

Safer Internet Day 2025

Resources for use with
7-11 year olds



**Too good to
be true?**

**Protecting
yourself and
others from
scams online**

Safer Internet Day is celebrated globally in February each year to promote the safe and positive use of digital technology for children and young people, and to inspire a national conversation about using technology responsibly, respectfully, critically, and creatively. Safer Internet Day 2025 is on Tuesday 11 February.

In the UK, Safer Internet Day is organised by the UK Safer Internet Centre (UKSIC), a partnership of three charities – Childnet International, the Internet Watch Foundation (IWF) and SWGfL.



With kind thanks to the Welsh Government for their support in the development of these resources in Welsh.

For more resources and advice visit: hwb.gov.wales/keeping-safe-online



Cefnogir gan
Lywodraeth Cymru

Supported by
Welsh Government

With kind thanks to the Safeguarding Board for Northern Ireland for their support in the development of these resources in Irish.

For more resources and advice visit: onlinesafetyhub.safeguardingni.org



4

5 things you need to know about participating in Safer Internet Day

5

Activity:
Signs of a scam

10

Activity:
Let's go phishing

15

Activity:
Protect your profile

18

Quiz:
Protecting yourself and others from scams online



5 things you need to know about participating in Safer Internet Day

1. Too good to be true?

We've all received an email with a suspicious link, a text claiming to be from our bank, or even seen a pop-up telling us we have been a lucky winner, but scams take many forms and can target anyone, including young people. This Safer Internet Day, we want to start conversations about how to spot, respond to and report all types of scams online.

2. Establish a safe space.

Consider how to establish a supportive environment for young people to learn and talk about potentially sensitive topics. For ideas visit: childnet.com/learning-environment.

3. Be ready to respond to safeguarding concerns.

While discussing their online lives, it is possible that children and young people will raise concerns about things they have experienced online. Make sure you are up to date with your school or setting's safeguarding procedures and for further advice visit: childnet.com/safeguarding.

4. Know where to get more information or help.

Remember that there's plenty of help and advice available if you need more information about anything online safety related.

The UK Safer Internet Centre's 'Need Help?' page contains further information on reporting specific concerns to organisations outside of your school or setting: saferinternet.org.uk/advice-centre/need-help

The Professionals Online Safety Helpline is a free helpline offering advice and support to all members of the children's workforce on any online safety issues: saferinternet.org.uk/professionals-online-safety-helpline

5. Kickstart conversations that last all year round.

The online world is changing all the time, but talking with young people about their online experiences can help you understand what's going on. Kickstart the conversation today but make it a regular habit all year round.



Activity: Signs of a scam

Time:

20 to 30 minutes

Learning objective:

- I can explain what is meant by the word scam and give examples.

You will need:

- 7-11 Slides (Signs of a scam, slides 2 to 14)
- Cut-out copies of the Signs of a scam cards

Activity guidelines:

This activity helps learners to understand what a scam is and the possible signs that something might be a scam.

1. Ask learners if they know what a scam is. They may want to give you some examples from their own experiences.
2. Display definition of a scam on slide 3 and read aloud to learners.
3. Ask learners how they can work out if something is a scam.
4. Display slide 4 and read out the SCAM acronym to explain four key signs that something might be an online scam.
5. Divide your learners into small groups and provide each group with cut-out copies of the 'Signs of a scam' cards.
6. Display each scam example on the slides (slides 5 to 11) one by one and ask groups to hold up their cards to show what signs can be seen in each example. Give them around 30 seconds to discuss each one. They may hold up more than one card if applicable. Click to reveal the answers on screen.
7. Finish the activity by asking learners what they should do if they think they see a scam online. Explain to learners that they should always talk to a trusted adult.

○○○ Ideas to challenge

○○○ Ideas to scaffold

Instead of working through all examples on the slides, select a few of the examples and work through them with learners in small groups.

