youth SCOTLAND

The network
of youth groups

Cyber Resilience Activity Toolkit

Cyber Resilience Activity Toolkit

This Cyber Resilience Activity Toolkit has been developed to encourage children/young people to think about their online interactions and encourage them to keep safe online. Activities within this toolkit can also be used to contribute to a Hi5, Dynamic Youth Award or Youth Achievement Award.

Health and safety

This toolkit has been designed to be run by youth workers or young leaders for young people. Some of these activities may encourage young people to think about the experiences they've had online, and they may wish to share unpleasant experiences with the group. Before starting a safe space should be created for young people to openly discuss their feelings in confidence and within a group agreement. Staff can then be prepared to follow up one-to-one with young people in confidence.

This toolkit has been designed to be run with older primary and secondary aged young people, but any of the activities can be adapted for the age and stage of the group. There are estimated times given but these may change based on the size and age range of the group.

Remember when leading activities it is your responsibility to ensure you use age-appropriate materials and equipment. In particular be aware and take any necessary precautions when using certain materials with children and young people such as magnets. You should also be aware of any risks associated with the environment you'll be working in. Children and young people should be supervised at all times and your own organisation's Health and Safety policy and any other relevant policies should be followed.

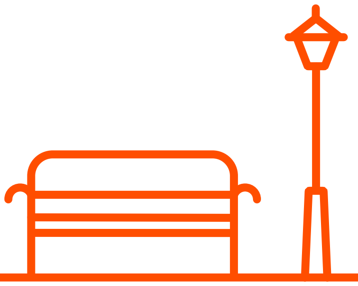
Please note that to the extent permitted by law, Youth Scotland shall not be liable to any person for any loss or damage that may arise through using this toolkit. You know your children/young people best and know what activities would suit them. It is always a good idea to try any activity yourself in advance, especially if it involves making something.

Useful links

For more information about keeping children and young people safe online please visit the following websites:

- **https://saferinternet.org.uk/**
- **https://www.nspcc.org.uk/keeping-children-safe/online-safety/talking-child-online-safety/**
- **https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/staying-safe-online/**
- **https://www.childnet.com/**
- **https://www.iwf.org.uk/**
- **https://swgfl.org.uk/**
- **https://www.ceop.police.uk/Safety-Centre/**

Contents



Password perks

In this activity young people understand the importance of strong passwords and learn how to make their own

Time:

20 minutes

What you need:

- Paper
- Pens

What to do:

1. Ask the group if they know what makes a good password or a bad password. This activity is about the importance of strong passwords so remind the group not to disclose any of their own
   - A good password is long, hard to guess and unique (having a different password for every account you have)
   - A bad password might contain personal data (such as your name, your pet's name, your birthday), be short or include the word 'password' or an obvious number pattern like '1234'
2. Give everyone 5 pieces of paper and a pen
3. On three pieces of paper write a random word (make sure it's not rude!)
4. On one piece of paper write a number
5. On the last piece of paper write a special character, for example a pound sign or an exclamation mark
6. Get the group to scrunch the paper into balls and throw them around the room. If a piece of paper lands near them pick it up and throw it again, like a snowball fight
7. After a few minutes stop the group. Ask them to find five pieces of paper each. They can get any combination they like, but encourage them to find at least two words
8. Flatten the paper and lay them out in front of them. Rearrange the pieces of paper to make a password. For example if the paper that they got said 'house' 'banana' 'extra' '577' '%' the password could be 'house577extrabanana%'
9. To make the password even stronger they could put some random letters as capitals, or switch Os and 0s, Es and 3s or Ls and 1s – for example "h0Use577eXtrAbanana%'
10. Discuss how you'd remember this password. It might be that you imagined a house (number 577) with lots of extra bananas on the roof, in the shape of a % sign, or it might be that you repeated it to yourself a lot, or given it a tune
11. Remind the group that if they've shared their passwords that they've created today with anyone that they shouldn't use it in real life, but can repeat the activity to make their own secret password

My digital footprint

In this activity young people understand what a digital footprint is and make a collage representing their own digital footprint

Time:

30 minutes

What you need:

- Paper
- Pens and pencils
- Old magazines and newspapers
- Scissors
- Glue sticks or PVA glue
- Glue/paint brush

What to do:

1. Ask the group to go through the newspapers and magazines to find things that represent them – for example the town that they live in, their pets, their likes and dislikes, groups they attend. Cut these out or tear around the images

2. Explain that a digital footprint is all the information that you share or is collected about you online. This includes:

- Photos
- Social media posts
- Online games that you've played
- Data from smart watches or fitness trackers
- Things you've bought
- Things you've looked at on websites but haven't bought
- Ads you've clicked on
- Information that you allow apps to access
- Voice searches
- Comments you've left (including arguments)

3. Get the group to draw round their feet onto a piece of paper. If they do this with their shoes off they should use pencil

4. Everyone is going to make a collage of their digital footprint. Using what they've already cut or torn out, think about if that information is part of their digital footprint, and stick it inside the foot outline

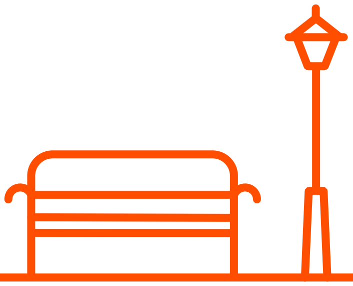
5. If there's anything that they think is missing they can go through the magazines and find more things to add, or draw it in

6. Digital footprints can be good for showing off skills or things that you're proud of. They can also keep a record of things you might be embarrassed by later, or show views you once had which have changed

7. Ask the group to look at their digital footprint and decide to themselves if they are happy with all that information being online

8. Remind the group of the following online safety tips:

- Keep your social media accounts private to restrict who can see your data
- Think about what you're going to put online before you post it, and consider who can see it
- Delete old posts that you no longer want online
- Check what data your device is collecting and don't give new apps permission to access your data
- Search your name on google to see what information is available about you online



My online rights

In this activity young people create their own set of rights to help them feel safe online

Time:

30 minutes

What you need:

