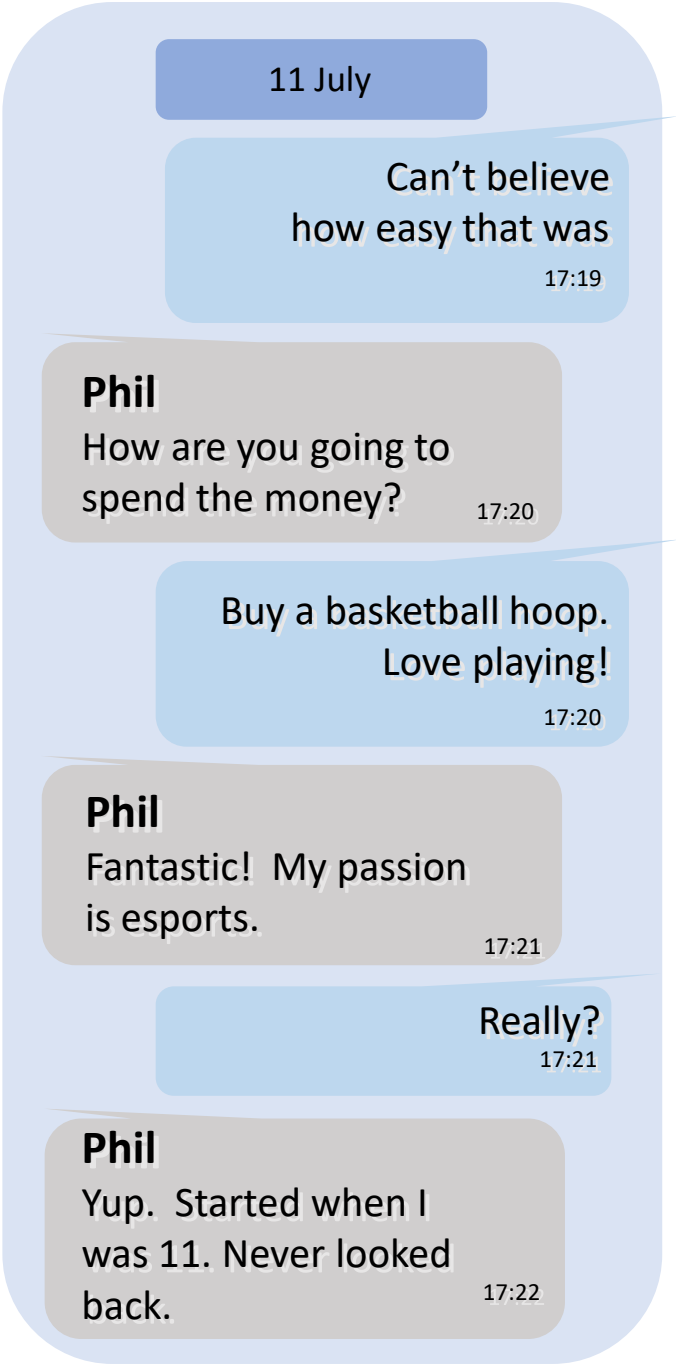
Nila picks up her phone and scrolls through her messages.

"*The conversations focused on me,*" she says, still scrolling "*They asked me lots of questions. I don't think...*" She stops speaking abruptly and holds up her phone to show you something.

Take a look

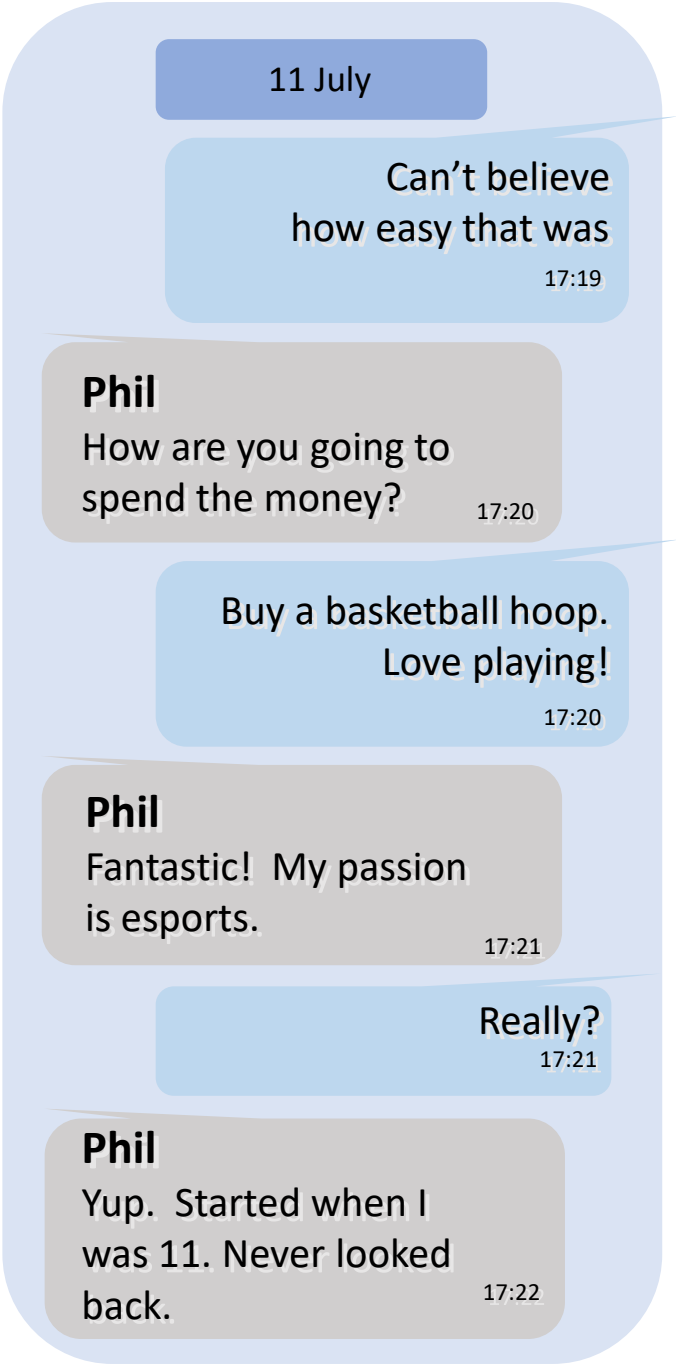
"*Right here!*" Nila points to one of the messages on her phone.

You take a look...



Ah-ha!

Nila explains "*I was telling him about how I love basketball. He said his passion is esports. He said he got involved when he was 11, and he's never looked back.*"
"*Ah-ha!*" you say and smile.
"*Does that help?!*" Nila asks.
"*It's all come together,*" you say. "*The fraudster is…*"



Tell Nila and explain the clues

“*It’s the President of the Esports Club at Bringham College!*” You exclaim. “*The fraudster used the username @trojan935 to share the video that tricked Ollie. Someone with the same username bought a book about esports online and shared a photo of the street next to Bringham College.*”

Keep explaining

“*The College has an Esports Club. On their website the Club’s President talks about getting involved in esports when they were 11 years old. Using the WayBack Machine we saw that your fraudster Phil had used the same profile picture as @trojan935. It’s the same person behind both accounts.*” You explain. Nila looks impressed!

“*Let’s contact the Police, and see what they can do.*” you say.
“*Thanks so much, you have become a real cyber security expert and I’m so glad you’re here!*” Nila beams.

Congratulations! You identified The Trojan!

Did you uncover all the clues? If you want to try some different paths through the story - you can!

Try different story choices