Use slides 12, 13 and 14 to challenge learners further, which explore how some things online may show signs of a scam but might not actually be scams, or that a scam might not show any of the signs initially. Ask learners what they should do if they're unsure about a situation online.



Signs of a scam cards

Sounds too good to be true

Contact you did not expect

Asking for personal information

Money or a trade is asked for

Not a scam



Signs of a scam cards

Sounds too good to be true

Contact you did not expect

Asking for personal information

Money or a trade is asked for

Not a scam

Additional teacher guidance: Signs of a scam

Scenario 1

You are on a website and a pop-up appears. It says: "You are a WINNER! CLICK HERE to claim your free gaming set worth over £1000! You only have 15 minutes to claim!"

Scam

This sounds too good to be true and it is contact you did not expect. It is very unlikely that you will have won a gaming set, especially if you didn't enter a competition. The scam tries to pressure you to click on it by pretending that you only have 15 minutes to claim the prize.

Scenario 2

You get a text message from an unknown mobile number. It says: "Your package cannot be delivered because of lost address. Pls deal with this immediately. Click on link postbo.xabcde.co.m and update your address and phone number."

Scam

This is contact you did not expect, and it is asking for personal information. The scam is pretending to be a delivery service and is trying to pressure you into clicking on the suspicious looking link "immediately." It also spells "please" as "pls" which is very informal.

Scenario 3

You see an account called @us56345 advertising wireless earphones for only £5! It says the quality of the earphones is better than many of the biggest brands.

Scam

This sounds too good to be true, and money is being asked for. It is very unlikely that £5 earphones will be better than earphones made by a big brand. The earphones also may not be sent or may not exist. The username of the seller is also suspicious and looks like it may be randomly generated.

Scenario 4

You are at the cinema with your friend. A trailer for a new superhero movie comes on. It looks really exciting.

Not a scam

It is just a film trailer, and it contains no risks that might be associated with a scam.

Additional teacher guidance: Signs of a scam

Scenario 5

You can see a lot of messages in the public group chat in the game you're playing. One says: "Click this link! fr.ee.bucks.co You can get free bucks! Just gotta give your name and phone number!"

Scam

This sounds too good to be true, and it is asking for personal information. It is very unlikely that you will be able to get free currency for an online game. The link you are being asked to click on also looks suspicious.

Scenario 6

You are playing an online fantasy game. You receive a message from someone you do not know. It says: "Hey! You can trade your goblin for my golden dragon – it's really rare and powerful!"

Scam

This sounds too good to be true, is contact you did not expect, and a trade is being asked for. This trade is not part of a game's official trading system, and you don't know the player, so you cannot trust that they will actually go ahead with the trade. You might give away your goblin and not get anything in return.

Scenario 7

You receive a message from someone you don't know on an online game you play. It says: "You're great! We'd like you to be part of our Gamer Pro talent agency! Send me your email, and I will send you a link to pay a small deposit to join us."

Scam

This sounds too good to be true, is contact you did not expect, is asking for personal information and money. It is likely that this person isn't actually a representative of a talent agency, and that all they want is your money and your personal information.

Additional teacher guidance: Signs of a scam

Scenario 8 (Challenge)

You are on a train, and you are trying to connect to the Wi-Fi. It says you need to provide your name and email address before you can connect to it.

Not a scam

This is asking for personal information, but it is not a scam. Sometimes, companies online will need your personal information, often because they are delivering a service (in this case, Wi-Fi).

Scenario 9 (Challenge)

You really want to buy a VR headset and find a good deal on a website you've not heard of before.

You feel reassured because you see five good reviews saying exactly the same thing about the headset.

Scam

Positive reviews can help you work out if a product is good quality, but it is important to remember that some reviews can be fake, created to trick you into thinking that the product is good. One sign that the reviews might be fake is if they are all saying very similar things or use very similar wording. The reviews themselves don't show the other signs of a scam, but they are added to trick people into making a purchase and losing money.