- Copies of the United Nations Convention on the Rights of the Child (UNCRC). This can be found on the Unicef website **https://www.unicef.org/sop/convention-rights-child-child-friendly-version**
- Pens
- Paper
- Scissors
- Glue sticks or PVA glue
- Glue/paint brush

What to do:

1. Ask the group if they are familiar with the UNCRC. Explain that all children across the world have the same rights. There are 42 rights, and all the adults that come into contact with children (ie parents, teachers, youth workers) are responsible for making sure these rights are upheld. Share the rights with the group

2. Split the group into teams, and give each team a copy of the UNCRC, paper, pens, scissors, paint brush and glue

3. Ask the teams to consider what those rights mean for them online and when accessing things digitally. For example, article 3 (adults must act in the best interests of the child) might mean that no adult should cyberbully a child, or that parents should turn parental controls on to stop children accessing unsafe websites

4. The teams should cut out the rights that they think apply to them online, and stick them on a piece of paper. Next to the right they should write how it applies online

(**Note:** they don't have to do this for every right, and they might think that they don't all apply)

5. Come back together as a whole group and discuss what the teams came up with

6. As a whole group write a group agreement for how they think they deserve to be treated online, and how they will treat other people, and ask the group to sign it

Display the group agreement in your meeting place. If possible, photocopy it so the group can take it home and display it where they normally access the internet

On or off

In this activity young people think about the benefits of spending time online and offline

Time:

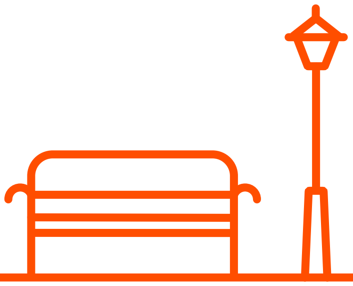
30 minutes

What you need:

- Four large pieces of paper
- Pens
- Pencils
- Paper plates (one per person)
- Rulers

What to do:

1. Split the group into four teams
2. Give each team a large piece of paper
3. Ask one team one to write down all the positives they can think of about spending time online, team two to write down all the negatives they can think of about spending time online, team three to write down all the positives they can think of about spending time offline and team four to write down all the negatives that they can think of about spending time offline
4. Bring the teams back together and ask them to share their positives and negatives, giving people from other teams the chance to add to the lists
5. Explain that it's good to have a balance of time spent online and offline for their wellbeing
6. Give each person a paper plate, and ask them to use a ruler to split it into 24 segments. **It may be easier to print the template on page 24 instead.**
7. Explain that each segment represents one hour of the day. Ask the group to think about a normal day, and decorate each hour to represent what they would normally be doing at that time (ie drawing a bed or a sleeping emoji over the time when they'd normally be asleep, or drawing food at lunchtime)
8. Once they've drawn out their days ask them to consider if they think they have a good balance between online and offline activities. They don't have to share this with the wider group
9. Ask the group to give ideas for improving this balance
10. Suggest that the group pay attention to their activities over the next week, and check in with themselves to see if they're spending a good amount of time online and offline



Secure devices

In this activity young people race against each other to think of ways to keep devices safe and secure

Time:

20 minutes

What you need:

- Large toy building bricks
- Sticky labels
- Pens

What to do:

1. Discuss with the group why it's important to keep devices safe, secure and private. A safe, secure and private device is one where no one can access the information on it without a password, and is one which is protected against viruses and malware. There will be personal information stored on a device and if this isn't kept safe then anyone can access it

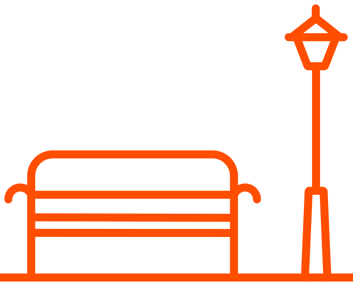
Note: some young people have an agreement with their parents that they can access their devices. What's important is that the group understand that they are keeping their devices safe from those who want to use them maliciously

2. Split the group into teams.
3. Give each team a pile of toy bricks, sticky labels and pens
4. Ask the young people to come up with as many ways as they can think of to keep a device safe. Write these on the sticky labels, and then stick one label to each brick
5. Once a brick has a label on it they can be stacked with the other bricks in a tower
6. The team with the tallest tower wins!
7. When finished, come back together as a large group and compare answers. Check that everyone knows the different ways to keep devices safe

P.T.O

Some examples of ways to keep devices safe and secure:

- Use a strong and unique pin, password or pattern to lock devices
- Never share passwords with anyone
- Avoid giving out personal information, especially if it looks like a company or stranger is asking (see the phishing activity for more information)
- If it's necessary to send personal data, password protect the file and send the password separately
- Only download apps from official app stores
- Regularly back up the data on your devices
- Regularly update the device's operating system and apps (because if a company learns about a weakness in a their software they will release an update that will fix it)
- Log out of websites after making a payment, so if anyone else accesses the device they can't access the payment details
- Log out of online banking apps and websites as soon as you have finished using them
- If a device is lost or stolen use a different device to change social media, email and banking passwords. Some platforms also have the option to log out of all devices
- Factory reset a device before selling it or giving it away
- Factory reset a second hand device before starting to use it
- If possible on your operating system, lock your apps
- Download an antivirus app
- Don't store personal information on devices – ie a note with all the passwords on
- If you're unsure about downloading an app or visiting a website double check with an adult first
- Check that websites are secure. (This means that information that you send or get through the site is private.) The ways to check that a website is secure are:
    - Check the URL. If it starts with **https://** it is secure (the s stands for secure). If it starts with **http://** it may not be secure
    - Check to see if there is a lock symbol to the left of the URL. If it is there then the browser thinks the website is secure. If there is a warning triangle or exclamation mark then the browser doesn't think the website is secure
    - An error message may appear saying that your connection is not private. This means either the website, the network or your device is not secure
    - Never connect to a WiFi network if without knowing who owns it
    - Don't make bank transactions or online purchases on public WiFi



Fake news detective

In this activity young people find clues to help them spot fake news

Time:

45 minutes

What you need:

- Pieces of paper with different words on them:
  - Images
  - URL
  - Sources
  - Quotes
  - Links
  - Repetition
  - Username
  - Statistics
  - Date
  - Author
  - Believable
  - Website

Set up:

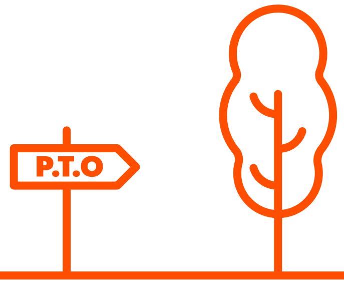
Take the pieces of paper with the various words on them and hide them around the room/ building. (Optional extra step: write clues to help the group find the words)

What to do:

1. Ask the group what they know about fake news. Explain that fake news is a news article or story on the internet that isn't true. Types of fake news include:

   - **Clickbait –** stories designed to grab the reader's attention to pull them to a webpage purely so the advertisers on that page get more money. These pages often have slideshows that the reader needs to click through, so the adverts can load over and over again
   - **Propaganda –** these stories are designed to promote a specific political view, damage someone's reputation or encourage the reader to vote in a certain way
   - **Humour –** sometimes fake news is designed as a joke for entertainment. This can be damaging if the reader believes it
   - **Misleading headlines –** some news stories have sensational headlines designed to make the reader believe something, assuming that they won't read the whole story and get all the facts
   - **Bad journalism –** sometimes journalists will believe fake news, or include fake news as their sources

2. Explain why it's important to spot fake news. No one wants to be taken in and believe a lie, and no one wants to be responsible for spreading false information further
3. Tell the group that there are lots of clues to help them spot fake news stories, and that they should act as detectives when reading an online story, using these clues to tell what is real and what is fake. Tell them that you've hidden hints to these clues around the room/ building and that they need to find them all



4. Once the group has returned, go through the list with them and discuss each one

- **Images –** do they look believable? Think about whether they could have been edited to back up the story. The pictures might also be real pictures that are totally unrelated. You can do a reverse image search to see if the pictures are elsewhere on the internet

- **URL –** what is the website address? Reputable websites tend to end in .com, .co.uk, .gov, .net, .edu or similar. If the URL ends in something that looks made up, for example com.co, it probably isn't a legitimate website

- **Sources –** have they said where they've got their information from and have they included links to it? If they haven't, how do you know they haven't made it up?

- **Quotes –** do the people they've spoken to fit the story? Have they said who they are? For example, if there's a quote from a 'Joe Bloggs' but we don't know who Joe is, why would we trust him? If it says their job title (and it's relevant) or that they were a witness it seems more reliable

- **Links –** are there any links in the article? If there are, where do they lead to when clicked? Some websites put them in to appear genuine assuming that readers won't click on them

- **Repetition –** is the story anywhere else online? If it's real news it will be covered by multiple journalists

- **Username –** if it's a social media post, who has published it? Often fake news is spread on accounts pretending to be real organisations, people or news outlets. For example, someone pretending to be Youth Scotland might tweet using the username @Y0uthSc0tland or @Youth_Scotland. At a first glance it looks normal, but actually it isn't the right username (@YouthScotland)

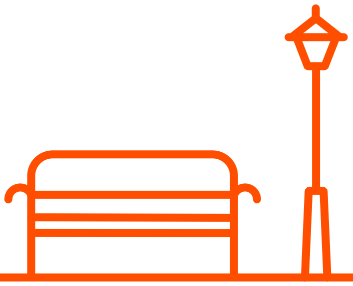
- **Statistics –** have they put in percentages or other statistics that don't have a source? It's very easy to write that 90% of people believe something but if it isn't shared where this data comes from there's no way of checking that this is true. Percentages should always have the number of people that were asked, otherwise someone could say that 100% of people believe that a political candidate is the best, but they might have only asked one person

- **Date –** when was the article published? It may be that someone is referencing an old story that was true at the time but has now been debunked

- **Author –** what else has the author has written. If they have written multiple very similar articles it may be that they're trying to push a viewpoint

- **Believable –** is the story believable? If it makes little sense to the reader that's a good sign that the story is untrue

- **Website –** does the website look professional? An unprofessional website might indicate unprofessional writing. Alternatively, if the website looks very similar to another news website it might be trying to trick the reader into believing that it's legitimate, or make the reader trust it more



Report and block

In this activity young people play a game to learn about the importance of reporting and blocking anyone sending nasty messages via the internet

Time:

15 minutes

What you need:

- A collection of bean bags in two colours
- An open space

What to do:

1. Discuss with the group how anyone can share a message on the internet, and if they're public these can be viewed by anyone. This means that useful or good messages can be shared, but also nasty messages – ones that bully, are cruel or spread hate (for example homophobia, transphobia, sexism or racism). This could be either on social media platforms, comments on articles or messages sent within online games. Ask the group what they would do if they saw a nasty message?

2. Explain that all platforms have a 'report' feature, which shares the message with the platform, who can delete it if it goes against their rules. Tell the group that if they see a message that is spreading hate or cruelty they should always report it as that will help get it deleted sooner.

   Platforms also have a 'block' feature. Blocking someone who is spreading nasty messages means that you can't see their further messages.

If someone interacts with a nasty message, even if they're commenting to disagree, they increase the chance of the conversation being shared with their followers, meaning the original message is shared with more people.

3. Ask the group to stand in a circle, with one person in the centre (maybe two depending on group size)

4. Give everyone on the edge of the circle a bean bag

5. Explain that the one colour bean bags represent 'good' information (for example the news, funny memes, harmless posts) and the other colour represents 'bad' information (for example sexist jokes, racist opinions)

Note: 'good' messages aren't necessarily positive. They might include news stories that are potentially upsetting or angering, but are still worth being shared

6. Get the group to throw their bean bags across the circle. When they catch a bean bag they throw it to someone else. This represents information moving around the internet

7. The person in the middle is going to report and block. They need to try and catch the bad coloured beanbags. When they catch them they can throw them out of the circle

8. If they catch a good coloured beanbag they can throw it to anyone at the edge of the circle

9. Eventually there should only be good beanbags left, and the only messages being shared are the 'good' messages. This shows that if we all report and block hateful messages they will be deleted. It's everyone's responsibility to report and block nasty messages.