Scenario 10 (Challenge)

You recently entered an official online giveaway competition hosted by @gamemastersuk to win a games console. One day, you receive a message from @gamemasterzuk saying: "You've won! Send me a message to confirm that you accept the prize, and I will message you with the next steps!"

Scam

This does not show any of the signs of being a scam. For example, this is not contact that you did not expect, as you may be expecting someone to contact you after entering the competition. However, if you look closely, the account that has messaged you is slightly different to the official account. It uses a 'z' instead of an 's'. This means it is probably not someone overseeing the official online giveaway competition. In this first message, they are not asking for personal information or money, but it is likely that they will ask you for one of these things next.



Activity: Let's go phishing

Time:

20 minutes

Learning objective:

- I can explain what is meant by the word phishing and give examples.

You will need:

- 7 to 11 slides (Let's go phishing, slides 15 to 19)
- Fish food sorting activity cards.
- Trustworthy trout's fishbowl

Activity guidelines:

This activity helps learners understand what 'phishing' is and how to spot it online.

1. Using the definition slides, introduce the term 'phishing' to learners. Ask if they have heard this word before and what they think it means.
2. Explain that phishing can come in different forms. It could be an email, text message, link in a game, social media message, or phone call. Normally they claim to be a well-known company. What companies can learners think of?
3. Explain to learners that they are going to feed 'Trustworthy trout'. They need to decide which food is safe and which food is an example of phishing.
4. In small groups, the children feed the reliable examples to Trustworthy trout, by putting them in the fishbowl. Question their decisions and ask how they know which examples are phishing.
5. Ask children if they have seen phishing examples before. What advice would they give to someone else about how to spot phishing?

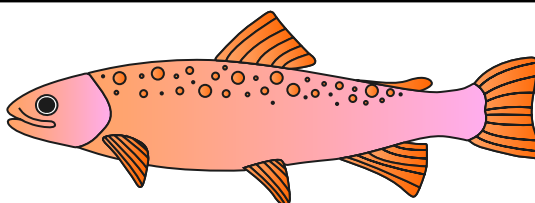
○○○ Ideas to challenge

Learners can annotate the scams using highlighters to show the signs of a scam. For example, spelling mistakes, suspicious email addresses, personal information requests.

○○○ Ideas to scaffold

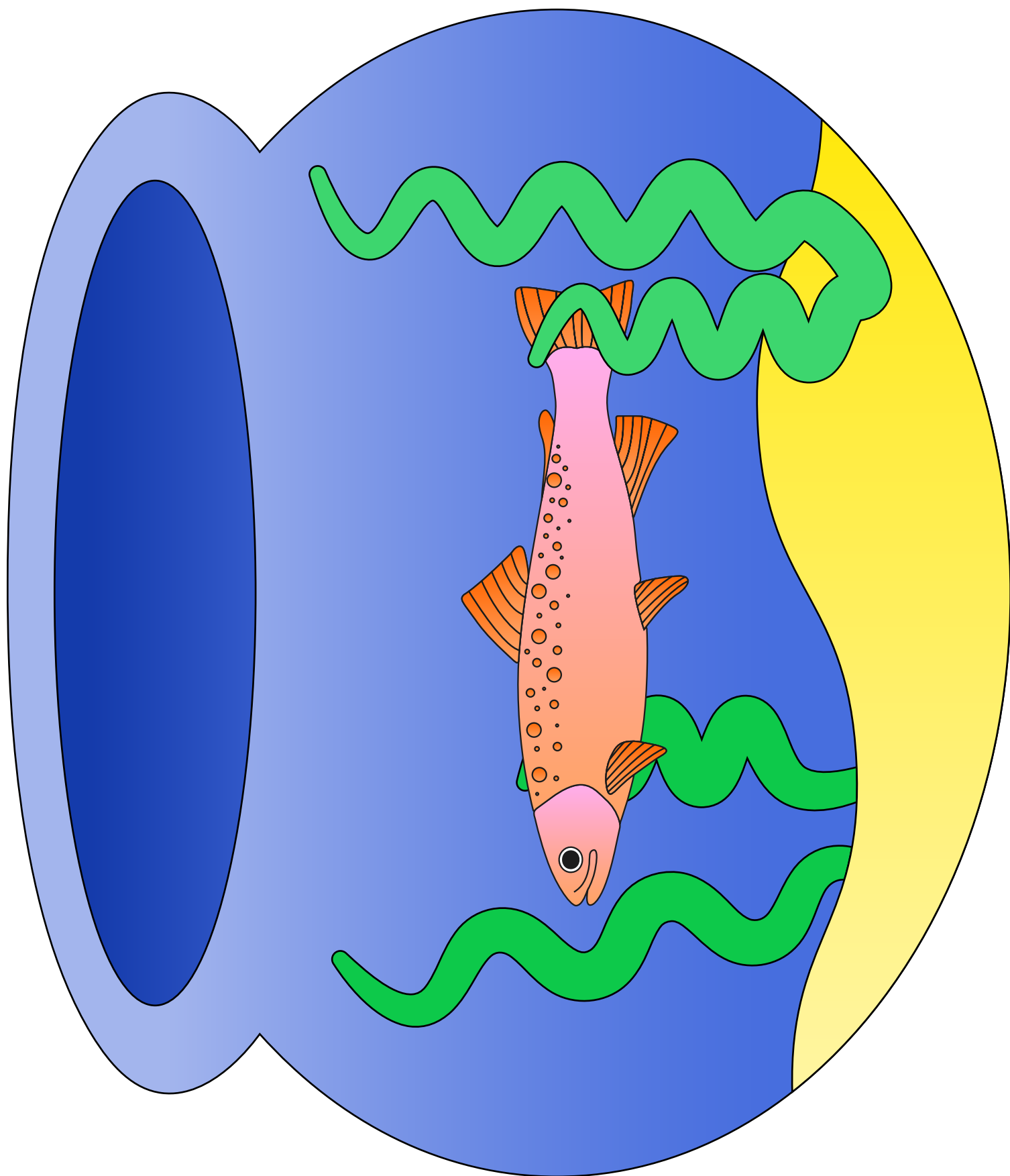
Before sorting the cards, learners can be a detective and spot any signs of somebody asking for personal information. Use a coloured pencil to show where this is.

○○○ Trustworthy Trout





Trustworthy trout's fishbowl





Fish food sorting cards

New Message

From: Deliver Your Parcel Customer support
(admin.283819@email.live.com)

Dear Customer,

The current storm in the UK has been affecting parcel deliveries and your order has been lost.

Take action NOW!!

Reply to the email with your address and full name in 24 hours.

From The Delivery Team

Grandma

Did you enjoy your first day back at school? xx

Yes thank you. I made a new friends too! xx

Would you like to video call later? it would be lovely to see u xx

Reply...

Unknown Number

We have detected a payment from your bank account. We can stop this. Please tell us the unique code we have just texted to you.

Zo

Hey! do you want to play on X-Box after dinner? I am free at about 7?

New Message

From: Happy Shoes
(orders@happyshoe.com)

Hello,

Thank you for your most recent order from Happy Shoes.

We are pleased to tell you that our order is now out for delivery!

Use the link below to track your parcel. Your 10-digit tracking number is: 6472836472