Note: remind the group that if they see a message that is upsetting that they should talk to an adult they trust who can talk through their feelings with them

Know your limits

In this activity the group learns the age limits of different social media platforms

Time:

15 minutes

What you need:

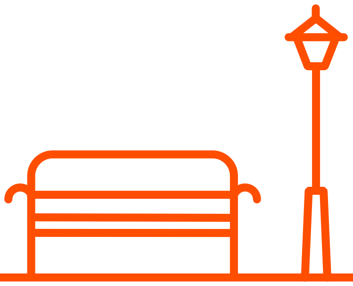
- Strips of paper with the names of various social media and gaming platforms written on them – one set per group (see below)

What to do:

1. Give each group a set of paper with the names of various social media and gaming platforms
2. Ask the group to guess what age limit the platforms have
3. Discuss why platforms have age limits and what safe and unsafe usage of the platforms looks like
4. Reveal the age limits. Were any surprising to the group?

Social media and gaming platforms and their age limits (please note, this information is accurate as of March 2022. You may need to double check that this hasn't changed):

- Facebook – 13
- Instagram – 13
- Snapchat – 13
- Tiktok – 13
- Twitter – 13
- Linkedin – 16
- Tumblr – 13
- Reddit – 13
- Pinterest – 13
- Youtube – 13
- Youtube Creator – 13 with parental permission
- Whatsapp – 16
- Fortnite – 12
- Minecraft – 7
- Roblox – 7



Understanding cyberbullying

In this activity young people learn about cyberbullying, and gain tools to help them spot and react to cyberbullying.

Time:

30 minutes

What you need:

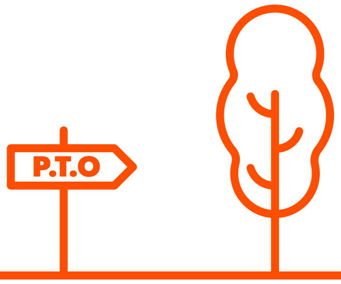
- Poster paper or two pieces of flip chart paper taped together
- Pens and pencils
- Sticky notes

What to do:

Before you start, set up a safe place that young people can go if they feel upset, and consider setting a group agreement that anything shared by the young people should not be passed on.

1. Ask someone to lie on a piece of paper and draw round their outline (in pencil)
2. Ask the group what they know about cyberbullying
3. Write the answers down on the inside of the person outline

   There are some facts below that you might wish to include to prompt the group
4. Ask the group how being cyberbullied might make someone feel
5. Draw these things onto the person outline, for example draw a sad face, a broken heart or a knot on the stomach
6. Pass out the post it notes. Ask the group to write on the post it notes things that they could do if they were being cyberbullied or if they suspected a friend was
7. Stick the post it notes onto the person outline to cover up all the previous writing and drawings
8. Ask the group how they think someone might feel when it was resolved. Remind the group that everyone reacts differently to things, and all of these emotional reactions are valid. Some people might be relieved and happy, some may be angry that it happened, some may be anxious that it could happen again, and some may have different or mixed feelings
9. Take the post it notes off the person outline and stick them to another piece of paper to display in your meeting place. This will give everyone a reminder of what to do it they ever start to be cyberbullied



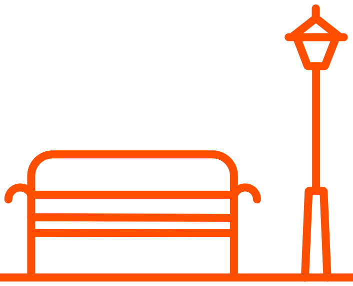
Cyberbullying includes:

- Name calling, teasing, humiliation
- Posting nasty videos, photos or posts about someone online, or commenting or liking these posts
- Starting rumours or group chats about someone
- Ignoring someone or leaving them out
- Sending nasty messages either privately or publicly
- Stealing someone's social media posts and reposting them as if they were their own
- Reporting someone for no reason
- Revealing someone's personal data without permission
- Targeting someone repeatedly in an online game
- Bullying someone because they are different in some way
- Sharing sexual images of someone without their consent
- Editing or manipulating photos of people without their permission

What to do if you think you're being cyberbullied:

- Remember that it is never your fault
- Report and block users
- Don't reply to abusive messages or posts
- Screenshot messages and keep a note of what has been happening
- Tell an adult you trust - for example a parent, youth worker or teacher
- Ask the person to stop
- Take a break from checking messages
- Don't share personal information with anyone online – especially what you look like and your address
- Keep in mind that it's very easy to lie on the internet – someone might not be exactly who they say they are
- If someone has shared sexual images of you online contact the Internet Watch Foundation who will remove them for you – **https://www.iwf.org.uk/**
- Contact Childline who can reassure you that it's not your fault and speak to you about your worries - **https://www.childline.org.uk/get-support/**
- Contact the police if the bullying is due to race or sexuality, if you are being threatened or if someone has shared sexual images of you

The Youth Scotland wellbeing toolkit has activities designed to help young people feel good about themselves, building confidence and self-esteem. You may wish to run an activity from that toolkit after this one.



Identifying grooming

In this activity young people learn what grooming is and what to do if they think someone is being groomed

Time:

30 minutes

What you need:

- Space to move around

What to do:

Before you start, set up a safe place that young people can go if they feel upset, and consider setting a group agreement that anything shared by the young people should not be passed on.

1. Explain to the group that grooming is when someone builds a relationship with someone, usually online, so that they can manipulate, exploit or abuse them, or trick, pressure or force them into doing something sexual
2. Designate one end of the room as 'true' and one end of the room as 'false'. Tell the group that you're going to read out statements and they should move to the end of the room that they think matches the statement. If they don't know they should stay in the middle. Allow time after each statement for questions or discussions

Statements:

Grooming always happens online. False – the groomer might build a relationship online and then try to meet up with the victim, or they might start the grooming offline

A groomer might ask you to do something sexual – for example sexting or sending a naked photo or video. True – it's never ok for anyone to pressure you into doing something sexual. Childline have information on sexting and sending nudes **https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/**

A groomer will jump straight in and send sexual or abusive messages. False – a groomer will often build the victim's trust first, maybe by pretending to be their friend or confidant, or by pretending to have similar interests. They might start subtly to build a 'friendship' and then start asking questions like "have you ever been kissed?" or start to say nice things about the victim's appearance

A groomer might blackmail the victim. True – this could be by threatening to share sexual images or messages of the victim if they don't send more

All groomers are men. False – it could be any body of any age, gender or sexuality

Only young people are groomed. False – it can happen to anyone but is more likely to happen where there's a power imbalance, for example an adult grooming a young person

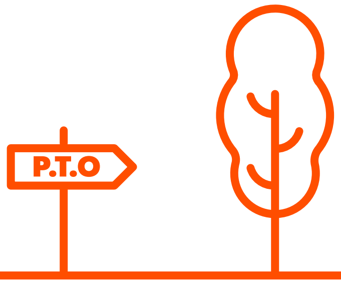
A groomer might know you in real life. True – it might be someone who knows the victim or a complete stranger

A groomer will encourage you to tell your friends and family about them. True or false – A groomer might try to befriend the victim's friends and families to make it seem like they are a safe person, or they might try to get the victim to keep them a secret so they don't get found out

A groomer is likely to tell the victim to keep their conversations secret. True – they will often frame the conversation as 'special' or 'ours'. This is because they know that anyone who reads it might spot that something isn't ok

Grooming only happens in chat rooms. False – it can happen anywhere on the internet, for example social media platforms, dating apps, online games, website comments sections

Grooming is never the victim's fault. True – they are a victim and it is definitely not because of anything they did or did not do

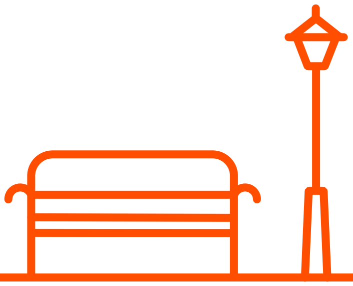


3. Gather the group back together and ask what they would do if they suspected that they or someone they knew was being groomed. Use the list below to prompt them

4. Tell the group that the two most important tools against grooming are knowing the signs, so that they can spot it and stop it, and telling a trusted adult who can help them work out what to do next

What to do if you think you're being groomed or you suspect someone you know is being groomed:

- Remember that it is never your fault
- Report and block users
- Don't reply to abusive messages or posts
- Screenshot messages and keep a note of what has been happening
- Tell an adult you trust – for example a parent, youth worker or teacher
- Ask the person to stop
- Take a break from checking messages
- Don't share personal information with anyone online – especially what you look like and your address
- Keep in mind that it's very easy to lie on the internet – someone might not be exactly who they say they are
- If someone has shared sexual images of you online contact the Internet Watch Foundation who will remove them for you – **https://www.iwf.org.uk/**
- Contact Childline who can reassure you that it's not your fault and speak to you about your worries – **https://www.childline.org.uk/get-support/**
- Contact the police if you are being threatened or if someone has shared sexual images of you



Good sharing

In this activity young people think about the information that they share online and consider who they should share it with

Time:

30 minutes

What you need:

- Pens or sticker sheets
- Pieces of paper with the following people written on them:
  - Best friend
  - Mum
  - A random person from school who I don't know
  - Someone in the year above who's known for being mean
  - Employer
  - A stranger
  - A hacker
  - A journalist
  - Ex-partner
  - Teacher

What to do:

1. Put the pieces of paper with the people written on them on the walls around the room

2. Explain that you're going to read out some pieces of information that you might put online. For each one, they need to go round the room, look at the pieces of paper and decide if they would be happy with that person knowing that information. If they would, put a tick on the paper, or add a sticker. Allow time for discussion in between each one

The information:

- What colour socks you're wearing
- Your full name
- What you had for lunch
- Your phone number
- Your favourite animal
- A picture of you at a party
- Your favourite film
- Your location
- A picture of you 5 years ago
- The Christmas presents you're going to give this year
- An ugly photo
- The views from your holiday last summer
- A nude photo

3. Look at each piece of paper. Were there some people who got to see all the information? Were there some who the group didn't want to share a lot of information with? Does everyone agree? Explain that by putting information openly online they don't have control about who can see it. They might be happy with some information being online but they should consider if they'd still be happy with that being online in a few years' time

4. Talk about different ways that we share information about ourselves online. For example, if a username on a platform was 'firstnamesurname' then everyone who saw your account would know your full name. If they post a picture wearing school uniform then they're letting people know what school they go to, or if they tag themselves at a location while they're still there people know where they are. There might also be information in the background of photos – if they post a photo of their lunch but there's an envelope in the background they might give away their address. Discuss why it might be a problem for people to know this information

5. Consider who else is in photos. If they take a photo with a friend and the friend doesn't like how they look, or the friend doesn't want everyone to know where they've been then they might upset them by posting the photo. Always double check with everyone in the photo that they're happy for it to be posted. Encourage the group to think about the captions that they put on posts, for example 'me and friend's name hanging out' will give away data about their friend

6. Show the group how to make accounts private, and explain that this gives them control over who sees what posts and who gets what information about them. This is usually in their account settings under privacy

Virus tig

In this activity young people play a game to learn more about anti-virus software

Time:

20 minutes

What you need:

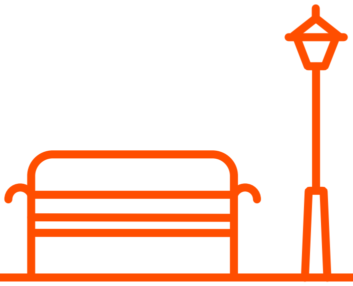
- Space to move around

What to do:

1. Ask the group if they know what a computer virus is

A virus is a code that can harm your devices and the data on them. A virus can steal your data, encrypt it (lock it) so you can't access it, or delete it. You can get a virus by visiting an unsecure website, opening a link in a suspicious email, downloading an illegitimate programme or media or from an infected USB. A virus can self-replicate, so if it's on one document that is downloaded onto your computer it will spread to all your other documents