<https://happyshoes.com>

1 NEW MESSAGE

from: CEOofRacingStars

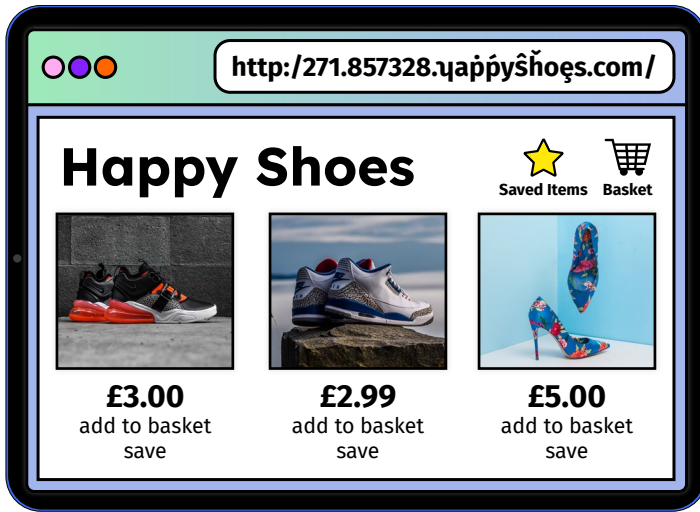
Dear user,

this is the CEO of Racing Stars. Your account has broken.

Send your username and password so I can fix this issue




Fish food sorting cards




http://271.857328.happyshoes.com/

Happy Shoes


Saved Items Basket



£3.00
add to basket
save



£2.99
add to basket
save



£5.00
add to basket
save

New Message

From: Brixpoint Primary School
(office@brixpointprimary.com)

Good Afternoon,

This is just an email to remind you that on **Friday 12th April** we will be having an own clothes day.

Donate £1 to wear your own clothes for the day.

Kind regards,

The School Office



Unknown Number

Congratulations! You have won a free holiday from
★ EasyPlane! ★
Reply to this message to claim your prize!

Reply...

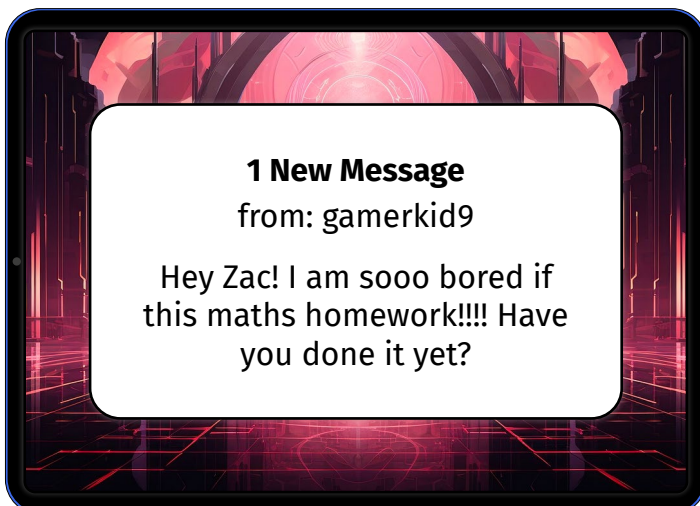
New Message

From: Google
(g.oo.g.lee@live.com)

Unusual Sign On Activity On Your Account

We noticed a suspicious sign in on your account. Please review your activity and take action immediately by clicking the link below:

[Review Activity](#)



1 New Message

from: gamerkid9

Hey Zac! I am sooo bored if this maths homework!!!! Have you done it yet?



1 New Message Request


@talentstaz888888
2 followers 348 following
You do not follow each other

Hi! I am from StarBound talent management and we love your page! we would love to sign you up! Can you send me your full name and phone number?

[Block](#) [Delete](#) [Accept](#)



Let's go phishing! Answers

Example 1: Phishing

- Unofficial email address.
- Doesn't use customer name.
- Asks for personal information.
- Using current events to seem more realistic.

Example 2: Not phishing

Example 3: Phishing

- Phone call claiming to be from your bank.
- Asking for two step verification (2SV) code to verify account ownership.
- Setting up 2SV can protect your account by adding another layer of security. When you try to log in on a new device or change your password, you will be sent a code to a trusted device which you can use to verify it's you.
- 2SV codes should not be shared over the phone or with anyone else.

Example 4: Not phishing

Example 5: Not phishing

Example 6: Phishing

- User is pretending to be CEO of the game.
- CEO would not message in this way.
- Spelling errors.