2. Explain that anti-virus software exists to combat computer viruses. You can buy antivirus software and download it onto your devices to protect them. This will scan programmes and files as they enter your device, and regularly check everything on your device for malicious code. It will then quarantine or remove the code, keeping your device safe
3. You're going to play tig. Ask one or two people to be the virus, and everyone else will be computer programmes. The viruses chase the computer programmes, and if they catch them the computer programmes are infected, they also become the virus and can run around to catch everyone else. Play until all the documents have been infected
4. The game is going to change, and the antivirus is going to be introduced. Ask one or two people to be the antivirus, and designate one part of the space as the 'safe zone'.
5. They have to chase the viruses, and if they do the virus is stopped, and has to sit down. They also have to chase the documents. If they catch a document the document goes into the safe zone. Play until either all the documents have been infected or all the viruses have been stopped
6. Discuss how this shows how the anti-virus software helps slow the spread of viruses and keep devices safe



Fishing phishing

In this activity young people play a fishing game to learn more about phishing

Time:

45 minutes

What you need:

- Paper
- Pens
- Scissors
- Magnets (one per group)
- Paper clips
- String
- Sticky tape

Set up:

1. Cut out fish shapes from paper – 5 for each group and write the words 'email address' 'time' 'urgency' 'spelling' 'suspicious links' on the fish. **It may be easier to print the template on page 25 instead.**

2. Put a paperclip on every fish, and spread them around the floor with the words facing downwards

3. Cut the string into pieces about a metre long, and tape a magnet to each piece of string. This is your fishing rod and can be used to pick up the fish

What to do:

1. Ask the group if they know what phishing is

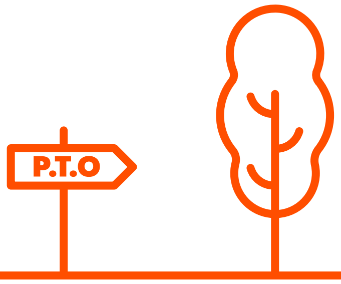
Phishing is when an attacker sends a fraudulent message designed to trick someone into revealing sensitive information (such as passwords or bank details) to the attacker or to leave a virus on the victim's infrastructure. It might be an email, text or phone call. It might download a file to your device which can do anything from steal stored passwords to locking your machine so they can ransom it to you

2. Put the group into teams and give each team a fishing rod

3. Explain that there are 5 different species of fish on the floor, and each one has a different word on it to explain one thing that you can look out for in an email to see if it's a phishing email

4. Teams use the rods to fish for the paper fish, racing against each other to be the first team to collect 5 different fish

5. If they catch a fish with a word that they've already got they must throw it back and try for a different one

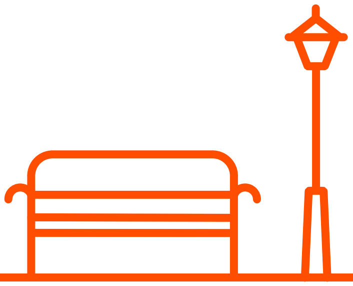


6. Once the teams have played the game they should have had some time to familiarise themselves with the words. Explain that the following things will help them spot a phishing email

- **Email address –** if the email is sent from an odd address, it's probably not legitimate. Ways to spot this are if it's got a funny domain name, for example @ggmail rather that @gmail, or a series of random letters instead of a name. It might be an email address pretending to be someone you know, but with a slight change
- **Time –** if the email is sent in the middle of the night or at a time when you knew the alleged sender was busy
- **Urgency –** if the email is telling you to do something straight away! Phishers want you to act before you think about it
- **Spelling –** phishing emails often have lots of spelling and grammar mistakes, or use unusual phrasing
- **Suspicious links –** if there's a link in the email asking you to open it or give out some of your data. Companies will never email you asking for your password or bank details. If you hover over a link then the web address it will take you to will appear either over the top of the link or in the bottom left corner of the page. Do this before clicking on links to check that they're really going to where they say they're going

7. Let the group know what to do if they get a phishing email:

- Delete the email straight away
- Don't open any links or attachments
- Contact the person who 'sent' it to you in another way to let them know someone is pretending to be them and check it wasn't actually them
- If the email has been sent to your school or work email address let the IT team know (but don't forward it onto them!)



Mis-communication game

In this activity young people play a game to demonstrate how easy it is to communicate badly on the internet

Time:

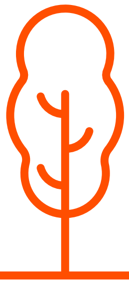
15 minutes

What you need:

- ○ Paper
- ○ Pens

What to do:

1. Split the group into teams of 3 or 4 people, and ask the teams to sit in lines one behind the other
2. Give each member of the team a bit of paper and a pen
3. Give the person at the back of each team a different silly scene (for example a giraffe on rollerskates or a summertime Christmas). They then have 30 seconds to draw their picture without telling anyone what it is
4. The person at the back then shows their picture to the person in front of them, who can only look at it once. They then have 30 seconds to try and draw what they saw
5. Repeat this, until the person at the front of the line has drawn the picture
6. Ask the person at the front of the line to guess what the drawing is of
7. Ask the group if they found it easy or hard to work out what the picture was meant to be
8. Explain that sometimes messages sent over the internet don't have enough context, or the right tone. This can lead to people being misrepresented, or to people getting upset if they misread the message. This is more likely to happen when you send a message quickly without thinking it through, or when a message is passed on to someone else
9. Remind the group to check messages or online posts they send to people before they send them to check that they make sense and won't offend anyone



In app purchases

In this activity young people play a game pretending to be a real life app to explore what the effects of in app purchases can be on your money

Time:

60 minutes

What you need:

- Tokens – 10 per player, which can be made using cut up pieces of paper. **It may be easier to print the template on page 26 instead.**
- Games equipment eg balls, bean bags, hula hoops, ropes, balloons skittles etc
- Prizes of varying standards (ie small, medium and large) bags of sweets – one per player

What to do:

Set up: Before you start, set up 5 challenge stations. The challenges are up to you based on the games equipment available, for example throwing a beanbag into a bucket or doing a certain amount of spins with a hula hoop. The challenges should be challenging (so something that not everyone will get right on the first go, but achievable). Each challenge should have an easy and a regular mode eg throwing a bean bag from a shorter or longer distance