Example 7: Phishing

- Fake website.
- Suspicious URL using characters from another language.
- Products are very cheap (seems too good to be true).

Example 8: Not phishing

Example 9: Phishing

- Fake giveaway.
- Pretending to be a holiday company.

Example 10: Phishing

- Pretending to be well-known company.
- Unofficial email address.
- Spelling errors.

Example 11: Not phishing

Example 12: Phishing

- Suspicious username and no profile picture.
- User is following a lot of people but does not have many followers.
- Pretending to be a talent agency.
- Asking for personal information.



Activity: Protect your profile

Time:

30 to 45 minutes

Learning objective:

- I can share simple steps to protect myself from scams.

You will need:

- 7 to 11 slides (Protect your profile, slides 20 to 23)
- Dice for each learner or group

Activity guidelines:

This is a risk spotting activity that covers a range of potential harms and safety measures relating to both scams and personal information.

1. Ask learners what information they should keep safe online? They may give answers such as passwords, their name and their age.
2. Introduce or remind them of the term personal information as details that can identify someone such as their full name, school or birthday.
3. Explain that scammers and criminals online often try to collect their victim's personal information because they can use it to make money or gain access to someone's online accounts.
4. Display or give out copies of slide 20. Ask learners to identify any potential risks they can spot on the image. This could be done individually or in groups.
5. Talk through the answers as shown on slide 21 and ask learners to explain how they would protect against each harm. Finish by looking at the passwords.
6. Explain to learners that passwords are one of the most important tools for keeping their accounts and information safe. When choosing passwords, it's important that they are long, difficult to guess and don't contain any personal information. They should use a mixture of letters, numbers and symbols and always avoid obvious passwords such as 123456. The National Cyber Security Centre suggests combining three random words. Passwords should be different for each account you have.



Activity: Protect your profile

7. Display slide 22 and say that you're going to generate a secure password using dice. Roll 5 times and use the corresponding words and symbols in the columns to make a note of the password as you create it. Do not share it with learners.
8. Challenge learners to guess your password, explaining that it only uses the elements shown on the slide.
9. If learners guess your password, explain that this is because they knew some of the options to guess from, but that it would be much harder with random words, numbers and symbols. This is what makes a secure password.
10. If learners do not guess your password, explain that even when they knew some of the options to guess from, it was hard because there were lots of options. Imagine how difficult it would be to guess a password made with random words, numbers and symbols. This is what makes a secure password.
11. Distribute dice amongst learners. Have learners generate their own password or challenge them to create an even stronger password by coming up with their own random words and symbols.

○○○ Ideas to challenge

Have learners use their creative skills to design a profile or website with some hidden risks. Get them to swap in pairs and see what they can spot.

○○○ Ideas to scaffold

Provide learners with the 'Risk checklist' to help guide them through the activity and know what to look out for.



Protect your profile: Risk checklist

○○○ **Can you find these risks on Jake's screen?**

- ☐ Public profile
- ☐ Full name
- ☐ Age
- ☐ Photo of Jake
- ☐ Jake's school
- ☐ Jake's football club
- ☐ The city Jake lives in
- ☐ A high amount of friends
- ☐ A suspicious website
- ☐ A link in the chat
- ☐ An unofficial trade
- ☐ Moving a chat outside of the game
- ☐ Insecure passwords
- ☐ A scam pop-up
- ☐ A scam email



Quiz: Protecting yourself and others from scams online

Time:

20 minutes

Learning objective:

- I can explain what is meant by the word scam and give examples.
- I can identify the best action to take when I see a scam online.

You will need:

- Protecting yourself and other from scams online quiz

Activity guidelines:

Use this quiz to help learners identify what action to take when they see a scam online, as well as reflect on the different forms scams can take.

The quiz can be found online at: saferinternet.org.uk/sid-quiz or use the questions from the separate word document with this pack to adapt into whatever format most suits your setting.