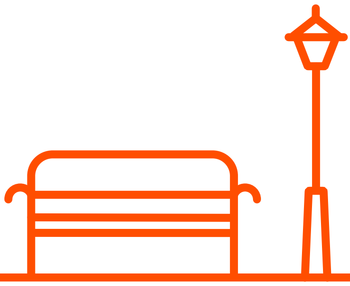
1. Explain that some apps have in-app purchases, where you can use real money to buy things within the app. There are two types of in-app purchases:

   Consumables – each purchase buys something that can be used once – for example in game money or health points

   Non-consumables – each purchase lasts forever, for example permanently removing adverts or levelling up in a game

   In app purchases might be a one off payment or they might be subscriptions, where you pay over and over again for the same thing (usually once a month)

2. Give everyone in the group 10 tokens each



3. Explain that we're going to pretend we're in an app with 5 levels, and they need to complete each level to win a prize. Explain the different challenges to the group. Each challenge has a regular mode, or an easy mode. To get to the easy mode they have to spend a token. They can have as many goes as they like on each challenge, but after every third go they need to sit on the floor for 30 seconds before they can have another go. This represents adverts in the game. They can get rid of the adverts on a challenge by paying a token, but that only gets rid of the adverts for that one challenge.

4. Tell the group that at the end of the game they can use their left over tokens to buy a prize. If they have 7 or more tokens left they can have a large prize, 4-6 tokens left means they can have a medium prize, 1-3 tokens left means they can have a small prize and if they have no tokens left then they can't have a prize

5. Play the challenges, spending tokens as you go

Note: to make the game easier to run it would be helpful to have an adult or young leader at each challenge to collect the tokens and manage the easy and regular modes, and the ad breaks

6. Once everyone's had a chance to play all the challenges, give out the prizes based on the amount of tokens everyone had left.

7. Discuss how the group found it. Did having the tokens make it easier and was it worth making the games easier at the cost of getting the prizes?

8. Tell the group that there is nothing wrong with making in app purchases as long as they are aware of the amount they are spending, and that they won't be able to spend that money on anything else. Remind them that it's easier to over spend in apps because you can't see the money or the purchases physically, so it's easier to forget that they're real. They should never spend someone else's money on an app without asking permission first

Who’s who online

In this activity young people play a game where they learn about how easy it can be for someone to pretend to be someone they’re not online

Time:

20 minutes

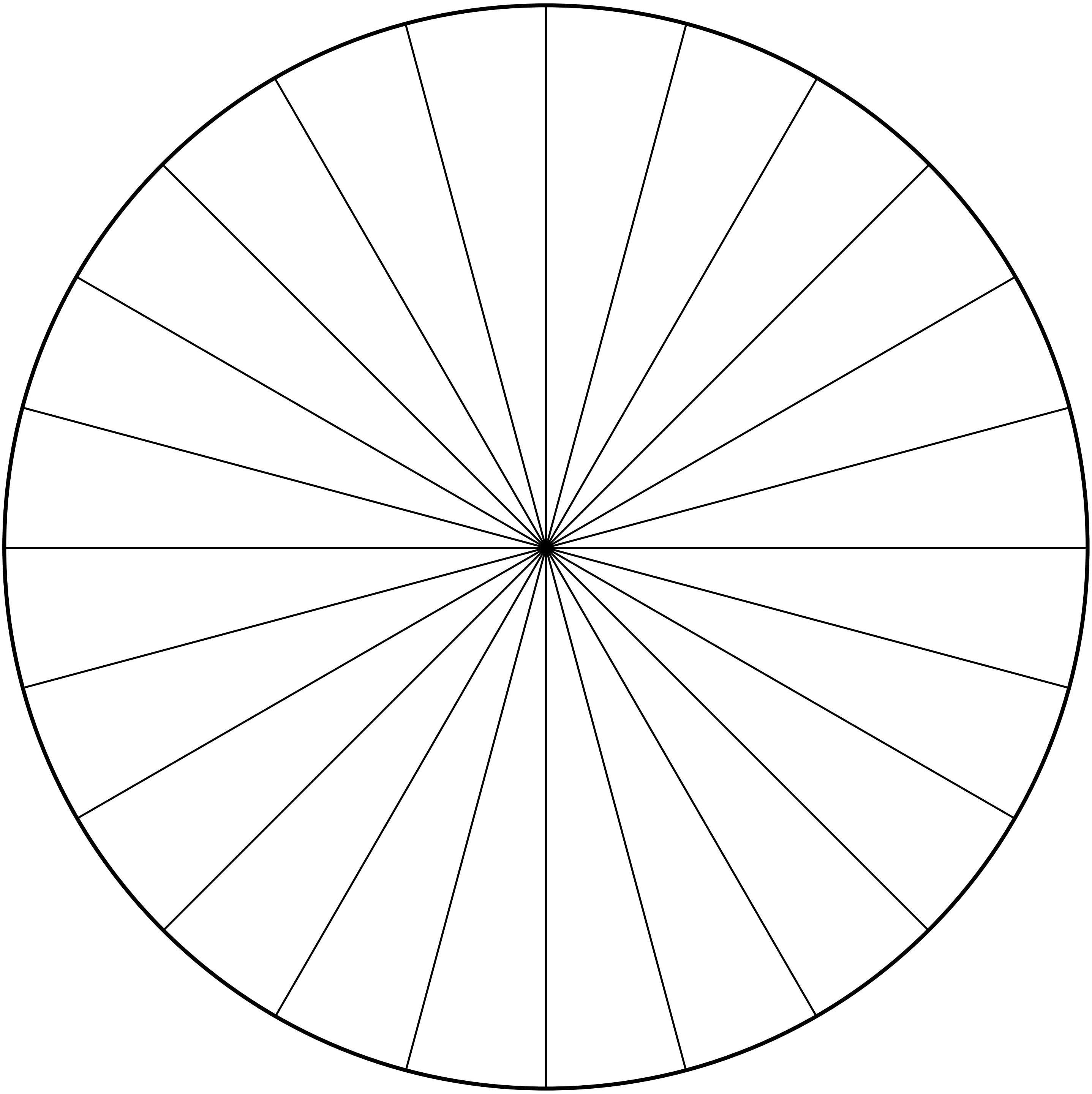
What you need:

- A list of different personas on separate pieces of paper (one per player), for example:
  - A teacher
  - The Queen
  - A man who has 10 cats and loves them all
  - A really enthusiastic friend
  - An overdramatic actor
  - A footballer who’s really proud of the goal she scored last weekend

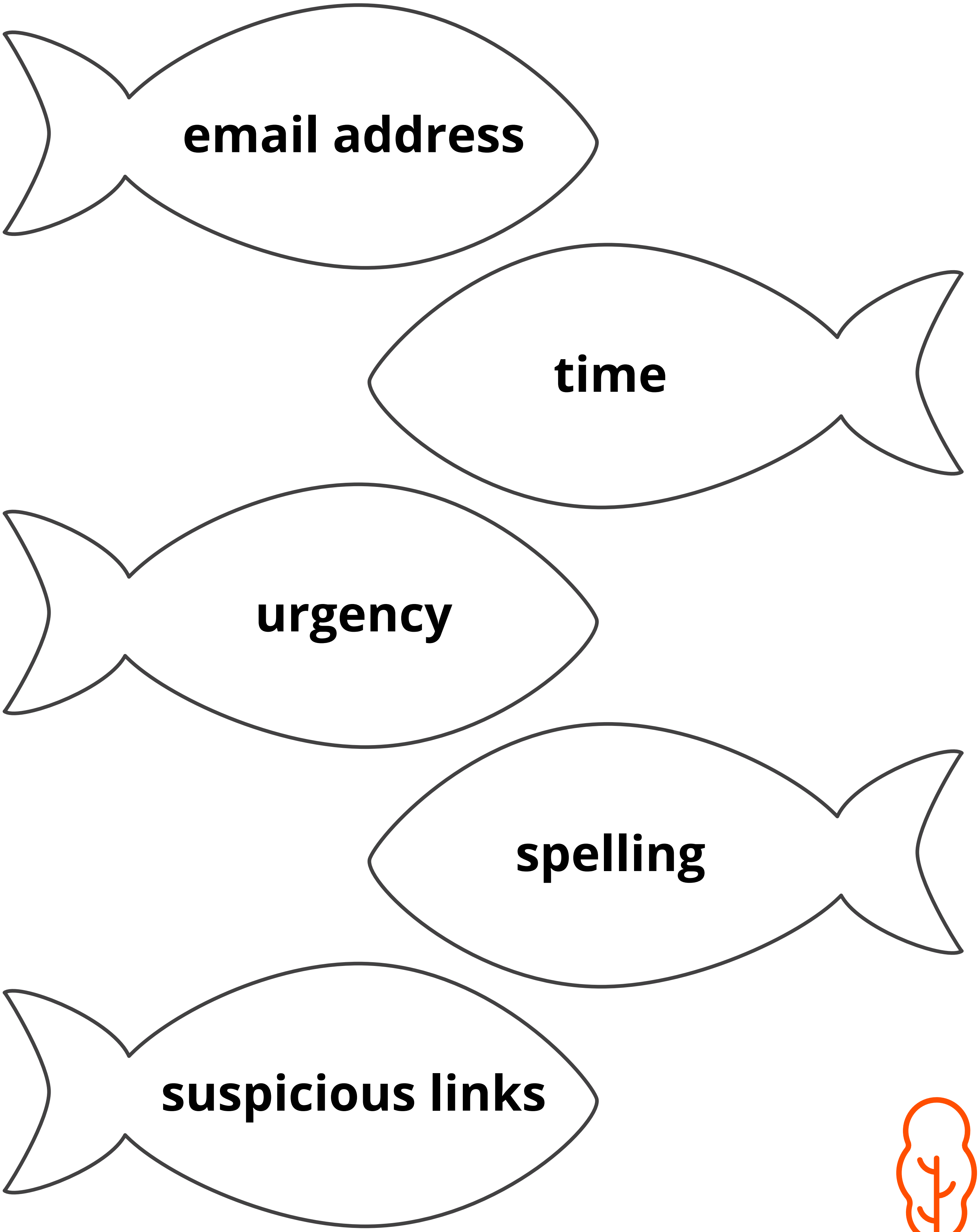
What to do:

1. Give everyone a piece of paper with a different persona on it, but ask them to keep it secret
2. Tell the group to find a partner, and have a chat, pretending to be the person that they have been secretly given
3. Both people need to try and guess who the other person is pretending to be
4. When one person in the pair has had their identity guessed the person who was guessed correctly gets a point
5. After a minute or so ask everyone to stop and find a new partner, and repeat this until most people have spoken to each other
6. Bring the group back together and ask who the top point scorers were. These people were very convincing!
7. Talk about how if you have a persona to follow it’s easy to think of a character and pretend to be them. When someone is trying to get information from someone using the internet or groom them, they often pretend to be someone they’re not. This is often someone similar to the victim, for example if someone was targeting a teenage girl they might also pretend to be a teenage girl, who likes the same music and tv shows as them. It can be hard to tell if someone is being genuine online, especially when you cannot see or hear them
8. Remind the group that if a stranger is talking to them online and asks for personal information or photos that they shouldn’t send it, and should instead ask an adult to double check. If anyone is asking them anything that makes them uncomfortable they should also share with an adult they trust
9. Ask if the group know how to keep their social media profiles private, and remind them that if their profiles are private it’s much harder for strangers to talk to them

On or off (template)



Fishing phishing (template)



In app purchases (template)

Version: 2022-04

Youth Scotland:
Balfour House, 19 Bonnington Grove, Edinburgh EH6 4BL

Tel: 0131 554 2561
Fax: 0131 454 3438
Email: office@youthscotland.org.uk
Twitter: @youthscotland
Facebook: fb.com/youthscotland

A company limited by guarantee No: 125456.
Scottish Charity No: SC000501.
Registered in Scotland.

www.youthscotland.org.uk